

IBM Spectrum Protect for UNIX and Linux
Versión 8.1.0

*Guía de instalación y del usuario de los
clientes de copia de seguridad y
archivado*



IBM Spectrum Protect for UNIX and Linux
Versión 8.1.0

*Guía de instalación y del usuario de los
clientes de copia de seguridad y
archivado*



Nota:

Antes de utilizar esta información y el producto al que da soporte, consulte la información de “Avisos” en la página 807.

Esta edición se aplica a la versión 8, release 1, modificación 0 de IBM Spectrum Protect (números de producto 5725-W98, 5725-W99 y 5725-X15) y a todos los releases y modificaciones posteriores hasta que se indique lo contrario en nuevas ediciones.

© Copyright IBM Corporation 1993, 2016.

Contenido

Tablas xi

Acerca de esta publicación xiii

A quién va dirigida esta publicación	xiv
Publicaciones	xiv
Convenciones utilizadas en esta publicación	xiv
Lectura de diagramas de sintaxis	xiv

Novedades de la versión 8.1 xvii

Capítulo 1. Instalación de los clientes de archivado y copia de seguridad de IBM Spectrum Protect. 1

Actualización del cliente de archivado y copia de seguridad	1
Actualización de la vía de acceso para clientes y servidores	1
Información adicional sobre la actualización	1
Despliegue automático del cliente de copia de seguridad y archivado	2
Requisitos del entorno del cliente	4
Entorno del cliente AIX	5
Componentes instalables del cliente AIX	5
Requisitos de sistema para el cliente de AIX	5
Métodos de comunicación del cliente AIX	5
Funciones de cliente de archivado y copia de seguridad disponibles en AIX	6
Entorno de la API de HP-UX Itanium 2	6
Componente instalable de la API de HP-UX Itanium 2	6
Requisitos del sistema para la API de HP-UX Itanium 2	6
Métodos de comunicación de la API de HP-UX Itanium 2	6
Entorno de clientes de Linux on Power Systems	7
Componentes instalables de cliente de Linux on Power Systems	7
Requisitos de sistema para clientes en Linux on Power Systems	7
Métodos de comunicación de cliente de Linux on Power Systems	7
Entorno de cliente Linux x86_64	7
Componentes instalables del cliente Linux x86_64	7
Requisitos de sistema para clientes Linux x86_64	8
Métodos de comunicación del cliente Linux x86_64	8
Entorno de cliente Linux on System z	8
Componentes instalables del cliente Linux on System z	8
Requisitos de sistema para clientes Linux on System z	8

Métodos de comunicación del cliente Linux on System z	9
Entorno del cliente Mac OS X	9
Componentes instalables del cliente Mac OS X	9
Requisitos de sistema para clientes Mac OS X	9
Métodos de comunicación del cliente Mac OS X	9
Entorno de cliente Oracle Solaris	10
Componentes instalables del cliente Oracle Solaris	10
Requisitos de sistema para clientes Oracle Solaris	10
Métodos de comunicación del cliente Oracle Solaris	10
Requisitos de soporte para NDMP (sólo Extended Edition).	11
Requisitos de instalación de copia de seguridad y archivado de datos de cliente de Tivoli Storage Manager FastBack	11
Instalar los clientes de archivado y copia de seguridad UNIX y Linux	12
Instalación del cliente AIX	12
Desinstalación del cliente AIX	15
Instalación de la API de HP-UX Itanium 2	16
Aumento del límite predeterminado del tamaño de segmento de datos	18
Desinstalación de la API de HP-UX Itanium 2	18
Instalación del cliente de copia de seguridad y archivado en Linux on Power Systems (Little Endian).	19
Desinstalación del cliente de copia de seguridad y archivado en Linux on Power Systems (Little Endian).	21
Instalación de la API del cliente de copia de seguridad y archivado en Ubuntu Linux on Power Systems (Little Endian)	22
Desinstalación del cliente en Ubuntu Linux on Power Systems (Little Endian)	24
Instalación de la API en Linux on Power Systems (Big Endian)	24
Desinstalación de la API en Linux on Power Systems (Big Endian)	27
Instalación del cliente Linux x86_64	28
Desinstalación del cliente Linux x86_64	31
Instalación del cliente Ubuntu Linux x86_64	33
Desinstalación del cliente Ubuntu Linux x86_64	36
Instalación del cliente Linux on System z	37
Desinstalación del cliente de Linux on System z	41
Instalación del cliente Mac OS X	42
Desinstalación del cliente Mac OS X	43
Instalación del cliente Oracle Solaris	44
Desinstalación del cliente Oracle Solaris	46
Actualizaciones de software	47
Instalación del servicio de gestión de cliente para recopilar información de diagnóstico	47

Capítulo 2. Configurar el cliente de IBM Spectrum Protect 49

Tareas de usuario root y autorizado del cliente de UNIX y Linux	49
Habilitar usuarios que no son administradores para gestionar sus propios datos	52
Restricción del acceso a IBM Spectrum Protect a un grupo de usuarios	52
Habilitar el cifrado para usuarios cliente de copia de seguridad y archivado.	53
Descripción general del archivo de opciones de cliente	54
Creación y modificación del archivo opciones del sistema del cliente	56
Creación de un archivo de opciones predeterminado de usuario-cliente.	58
Creación de un archivo de opciones del usuario cliente personalizado	60
Variables de entorno	61
Definir variables de entorno de idioma	61
Definir variables de entorno de proceso	62
Definir variables de shell Bourne y Korn	64
Definir variables de shell C	64
Definir variables de entorno de la API	64
Descripción general de la configuración del cliente web	65
Configuración del cliente web en sistemas AIX, Linux, Mac y Solaris	66
Configuración del planificador	66
Comparación entre servicios del gestionados por el aceptador de cliente y servicios del planificador tradicional	67
Configuración del cliente para que utilice el servicio del aceptador de cliente para gestionar el planificador	68
Iniciar el planificador cliente.	69
Planificación de sucesos mediante el cliente de línea de mandatos	69
Configuración de las comunicaciones cliente/servidor de IBM Spectrum Protect a través de un cortafuegos	72
Configuración de las comunicaciones cliente/servidor de IBM Spectrum Protect con Secure Sockets Layer	74
Certificados raíz de entidades emisoras de certificados	77
Configuración del sistema para copia de seguridad con registro por diario.	78
Configuración del daemon de registro por diario	78
Sección JournalSettings	80
Sección JournalExcludeList	81
Sección JournalFileSystemSettings	82
Modificación de stanzas	85
Deduplicación de datos del lado del cliente.	86
Configuración del cliente para la eliminación de duplicados de datos	90
Excluir archivos de la eliminación de duplicados de datos	93
Configuración y uso de la migración tras error automática del cliente	94

Visión general de migración tras error de cliente automatizado.	94
Requisitos para la migración tras error automática del cliente	95
Restricciones de la migración tras error automática de cliente	96
Funciones de migración tras error de los componentes de IBM Spectrum Protect	97
Configuración del cliente de migración automática tras error	98
Determinación del estado los datos replicados del cliente	100
Prevención de la migración tras error automática del cliente	101
Forzar al cliente a la migración tras error	101
Configuración del cliente para realizar una copia de seguridad y archivado de los datos de Tivoli Storage Manager FastBack	102
Configuración y utilización del entorno en clúster	103
Visión general de entornos en clúster	104
Activa/Activa: Agrupación de recursos de clúster.	104
Activa/Pasiva: Tolerante a errores	104
Acceso simultáneo.	104
Configuración de un cliente de copia de seguridad/archivado en un entorno de clúster	104
Habilitación del acceso al cliente web en un entorno de clúster	111
Migración de configuraciones de AIX/IBM PowerHA SystemMirror antiguas.	113
Consideraciones para la configuración de AIX antes de realizar copias de seguridad y archivado basadas en instantáneas	114
Configuración de NetApp y IBM Spectrum Protect para copias de seguridad incrementales de diferencia de instantánea	114
Protección de volúmenes de servidor de archivos ONTAP NetApp de datos en clúster.	116
Soporte de SnapMirror para la copia de seguridad a incrementos progresivos asistida por instantáneas NetApp (snapdiff)	120
Registrar la estación de trabajo en un servidor	123
Inscripción cerrada	124
Inscripción abierta.	124
Creación de una lista de inclusión/exclusión	124
Opciones de inclusión/exclusión	126
Exclusión de espacios de archivos y directorios	126
Excluir archivos y directorios de la copia de seguridad con registro por diario.	127
Controlar proceso de sentencias de exclusión	127
Archivos del sistema a excluir.	129
Incluir y excluir archivos con caracteres comodín	130
Inclusión y exclusión de grupos de archivos con caracteres comodín	131
Ejemplos de utilización de caracteres comodín en patrones de inclusión y exclusión	132
Proceso de enlaces simbólicos y alias	134
Determinar el proceso de compresión y cifrado	134

Vista previa de los archivos de la lista de inclusión-exclusión	135
Inclusión y exclusión de proceso de opciones	136
Capítulo 3. Cómo empezar.	141
Autenticación del cliente de IBM Spectrum Protect	141
Inicio de una sesión en la GUI Java	142
contraseña de IBM Spectrum Protect	143
Asistente para la instalación	144
Inicio de una sesión de línea de mandatos.	144
Utilización de la modalidad por lotes	144
Emisión de una serie de mandatos mediante la modalidad interactiva	145
Especificación de cadenas de entrada que contengan espacios en blanco o comillas	145
Inicio: consideraciones adicionales	146
Inicio de una sesión de cliente web	147
Privilegios de usuario	147
Iniciar automáticamente el planificador cliente	148
Cambio de la contraseña	148
Ordenación de listas de archivos mediante la GUI del cliente de copia de seguridad y archivado	150
Visualización de ayuda en línea	151
Finalización de una sesión	152
Foros en línea	152

Capítulo 4. Copia de seguridad de los datos	155
Planificación de las copias de seguridad	155
Los archivos de los que se hace copia de seguridad	156
Cuándo realizar copias de seguridad y cuándo archivar copias	156
Consideraciones previas a la copia de seguridad (UNIX y Linux)	157
traspaso de datos sin LAN	158
Requisitos previos del soporte para fuera de la LAN	158
Opciones de traspaso de datos fuera de la LAN	158
Copias de seguridad incrementales en sistemas con restricción de memoria	159
Copias de seguridad incrementales en sistemas con un gran número de archivos	159
Opciones de inclusión/exclusión para controlar el proceso	160
Cifrado de datos durante una operación de copia de seguridad o archivado	161
Soporte para sistemas de archivos y ACL	162
Tamaño máximo de archivo para operaciones	166
Nombres de usuario y de grupo largos	166
Nombres de volumen en Mac OS X	167
Precauciones respecto a la asignación de nombres de volumen en Mac OS X	167
Precauciones respecto a la asignación de nombres de volumen en Mac OS X en sistemas de arranque dual	168
Habilitación de Unicode para Mac OS X	168
Disco de copia de seguridad Time Machine de Mac OS X	169

Realización de una copia de seguridad incremental selectiva o incremental por fecha (UNIX y Linux)	170
Copia de seguridad incremental completa y parcial.	170
Copia de seguridad basada en el diario en AIX y Linux.	172
Copia de seguridad incremental por fecha.	175
Comparación de copias de seguridad incrementales por fecha, con registro por diario y copias de seguridad diferenciales de instantánea de NetApp con las copias de seguridad incrementales completas y parciales	176
Copia de seguridad diferencial de la instantánea con una conexión HTTPS	178
Ejecutar una instantánea de la copia de seguridad diferencial con una conexión HTTPS	179
Copia de seguridad selectiva	179
Zona global Solaris y copias de seguridad de zonas no globales	180
Cómo guardar permisos de acceso	180
Establecimiento de un punto de montaje virtual	180
Copia de seguridad de datos mediante la GUI Java	181
Copia de seguridad de datos mediante la línea de mandatos	182
Supresión de datos de copia de seguridad.	185
Supresión de espacios de archivos	186
Copia de seguridad de archivos desde uno o varios espacios de archivos para una copia de seguridad de grupo (UNIX y Linux)	187
Copia de seguridad con soporte de proxy de nodo cliente (UNIX y Linux)	188
Habilitación de varias operaciones de nodos desde la GUI	189
Configuración del cifrado	189
Copias de seguridad de planificación con soporte de proxy de nodo cliente.	190
Ejemplos de cómo planificar una copia de seguridad de un clúster de IBM PowerHA SystemMirror	191
Planificar una copia de seguridad de un sistema de archivos de GPFS	193
Asociar una instantánea local con un espacio de archivos del servidor (UNIX y Linux)	194
Copia de seguridad de imagen	194
Realización de tareas de requisitos previos antes de crear una copia de seguridad de imágenes	196
Soporte de tipo de dispositivo de volumen para una copia de seguridad de imagen	197
Utilización de las copias de seguridad de imagen para realizar copias de seguridad incrementales del sistema de archivos	199
Método 1: Uso de las copias de seguridad de imagen con la copias de seguridad incrementales de sistemas de archivos	199
Método 2: Uso de las copias de seguridad de imagen con las copias de seguridad de imagen incremental por fecha	200
Comparación de los métodos 1 y 2	201

Realización de una copia de seguridad de imagen mediante la GUI	201
Realización de una copia de seguridad de imagen mediante la línea de mandatos	203
Copia de seguridad y archivado de archivo basada en instantánea y copia de seguridad de imágenes basada en instantánea	203
Protección de los sistemas de archivos Btrfs	204
Realizar la copia de seguridad y la restauración de los sistemas de archivos Btrfs	205
Copia de seguridad y restauración de los subvolumenes Btrfs	207
Realice la copia de seguridad de los sistemas de archivos NAS utilizando el Protocolo de gestión de datos de redes	208
Copia de seguridad de los sistemas de archivos NAS con la GUI del cliente web utilizando el Protocolo de gestión de datos de redes NDMP	209
Copia de seguridad de sistemas de archivos NAS mediante la línea de mandatos	211
Copia de seguridad de sistemas de archivos de red NFS con la función de espacio de nombres global	214
Copia de seguridad de los sistemas de archivos con partición de carga de trabajo de AIX	215
Realizar la copia de seguridad de sistemas de archivos Solaris Zettabyte	216
Copia de seguridad del sistema de archivos cifrado de JFS2 de AIX	217
Copia de seguridad de los atributos ampliados de AIX	218
Realización de copia de seguridad de máquinas virtuales VMware	219
Preparación del entorno para copias de seguridad paralelas de máquinas virtuales VMware	220
Creación de copias de seguridad completas de máquinas virtuales VMware	222
Copias de seguridad paralelas de máquinas virtuales	223
Copia de seguridad y archivado de los datos de Tivoli Storage Manager FastBack	224
Visualización del estado del proceso de copia de seguridad	224
Copia de seguridad(UNIX y Linux):	
Consideraciones adicionales	227
Archivos almacenados	227
Sistemas de archivos especiales	228
NFS o puntos de montaje virtuales	229
Clases de gestión	229
Copias de seguridad de enlaces simbólicos	229
Ejemplos: copia de seguridad incremental o selectiva de enlaces simbólicos	230
Copia de seguridad incremental de un dominio solamente	231
Enlaces fijos	232
Archivos dispersos	232
Montajes de hard y soft de NFS	232
Sistemas de archivos suprimidos	233
Archivos abiertos	234

Caracteres comodín	234
------------------------------	-----

Capítulo 5. Restauración de los datos 237

Restauración de una imagen	237
Restauración de una imagen mediante la GUI	239
Restauración de una imagen mediante la línea de mandatos	240
Restauración de datos desde un conjunto de copias de seguridad	240
Restauración de conjuntos de copias de seguridad: consideraciones y restricciones	243
Restauración del conjunto de copias de seguridad	244
Restauración de conjuntos de copias de seguridad mediante la GUI.	245
Restauraciones de los conjuntos de copia de seguridad utilizando una interfaz de línea de mandatos.	246
Restaurar o recuperar datos durante una migración tras error	247
Restaurar una imagen en archivo.	248
Gestión de datos del sistema de archivos GPFS con agrupaciones de almacenamiento.	249
Restauración de datos a un instante específico	251
Restauración de archivos cifrados AIX	252
Restaurar sistemas de archivos con partición de carga de trabajo de AIX	253
Restaurar sistemas de archivos NAS.	254
Restauración de sistemas de archivos NAS utilizando el cliente web.	255
Opciones y mandatos para restaurar sistemas de archivos NAS desde la línea de mandatos.	256
Restaurar copias de seguridad activas o inactivas	257
Restauración de datos mediante la GUI.	258
Ejemplos de restauración desde la línea de mandatos.	258
Ejemplos: restauraciones mediante la línea de mandatos para grandes cantidades de datos	260
Restauración estándar de la consulta, sin restauración de la consulta y restauración reinicialable	261
Proceso de restauración de consulta estándar	261
Sin consulta de proceso de restauración	261
Proceso de restauración reinicialable	262
Restauración de sistemas de archivos ZFS de Solaris.	263
Tareas de restauración adicionales	263
Cómo autorizar a otro usuario para que restaure o recupere archivos	264
Restauración o recuperación de archivos de otro nodo cliente	265
Restaurar o recuperar archivos en otra estación de trabajo	266
Restauración de un disco en caso de pérdida del mismo.	266
Supresión de espacios de archivos	267
Habilite SELinux para restaurar los archivos en el cliente de Red Hat Enterprise Linux 5	268

Capítulo 6. Archivar y recuperar datos (UNIX y Linux) 269

Copias de archivado	269
Archivado de datos con la GUI	269
Ejemplos de archivado de datos utilizando la línea de mandatos	270
Asociación de una instantánea local a un espacio de archivos del servidor	272
Archivado de datos mediante el proxy de nodo cliente	272
Supresión de datos archivados	274
Tareas de archivado avanzadas	274
Permisos de acceso	274
Archivar y recuperar enlaces simbólicos	275
Enlaces fijos	276
Recuperar archivos	276
Recuperación de datos con la GUI	277
Recupere los ejemplos de datos utilizando la línea de mandatos	277
Archivar clases de gestión	278

Capítulo 7. Visión general del planificador de IBM Spectrum Protect. 281

Ejemplos: manejo de espacios en blanco en nombres de archivos de definiciones de planificación.	282
Horas de inicio preferentes para determinados nodos	283
Opciones de proceso de planificador	283
Evaluar códigos de retorno de planificación en scripts de planificación	285
Códigos de retorno de los scripts preschedulecmd y postschedulecmd	285
Servicios del planificador de aceptación de clientes frente a los servicios del planificador tradicional.	286
Establecimiento del proceso del planificador cliente para que se ejecute como una tarea de fondo y se inicie automáticamente al arrancar	287
Ejemplos: visualización de información sobre trabajo planificado.	289
Visualizar información sobre el trabajo completado	291
Especificar opciones de planificación	292
Opciones del planificador para los mandatos	292
Activar o desactivar mandatos planificados	292
Gestionar varios requisitos de planificador en un sistema	293

Capítulo 8. Códigos de retorno del cliente 297

Capítulo 9. Políticas de gestión de almacenamiento 299

Dominios de políticas y juegos de políticas	299
Clases de gestión y grupos de copia	300
Visualizar información sobre clases de gestión y grupos de copia	301
Atributo Nombre de grupo de copias	302
Atributo Tipo de copia	302
Atributo Frecuencia de copia	302

Atributo Versiones si datos existen	302
Atributo Versiones si datos suprimidos	303
Atributo Retener versiones adicionales	303
Atributo Retener única versión	303
Atributo Serialización de copia	303
Parámetro de modalidad de copia	304
Atributo Destino de copia	305
Atributo Retener versiones	305
Atributo Eliminar duplicados de datos	305
Seleccionar una clase de gestión para los archivos	305
Asignar una clase de gestión a los archivos	306
Sustituirla clase de gestión para las copias archivadas	307
Seleccionar una clase de gestión para los directorios	308
Vincular clases de gestión a archivos	308
Revincular las versiones de copias de seguridad a los archivos	309
Período de gracia de retención	309
Protección de retención de políticas basadas en sucesos	310
Archivar archivos en un servidor de retención de datos	311

Capítulo 10. Opciones de proceso . . . 313

Visión general de las opciones de proceso	313
Opciones de comunicación	314
Opciones de TCP/IP	314
Opciones de memoria compartida	315
Opciones de servidor.	315
Opciones de proceso de copia de seguridad/archivado	316
Opciones de proceso de restauración y recuperación.	327
Opciones de planificación	330
Opciones de formato e idioma.	332
Opciones de proceso de mandatos	332
Opciones de autorización	333
Opciones de proceso de errores	333
Opciones de proceso de transacciones	334
Opciones de cliente Web.	335
Opciones de diagnóstico.	335
Utilización de opciones con mandatos	336
Especificación de opciones con un mandato	336
Opciones que sólo son válidas en la línea de mandatos inicial	343
Opciones del cliente que pueden establecerse con el servidor de IBM Spectrum Protect	343
Consulta de opciones del cliente	345
Absolute	345
Afmskipuncachedfiles	346
Archmc.	347
Archsymlinksfile	348
Asnodename	349
Valores de sesión y planificaciones de una operación de proxy	350
Auditlogging	351
Auditlogname	353
Autodeploy	355
Autofsrename	356
Automount	358

Backmc	359	Filesonly	443
Backupsetname	360	Followsymbolic	444
Basesnapshotname	361	Forcefailover	445
Cadlistenonport	362	Fromdate	446
Changingretries	363	Fromnode	447
Class	364	Fromowner	448
Collocatebyfilespec	365	Fromtime	448
Commmethod	366	Groupname	449
Commrestartduration	367	Grupos (obsoleto)	450
Commrestartinterval	368	Host	450
Compressalways	369	Httpport	450
Compression	370	Hsmreparsetag	451
Console	372	Ieobjtype	452
Createnewbase	373	Ifnewer	453
Datacenter	375	Imagegapsize	454
Datastore	376	Imagetofile	455
Dateformat	376	Inactive	456
Dedupcachepath	380	Incllexcl	456
Dedupcachesize	381	Consideraciones sobre los clientes habilitados	
Eliminación de duplicados	381	para Unicode	457
Defaultserver	383	Opciones include	458
Deletefiles	383	Control del proceso de enlaces simbólicos y	
Descripción	384	alias	464
Detail	385	Proceso de compresión y cifrado de copia de	
Diffsnapshot	387	seguridad	464
Diffsnapshotname	388	Proceso de sistemas de archivos NAS	464
Dirmc	389	Opciones include de la máquina virtual	465
Dirsonly	390	Incrbydate	474
Disablenqr	391	Incremental	475
Diskbuffsize	392	Instrlogmax	476
Diskcachelocation	393	Instrlogname	477
Domain	394	Lanfreecommmethod	478
Domain.image	399	Lanfreeshmport	480
Domain.nas	400	Lanfreetcppport	481
Domain.vmfull	401	Lanfreessl	481
Dontload	408	Lanfreetcpserveraddress	482
Dynamicimage	410	Latest	483
Efsdecrypt	410	Localbackupset	484
Enablearchiveretentionprotection	412	Makesparsefile	484
Enablededupcache	413	Managedservices	486
Enableinstrumentation	414	Maxcmdretries	488
Enablelanfree	416	Mbobjrefreshthresh	489
Encryptiontype	417	Mbpctrefreshthresh	490
Encryptkey	418	Memoryefficientbackup	491
Errorlogmax	420	Mode	492
Errorlogname	422	Monitor	496
Errorlogretention	423	Myreplicationserver	497
Opciones exclude	425	Nasnodename	498
Control del proceso de enlaces simbólicos y		Nfstimeout	500
alias	428	Nodename	501
Control del proceso de compresión	428	Nojournal	502
Proceso de sistemas de archivos NAS	429	Noprompt	503
Opciones exclude de la máquina virtual	429	Nrtablepath	503
Fbbranch	431	Numberformat	504
Fbclientname	432	Optfile	506
Fbpolicyname	434	Contraseña	507
Fbreposlocation	435	Passwordaccess	509
Fbserver	436	Passworddir	511
Fbvolumename	438	Pick	512
Filelist	439	Pitdate	512
Filename	442	Pittime	513

Postschedulecmd/Postnschedulecmd	514
Postsnapshotcmd	516
Preschedulecmd/Prenschedulecmd	517
Preserveaccessdate	519
Preservepath	520
Presnapshotcmd	523
Queryschedperiod	524
Querysummary	525
Quiet	526
Quotesareliteral	527
Removeoperandlimit	528
Replace	529
Replserverguid	531
Replservername	532
Replsslport	534
Repltcpport	536
Repltcpserveraddress	537
Resourceutilization	539
Regulación de las sesiones de copia de seguridad/archivado	540
Regulación de las sesiones de restauración Consideraciones relacionadas con la utilización de varias sesiones de cliente	541
Retryperiod	542
Revokeremoteaccess	543
Schedcmddisabled	544
Schedcmdexception	544
Schedlogmax	545
Schedlogname	547
Schedlogretention	549
Schedmode	550
Schedrestretrdisabled	552
Scrolllines	552
Scrollprompt	553
Servname	555
Sessioninitiation	556
Shmport	558
Showmembers	559
Skipacl	559
Skipaclupdatecheck	560
Snapdiff	561
Snapdiffhttps	566
Snapshotsizes	567
Snapshotsproviderfs	569
Snapshotsproviderimage	570
Snapshotsroot	571
Srvoptsetencryptiondisabled	573
Srvprepostscheddisabled	574
Srvprepostsnapdisabled	575
Ssl	576
Sslfipsmode	577
Sslrequired	578
Ssldisablelegacysql	580
Stagingdirectory	581
Subdir	581
Tapeprompt	583
Tcpadminport	585
Tcpbuffsize	586
Tcpaddress	586
Tcpclientaddress	587
Tcpclientport	588

Tcpnode	589
Tcpport	590
Tcpserveraddress	590
Tcpwindow	591
Timeformat	592
Toc	596
Todate	597
Totime	598
Txnbytelimit	599
Type	600
Update	601
Useexistingbase	601
Userreplicationfailover	602
Usuarios (obsoleto)	603
V2archive	603
Verbose	604
Verifyimage	605
Virtualfsname	606
Virtualmountpoint	606
Virtualnodename	608
Vmbackdir	609
Vmbackupmailboxhistory	610
Vmbackuptype	611
Vmchost	612
Vmcpw	613
Vmctlmc	614
Vmcuser	615
Vmdatastorethreshold	616
Vmdefaultdvportgroup	618
Vmdefaultdvswitch	619
Vmdefaultnetwork	619
Vmenabletemplatebackups	620
Vmlimitperdatastore	622
Vmlimitperhost	623
Vmmaxbackupsessions	625
Vmmaxparallel	627
Vmmaxrestoresessions	628
Vmmaxvirtualdisks	629
Vmmc	631
Vmnoprmdisks	631
Vmnovrmdisks	633
Vmpreferdagpassive	634
Vmprocessvmwithindependent	634
Vmprocessvmwithprdm	636
Vmskipctlcompression	637
Vmskipmaxvirtualdisks	638
Vmskipmaxvmdks	639
Vmtagdefaultdatamover	639
Vmtagdatamover	641
Vmverifyifaction	644
Vmverifyiflatest	646
Vmvstortransport	648
Vmtimeout	649
Webports	650
Wildcardsareliteral	651

Capítulo 11. Utilización de los mandatos 655

Inicio y finalización de una sesión de mandatos de cliente	658
Proceso de mandatos en modalidad por lotes	658

Proceso de mandatos en modalidad interactiva	659	Query Node	735
Especificación de los nombres, opciones y		Query Options	736
parámetros de los mandatos de cliente	660	Query Restore	737
Nombre de mandato	660	Query Schedule	738
Opciones	660	Query Session	738
Opciones en la modalidad interactiva	661	Query Systeminfo	739
Parámetros	661	Query VM	741
Sintaxis de especificación de archivo.	661	Restart Restore.	743
Caracteres comodín	663	Restore	744
Consulta de mandatos de cliente	664	Restauración desde espacios de archivos que no	
Archive	664	están activados para Unicode	749
Archivado de FastBack	667	Restore Backupset	749
Copia de seguridad de FastBack	669	Restauración de conjuntos de copias de	
Backup Group	672	seguridad: consideraciones y restricciones	752
Backup Image	674	Restauración de conjuntos de copias de	
Copia de seguridad de imagen estática,		seguridad en un entorno SAN.	753
dinámica y de instantánea	678	restore Backupset sin el parámetro	
Utilización de la copia de seguridad de imagen		backupsetname	754
para realizar una copia de seguridad		Restore Group	756
incremental del sistema de archivos	679	Restore Image	758
Backup NAS	680	Restore NAS	762
Backup VM.	683	Restore VM.	764
Cancel Process	691	Retrieve	770
Cancel Restore	692	Recuperación de archivos desde espacios de	
Delete Access	692	archivos que no están activados para Unicode	772
Delete Archive.	693	Schedule	773
Delete Backup	694	Selective	775
Delete Filespace	698	Asociación de una instantánea local a un	
Delete Group	699	espacio de archivos del servidor	778
Expire.	701	Set Access	778
Help	703	Set Event.	781
Incremental	704	Establecer Netappsvm	783
Copia de seguridad con registro por diario	709	Establecer contraseña	784
Incremental por fecha	711	Set Vmtags	790
Asociación de una instantánea local a un		Visión general de los códigos de protección de	
espacio de archivos del servidor	711	datos	792
Loop	712	Representación de códigos en Extensión de	
Macro	713	IBM Spectrum Protect	792
Monitor Process	714	Códigos de protección de datos admitidos	793
Preview Archive	715	Herencia de valores de protección de datos	800
Previsualizar copia de seguridad	716	Consejos para la codificación de la protección	
Query Access	717	de datos	802
Query Archive	718		
Query Backup	720	Apéndice. Funciones de accesibilidad	
Consultar imágenes de sistemas de archivos		para la familia de productos IBM	
NAS	723	Spectrum Protect.	805
Query Backupset	723		
query Backupset sin el parámetro		Avisos	807
backupsetname	725		
Query Filespace	727	Glosario.	811
Consulta de espacios de archivos NAS	729		
Query Group	729	Índice.	813
Query Image	731		
Query Inclexcl	733		
Query Mgmtclass	734		

Tablas

1. Espacio de disco mínimo necesario para el despliegue automático del cliente	3
2. Ubicación del archivo de anotaciones predeterminado.	4
3. Métodos de comunicación del cliente AIX	5
4. Funciones admitidas en AIX	6
5. Métodos de comunicación de la API de HP-UX Itanium 2	6
6. Métodos de comunicación de cliente de Linux on Power Systems.	7
7. Métodos de comunicación del cliente Linux on Intel x86_64	8
8. Métodos de comunicación del cliente Linux on System z	9
9. Métodos de comunicación del cliente Mac OS X	10
10. Métodos de comunicación del cliente Oracle Solaris	10
11. Cliente de HP-UX Itanium 2: códigos de idioma para paquetes de instalación	17
12. Nombres de paquetes, contenido y directorio predeterminado	19
13. Nombres de paquetes, contenido y directorio predeterminado	22
14. Nombres de paquetes, contenido y directorio predeterminado	25
15. Identificadores del paquete de idioma.	28
16. Nombres de paquetes, contenido y directorio predeterminado	29
17. Identificadores del paquete de idioma.	32
18. Nombres de paquetes, contenido y directorio predeterminado	33
19. Identificadores del paquete de idioma.	37
20. Nombres de paquetes, contenido y directorio predeterminado	38
21. Identificadores del paquete de idioma.	41
22. Nombres y descripciones de los paquetes de instalación	45
23. Tareas de usuarios root, usuarios autorizados y otros usuarios.	49
24. Herramientas de autorización de Mac OS X y aplicaciones de IBM Spectrum Protect asociadas	52
25. Servicios gestionados por el aceptador de cliente frente a servicios del planificador tradicional	67
26. Configuración de eliminación de duplicados de datos: cliente y servidor	89
27. Opciones para excluir espacios de archivos y directorios	126
28. Opciones para controlar el proceso utilizando sentencias de inclusión y exclusión	128
29. Caracteres comodín y otros caracteres especiales	131
30. Utilización de caracteres comodín con patrones de inclusión y exclusión	132
31. Opciones para controlar el proceso de vínculos simbólicos y alias	134
32. Opciones para controlar la compresión y el cifrado.	134
33. Trabajar con archivos mediante la GUI del cliente de copia de seguridad y archivado	150
34. Sistemas de archivos admitidos y soporte para ACL	162
35. Tamaño máximo de archivo.	166
36. Ejemplos de copia de seguridad desde la línea de mandatos	182
37. Soporte de tipo de dispositivo de volumen para una copia de seguridad de imagen	197
38. Comparación de métodos de copia de seguridad de imagen incremental.	201
39. Comparaciones de las operaciones de imagen de LVM1 y LVM2	202
40. Opciones y mandatos NAS	211
41. Prestaciones de copia de seguridad y restauración para máquinas virtuales VMware en plataformas Linux	219
42. Mensajes informativos de la línea de mandatos del cliente	224
43. Restricciones de restauración del conjunto de copias de seguridad de la GUI.	242
44. Restricciones de restauración de los conjuntos de copias de seguridad de la línea de mandatos	242
45. mandatos de restauración de WPAR de ejemplo con el archivo dsm.opt	254
46. Opciones y mandatos NAS	256
47. Ejemplos de restauración desde la línea de mandatos	259
48. Ejemplos de archivado desde la línea de mandatos	270
49. Tabla de gestión de vínculos simbólicos para archivado y recuperación	275
50. Ejemplos de recuperación de archivos desde la línea de mandatos	277
51. Ejemplo de la salida clásica de query schedule	290
52. Ejemplo de salida ampliada del mandato query schedule	291
53. Códigos de retorno del cliente y significado de éstos	297
54. Valores de atributo predeterminados de la clase de gestión estándar.	301
55. Opciones de TCP/IP	314
56. Opciones de comunicación de memoria compartida	315
57. Archivo de opciones del sistema cliente de ejemplo	316
58. Opciones de proceso de copia de seguridad/archivado	316
59. Opciones de proceso de restauración y recuperación	327

60. Opciones de planificación	330	87. mandato delete archive: opciones relacionadas	694
61. Opciones de formato e idioma	332	88. Mandato Delete Backup: opciones relacionadas	697
62. Opciones de proceso de mandatos	332	89. mandato delete filespace: opciones relacionadas	699
63. Opciones de autorización	333	90. mandato delete group: opciones relacionadas	700
64. Opciones de proceso de errores	334	91. Mandato expire: opciones relacionadas	702
65. Opciones de proceso de transacciones	334	92. Mandato Incremental: opciones relacionadas	706
66. Opciones de cliente Web	335	93. Mandato query archive: opciones relacionadas	718
67. Opciones de diagnóstico	335	94. mandato query backup: opciones relacionadas	721
68. Opciones de mandatos de cliente	338	95. mandato query backupset: opciones relacionadas	724
69. Opciones que sólo son válidas en la línea de mandatos inicial	343	96. mandato query backupset: opciones relacionadas	726
70. Opciones que pueden establecerse con el servidor de IBM Spectrum Protect	344	97. Mandato query filespace: opciones relacionadas	728
71. Valores del formato de hora de ejemplo en la configuración del entorno regional (línea t_fmt)	379	98. Mandato query group: opciones relacionadas	730
72. Valores del formato de fecha de ejemplo en la configuración del entorno regional (línea d_fmt)	380	99. Mandato query image: opciones relacionadas	732
73. Interacción de definiciones de dominio de distintos orígenes	398	100. Mandato query mgmtclass: opciones relacionadas	734
74. Otros parámetros opcionales	462	101. Mandato query node: opciones relacionadas	735
75. Mandato Incremental: opciones relacionadas	563	102. Mandato query options: opciones relacionadas	736
76. Efectos de los valores SSL de servidor y cliente en el éxito o el fracaso de los intentos de inicio de sesión	579	103. mandato query systeminfo: opciones relacionadas	740
77. Valores del formato de hora de ejemplo en la configuración del entorno regional (línea t_fmt)	595	104. Mandato Query VM: opciones relacionadas para consultas de la máquina virtual VMwar. .	741
78. Valores del formato de fecha de ejemplo en la configuración del entorno regional (línea d_fmt)	595	105. mandato Restore: opciones relacionadas	747
79. Mandatos	655	106. mandato Restore Backupset: opciones relacionadas	751
80. Caracteres comodín	663	107. Mandato restore Group: opciones relacionadas	757
81. mandato Archive: opciones relacionadas	665	108. Comando restore image: opciones relacionadas	760
82. mandato Archive Fastback: opciones relacionadas	668	109. Mandato restore NAS: opciones relacionadas	763
83. mandato Backup FastBack: opciones relacionadas	670	110. Mandato Restore VM: opciones relacionadas cuando se restauran máquinas virtuales VMware	767
84. Mandato backup group: opciones relacionadas	673	111. mandato Retrieve: opciones relacionadas	771
85. Mandato Backup Image: opciones relacionadas	676	112. mandato Schedule: opciones relacionadas	774
86. mandato backup NAS: opciones relacionadas	682	113. Mandato selective: opciones relacionadas	777
		114. Orden de prelación de los objetos de inventario de vSphere.	801

Acerca de esta publicación

IBM Spectrum Protect es un producto de cliente/servidor con licencia que proporciona servicios de gestión de almacenamiento en un entorno de sistemas multiplataforma.

El programa cliente de archivado y copia de seguridad permite a los usuarios realizar copias de seguridad de archivos o archivarlos desde las estaciones de trabajo o servidores de archivos y restaurar y recuperar versiones de copia de seguridad y copias archivadas de archivos en las estaciones de trabajo locales.

Además del cliente de copia de seguridad/archivado, IBM Spectrum Protect incluye los siguientes componentes:

- Un programa de servidor que actúa como servidor de archivado y copia de seguridad para las estaciones de trabajo distribuidas y los servidores de archivo. El programa servidor también proporciona servicios de gestión de almacenamiento jerárquico (HSM), y permite que los sistemas actúen como un servidor de migración.
- Un programa del cliente administrativo que puede acceder desde un navegador web o desde una línea de mandatos. El programa permite que el administrador de IBM Spectrum Protect controle y supervise las actividades del servidor, defina políticas de gestión de almacenamiento para servicios de gestión de espacio, copias de seguridad y archivado, y establezca planificaciones para ejecutar dichos servicios en intervalos regulares.
- Una interfaz de programas de aplicación (API) que puede utilizar para mejorar una aplicación existente con los servicios de gestión de almacenamiento. Cuando se inscribe una aplicación con un servidor como nodo cliente, la aplicación puede realizar copias de seguridad, restaurar, archivar y recuperar objetos del almacenamiento.
- Un cliente de archivado y copia de seguridad que permite que un administrador autorizado, el personal de help desk y otros usuarios lleven a cabo copias de seguridad, restauración archivado y servicios de recuperación utilizando un navegador web en un sistema remoto.

Los programas de cliente de IBM Spectrum Protect for Space Management e IBM Spectrum Protect HSM for Windows están asociados a IBM Spectrum Protect, pero se venden por separado. Estos productos migran automáticamente los archivos elegibles al almacenamiento para conservar niveles de espacio libre en los sistemas de archivos locales y recuperan los archivos migrados cuando se accede a éstos. Además, permite a los usuarios migrar y recuperar archivos específicos.

Los términos *gestión de almacenamiento jerárquico* y *gestión del espacio* tienen el mismo significado en esta publicación.

Conceptos relacionados:

“Planificación de las copias de seguridad” en la página 155

“Novedades de la versión 8.1” en la página xvii

Capítulo 1, “Instalación de los clientes de archivado y copia de seguridad de IBM Spectrum Protect”, en la página 1

A quién va dirigida esta publicación

Esta publicación proporciona instrucciones para que un usuario instale, configure y utilice el cliente de IBM Spectrum Protect.

Publicaciones

La familia de productos IBM Spectrum Protect incluye IBM Spectrum Protect Snapshot, IBM Spectrum Protect for Space Management, IBM Spectrum Protect for Databases y varios otros productos de gestión de almacenamiento desde IBM®.

Para ver la documentación del producto de IBM, consulte IBM Knowledge Center.

Convenciones utilizadas en esta publicación

Esta publicación utiliza las siguientes convenciones tipográficas:

Ejemplo	Descripción
autoexec.ncf hsmgui.exe	Cadena de letras minúsculas con una extensión que indica nombres de archivos de programa.
DSMI_DIR	Una cadena de letras mayúsculas que indica códigos de retornos y otras variables u otros valores.
dsmQuerySessInfo	La letra negrita indica un mandato que se especifica en una línea de mandatos, el nombre de una llamada a función, el nombre de una estructura, un campo dentro de una estructura o un parámetro.
<i>timeformat</i>	El tipo de letra en cursiva y negrita indica una opción de cliente de archivado y copia de seguridad. El tipo de letra negrita se utiliza para especificar la opción o bien en un ejemplo.
<i>dateformat</i>	El tipo de letra cursiva y negrita indica una opción, el valor de una opción, un nuevo término, una información que el usuario proporciona o para hacer hincapié en determinadas palabras del texto.
maxcmdretries	El tipo de letra monoespaciado indica fragmentos de un programa o información tal y como se visualizaría en pantalla, como un ejemplo de mandato.
signo más (+)	Un signo más entre dos teclas indica que se pulsan ambas teclas al mismo tiempo.

Lectura de diagramas de sintaxis

Para leer un diagrama de sintaxis para especificar un mandato, siga la vía de acceso de la línea. Lea de izquierda a derecha y de arriba abajo.

- El símbolo ►— indica el comienzo de un diagrama de sintaxis.
- El símbolo —► al final de una línea indica que el diagrama de sintaxis continúa en la siguiente línea.
- El símbolo ►— al principio de una línea indica que un diagrama de sintaxis continúa desde la línea anterior.
- El símbolo —► indica el final de un diagrama de sintaxis.

Elementos de sintaxis, como una palabra clave o una variable, puede estar:

- En la línea (elemento obligatorio)
- Por encima de la línea (elemento predeterminado)
- Por debajo de la línea (elemento opcional)

Símbolos

Especifique estos símbolos *exactamente* como aparecen en el diagrama de sintaxis.

- * Asterisco
- { } Llaves
- : Dos puntos
- , Coma
- = Signo de igual
- - Guión
- () Paréntesis
- . Punto
- Espacio
- " comillas
- ' comillas simples

Variables

Los elementos en minúscula y en cursiva, como *<nombre_var>*, indican variables. En este ejemplo, puede especificar un *<nombre_var>* cuando indique el mandato **nombre_man**.

►►—nombre_mand—*<nombre_var>*—————►◄

Repetición

Una flecha que gira hacia la izquierda indica que el elemento se puede repetir. Un carácter dentro de una flecha significa que debe separar los elementos repetidos con un carácter.

►►——repetir—————►◄

Una nota a pie de página (1) junto a la flecha se refiere a un límite que indica el número de veces que se puede repetir un elemento.

►►——repetir—————►◄

Notas:

- 1 Especifique *repetir* hasta un máximo de cinco veces.

Opciones necesarias

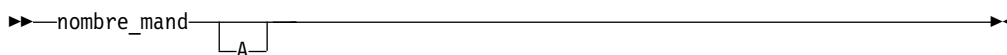
Cuando hay uno o varios elementos en una pila y uno de ellos se encuentra en la línea, *debe* especificar un elemento.

En este ejemplo, debe elegir A, B o C.

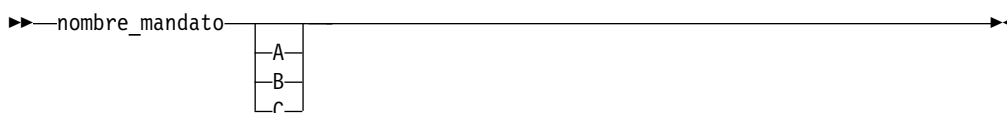


Opciones opcionales

Cuando un elemento está *por debajo* de la línea, ese elemento es opcional. En el primer ejemplo, puede seleccionar A o nada.



Cuando dos o más elementos están en una pila debajo de la línea, todos los elementos son opcionales. En el segundo ejemplo, puede elegir A, B, C o nada en absoluto.



Opciones repetibles

Una pila de elementos seguida de una flecha que gira hacia la izquierda indica que puede seleccionar más de un elemento, o en algunos casos, repetir un elemento individual.

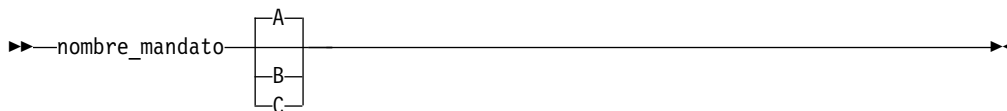
En este ejemplo, puede seleccionar cualquier combinación de A, B o C.



Valores predeterminados

Los valores predeterminados se encuentran por encima de la línea. El valor predeterminado se selecciona a menos que lo sustituya o puede seleccionarlo de forma explícita. Para sustituir el valor predeterminado, incluya una opción de la pila debajo de la línea.

En este ejemplo, A es el valor predeterminado. Seleccione B o C para modificar A.



Novedades de la versión 8.1

IBM Spectrum Protect Versión 8.1 presenta nuevas características y actualizaciones.

Para obtener una lista de las nuevas características y actualizaciones de este release, consulte el apartado Actualizaciones del cliente de archivado y copia de seguridad.

Información relacionada:

“Acerca de esta publicación” en la página xiii

Capítulo 1. Instalación de los clientes de archivado y copia de seguridad de IBM Spectrum Protect

El cliente de archivado y copia de seguridad de IBM Spectrum Protect le ayuda a proteger la información de las estaciones de trabajo.

Puede conservar versiones de copia de seguridad de los archivos que puede restaurar si los archivos originales se pierden o resultan dañados. También puede archivar archivos usados con poca frecuencia, mantenerlos en su estado actual y recuperarlos cuando los necesite.

El cliente de copia de seguridad y archivado funciona conjuntamente con el servidor de IBM Spectrum Protect. Póngase en contacto con el administrador del servidor de IBM Spectrum Protect para obtener acceso a las copias de seguridad y copias archivadas en el servidor o consulte las publicaciones del servidor para obtener información sobre la instalación y configuración del servidor de IBM Spectrum Protect.

Conceptos relacionados:

“Novedades de la versión 8.1” en la página xvii

“Planificación de las copias de seguridad” en la página 155

Actualización del cliente de archivado y copia de seguridad

En los siguientes apartados se explica qué debe hacer si desea realizar una actualización a la versión 8.1.0 del cliente de archivado y copia de seguridad de IBM Spectrum Protect desde una versión anterior.

Actualización de la vía de acceso para clientes y servidores

Los clientes y los servidores de IBM Spectrum Protect se pueden actualizar en momentos diferentes. La combinación de servidores y clientes que despliega debe ser compatible.

Para evitar interrupciones de las actividades de archivado y copia de seguridad mientras actualiza de un release a otro, siga las directrices de compatibilidad para los clientes y servidores de IBM Spectrum Protect en la nota técnica 1053218.

Para obtener información sobre cómo actualizar las configuraciones de AIX IBM PowerHA SystemMirror, consulte “Migración de configuraciones de AIX IBM PowerHA SystemMirror antiguas” en la página 113.

Información adicional sobre la actualización

Cuando actualiza un cliente de copia de seguridad y archivado, hay información adicional que debe tenerse en cuenta antes de utilizar el nuevo software de cliente.

Tenga en cuenta la información siguiente al actualizar un cliente de archivado y copia de seguridad:

- Si está actualizando desde el cliente de archivado y copia de seguridad de IBM Tivoli Storage Manager Versión 7.1.2 o anterior en el sistema operativo Oracle Solaris, tiene que desinstalar los paquetes de idioma previamente instalados para poder continuar con la actualización.

- Para usuarios de Mac, las actualizaciones realizadas en el cliente de Mac OS X contenidas en IBM Spectrum Protect V6.3 o versiones más nuevas, requieren que tenga en cuenta los siguientes artículos:
 - Cuando utilice el cliente de Mac OS X que se proporciona en esta versión, asegúrese de que los archivos `dsm.sys` y `dsm.opt` se codifican mediante Unicode (UTF-8). La codificación UTF-8 permite el uso de caracteres de cualquier idioma en los archivos de opciones. Si los archivos `dsm.sys` o `dsm.opt` se codificaron anteriormente como MacRoman (o cualquier otro distinto a UTF-8), ábralos en un editor como TextEdit y guárdelos con la codificación UTF-8, y sin la extensión `.txt`. Las listas include-exclude se pueden codificar bien como UTF-8 o UTF-16. Para obtener más información sobre el uso de Unicode, consulte “Consideraciones sobre los clientes habilitados para Unicode” en la página 457.
 - Los espacios de archivos del servidor de IBM Spectrum Protect que se crearon mediante clientes de Mac OS 9 no se pueden gestionar mediante el cliente de Mac OS X que se proporcionó en IBM Spectrum Protect V6.3. Utilice `q file nodo f=d` en el servidor para listar archivos almacenados para un nodo. Los archivos de plataforma Mac que no empiezan por una barra inclinada (/) los ha creado probablemente un cliente Mac más antiguo. No puede restaurar ni gestionar estos archivos mediante el cliente de Mac OS X que se proporciona en esta versión. Puede gestionar estos archivos, pero tiene que utilizar un cliente de Mac que esté instalado en un nodo de cliente de la versión 6.2.2 o anterior.
- Para obtener una lista de mensajes nuevos y cambiados desde la versión anterior de IBM Spectrum Protect, consulte el archivo `client_message.chg` en el paquete del clúster.

Despliegue automático del cliente de copia de seguridad y archivado

El administrador del servidor de IBM Spectrum Protect puede desplegar de forma automática un cliente de archivado y copia de seguridad para las estaciones de trabajo que ya tienen instalado el cliente de archivado y copia de seguridad.

Al planificar despliegues de cliente de archivado y copia de seguridad, los paquetes del cliente actualizados (que incluyen los componentes del cliente y la biblioteca API) se instalan en las estaciones de trabajo que los reciben. El programa de instalación del cliente realiza una comprobación de dependencias para asegurarse de que la biblioteca API no entra en conflicto con el paquete del cliente instalado actualmente.

Las aplicaciones de IBM Spectrum Protect for ERP no utilizan la misma tecnología de instalación que el programa de instalación del cliente. Por ello, la comprobación de dependencias de la instalación del cliente no detecta si la biblioteca API que utilizan las aplicaciones de IBM Spectrum Protect for ERP son compatibles con la biblioteca API que va a ser instalada por los despliegues automáticos del cliente. Si un paquete de cliente se despliega e instala automáticamente en una estación de trabajo, la biblioteca API instalada podría no ser compatible con la biblioteca API que haya sido instalada por la aplicación de IBM Spectrum Protect for ERP. La biblioteca de API recién desplegada puede hacer que fallen las aplicaciones de IBM Spectrum Protect for ERP.

No planifique despliegues de cliente automáticos en estaciones de trabajo que tengan una aplicación de IBM Spectrum Protect for ERP instalada.

El servidor de IBM Spectrum Protect se puede configurar para actualizar automáticamente los clientes de archivado y copia de seguridad en sistemas Linux y UNIX soportados. Los clientes existentes deben ser de la versión 5.5 o posterior.

Importante: Para que el despliegue automático del cliente funcione, es necesario que se cumplan las siguientes condiciones:

- El sistema cliente debe tener como mínimo espacio de disco libre como se muestra en Tabla 1.

Tabla 1. Espacio de disco mínimo necesario para el despliegue automático del cliente

Sistemas operativos	Espacio de disco libre necesario
AIX	1500 MB
Solaris	1200 MB
Linux on Power	350 MB
Linux x86_64	950 MB
Linux on System z	350 MB
Mac OS X	200 MB

- En IBM Spectrum Protect 6.3 y posterior, los clientes de archivado y copia de seguridad de 32 bits ya no están admitidos. Si el gestor de despliegue detecta un cliente de archivado y copia de seguridad de 32 bits en ejecución en un sistema operativo de 64 bits, actualizará el cliente a la versión de 64 bits.
- La opción `passwordaccess` debe estar establecida en **generate**.

Para almacenar la contraseña en el cliente, un usuario debe iniciar sesión en la estación de trabajo local al menos una vez, para proporcionar la contraseña. Si el proceso de despliegue automático del cliente no puede encontrar la contraseña de nodo, se producirán los siguientes eventos:

- El proceso de despliegue no se iniciará.
- Se registrará un mensaje de aviso en el archivo `setup.log`.

Los mensajes siguientes son ejemplos de los mensajes que se pueden registrar durante un despliegue.

```
Sun 10/11/2009 10:16:04.35 The deployclient.sh script is started.
Sun 10/11/2009 10:16:04.37 deployclient.sh is removing the deployment
manager and temporary files possibly left from the previous installation.
Sun 10/11/2009 10:17:10.53 WARNING: Still waiting for the result of query
system information.
Ensure that "PASSWORDACCESS GENERATE" is set in the client options file
and that a connection to the server can be made without being prompted
for a password.
```

Si ve estos errores y `PASSWORDACCESS` está establecido en **GENERATE**, los errores se deberán a un problema de red (el cliente no se puede alcanzar).

- El mandato `dsmc query systeminfo` se queda ejecutándose.
- El proceso de despliegue no se puede iniciar, por lo que no se envía ningún mensaje al servidor.
- El cliente se despliega en el servidor como una tarea planificada; el daemon del planificador del cliente debe estar en ejecución.
- El cliente se despliega como un mandato de sistema operativo posterior a la planificación; los mandatos de sistema operativo planificados deben habilitarse en el cliente.

Nota: El mandato especificado por la opción `postschedulecmd` del archivo de opciones de sistema de cliente (`dsm.sys`) se sustituirá mediante el script de

despliegue, pero se ejecutará el mandato especificado por la opción `preschedulecmd`. Suprime la opción `preschedulecmd` de la tarea de despliegue especificando la opción siguiente en la definición de planificación:

`-preschedulecmd=""`

- Debe configurar el servidor para llevar a cabo los despliegues automáticos del cliente de archivado y copia de seguridad. Consulte la documentación del servidor de IBM Spectrum Protect para obtener instrucciones.

El gestor de despliegue graba los datos de rastreo y de anotaciones para una operación de despliegue en el disco del cliente. La ubicación predeterminada de los registros se muestra en Tabla 2. `xxxx` representa la versión, el release, la modificación y la información del fixpack para el cliente de archivado y copia de seguridad desplegado.

Tabla 2. Ubicación del archivo de anotaciones predeterminado.

Sistema operativo	Directorio
AIX	<code>/usr/tivoli/client/IBM_ANR_UNX/Vxxxx/log/</code>
Oracle Solaris, Linux	<code>/opt/tivoli/tsm/client/IBM_ANR_UNX/Vxxxx/log/</code>
Mac	<code>/Library/Application Support/tivoli/tsm/client/ba/bin/IBM_ANR_MAC/Vxxxx/log</code>

Cuando define una planificación para desplegar las actualizaciones del cliente, puede especificar una recuperación no predeterminada para las plataformas de UNIX yLinux. Especificar una ubicación de destino de recuperación no predeterminada cambia la ubicación de los archivos de rastreo y registro. Por ejemplo, la ubicación de destino de recuperación predeterminada paraAIX es `/usr/tivoli/client/`. Si especifica `/tmp/tivoli/client` como ubicación de destino, los archivos de rastreo y registro estarán en `/tmp/tivoli/client/IBM_ANR_UNX/Vxxxx/log`.

En la plataforma Mac OS X, no puede cambiar la ubicación de destino de recuperación. El directorio de trabajo del gestor de despliegue está relacionado con el directorio de trabajo del planificador del cliente. Por ejemplo, si el usuario inicia el planificador del cliente desde `/mydir`, los archivos de rastreo y registro estarán en `/mydir/IBM_AMR_MAC/Vxxxx/log`.

Se utilizará un semáforo para evitar que actualicen un cliente distintos gestores de despliegue al mismo tiempo. El semáforo caducará a las 24 horas desde el último despliegue del cliente. Los clientes nuevos no se pueden desplegar hasta que el semáforo caduque.

Referencia relacionada:

“Autodeploy” en la página 355

Requisitos del entorno del cliente

Cada uno de los clientes de IBM Spectrum Protect tiene requisitos de hardware y software.

En la lista siguiente se muestra la ubicación de los requisitos previos de entorno para cada plataforma admitida.

- “Entorno del cliente AIX” en la página 5

- “Entorno de la API de HP-UX Itanium 2” en la página 6
- “Entorno de clientes de Linux on Power Systems” en la página 7
- “Entorno de cliente Linux x86_64” en la página 7
- “Entorno de cliente Linux on System z” en la página 8
- “Entorno del cliente Mac OS X” en la página 9
- “Entorno de cliente Oracle Solaris” en la página 10
- “Requisitos de soporte para NDMP (sólo Extended Edition)” en la página 11

Para obtener la información actual sobre los requisitos previos de entorno de cliente para todas las plataformas de cliente de copia de seguridad y archivado admitidas, consulte la nota técnica 1243309.

Entorno del cliente AIX

Este apartado contiene información sobre el entorno de cliente, sobre los componentes del cliente de copia de seguridad y archivado y sobre los requisitos de hardware y de software para la plataforma AIX.

Componentes instalables del cliente AIX

El cliente de archivado y copia de seguridad consta de varios componentes instalables.

Los componentes instalables para el cliente AIX son los siguientes:

- Cliente de línea de mandatos de copia de seguridad/archivado
- Cliente de administración
- Interfaz gráfica de usuario de cliente de archivado y copia de seguridad, que utiliza tecnología Oracle Java™
- Cliente web de archivado y copia de seguridad
- API de 64 bits de IBM Spectrum Protect

La API se puede instalar de forma separada. Los demás componentes se instalan todos cuando se instala el paquete AIX (`tivoli.tsm.client.api.64bit`).

Requisitos de sistema para el cliente de AIX

Los clientes de IBM Spectrum Protect AIX requieren un mínimo de hardware, espacio de disco, memoria y software.

Para conocer los requisitos de software y hardware para todas las versiones admitidas de los clientes de AIX, incluidos los fixpacks más recientes, consulte la nota técnica 1052226.

Métodos de comunicación del cliente AIX

Existen métodos de comunicación de memoria compartida y TCP/IP para el cliente de archivado y copia de seguridad AIX.

Utilice los siguientes métodos de comunicación con el cliente IBM Spectrum Protect Versión 8.1.0 AIX:

Tabla 3. Métodos de comunicación del cliente AIX

Para utilizar este método de comunicación:	Instale este software:	Para conectarse a estos servidores de IBM Spectrum Protect:
TCP/IP	TCP/IP (estándar con plataformas AIX admitidas)	AIX, Linux, Windows

Tabla 3. Métodos de comunicación del cliente AIX (continuación)

Para utilizar este método de comunicación:	Instale este software:	Para conectarse a estos servidores de IBM Spectrum Protect:
Memoria compartida	TCP/IP (estándar con plataformas AIX admitidas)	AIX

Funciones de cliente de archivado y copia de seguridad disponibles en AIX

En esta lista se muestran las funciones admitidas en AIX.

Tabla 4. Funciones admitidas en AIX

Funciones	¿Admitidas en AIX?
Línea de mandatos y GUI de copia de seguridad y archivado	sí
Copia de seguridad con registro por diario	sí
Operaciones fuera de la LAN	sí
Copia de seguridad de imagen activada	sí
Copia de seguridad de imagen fuera de línea	sí

Entorno de la API de HP-UX Itanium 2

Revise la información sobre el entorno de la API, los componentes instalables y los requisitos de hardware y software de la plataforma de HP-UX Itanium 2.

Componente instalable de la API de HP-UX Itanium 2

Solo puede instalar la API de HP-UX Itanium 2 en IBM Spectrum Protect versión 8.1.0.

Requisitos del sistema para la API de HP-UX Itanium 2

La API de HP-UX Itanium 2 de IBM Spectrum Protect requiere un mínimo de hardware, espacio de disco, memoria y software.

Para conocer los requisitos de software y hardware de todas las versiones soportadas de la API de HP-UX Itanium 2, incluidos los fixpacks más recientes, consulte la nota técnica 1197146.

Métodos de comunicación de la API de HP-UX Itanium 2

Los métodos de comunicación de memoria compartida y TCP/IP están disponibles para la API de HP-UX Itanium 2.

Tabla 5. Métodos de comunicación de la API de HP-UX Itanium 2

Para utilizar este método de comunicación:	Instale este software:	Para conectarse a estos servidores de IBM Spectrum Protect:
TCP/IP	TCP/IP (estándar con HP-UX)	AIX, Linux, Windows

Entorno de clientes de Linux on Power Systems

Esta sección contiene información de entorno de cliente, los componentes del cliente de copia de seguridad y archivado y los requisitos de hardware y software para las plataformas de cliente de Linux on Power Systems.

Componentes instalables de cliente de Linux on Power Systems

La línea de mandatos de del cliente de copia de seguridad y archivado, la GUI de Java, el archivado y copia de seguridad web y la API constan de los componentes instalables de cliente de archivado y copia de seguridad de Linux on Power Systems.

Puede instalar los siguientes componentes con IBM Spectrum Protect Versión 8.1.0:

- Cliente de archivado y copia de seguridad
- Cliente de administración
- Interfaz gráfica de usuario (GUI) de Java de copia de seguridad y archivado
- Cliente Web de copia de seguridad/archivado
- API (64 bits) de IBM Spectrum Protect

Requisitos de sistema para clientes en Linux en Power Systems

Los clientes de IBM Spectrum Protect en Linux en Power Systems necesitan una cantidad mínima de hardware, espacio de disco, memoria y software.

Para conocer los requisitos de software y hardware para todas las versiones soportadas de los clientes de en Linux en Power Systems, incluidos los fixpacks más recientes, consulte nota técnica 1169963.

Métodos de comunicación de cliente de Linux on Power Systems

Los clientes de archivado y copia de seguridad en Linux on Power Systems pueden utilizar TCP/IP o la memoria compartida como método de comunicaciones para las comunicaciones de cliente-servidor.

Tabla 6 lista los métodos de comunicaciones de cliente de Linux on Power Systems disponibles y los sistemas operativos de servidor de IBM Spectrum Protect con los que los puede utilizar.

Tabla 6. Métodos de comunicación de cliente de Linux on Power Systems

Para utilizar este método de comunicación:	Instale este software:	Para conectarse a estos servidores de IBM Spectrum Protect:
TCP/IP	TCP/IP (estándar con Linux)	AIX, Linux, Windows
Memoria compartida	TCP/IP (estándar con Linux)	Linux en Power Systems

Entorno de cliente Linux x86_64

Esta sección contiene información sobre el entorno del cliente, los componentes del cliente de copia de seguridad y archivado y los requisitos de hardware y software para Linux on Intel (Linux x86_64) .

Componentes instalables del cliente Linux x86_64

La línea de mandatos del cliente de copia de seguridad y archivado, la GUI de Java, el archivado y copia de seguridad web, el cliente de administración y la API son los componentes instalables del cliente de copia de seguridad y archivado de Linux on Intel (Linux x86_64).

Puede instalar los siguientes componentes con IBM Spectrum Protect Versión 8.1.0:

- Cliente de archivado y copia de seguridad
- Cliente de administración
- Interfaz gráfica de usuario (GUI) de Java de copia de seguridad y archivado
- Cliente Web de copia de seguridad/archivado
- API de IBM Spectrum Protect

Requisitos de sistema para clientes Linux x86_64

Los clientes IBM Spectrum Protect Linux x86_64 requieren un mínimo de hardware, espacio de disco, memoria y software.

Para conocer los requisitos de software y hardware para todas las versiones soportadas de los clientes de Linux x86_64, incluidos los fixpacks más recientes, consulte la nota técnica 1052223.

Métodos de comunicación del cliente Linux x86_64

Existen métodos de comunicación de memoria compartida y TCP/IP para el cliente de archivado y copia de seguridad de Linux on Intel (Linux x86_64).

Puede utilizar los siguientes métodos de comunicación con el cliente de IBM Spectrum Protect versión 8.1.0 Linux en Intel (Linux x86_64)

Tabla 7. Métodos de comunicación del cliente Linux on Intel x86_64

Para utilizar este método de comunicación:	Instale este software:	Para conectarse a estos servidores de IBM Spectrum Protect:
TCP/IP	TCP/IP (estándar con Linux)	AIX, Linux, Windows
Memoria compartida	TCP/IP (estándar con Linux)	Linux x86_64

Entorno de cliente Linux on System z

Esta sección contiene información sobre el entorno de cliente, los componentes del cliente de copia de seguridad y archivado y los requisitos de hardware y de software para la plataforma Linux on System z.

Componentes instalables del cliente Linux on System z

La línea de mandatos del cliente de copia de seguridad y archivado, el cliente administrativo, el cliente de archivado y copia de seguridad web y la API son los componentes instalables del cliente de archivado y copia de seguridad de Linux on System z.

Puede instalar los siguientes componentes con IBM Spectrum Protect Versión 8.1.0:

- Cliente de archivado y copia de seguridad
- Cliente de administración
- Cliente Web de copia de seguridad/archivado
- API de IBM Spectrum Protect

Requisitos de sistema para clientes Linux on System z

Los clientes de IBM Spectrum Protect Linux System z requieren una cantidad mínima de hardware, espacio de disco, memoria y software.

Para conocer los requisitos de hardware y software para todas las versiones soportadas de los clientes de Linux System z, incluidos los fixpacks más recientes, consulte la nota técnica 1066436.

Métodos de comunicación del cliente Linux on System z

Existen métodos de comunicación de memoria compartida y TCP/IP para el cliente de archivado y copia de seguridad Linux on System z.

Utilice los siguientes métodos de comunicación con el cliente IBM Spectrum Protect Versión 8.1.0 Linux en System z:

Tabla 8. Métodos de comunicación del cliente Linux on System z

Para utilizar este método de comunicación:	Instale este software:	Para conectarse a estos servidores de IBM Spectrum Protect:
TCP/IP	TCP/IP (estándar con Linux)	AIX, Linux, Windows
Memoria compartida	TCP/IP (estándar con Linux)	Linux on System z

Entorno del cliente Mac OS X

Este apartado contiene información sobre el entorno de cliente, sobre los componentes del cliente de copia de seguridad y archivado y sobre los requisitos de hardware y de software para el cliente de Mac OS X.

Componentes instalables del cliente Mac OS X

La línea de mandatos del cliente de copia de seguridad y archivado, la GUI Java, el archivado y copia de seguridad web y la API constituyen los componentes instalables del cliente de archivado y copia de seguridad Mac OS X.

Los componentes siguientes se instalan con IBM Spectrum Protect Versión 8.1.0:

- Cliente de archivado y copia de seguridad
- Cliente de administración
- Cliente Web de copia de seguridad/archivado
- API de IBM Spectrum Protect
- Interfaz gráfica de usuario (GUI) de Java de copia de seguridad y archivado

Consejo: El archivo de script de shell dsmj para la GUI Java está instalado en la siguiente ubicación:

/Library/Application Support/tivoli/tsm/client/ba/bin

Requisitos de sistema para clientes Mac OS X

Los clientes Mac OS X de IBM Spectrum Protect requieren un mínimo de hardware, espacio de disco, memoria y software.

Para conocer los requisitos de software y hardware para todas las versiones soportadas de los clientes Mac OS X, incluidos los fixpacks más recientes, consulte la nota técnica 1053584.

Métodos de comunicación del cliente Mac OS X

Existen métodos de comunicación TCP/IP para el cliente de archivado y copia de seguridad Mac OS X.

Utilice los siguientes métodos de comunicación con el cliente IBM Spectrum Protect Versión 8.1.0 Mac OS X:

Tabla 9. Métodos de comunicación del cliente Mac OS X

Para utilizar este método de comunicación:	Instale este software:	Para conectarse a estos servidores de IBM Spectrum Protect:
TCP/IP	TCP/IP (estándar con Mac OS X)	AIX, Linux, Windows

Entorno de cliente Oracle Solaris

Este apartado contiene información sobre el entorno de cliente, sobre los componentes del cliente de copia de seguridad y archivado y sobre los requisitos de hardware y de software para la plataforma Oracle Solaris.

Componentes instalables del cliente Oracle Solaris

La línea de mandatos de IBM Spectrum Protect, la GUI Java, la copia de seguridad y archivado web y la API constituyen los componentes instalables del cliente de archivado y copia de seguridad de Solaris.

Puede instalar los siguientes componentes del cliente:

- Cliente de archivado y copia de seguridad
- Cliente de administración
- Interfaz gráfica de usuario (GUI) de Java de copia de seguridad y archivado
- Cliente Web de copia de seguridad/archivado
- API de IBM Spectrum Protect

Requisitos de sistema para clientes Oracle Solaris

Los clientes Oracle Solaris de IBM Spectrum Protect requieren una cantidad mínima de hardware, espacio de disco, memoria y software.

Para conocer los requisitos de hardware y software de todas las versiones soportadas de clientes de IBM Spectrum Protect Oracle Solaris, incluidos los fixpacks más recientes, consulte las siguientes páginas de soporte de IBM:

- Para conocer los requisitos de cliente de Oracle Solaris SPARC, consulte la nota técnica 1052211.
- Para conocer los requisitos de cliente de Oracle Solaris x86_64, consulte la nota técnica 1232956.

Métodos de comunicación del cliente Oracle Solaris

Existen métodos de comunicación de memoria compartida y TCP/IP para el cliente de archivado y copia de seguridad Oracle Solaris.

Utilice los siguientes métodos de comunicación con el cliente Oracle Solaris:

Tabla 10. Métodos de comunicación del cliente Oracle Solaris

Para utilizar este método de comunicación:	Instale este software:	Para conectarse a estos servidores de IBM Spectrum Protect:
TCP/IP	TCP/IP (estándar con Solaris)	AIX, Linux, Windows

Requisitos de soporte para NDMP (sólo Extended Edition)

Utilice el protocolo NDMP (Network Data Management Protocol) para realizar copias de seguridad y restaurar sistemas de archivos NAS en bibliotecas o unidades de cintas que están conectadas localmente a los servidores de archivos NAS de Network Appliance y EMC Celerra.

El soporte de NDMP solo está disponible en IBM Spectrum Protect Extended Edition.

El soporte para NDMP requiere el hardware y software siguiente:

- IBM Spectrum Protect Edición ampliada
- Unidad de cintas y biblioteca de cintas. Para conocer las combinaciones admitidas, consulte: Información del producto

Requisitos de instalación de copia de seguridad y archivado de datos de cliente de Tivoli Storage Manager FastBack

Antes de poder realizar una copia de seguridad o archivado de los datos del cliente de FastBack, tiene que instalar el software necesario.

Debe instalar el siguiente software:

- Tivoli Storage Manager FastBack Versión 6.1
- Cliente de Tivoli Storage Manager V6.1.3.x (donde x es 1 o superior) o V6.2 o posterior
- Servidor de Tivoli Storage Manager V6.1.3 o superior
- Tivoli Storage Manager Administration Center V6.1.3
 - Solo es necesario si quiere utilizar Tivoli Storage Manager FastBack integrado - administración.

A partir de la versión 7.1, el componente del Centro de administración ya no se distribuye con Tivoli Storage Manager o IBM Spectrum Protect. Los usuarios de FastBack que tengan un Centro de administración de una versión de servidor anterior pueden seguir utilizándolo para crear y modificar planificaciones de FastBack. Si no tiene instalado el Centro de administración, puede descargar la versión anterior de <http://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/admincenter/v6r3/>. Si no tiene instalado el Centro de administración, tiene que crear y modificar las planificaciones de FastBack en el servidor de IBM Spectrum Protect. Para obtener información sobre la creación de planificaciones en el servidor, consulte la documentación del servidor IBM Spectrum Protect.

El entorno de Tivoli Storage Manager FastBack debe estar en ejecución. Para obtener información sobre cómo instalar y configurar Tivoli Storage Manager FastBack, consulte la información sobre el producto en Tivoli Storage Manager FastBack.

Para obtener información sobre cómo integrar IBM Spectrum Protect y Tivoli Storage Manager FastBack, consulte Integración de Tivoli Storage Manager FastBack y IBM Spectrum Protect.

Podrá instalar el cliente de IBM Spectrum Protect de una de estas maneras:

- Instale el cliente de copia de seguridad y archivado en una estación de trabajo que tenga instalado FastBack Disaster Recovery Hub. En este caso, los requisitos previos son: configuración de FastBack Disaster Recovery Hub y shell de FastBack.
- Instale el cliente de copia de seguridad y archivado en una estación de trabajo que no tenga instalado el servidor de FastBack ni FastBack Disaster Recovery Hub. En este caso, el shell de FastBack sigue siendo necesario.

Conceptos relacionados:

“Configuración del cliente para realizar una copia de seguridad y archivado de los datos de Tivoli Storage Manager FastBack” en la página 102

Instalar los clientes de archivado y copia de seguridad UNIX y Linux

En este apartado se proporcionan instrucciones para instalar y configurar clientes de IBM Spectrum Protect UNIX y Linux.

Nota: Debe iniciar la sesión como usuario root para instalar el cliente de copia de seguridad y archivado en una estación de trabajo UNIX o Linux.

Aquí figuran los clientes de UNIX y Linux soportados y la ubicación de las instrucciones de instalación de cada cliente.

- “Instalación del cliente AIX”
- “Instalación de la API de HP-UX Itanium 2” en la página 16
- “Instalación del cliente de copia de seguridad y archivado en Linux on Power Systems (Little Endian)” en la página 19
- “Instalación de la API del cliente de copia de seguridad y archivado en Ubuntu Linux on Power Systems (Little Endian)” en la página 22
- “Instalación de la API en Linux on Power Systems (Big Endian)” en la página 24
- “Instalación del cliente Linux x86_64” en la página 28
- “Instalación del cliente Ubuntu Linux x86_64” en la página 33
- “Instalación del cliente Linux on System z” en la página 37
- “Instalación del cliente Mac OS X” en la página 42
- “Instalación del cliente Oracle Solaris” en la página 44

Conceptos relacionados:

Capítulo 2, “Configurar el cliente de IBM Spectrum Protect”, en la página 49

Instalación del cliente AIX

Puede instalar el cliente de archivado y copia de seguridad de AIX desde el soporte de instalación del producto.

Acerca de esta tarea

En IBM Spectrum Protect Versión 8.1.0 se facilita una versión de 64 bits del cliente AIX en las bibliotecas de distribución. No puede actualizar un cliente AIX de 32 bits previamente instalado al nuevo cliente AIX de 64 bits. Si tiene un cliente de 32 bits instalado desde una versión anterior de IBM Spectrum Protect, puede utilizar SMIT para llevar a cabo las siguientes tareas:

1. Desinstale el cliente de 32 bits (tivoli.tsm.client.ba).
2. Desinstale todos los archivos de idioma nacional que se hayan instalado anteriormente.
3. Desinstale la API (tivoli.tsm.client.api.32bit).

A continuación, utilice SMIT para instalar los siguientes paquetes en las bibliotecas de distribución de IBM Spectrum Protect V8.1.0, siguiendo el orden indicado:

1. Instale la API de 64 bits (tivoli.tsm.client.api.64bit).
2. Instale el cliente de 64 bits (tivoli.tsm.client.ba.64bit).

Si ya tiene instalado el cliente IBM Spectrum Protect V6.3 de 64 bits (o más nuevo), puede actualizar el cliente en vez de desinstalarlo y volver a instalarlo.

Si tiene un cliente de 64 bits de una versión anterior de IBM Spectrum Protect instalado (por ejemplo, versión 6.1 o V6.2) debe desinstalar el cliente, los paquetes de idiomas y la API. A continuación, instale la API y el cliente de IBM Spectrum Protect nuevos.

Todos los paquetes necesarios para instalar el cliente se incluyen en el paquete del cliente AIX y se grabarán encima de cualquier aplicación en tiempo de ejecución anterior del sistema durante la instalación. Se requiere el LibC (C Set ++) en tiempo de ejecución.

Cuando utilice el mandato **installp** para instalar este cliente, no cambie los valores de campo predeterminados de las dos opciones siguientes:

- **¿Instalar AUTOMÁTICAMENTE el software de requisito?**
- **¿SOBREGRABAR las mismas versiones o las más recientes?**

La inhabilitación o el cambio de los valores permite a un componente del cliente de nivel inferior instalar sobre un componente de nivel superior instalado actualmente. En tales circunstancias, puede que las llamadas a función entre los componentes de distintos niveles dejen de ser válidas.

Instale los siguientes paquetes. Todos se proporcionan en los medios de instalación. Necesitará la edición ampliada, Extended Edition, para poder utilizar el cliente de NAS.

Los archivos siguientes se listan en orden de dependencia. Por ejemplo, la API depende de Global Security Kit (GSKit). Cuando instale cualquiera de ellos mediante SMIT, puede seleccionarlos (F7) en cualquier orden.

GSKit8.gskcrypt64.ppc.rte y GSKit8.gskssl64.ppc.rte

IBM GSKit de 64 bits (necesario para la API del cliente de 64 bits).

tivoli.tsm.client.api.64bit

Instala la API de 64 bits.

tivoli.tsm.client.ba.64bit

Instala los siguientes archivos del cliente de 64 bits:

- Cliente de archivado y copia de seguridad de Java (GUI)
- Cliente web de archivado y copia de seguridad
- Cliente de copia de seguridad NAS

tivoli.tsm.filepath_aix

Instala la extensión de kernel de vía de acceso de archivo que es necesaria para la copia de seguridad basada en el diario.

tivoli.tsm.client.jbb.64bit

Instala el componente de copia de seguridad con registro por diario.

Cada paquete se instala en el siguiente directorio de instalación predeterminado:

- Los archivos de copia de seguridad-archivado, de cliente web y de cliente administrativo (**dsmadmc**) de 64 bits se instalan en el directorio `/usr/tivoli/tsm/client/ba/bin64`.
- Los archivos de la API de 64 bits de IBM Spectrum Protect se instalan en el directorio `/usr/tivoli/tsm/client/api/bin64`.
- El archivo de opciones del sistema de ejemplo, `dsm.sys.smp`, se ubica en el directorio de instalación.

Este procedimiento de instalación puede utilizarse para instalar nuevas distribuciones o actualizaciones del soporte de instalación descargado. Es posible que los archivos descargados que se utilizan para instalar el cliente estén comprimidos. En función del formato de archivo de paquete, copie o extraiga los archivos en el disco y utilice estas instrucciones para instalar los componentes.

Puede descargar el archivo de paquete correspondiente de uno de los siguientes sitios web:

- Descargue el paquete de cliente de Passport Advantage o de Fix Central.
- Para obtener la información más reciente, actualizaciones y arreglos de mantenimiento, vaya a IBM Support Portal.

Si está copiando primero los archivos de cliente en un directorio local, el mandato **installp** crea automáticamente un archivo a `.toc`. Para crear manualmente un archivo `.toc`, ejecute `/usr/sbin/inutoc` en el directorio local en el que se ha copiado la imagen de IBM Spectrum Protect. En la línea de mandatos de AIX, escriba:

```
/usr/sbin/inutoc /usr/sys/inst.images
```

Se creará un archivo `.toc` en ese directorio.

Procedimiento

1. Inicie la sesión como el usuario root.
2. Monte el volumen desde el que está realizando la instalación.
3. Desde la línea de mandatos de AIX, escriba `smitty install` y pulse Intro.
4. Seleccione **Instalar y actualizar software** y pulse Intro.
5. Seleccione **Instalar y actualizar desde todo el software disponible** y pulse Intro.
6. En el indicador `INPUT device/directory for software`, pulse la tecla F4, especifique el directorio que contiene las imágenes de ilustración y pulse Intro.
7. En el indicador `SOFTWARE a instalar`, pulse la tecla F4. Seleccione los juegos de archivos de IBM Spectrum Protect que desee instalar pulsando la tecla F7. Después, pulse la tecla Intro.
8. En el panel `Instalar y actualizar desde todo el software disponible`, pulse la tecla F4 para cambiar cualquiera de los campos de entrada o bien utilice los campos predeterminados. Pulse Intro dos veces para iniciar la instalación.
9. Cuando finalice la instalación, pulse F10 para salir.

Resultados

Cuando se instalan juegos de archivos, estos se validan automáticamente en el sistema. La versión anterior del software del cliente de copia de seguridad y archivado se sustituye por la versión que acaba de instalarse.

Los archivos del cliente de copia de seguridad y archivado se instalan en el directorio `/usr/tivoli/tsm/client/ba/bin64`. Si traspasa los archivos del cliente a otro directorio, deberá realizar los siguientes pasos:

1. Asegúrese de que no han cambiado los permisos de los archivos instalados.
2. Actualice los vínculos simbólicos para los archivos instalados en los siguientes directorios:
 - El directorio `/usr/bin`
 - El directorio `/usr/lib` para las bibliotecas de IBM Spectrum Protect
3. Asegúrese de que todos los usuarios del cliente de copia de seguridad y archivado definen la variable de entorno `DSM_DIR` en el directorio recién instalado.

Qué hacer a continuación

Una vez finalizada la instalación, consulte el apartado Capítulo 2, “Configurar el cliente de IBM Spectrum Protect”, en la página 49 para obtener información sobre la realización de tareas obligatorias y opcionales antes de utilizar el cliente de copia de seguridad y archivado.

Nota:

- Las particiones de carga de trabajo de AIX (WPAR) están soportadas como sigue:
 - Soportadas en entornos globales
 - Soportadas con las WPAR de sistemas no compartidos
 - Soportadas con las WPAR de sistemas compartidos (los archivos de configuración y los registros del cliente de copia de seguridad y archivado se deben definir en ubicaciones no predeterminadas)
 - Sin soporte para las WPAR de aplicación
 - Sin soporte para copia de seguridad de imágenes
 - Sin soporte para restauración de conjunto de copias de seguridad desde cinta
- En AIX versión 6.1, si va a utilizar sistemas de archivos cifrados (EFS) con el cliente de copia de seguridad y archivado, y si la contraseña del almacén de claves de usuario de EFS difiere de la contraseña de inicio de sesión de usuario, el almacén de claves de EFS no se abrirá automáticamente cuando se inicie una sesión. Si el almacén de claves de EFS no se abre al iniciar sesión, es posible que el cliente no restaure un archivo que no sea EFS en un sistema de archivos EFS. Podrá evitar el problema de restauración del sistema de archivos EFS de una de las siguientes maneras:
 - Inicie el cliente de copia de seguridad y archivado mediante el mandato **`efskeymgr -o`**. Por ejemplo: **`efskeymgr -o ./dsmj`**
 - Sincronice la contraseña de almacén de claves con la contraseña de inicio de sesión utilizando el mandato **`efskeymgr -n`**. Por ejemplo: **`efskeymgr -n`**

Desinstalación del cliente AIX

Utilice los siguientes procedimientos para desinstalar el cliente de copia de seguridad y archivado AIX de IBM Spectrum Protect.

Antes de empezar

Los módulos y los componentes del cliente de IBM Spectrum Protect están estrechamente integrados, y los juegos de archivos instalados se validan automáticamente. No existe la opción de retrotracción de componentes desinstalados.

Procedimiento

1. Escriba el siguiente mandato de AIX: **smitty remove**.
2. Pulse la tecla Intro.
3. En el campo del nombre de **SOFTWARE**, pulse F4 para que se muestre una lista de los juegos de archivos de IBM Spectrum Protect que desea desinstalar; pulse la tecla Intro.
4. Seleccione los juegos de archivos de IBM Spectrum Protect que desea desinstalar; pulse la tecla Intro.

Nota: La característica de copia de seguridad con registro por diario está en dos conjuntos de archivos. Seleccione `tivoli.tsm.client.jbb.64bit` y `tivoli.tsm.filepath_aix`. Si desinstala los conjuntos de archivos de uno en uno, desinstale primero el conjunto de archivos `tivoli.tsm.client.jbb.64bit`.

5. En el campo **PREVIEW only?** (la operación de eliminación no tendrá lugar), seleccione **No**; pulse la tecla Intro.

Instalación de la API de HP-UX Itanium 2

Puede instalar la API de HP-UX Itanium 2 desde el soporte de instalación del producto.

Acerca de esta tarea

Los siguientes paquetes de origen están disponibles en los medios de instalación:

tsmcli/hp11ia64/gskcrypt64-8.x.x.x.hpux.ia64.tar.Z and **tsmcli/hp11ia64/gskssl64-8.x.x.x.hpux.ia64.tar.Z**

Contiene el GSKit. Si tiene una versión anterior de GSKit, desinstálela antes de instalar la nueva versión.

tsmcli/hp11ia64/TIVsmCapi64

En este paquete, el nombre de selección de software utilizado por **swlist** para el nombre de producto de nivel superior es TIVsm64. Bajo TIVsm64 se encuentra el componente TIVsm.CLIENT_API64.

Directorios de instalación predeterminados

A continuación, figuran los directorios predeterminados donde se almacenan determinados archivos como parte de la instalación del cliente:

- Los archivos de la API de IBM Spectrum Protect están instalados en el directorio `/opt/tivoli/tsm/client/api/bin64`.
- El archivo de opciones del sistema de ejemplo, `dsm.sys.smp`, se ubica en el directorio de instalación.

Para eliminar las versiones anteriores del cliente de copia de seguridad y archivado, conéctese como usuario root y escriba el mandato siguiente:

```
/usr/sbin/swremove -x mount_all_filesystems=false -v TIVsm64
```

Si ha instalado idiomas adicionales en un cliente de la Versión 7.1.2 o anterior, ejecute el mandato siguiente para eliminarlos:

```
/usr/sbin/swremove -x mount_all_filesystems=false -v TIVsm64.CLIENT_msg_idioma
```

Sustituya *idioma* por el código de idioma adecuado de la Tabla 11 en la página 17.

Tabla 11. Cliente de HP-UX Itanium 2: códigos de idioma para paquetes de instalación

Idioma	Código de idioma
Chino simplificado	ZH_CN
Chino tradicional	ZH_TW
Checo	CS_CZ
Francés	FR_FR
Alemán	DE_DE
Húngaro	HU_HU
Italiano	IT_IT
Japonés	JA_JP
Coreano	KO_KR
Polaco	PL_PL
Portugués de Brasil	PT_BR
Ruso	RU_RU
Español	ES_ES

Este procedimiento de instalación puede utilizarse para instalar nuevas distribuciones o actualizaciones del soporte de instalación descargado. Es posible que los archivos descargados que se utilizan para instalar el cliente estén comprimidos. En función del formato de archivo de paquete, copie o extraiga los archivos en el disco y utilice estas instrucciones para instalar los componentes.

Puede descargar el archivo de paquete correspondiente de uno de los siguientes sitios web:

- Descargue el paquete de cliente de Passport Advantage o de Fix Central.
- Para obtener la información más reciente, actualizaciones y arreglos de mantenimiento, vaya a IBM Support Portal.

Procedimiento

1. Inicie la sesión como el usuario root.
2. Monte el volumen desde el que está realizando la instalación.
3. Para instalar GSKit: Si tiene instalada una versión anterior de GSKit, elimínela antes de instalar la nueva versión. Extraiga el contenido de gskcrypt64-8.x.x.x.hpux.ia64.tar.Z y gskssl64-8.x.x.x.hpux.ia64.tar.Z en un directorio del disco duro. Escriba los siguientes mandatos para instalar los paquetes:

```
/usr/sbin/swinstall -x mount_all_filesystems=false -v -s `pwd`
/gskcrypt64 gskcrypt64
/usr/sbin/swinstall -x mount_all_filesystems=false -v -s `pwd`
/gskssl64 gskssl64
```

4. Si lo ha descargado del FTP, vaya al directorio donde se encuentra la imagen instalable. Especifique el siguiente mandato:

```
/usr/sbin/swinstall -x mount_all_filesystems=false -v -s
`pwd`/TIVsmCapi64 TIVsm64
```

Puede utilizarse `pwd` en lugar del nombre absoluto del directorio actual.

Conceptos relacionados:

Capítulo 2, “Configurar el cliente de IBM Spectrum Protect”, en la página 49

Aumento del límite predeterminado del tamaño de segmento de datos

El límite predeterminado del tamaño de los segmentos de datos de un proceso en HP-UX 11i v2 es de 64 MB. Si realiza copias de seguridad de grandes sistemas de archivos, es posible que la API supere este límite y se quede sin memoria.

Para aumentar este límite, puede modificar el kernel de la manera siguiente:

1. Como usuario root, inicie **sam**.
2. Seleccione **Kernel Configuration**.
3. Seleccione **Configurable Parameters**.
4. Localice **maxdsize** y aumente su valor mediante la entrada de menú **Actions/Modify Configurable Parameter...** (por ejemplo, establezca **maxdsize** en 268435456 para un tamaño máximo de 256 MB del segmento de datos).
5. Después de este cambio, **sam** vuelve a compilar el kernel. Debe reiniciar el sistema para que el nuevo valor entre en vigor.

Desinstalación de la API de HP-UX Itanium 2

Puede utilizar los procedimientos siguientes para desinstalar la API de IBM Spectrum Protect HP-UX Itanium 2.

Antes de empezar

Importante: Asegúrese de que desinstala los paquetes en el orden que se muestra.

Procedimiento

1. Para eliminar el conjunto de archivos CLIENT_API, escriba el siguiente mandato:

```
/usr/sbin/swremove -x mount_all_filesystems=false -v TIVsm64
```
2. Para eliminar Global Security Kit (GSKit), escriba los siguientes mandatos:

```
/usr/sbin/swremove -x mount_all_filesystems=false gskssl64  
/usr/sbin/swremoveswremove -x mount_all_filesystems=false gskcrypt64
```

Qué hacer a continuación

Después de desinstalar la API de HP-UX, varios directorios vacíos permanecen en el sistema de archivos, por ejemplo los directorios siguientes:

- El directorio de licencia (/opt/tivoli/tsm/license)
- Uno o varios directorios de idioma (/opt/tivoli/tsm/client/ba/bin/xx_XX), donde xx_XX representa uno de los siguientes códigos de idioma: cs_CZ, de_DE, es_ES, it_IT, fr_FR, hu_HU, ja_JP, ko_KR, pl_PL, pt_BR, ru_RU, zh_CN and zh_TW
- /opt/tivoli/tsm/client/ba/bin/cit
- /opt/tivoli/tsm/client/ba/bin/images
- /opt/tivoli/tsm/client/ba/bin/plugin

Si desea eliminar estos directorios vacíos, puede eliminarlos manualmente.

Instalación del cliente de copia de seguridad y archivado en Linux on Power Systems (Little Endian)

Puede instalar el cliente de archivado y copia de seguridad del soporte de instalación del producto.

Antes de empezar

Debe haber iniciado la sesión como usuario root para instalar el producto.

Este procedimiento de instalación puede utilizarse para instalar nuevas distribuciones o actualizaciones del soporte de instalación descargado. Es posible que los archivos descargados que se utilizan para instalar el cliente estén comprimidos. En función del formato de archivo de paquete, copie o extraiga los archivos en el disco y utilice estas instrucciones para instalar los componentes.

Puede descargar el archivo de paquete correspondiente de uno de los siguientes sitios web:

- Descargue el paquete de cliente de Passport Advantage o de Fix Central.
- Para obtener la información más reciente, actualizaciones y arreglos de mantenimiento, vaya a IBM Support Portal.

Acerca de esta tarea

Las siguientes opciones de instalación están disponibles en paquetes no comprimidos en el soporte de instalación.

Tabla 12. Nombres de paquetes, contenido y directorio predeterminado

Nombre del paquete	Contenido	Directorio predeterminado
gskcrypt64-8.x.x.x.linux.ppcle.rpm gskssl64-8.x.x.x.linux.ppcle.rpm	Paquetes de Global Security Kit (GSKit) de 64 bits	/usr/local/ibm/gsk8
TIVsm-API64.ppc64le.rpm	Interfaz de programación de aplicaciones (API), que contiene las bibliotecas compartidas y los ejemplos de la API de IBM Spectrum Protect.	/opt/tivoli/tsm/client/api/bin64

Tabla 12. Nombres de paquetes, contenido y directorio predeterminado (continuación)

Nombre del paquete	Contenido	Directorio predeterminado
TIVsm-BA.ppc64le.rpm	Cliente de archivado y copia de seguridad (línea de mandatos y GUI), cliente administrativo (dsmadm) y el cliente web.	/opt/tivoli/tsm/client/ba/bin Normalmente este directorio es el directorio de instalación predeterminado para muchos archivos de cliente de archivado y copia de seguridad. El archivo de opciones del sistema de ejemplo (dsm.sys.smp) se graba en este directorio. Si no establece la variable de entorno DSM_DIR, el archivo ejecutable dsmc, los archivos de recursos y el archivo dsm.sys se almacenan en este directorio. Si no establece la variable de entorno DSM_CONFIG, el archivo de opciones de usuario de cliente debe estar en este directorio. Si no establece la variable de entorno DSM_LOG, el cliente de copia de seguridad y archivado graba mensajes en los archivos dsmerror.log y dsmsched.log en el directorio de trabajo actual.
TIVsm-filepath- <i>versión</i> - <i>linuxOS</i> .ppc64le.rpm Donde: <i>versión</i> indica la versión de IBM Spectrum Protect y <i>linuxOS</i> indica el sistema operativo Linux en el que está instalando el componente filepath. TIVsm-filepath-source.tar.gz TIVsm-JBB.ppc64le.rpm	Archivos necesarios para las copias de seguridad basadas en diarios.	Los paquetes filepath y TIVsm-JBB solo son necesarios si tiene previsto utilizar copias de seguridad basadas en el diario. Filepath se instala en /opt/filepath El paquete TIVsm-JBB.ppc64le.rpm se instala en /opt/tivoli/tsm/client/ba/bin.

Procedimiento

1. Monte el volumen desde el que vaya a instalar los paquetes.
2. Cambie el directorio en el que se guardan los paquetes de instalación.
3. Instale los paquetes de GSKit de 64 bits. En el ejemplo de mandato siguiente, los caracteres "8.x.x.x" representan la versión de GSKit:
rpm -U gskcrypt64-8.x.x.x.linux.ppc64le.rpm gskssl64-8.x.x.x.linux.ppc64le.rpm
4. Instale la API de IBM Spectrum Protect:
rpm -ivh TIVsm-API64.ppc64le.rpm

Si solo necesita instalar la API, puede detenerse aquí. Los resto de los pasos de este procedimiento describen cómo instalar los componentes de cliente de archivado y copia de seguridad. En los pasos subsiguientes también se describe la instalación de los paquetes que son necesarios si desea ejecutar copias de seguridad basadas en el diario.

5. Instale los componentes de cliente de archivado y copia de seguridad:
rpm -ivh TIVsm-BA.ppc64le.rpm
6. Opcional: Si desea utilizar las copias de seguridad basadas en diarios, instale los paquetes necesarios para el componente de la vía de acceso de archivos y las copias de seguridad basadas en diarios.

- a. Instale el componente de vía de acceso en primer lugar y asegúrese de que instala el paquete de filepath que sea correcto para el sistema operativo en el sistema cliente. Especifique uno de los siguientes nombres de paquetes para el nombre de paquete de filepath:

- TIVsm-filepath-7.1.4-0-rhel7.ppc64le.rpm, para Red Hat Enterprise Linux 7.1.
- TIVsm-filepath-7.1.4-0-sles12.ppc64le.rpm, para SUSE Linux Enterprise Server 12.

Utilice el mandato `ls` para visualizar los nombres de los paquetes de Filepath que se incluyen en este release. A continuación, utilice `rpm -ivh nombre_paquete_Filepath.rpm` para instalar el paquete de Filepath apropiado.

Si los paquetes de vía de acceso de archivo de la distribución no se aplican a la versión de Linux, debe compilar la vía de acceso del código fuente. Extraiga TIVsm-filepath-source.tar.gz y consulte el archivo README para obtener instrucciones de compilación e instalación. El módulo de kernel de Linux Filepath tiene licencia de conformidad con los términos de la "GPL" (GNU General Public License).

- b. Instale el paquete de copia de seguridad basada en el diario:

```
rpm -ivh TIVsm-JBB.ppc64le.rpm
```

Conceptos relacionados:

Capítulo 2, "Configurar el cliente de IBM Spectrum Protect", en la página 49

Desinstalación del cliente de copia de seguridad y archivado en Linux on Power Systems (Little Endian)

Puede desinstalar el IBM Spectrum Protect cliente en Linux on Power Systems (Little Endian).

Antes de empezar

Debe haber iniciado la sesión como usuario root para desinstalar el producto. Debe desinstalar los paquetes en el orden que se muestra, de lo contrario la desinstalación fallará.

Procedimiento

Para desinstalar el cliente de copia de seguridad y archivado, entre los mandatos siguientes para eliminar los paquetes para la copia de seguridad basada en el diario, el componente de vía de acceso de archivo, el cliente de archivado y copia de seguridad, la API y el IBM Global Security Kit (GSKit).

Consejo: El número de versión de los paquetes no es necesario.

1. Para desinstalar sólo los componentes de la copia de seguridad con registro por diario, elimine ambos paquetes (vía de acceso y copia de seguridad con registro por diario). El paquete TIVsm-JBB depende del paquete filepath. Si utiliza dos mandatos `rpm -e` diferentes para desinstalar los componentes de uno en uno, desinstale antes el paquete TIVsm-JBB.

```
rpm -e TIVsm-JBB TIVsm-filepath
```

2. Desinstale el paquete de cliente de archivado y copia de seguridad:

```
rpm -e TIVsm-BA
```

3. Desinstale los productos que dependan de la API, como por ejemplo IBM Spectrum Protect for Databases y IBM Spectrum Protect for Mail. Cualquier

producto dependiente de la API debe desinstalarse antes de desinstalar el paquete de la API. Si desinstala un producto dependiente de la API, tendrá que volver a instalarlo después de instalar una versión más reciente de los paquetes de cliente de archivado y copia de seguridad y de la API. Siga las instrucciones de los productos dependientes de la API para determinar qué necesita realizar para evitar la pérdida de datos al desinstalar y volver a instalar los productos.

4. Desinstale el paquete de la API mediante el mandato siguiente:

```
rpm -e TIVsm-API64
```

5. Desinstale GSKit entrando el mandato siguiente:

```
rpm -e gskcrypt64 gskssl64
```

Tareas relacionadas:

“Instalación del cliente de copia de seguridad y archivado en Linux on Power Systems (Little Endian)” en la página 19

Instalación de la API del cliente de copia de seguridad y archivado en Ubuntu Linux on Power Systems (Little Endian)

Puede instalar el cliente de archivado y copia de seguridad del soporte de instalación del producto.

Antes de empezar

Debe haber iniciado la sesión como usuario root para instalar el producto.

Este procedimiento de instalación puede utilizarse para instalar nuevas distribuciones o actualizaciones del soporte de instalación descargado. Es posible que los archivos descargados que se utilizan para instalar el cliente estén comprimidos. En función del formato de archivo de paquete, copie o extraiga los archivos en el disco y utilice estas instrucciones para instalar los componentes.

Puede descargar el archivo de paquete correspondiente de uno de los siguientes sitios web:

- Descargue el paquete de cliente de Passport Advantage o de Fix Central.
- Para obtener la información más reciente, actualizaciones y arreglos de mantenimiento, vaya a IBM Support Portal.

Acerca de esta tarea

Los siguientes paquetes de instalación están disponibles en el soporte de instalación.

Tabla 13. Nombres de paquetes, contenido y directorio predeterminado

Nombre del paquete	Contenido	Directorio predeterminado
gskcrypt64_8.x.x.x.ppc64el.deb gskssl64_8.x.x.x.ppc64el.deb	Paquetes de Global Security Kit (GSKit) de 64 bits	/usr/local/ibm/gsk8
tivsm-api64.ppc64el.deb	Interfaz de programación de aplicaciones (API), que contiene la biblioteca compartida y los ejemplos de la API de IBM Spectrum Protect.	/opt/tivoli/tsm/client/api/bin64

Tabla 13. Nombres de paquetes, contenido y directorio predeterminado (continuación)

Nombre del paquete	Contenido	Directorio predeterminado
tivsm-ba.ppc64el.deb	Cliente de archivado y copia de seguridad (línea de mandatos y GUI), cliente administrativo (dsmadm) y el cliente web.	<p>/opt/tivoli/tsm/client/ba/bin</p> <p>Normalmente este directorio es el directorio de instalación predeterminado para muchos archivos de cliente de archivado y copia de seguridad. El archivo de opciones del sistema de ejemplo (dsm.sys.smp) se graba en este directorio.</p> <p>Si no establece la variable de entorno DSM_DIR, el archivo ejecutable dsmc, los archivos de recursos y el archivo dsm.sys se almacenan en este directorio.</p> <p>Si no establece la variable de entorno DSM_CONFIG, el archivo de opciones de usuario de cliente debe estar en este directorio.</p> <p>Si no establece la variable de entorno DSM_LOG, el cliente de copia de seguridad y archivado graba mensajes en los archivos dsmerror.log y dsmsched.log en el directorio de trabajo actual.</p>
TIVsm-filepath-source.tar.gz tivsm-jbb.ppc64el.deb	Archivos necesarios para las copias de seguridad basadas en diarios.	<p>El paquete TIVsm-filepath-source.tar.gz se instala en el directorio /opt/filepath.</p> <p>El paquete tivsm-jbb.ppc64el.rpm se instala en el directorio /opt/tivoli/tsm/client/ba/bin.</p>

Procedimiento

1. Monte el volumen desde el que vaya a instalar los paquetes.
2. Cambie el directorio en el que se guardan los paquetes de instalación.
3. Instale los paquetes de GSKit de 64 bits. En el siguiente ejemplo de mandato, los caracteres "8.x.x.x" representan la versión de GSKit:

```
dpkg -i gskcrypt64_8.x.x.x.ppc64el.deb gskssl64_8.x.x.x.ppc64el.deb
```
4. Instale la API de IBM Spectrum Protect:

```
dpkg -i tivsm-api64.ppc64el.deb
```

Si solo necesita instalar la API, puede detenerse aquí. Siga los pasos siguientes para instalar el cliente de copia de seguridad y archivado y los paquetes que se necesitan para ejecutar copias de seguridad basadas en el registro de diario.
5. Instale el cliente de archivado y copia de seguridad:

```
dpkg -i tivsm-ba.ppc64el.deb
```
6. Opcional: Si desea utilizar copias de seguridad con registro por diario, instale los paquetes siguientes:
 - a. Extraiga TIVsm-filepath-source.tar.gz y revise el archivo README para ver instrucciones sobre cómo compilar e instalar el software. El módulo de kernel de Linux Filepath tiene licencia de conformidad con los términos de la "GPL" (GNU General Public License).
 - b. Instale el paquete de copia de seguridad basada en el diario:

```
dpkg -i tivsm-jbb.ppc64el.deb
```

Conceptos relacionados:

Capítulo 2, “Configurar el cliente de IBM Spectrum Protect”, en la página 49

Desinstalación del cliente en Ubuntu Linux on Power Systems (Little Endian)

Puede desinstalar el cliente de copia de seguridad y archivado de IBM Spectrum Protect en Ubuntu Linux on Power Systems (Little Endian).

Antes de empezar

Debe haber iniciado la sesión como usuario root para desinstalar el producto.

Requisito: Debe desinstalar los paquetes en el orden que se muestra, de lo contrario la desinstalación fallará.

Procedimiento

Para desinstalar el cliente de copia de seguridad y archivado, entre los mandatos siguientes para eliminar los paquetes para la copia de seguridad basada en el diario, el cliente de archivado y copia de seguridad, la API e IBM Global Security Kit (GSKit). Las instrucciones para desinstalar el componente Filepath se proporcionan junto con el código fuente de Filepath al obtener el software de IBM.

Consejo: El número de versión de los paquetes no es necesario.

1. Para desinstalar sólo los componentes de la copia de seguridad con registro por diario, elimine tivsm-jbb y los paquetes de la ruta al archivo. El paquete tivsm-jbb depende del paquete Filepath. Primero desinstale el paquete tivsm-jbb.
 - a. `dpkg -r tivsm-jbb`
 - b. `dpkg -r TIVsm-filepath`
2. Desinstale el paquete de cliente de archivado y copia de seguridad:
`dpkg -r tivsm-ba`
3. Desinstale los productos que dependan de la API, como por ejemplo IBM Spectrum Protect for Databases y IBM Spectrum Protect for Mail.
Si desinstala un producto dependiente de la API, tendrá que volver a instalarlo después de instalar una versión más reciente de los paquetes de cliente de archivado y copia de seguridad y de la API. Siga las instrucciones de los productos dependientes de la API para determinar qué necesita realizar para evitar la pérdida de datos al desinstalar y volver a instalar los productos.
4. Desinstale el paquete de API emitiendo el mandato siguiente:
`dpkg -r tivsm-api64`
5. Elimine los paquetes de GSKit:
`dpkg -r gskcrypt64 gskssl64`

Tareas relacionadas:

“Instalación de la API del cliente de copia de seguridad y archivado en Ubuntu Linux on Power Systems (Little Endian)” en la página 22

Instalación de la API en Linux on Power Systems (Big Endian)

Puede instalar la API de IBM Spectrum Protect desde el soporte de instalación del producto.

Antes de empezar

Debe haber iniciado la sesión como usuario root para instalar el producto.

Acerca de esta tarea

Si tiene IBM Spectrum Protect versión 6.2 (o una versión anterior) instalada, elimínela (**rpm -e**) y cualquier otro programa de software dependiente antes de instalar una versión más reciente.

Si tiene IBM Spectrum Protect versión 6.3 (o más reciente) instalado, puede utilizar la opción de actualización rpm (**rpm -U**) o la opción de renovación rpm (**rpm -F**) para actualizar el software existente a una versión más reciente. El mandato **rpm -U** se puede utilizar para instalar nuevos paquetes o actualizar paquetes existentes; **rpm -F** sólo puede actualizar paquetes que ya estén instalados.

Detenga los procesos del cliente en ejecución antes de desinstalar o actualizar la API o el cliente de archivado y copia de seguridad de IBM Spectrum Protect. Si está ejecutando un cliente de la Versión 7.1.2 o anterior, debe desinstalar los paquetes de idioma antes de continuar con la actualización.

Tabla 14 muestra las opciones de instalación disponibles en paquetes no comprimidos del soporte de instalación.

Tabla 14. Nombres de paquetes, contenido y directorio predeterminado

Nombre del paquete	Contenido	Directorio predeterminado
gskcrypt64-8.x.x.x.linux.ppc.rpm gskssl64-8.x.x.x.linux.ppc.rpm	Paquetes de Global Security Kit (GSKit) de 64 bits	/usr/local/ibm/gsk8
TIVsm-API64.ppc64.rpm	Interfaz de programación de aplicaciones (API), que contiene las bibliotecas compartidas de la API de IBM Spectrum Protect y ejemplos.	/opt/tivoli/tsm/client/api/bin64

Tabla 14. Nombres de paquetes, contenido y directorio predeterminado (continuación)

Nombre del paquete	Contenido	Directorio predeterminado
TIVsm-APIcit.ppc64.rpm	Opcional. Estos archivos proporcionan los componentes de Common Inventory Technology que puede utilizar para obtener información acerca del número de dispositivos de número de clientes y servidores conectados al sistema, y la utilización de las unidades de valor de procesador (PVU) mediante los dispositivos del servidor. Para obtener más información sobre las PVU, consulte Estimación de las unidades de valor de procesador en la documentación del servidor de IBM Spectrum Protect.	APIcit está instalado en tivoli/tsm/client/api/bin64/cit/

Este procedimiento de instalación puede utilizarse para instalar nuevas distribuciones o actualizaciones del soporte de instalación descargado. Es posible que los archivos descargados que se utilizan para instalar el cliente estén comprimidos. En función del formato de archivo de paquete, copie o extraiga los archivos en el disco y utilice estas instrucciones para instalar los componentes.

Puede descargar el archivo de paquete correspondiente de uno de los siguientes sitios web:

- Descargue el paquete de cliente de Passport Advantage o de Fix Central.
- Para obtener la información más reciente, actualizaciones y arreglos de mantenimiento, vaya a IBM Support Portal.

Procedimiento

1. Monte el volumen desde el que está realizando la instalación.
2. Cambie el directorio en el que se guardan los paquetes de instalación.
3. Instale los paquetes de GSKit de 64 bits. En este ejemplo, los caracteres "8.x.x.x" representan la versión de GSKit:

```
rpm -U gskcrypt64-8.x.x.x.linux.ppc.rpm gskssl64-8.x.x.x.linux.ppc.rpm
```
4. Instale la API de IBM Spectrum Protect y opcionalmente instale el paquete de Common Inventory Technology que se necesita para soportar los cálculos de PVU (processor value unit - value unit de procesador).
 - a. Necesario: Instale la API:

```
rpm -i TIVsm-API64.ppc64.rpm
```

- b. Opcional: Instale el paquete de Common Inventory Technology que utiliza la API. Este paquete depende de la API, por lo que debe instalarse una vez que se instale el paquete de la API.

```
rpm -i TIVsm-APIcit.ppc64.rpm
```

Conceptos relacionados:

Capítulo 2, “Configurar el cliente de IBM Spectrum Protect”, en la página 49

Desinstalación de la API en Linux on Power Systems (Big Endian)

Puede desinstalar la API de IBM Spectrum Protect en IBM Spectrum Protect Linux on Power Systems (Big Endian).

Antes de empezar

Debe haber iniciado sesión como root para desinstalar el producto. Desinstale los paquetes en el orden que se muestra.

Procedimiento

Para desinstalar un paquete de IBM Spectrum Protect previamente instalado, introduzca los mandatos siguientes para eliminar los paquetes de la copia de seguridad basada en el diario, el componente de la vía de acceso, el cliente de archivado y copia de seguridad (si corresponde), la API y el Global Security Kit (GSKit) de IBM.

Consejo: Para la desinstalación no se necesita el número de versión de los paquetes.

1. Complete este paso si se ha instalado previamente una versión 7.1 o anterior del cliente.

Para desinstalar sólo los componentes de la copia de seguridad con registro por diario, elimine ambos paquetes (vía de acceso y copia de seguridad con registro por diario). El paquete TIVsm-JBB depende del paquete filepath. Si utiliza dos mandatos **rpm -e** diferentes para desinstalar los componentes de uno en uno, desinstale antes el paquete TIVsm-JBB.

```
rpm -e TIVsm-JBB TIVsm-filepath
```

2. Si se había instalado previamente una versión 7.1 o anterior del cliente, desinstale los paquetes del cliente de archivado y copia de seguridad.
 - a. si ha instalado el paquete TIVsmBACit opcional, desinstálelo utilizando el siguiente mandato:

```
rpm -e TIVsm-BACit
```
 - b. Desinstale el paquete de cliente de archivado y copia de seguridad:

```
rpm -e TIVsm-BA
```

Nota: Si hay paquetes de idioma instalados en un cliente de la Versión 7.1.2 o anterior, debe eliminarlos antes de eliminar el paquete de API. Escriba el siguiente mandato y sustituya `xx_xx` por el código de idioma para cada idioma adicional que haya instalado. Para obtener una lista de identificadores de códigos de idioma, consulte Tabla 15 en la página 28.

```
rpm -e TIVsm-BA.msg.xx_xx
```

Tabla 15. Identificadores del paquete de idioma

Idioma	Identificador de idioma
Checo	CS_CZ
Francés	FR_FR
Alemán	DE_DE
Húngaro	HU_HU
Italiano	IT_IT
Japonés	JA_JP
Coreano	KO_KR
Polaco	PL_PL
Portugués	PT_BR
Ruso	RU_RU
Español	ES_ES
Chino tradicional (EUC)	ZH_CN
Chino tradicional Big5	ZH_TW

- Desinstale los productos que dependan de la API, como por ejemplo IBM Spectrum Protect for Databases y IBM Spectrum Protect for Mail. Cualquier producto dependiente de la API debe desinstalarse antes de desinstalar el paquete de la API. Si desinstala un producto dependiente de la API, tendrá que volver a instalarlo tras instalar una versión más reciente del paquete de la API. Consulte la documentación del producto dependiente para determinar lo que necesita hacer para evitar pérdidas de datos al desinstalar y volver a instalar los productos.
- Si instala el paquete de inventario común de la API opcional (TIVsm-APIcit), utilice el siguiente mandato para desinstalar el paquete:
rpm -e TIVsm-APIcit
- Desinstale el paquete de la API mediante el mandato siguiente:
rpm -e TIVsm-API64
- Desinstale GSKit con el mandato siguiente:
rpm -e gskcrypt64 gskss164

Tareas relacionadas:

“Instalación de la API en Linux on Power Systems (Big Endian)” en la página 24

Instalación del cliente Linux x86_64

Puede instalar el cliente de archivado y copia de seguridad de Linux x86_64 desde el soporte de instalación del producto.

Antes de empezar

- Debe haber iniciado la sesión como root para instalar el producto.
- Si tiene IBM Spectrum Protect versión 6.2 (o una versión anterior) instalada, elimínela (**rpm -e**) y cualquier otro programa de software dependiente antes de instalar una versión más reciente.
- Si tiene IBM Spectrum Protect versión 6.3 (o posterior) instalado, puede utilizar la opción de actualización rpm (**rpm -U**) o la opción de renovación rpm (**rpm -F**) para actualizar el software existente a una versión más reciente. El mandato **rpm -U** se puede utilizar para instalar paquetes nuevos o actualizar paquetes

existentes solo si no ha instalado anteriormente ningún paquete de idioma. El mandato **rpm -F** solo puede actualizar paquetes que ya están instalados.

- Detenga los procesos del cliente en ejecución antes de desinstalar o actualizar la API o el cliente de archivado y copia de seguridad de IBM Spectrum Protect.
- Si se han instalado paquetes de idioma, tiene que desinstalarlos antes de instalar o actualizar la API o el cliente de archivado y copia de seguridad de IBM Spectrum Protect.

Acerca de esta tarea

Las siguientes opciones de instalación están disponibles en paquetes no comprimidos en el soporte de instalación.

Tabla 16. Nombres de paquetes, contenido y directorio predeterminado

Nombre del paquete	Contenido	Directorio predeterminado
gskcrypt64-8.x.x.x.linux.x86_64.rpm gskssl64-8.x.x.x.linux.x86_64.rpm	Paquetes de Global Security Kit (GSKit) de 64 bits	/usr/local/ibm/gsk8
TIVsm-API64.x86_64.rpm	Interfaz de programación de aplicaciones (API), que contiene las bibliotecas compartidas de la API de IBM Spectrum Protect y ejemplos.	/opt/tivoli/tsm/client/api/bin64
TIVsm-BA.x86_64.rpm	Cliente de archivado y copia de seguridad (línea de mandatos y GUI), cliente administrativo (dsmadmc) y el cliente web.	ient/ba/bin Este directorio se considera como el directorio de instalación predeterminado para muchos archivos del cliente de archivado y copia de seguridad. El archivo de opciones del sistema de ejemplo (dsm.sys.smp) se graba en este directorio. Si no se ha establecido la variable de entorno DSM_DIR, el archivo ejecutable dsmc, los archivos de recursos y el archivo dsm.sys se almacenan en este directorio. Si no se ha establecido DSM_CONFIG, el archivo de opciones de usuario del cliente debe estar en este directorio. Si no define DSM_LOG, escribe mensajes en los archivos dsmerror.log y dsmsched.log en el directorio de trabajo actual.

Tabla 16. Nombres de paquetes, contenido y directorio predeterminado (continuación)

Nombre del paquete	Contenido	Directorio predeterminado
TIVsm-APIcit.x86_64.rpm TIVsm-BAcit.x86_64.rpm	Opcional. Estos archivos proporcionan los componentes de Common Inventory Technology que puede utilizar para obtener información acerca del número de dispositivos de número de clientes y servidores conectados al sistema, y la utilización de las unidades de valor de procesador (PVU) mediante los dispositivos del servidor. Para obtener más información sobre las PVU, consulte Estimación de las unidades de valor de procesador en la documentación del servidor de IBM Spectrum Protect.	APIcit está instalado en tivoli/tsm/client/api/bin64/cit/ BAcit está instalado en tivoli/tsm/client/ba/bin/cit/
TIVsm-filepath-source.tar.gz TIVsm-JBB.x86_64.rpm	Los archivos deben ser compatibles con las copias de seguridad basadas en diarios.	Filepath se instala en /opt/filepath JBB se instala en /opt/tivoli/tsm/client/ba/bin
TIVsm_BAhdw.x86_64.rpm	Proporciona soporte para la copia de seguridad incremental de instantáneas para servidores de archivos NetAPP y N-Series.	/opt/tivoli/tsm/client/ba/bin/plugins

Este procedimiento de instalación puede utilizarse para instalar nuevas distribuciones o actualizaciones del soporte de instalación descargado. Es posible que los archivos descargados que se utilizan para instalar el cliente estén comprimidos. En función del formato de archivo de paquete, copie o extraiga los archivos en el disco y utilice estas instrucciones para instalar los componentes.

Puede descargar el archivo de paquete correspondiente de uno de los siguientes sitios web:

- Descargue el paquete de cliente de Passport Advantage o de Fix Central.
- Para obtener la información más reciente, actualizaciones y arreglos de mantenimiento, vaya a IBM Support Portal.

Procedimiento

Para instalar el cliente de copia de seguridad y archivado Linux x86_64, complete los siguientes pasos:

1. Monte el volumen desde el que está realizando la instalación.
2. Cambie el directorio en el que se guardan los paquetes de instalación.
3. Instale los paquetes de GSKit de 64 bits. En este ejemplo, los caracteres "8.x.x.x" representan la versión de GSKit:

```
rpm -U gskcrypt64-8.x.x.x.linux.x86_64.rpm gskssl64-8.x.x.x.linux.x86_64.rpm
```

4. Instale la API de IBM Spectrum Protect y, opcionalmente, instale el paquete de Common Inventory Technology que se necesita para soportar los cálculos de PVU (value unit de procesador).

- a. Necesario: Instale la API:

```
rpm -i TIVsm-API64.x86_64.rpm
```

- b. Opcional: Instale el paquete de Common Inventory Technology que utiliza la API. Este paquete depende de la API, por lo que debe instalarse una vez que se instale el paquete de la API.

```
rpm -i TIVsm-APIcit.x86_64.rpm
```

Si solo necesita instalar la API, puede detenerse aquí. El resto de los pasos de este procedimiento describen cómo instalar los componentes del cliente de archivado y copia de seguridad y un paquete del cliente opcional que sólo es necesario si desea que el cliente envíe métricas de PVU al servidor. En los pasos subsiguientes también se describe la instalación de los paquetes que son necesarios si desea realizar copias de seguridad basadas en el diario.

5. Instale el cliente de archivado y copia de seguridad y, opcionalmente, instale el paquete de Common Inventory Technology que se necesita para soportar los cálculos de PVU (value unit de procesador).

- a. Instale los componentes del cliente de archivado y copia de seguridad.

```
rpm -i TIVsm-BA.x86_64.rpm
```

- b. Opcional: Instale el paquete de tecnología común de inventario que el cliente utiliza para enviar medidas de PVU al servidor. Este paquete depende del paquete del cliente, por lo que debe instalarse una vez que se instale el paquete del cliente.

```
rpm -i TIVsm-BAcit.x86_64.rpm
```

6. Opcional: Si desea utilizar copias de seguridad basadas en el diario, debe compilar e instalar el componente filepath que coincide con el kernel de Linux en el sistema de cliente. Extraiga TIVsm-filepath-source.tar.gz y consulte el archivo README para obtener instrucciones de compilación e instalación. El módulo de kernel filepath de Linux tiene licencia en conformidad con los términos de la "GPL" (General Public License) de GNU.

7. Para instalar la copia de seguridad incremental por diferencia de instantánea para los servidores de archivos de NetApp y N-Series, especifique el siguiente mandato:

```
rpm -i TIVsm-BAhdw.x86_64.rpm
```

Conceptos relacionados:

Capítulo 2, "Configurar el cliente de IBM Spectrum Protect", en la página 49

Desinstalación del cliente Linux x86_64

Utilice el siguiente procedimiento para desinstalar el cliente IBM Spectrum Protect Linux x86_64.

Antes de empezar

Debe haber iniciado sesión como root para desinstalar el producto. Desinstale los paquetes en el orden que se muestra.

Procedimiento

Para desinstalar un paquete de cliente de IBM Spectrum Protect instalado anteriormente, entre los mandatos siguientes para eliminar los paquetes para la copia de seguridad basada en el diario, el componente de vía de acceso de archivo, el cliente de copia de seguridad y archivado, la API y el IBM Global Security Kit (GSKit).

Consejo: Para la desinstalación no se necesita el número de versión de los paquetes.

1. Para desinstalar sólo los componentes de la copia de seguridad con registro por diario, elimine ambos paquetes (vía de acceso y copia de seguridad con registro por diario). El paquete TIVsm-JBB depende del paquete de vía de acceso. Si utiliza dos mandatos **rpm -e** diferentes para desinstalar los componentes de uno en uno, desinstale antes el paquete TIVsm-JBB.

```
rpm -e TIVsm-JBB TIVsm-filepath
```

2. Desinstale los paquetes del cliente de archivado y copia de seguridad:

- a. Si ha instalado el paquete TIVsm-BACit opcional, desinstálelo antes de desinstalar el cliente.

```
rpm -e TIVsm-BACit
```

- b. Desinstale el cliente de archivado y copia de seguridad.

```
rpm -e TIVsm-BA
```

Nota: Si hay paquetes de idioma instalados en un cliente de la Versión 7.1.2 o anterior, debe eliminarlos antes de eliminar el paquete de API. Escriba el siguiente mandato y sustituya *xx_xx* por el código de idioma para cada idioma adicional que haya instalado. Para obtener una lista de identificadores de códigos de idioma, consulte Tabla 17.

```
rpm -e TIVsm-msg.xx_xx
```

Tabla 17. Identificadores del paquete de idioma

Idioma	Identificador de idioma
Checo	CS_CZ
Francés	FR_FR
Alemán	DE_DE
Húngaro	HU_HU
Italiano	IT_IT
Japonés	JA_JP
Coreano	KO_KR
Polaco	PL_PL
Portugués	PT_BR
Ruso	RU_RU
Español	ES_ES
Chino tradicional (EUC)	ZH_CN
Chino tradicional Big5	ZH_TW

3. Desinstale los productos que dependan de la API, como por ejemplo IBM Spectrum Protect for Databases y IBM Spectrum Protect for Mail. Cualquier producto dependiente de la API debe desinstalarse antes de desinstalar el paquete de la API. Si desinstala un producto dependiente de la API, tendrá que

volver a instalarlo después de instalar una versión más reciente de los paquetes de cliente de archivado y copia de seguridad y de la API. Consulte la documentación del producto dependiente para determinar lo que necesita hacer para evitar pérdidas de datos al desinstalar y volver a instalar los productos.

- a. Si ha instalado el paquete de inventario común de la API opcional (TIVsm-APIcit), desinstálelo antes de desinstalar el paquete de la API. Utilice el mandato siguiente para desinstalar el paquete:

```
rpm -e TIVsm-APIcit
```

- b. Desinstale el paquete de la API mediante el mandato siguiente:

```
rpm -e TIVsm-API64
```

4. Para eliminar el paquete de GSKit de 64 bits, escriba el siguiente mandato:

```
rpm -e gskcrypt64 gskssl64
```

Tareas relacionadas:

“Instalación del cliente Linux x86_64” en la página 28

Instalación del cliente Ubuntu Linux x86_64

Puede instalar el cliente de archivado y copia de seguridad de Ubuntu Linux de 64 bits desde el soporte de instalación del producto.

Acerca de esta tarea

Las siguientes opciones de instalación están disponibles en paquetes no comprimidos en el soporte de instalación.

Tabla 18. Nombres de paquetes, contenido y directorio predeterminado

Nombre del paquete	Contenido	Directorio predeterminado
gskcrypt64_8.0-50.40.linux.x86_64.deb gskssl64_8.0-50.40.linux.x86_64.deb	Paquetes de Global Security Kit (GSKit) de 64 bits	/usr/local/ibm/gsk8
tivsm-api64.amd64.deb	Interfaz de programación de aplicaciones (API), que contiene las bibliotecas compartidas de la API de IBM Spectrum Protect y ejemplos.	/opt/tivoli/tsm/client/api/bin64

Tabla 18. Nombres de paquetes, contenido y directorio predeterminado (continuación)

Nombre del paquete	Contenido	Directorio predeterminado
tivsm-ba.amd64.deb	Cliente de archivado y copia de seguridad (línea de mandatos y GUI), cliente administrativo (dsmadm) y el cliente web.	<p>/opt/tivoli/tsm/client/ba/bin</p> <p>Este directorio se considera como el directorio de instalación predeterminado para muchos archivos del cliente de archivado y copia de seguridad. El archivo de opciones del sistema de ejemplo (dsm.sys.smp) se graba en este directorio. Si no se ha establecido la variable de entorno DSM_DIR, el archivo ejecutable dsmc, los archivos de recursos y el archivo dsm.sys se almacenan en este directorio.</p> <p>Si no se ha establecido DSM_CONFIG, el archivo de opciones de usuario del cliente debe estar en este directorio.</p> <p>Si no define DSM_LOG, escribe mensajes en los archivos dsmerror.log y dsmsched.log en el directorio de trabajo actual.</p>
tivsm-apicit.amd64.deb tivsm-bacit.amd64.deb	Opcional. Estos archivos proporcionan los componentes de Common Inventory Technology que puede utilizar para obtener información acerca del número de dispositivos de número de clientes y servidores conectados al sistema, y la utilización de las unidades de valor de procesador (PVU) mediante los dispositivos del servidor. Para obtener más información sobre las PVU, consulte Estimación de las unidades de valor de procesador en la documentación del servidor de IBM Spectrum Protect.	<p>APicit está instalado en tivoli/tsm/client/api/bin64/cit/</p> <p>BACit está instalado en tivoli/tsm/client/ba/bin/cit/</p>
tivsm-filepath-source.tar.gz tivsm-jbb.amd64.deb	Los archivos deben ser compatibles con las copias de seguridad basadas en diarios.	<p>Los paquete filepath y tivsm-jbb solo son obligatorios si tiene previsto utilizar copias de seguridad con registro por diario.</p> <p>El paquete tivsm-jbb.x86_64.deb se instala en /opt/tivoli/tsm/client/ba/bin.</p>

Tabla 18. Nombres de paquetes, contenido y directorio predeterminado (continuación)

Nombre del paquete	Contenido	Directorio predeterminado
tivsm-bahdw.amd64.deb	Proporciona soporte para la copia de seguridad incremental de instantáneas para servidores de archivos NetAPP y N-Series.	/opt/tivoli/tsm/client/ba/bin/plugins

Este procedimiento de instalación puede utilizarse para instalar nuevas distribuciones o actualizaciones del soporte de instalación descargado. Es posible que los archivos descargados que se utilizan para instalar el cliente estén comprimidos. En función del formato de archivo de paquete, copie o extraiga los archivos en el disco y utilice estas instrucciones para instalar los componentes.

Puede descargar el archivo de paquete correspondiente de uno de los siguientes sitios web:

- Descargue el paquete de cliente de Passport Advantage o de Fix Central.
- Para obtener la información más reciente, actualizaciones y arreglos de mantenimiento, vaya a IBM Support Portal.

Procedimiento

Para instalar el cliente de copia de seguridad y archivado Ubuntu Linux x86_64, complete los siguientes pasos.

1. Monte el volumen desde el que está realizando la instalación.
2. Cambie el directorio en el que se guardan los paquetes de instalación.
3. Instale los paquetes de GSKit de 64 bits.

```
sudo dpkg -i gskcrypt64_8.0-50.40.linux.x86_64.deb gskssl64_8.0-50.40.linux.x86_64.deb
```
4. Instale la API de IBM Spectrum Protect y, opcionalmente, instale el paquete de Common Inventory Technology que se necesita para soportar los cálculos de PVU (value unit de procesador).
 - a. Necesario: Instale la API:

```
sudo dpkg -i tivsm-api64.amd64.deb
```
 - b. Opcional: Instale el paquete de Common Inventory Technology que utiliza la API. Este paquete depende de la API, por lo que debe instalarse una vez que se instale el paquete de la API.

```
sudo dpkg -i tivsm-apicit.amd64.deb
```

Si solo necesita instalar la API, puede detenerse aquí. El resto de los pasos de este procedimiento describen cómo instalar los componentes del cliente de archivado y copia de seguridad y un paquete del cliente opcional que sólo es necesario si desea que el cliente envíe métricas de PVU al servidor. En los pasos subsiguientes también se describe la instalación de los paquetes que son necesarios si desea realizar copias de seguridad basadas en el diario.
5. Instale el cliente de archivado y copia de seguridad y, opcionalmente, instale el paquete de Common Inventory Technology que se necesita para soportar los cálculos de PVU (value unit de procesador).
 - a. Instale los componentes del cliente de archivado y copia de seguridad.

```
sudo dpkg -i tivsm-ba.amd64.deb
```

- b. Opcional: Instale el paquete de tecnología común de inventario que el cliente utiliza para enviar medidas de PVU al servidor. Este paquete depende del paquete del cliente, por lo que debe instalarse una vez que se instale el paquete del cliente.
`sudo dpkg -i tivsm-bacit.amd64.deb`
- 6. Opcional: Realice este paso solo si piensa utilizar copias de seguridad basadas en el diario.
 - a. Extraiga `tivsm-filepath-source.tar.gz` y consulte el archivo README para obtener instrucciones de compilación e instalación. El módulo de kernel de Filepath tiene licencia de conformidad con los términos de la "GPL" (GNU General Public License).
 - b. Instale el paquete de copia de seguridad con registro por diario: `dpkg -i tivsm-jbb.amd64.deb`.
- 7. Para instalar la copia de seguridad incremental por diferencia de instantánea para los servidores de archivos de NetApp y N-Series, especifique el siguiente mandato:
`sudo dpkg -i tivsm-bahdw.amd64.deb`

Conceptos relacionados:

Capítulo 2, "Configurar el cliente de IBM Spectrum Protect", en la página 49

Desinstalación del cliente Ubuntu Linux x86_64

Puede utilizar el siguiente procedimiento para desinstalar el cliente de IBM Spectrum Protect Ubuntu Linux de 64 bits.

Procedimiento

Para desinstalar un paquete de cliente de IBM Spectrum Protect instalado anteriormente, entre los mandatos siguientes para eliminar los paquetes para la copia de seguridad basada en el diario, el cliente de archivado y copia de seguridad, la API y el IBM Global Security Kit (GSKit). Las instrucciones para desinstalar el componente Filepath se proporcionan junto con el código fuente de Filepath al obtener el software de IBM.

1. Para desinstalar sólo los componentes de la copia de seguridad con registro por diario, elimine el componente `tivsm-jbb` y el componente Filepath. El paquete `tivsm-jbb` depende del paquete Filepath. Primero desinstale el paquete `tivsm-jbb`.
 - a. `sudo dpkg -r tivsm-jbb`
 - b. `sudo dpkg -r tivsm-filepath`
2. Desinstale los paquetes del cliente de archivado y copia de seguridad:
 - a. Si ha instalado el paquete `tivsm-bacit` opcional, desinstálelo antes de desinstalar el cliente.
`sudo dpkg -r tivsm-bacit`
 - b. Desinstale el cliente de archivado y copia de seguridad.
`sudo dpkg -r tivsm-ba`

Nota: Si hay paquetes de idioma instalados en un cliente de la Versión 7.1.2 o anterior, debe eliminarlos antes de eliminar el paquete de API. Escriba el siguiente mandato y sustituya `xx-xx` por el código de idioma para cada idioma adicional que haya instalado. Para obtener una lista de identificadores de códigos de idioma, consulte Tabla 19 en la página 37.

`dpkg -r tivsm-msg.xx-xx`

Tabla 19. Identificadores del paquete de idioma

Idioma	Identificador de idioma
Checo	cs-cz
Francés	fr-fr
Alemán	de-de
Húngaro	hu-hu
Italiano	it-it
Japonés	ja-jp
Coreano	ko-kr
Polaco	pl-pl
Portugués	pt-br
Ruso	ru-ru
Español	es-es
Chino tradicional (EUC)	zh-cn
Chino tradicional Big5	zh-tw

3. Desinstale los productos que dependan de la API, como por ejemplo los productos de IBM Spectrum Protect Data Protection. Cualquier producto dependiente de la API debe desinstalarse antes de desinstalar el paquete de la API. Si desinstala un producto dependiente de la API, tendrá que volver a instalarlo después de instalar una versión más reciente de los paquetes de cliente de archivado y copia de seguridad y de la API. Consulte la documentación del producto dependiente para determinar lo que necesita hacer para evitar pérdidas de datos al desinstalar y volver a instalar los productos.
 - a. Si ha instalado el paquete de inventario común de la API opcional (tivsm-apicit), desinstálelo antes de desinstalar el paquete de la API. Utilice el mandato siguiente para desinstalar el paquete:


```
sudo dpkg -r tivsm-apicit
```
 - b. Desinstale el paquete de la API mediante el mandato siguiente:


```
sudo dpkg -r tivsm-api64
```
4. Para eliminar los paquetes de GSKit de 64 bits, escriba el siguiente mandato:


```
sudo dpkg -r gskcrypt64 gskssl64
```

Tareas relacionadas:

“Instalación del cliente Ubuntu Linux x86_64” en la página 33

Instalación del cliente Linux on System z

Puede instalar el cliente de archivado y copia de seguridad de Linux on System z desde el soporte de instalación del producto.

Antes de empezar

Debe haber iniciado la sesión como root para instalar el producto.

Acerca de esta tarea

Si tiene IBM Spectrum Protect versión 6.2 (o una versión anterior) instalada, elimínela (**rpm -e**) y cualquier otro programa de software dependiente antes de instalar una versión más reciente.

Si tiene IBM Spectrum Protect versión 6.3 (o más reciente) instalado, puede utilizar la opción de actualización rpm (**rpm -U**) o la opción de renovación rpm (**rpm -F**) para actualizar el software existente a una versión más reciente. El mandato **rpm -U** se puede utilizar para instalar nuevos paquetes o actualizar paquetes existentes; **rpm -F** sólo puede actualizar paquetes que ya estén instalados.

Detenga los procesos del cliente en ejecución antes de desinstalar o actualizar la API o el cliente de archivado y copia de seguridad de IBM Spectrum Protect. Si está ejecutando un cliente de la Versión 7.1.2 o anterior, debe desinstalar los paquetes de idioma antes de continuar con la actualización.

Las siguientes opciones de instalación están disponibles en paquetes no comprimidos en el soporte de instalación.

Tabla 20. Nombres de paquetes, contenido y directorio predeterminado

Nombre del paquete	Contenido	Directorio predeterminado
gskcrypt64-8.x.x.x.linux.s390x.rpm gskssl64-8.x.x.x.linux.s390x.rpm	Paquetes de Global Security Kit (GSKit) de 64 bits	/usr/local/ibm/gsk8
TIVsm-API64.s390x.rpm	Interfaz de programación de aplicaciones (API), que contiene las bibliotecas compartidas de la API de IBM Spectrum Protect y ejemplos.	/opt/tivoli/tsm/client/api/bin64
TIVsm-BA.s390x.rpm	Cliente de archivado y copia de seguridad (línea de mandatos y GUI), cliente administrativo (dsmadm) y el cliente web.	/opt/tivoli/tsm/client/ba Este directorio se considera como el directorio de instalación predeterminado para muchos archivos del cliente de archivado y copia de seguridad. El archivo de opciones del sistema de ejemplo (dsm.sys.smp) se graba en este directorio. Si no se ha establecido la variable de entorno DSM_DIR, el archivo ejecutable dsmc, los archivos de recursos y el archivo dsm.sys se almacenan en este directorio. Si no se ha establecido DSM_CONFIG, el archivo de opciones de usuario del cliente debe estar en este directorio. Si no define DSM_LOG, el cliente de copia de seguridad y archivado escribe mensajes en los archivos dsmerror.log y dsmsched.log en el directorio de trabajo actual.

Tabla 20. Nombres de paquetes, contenido y directorio predeterminado (continuación)

Nombre del paquete	Contenido	Directorio predeterminado
TIVsm-APIcit.s390x.rpm TIVsm-BAcit.s390x.rpm	Opcional. Estos archivos proporcionan los componentes de Common Inventory Technology que puede utilizar para obtener información acerca del número de dispositivos de número de clientes y servidores conectados al sistema, y la utilización de las unidades de valor de procesador (PVU) mediante los dispositivos del servidor. Para obtener más información sobre las PVU, consulte Estimación de las unidades de valor de procesador en la documentación del servidor de IBM Spectrum Protect.	APIcit está instalado en tivoli/tsm/client/api/bin64/cit/ BAcit está instalado en tivoli/tsm/client/ba/bin/cit/
TIVsm-filepath-source.tar.gz TIVsm-JBB.s390x.rpm	Los archivos deben ser compatibles con las copias de seguridad basadas en diarios.	Filepath se instala en /opt/filepath JBB se instala en /opt/tivoli/tsm/client/ba/bin

Este procedimiento de instalación puede utilizarse para instalar nuevas distribuciones o actualizaciones del soporte de instalación descargado. Es posible que los archivos descargados que se utilizan para instalar el cliente estén comprimidos. En función del formato de archivo de paquete, copie o extraiga los archivos en el disco y utilice estas instrucciones para instalar los componentes.

Puede descargar el archivo de paquete correspondiente de uno de los siguientes sitios web:

- Descargue el paquete de cliente de Passport Advantage o de Fix Central.
- Para obtener la información más reciente, actualizaciones y arreglos de mantenimiento, vaya a IBM Support Portal.

Procedimiento

1. Monte el volumen desde el que está realizando la instalación.
2. Cambie el directorio en el que se guardan los paquetes.
3. Instale los paquetes de GSKit de 64 bits. En este ejemplo, los caracteres "8.x.x.x" representan la versión de GSKit:
rpm -U gskcrypt64-8.x.x.x.linux.s390x.rpm gskssl64-8.x.x.x.linux.s390x.rpm
4. Instale la API de IBM Spectrum Protect y opcionalmente instale el paquete de Common Inventory Technology que se necesita para soportar los cálculos de PVU (processor value unit - value unit de procesador).

a. Necesario: Instale la API:

```
rpm -i TIVsm-API64.s390x.rpm
```

b. Opcional: Instale el paquete de Common Inventory Technology que utiliza la API. Este paquete depende de la API, por lo que debe instalarse una vez que se instale el paquete de la API.

```
rpm -i TIVsm-APIcit.s390x.rpm
```

Si solo necesita instalar la API, puede detenerse aquí. El resto de los pasos de este procedimiento describen cómo instalar los componentes del cliente de archivado y copia de seguridad y un paquete del cliente opcional que sólo es necesario si desea que el cliente envíe métricas de PVU al servidor. En los pasos subsiguientes también se describe la instalación de los paquetes que son necesarios si desea realizar copias de seguridad basadas en el diario.

5. Instale el cliente de archivado y copia de seguridad y opcionalmente instale el paquete de Common Inventory Technology que se necesita para soportar los cálculos de PVU (value unit de procesador).

a. Instale los componentes del cliente de archivado y copia de seguridad.

```
rpm -i TIVsm-BA.s390x.rpm
```

b. Opcional: Instale el paquete de tecnología común de inventario que el cliente utiliza para enviar medidas de PVU al servidor. Este paquete depende del paquete del cliente, por lo que debe instalarse una vez que se instale el paquete del cliente.

```
rpm -i TIVsm-BAcit.s390x.rpm
```

6. Opcional: Si desea utilizar copias de seguridad con registro por diario, instale los paquetes necesarios para dar soporte al componente de vía de acceso y a las copias de seguridad basadas en el registro por diario. Instale el componente de vía de acceso en primer lugar y asegúrese de que instala el paquete de filepath que sea correcto para el sistema operativo en el sistema cliente. Especifique uno de los siguientes nombres de paquetes para el nombre de paquete Filepath.

- `TIVsm-filepath-version-rhel64.s390x.rpm`, for Red Hat Enterprise Linux 6.4.
- `TIVsm-filepath-versión-rhel70.s390x.rpm`, para Red Hat Enterprise Linux 7.0.
- `TIVsm-filepath-versión-sles11sp2.s390x.rpm`, para SUSE Linux Enterprise Server 11, SP 2.

Utilice el mandato `ls` para visualizar los nombres de los paquetes de Filepath que se incluyen en este release. A continuación, utilice `rpm -i nombre_paquete_Filepath.rpm` para instalar el paquete de Filepath apropiado.

Si está ejecutando GPFS para Linux en z Systems, debe especificar el nombre de paquete de filepath para Red Hat Enterprise Linux 7.0 o SUSE Linux Enterprise Server 11, SP 2.

Si los paquetes de vía de acceso de archivo de la distribución no se aplican a la versión de Linux, debe compilar la vía de acceso del código fuente. Extraiga `TIVsm-filepath-source.tar.gz` y consulte el archivo README para obtener instrucciones de compilación e instalación. El módulo de kernel de Linux Filepath tiene licencia de conformidad con los términos de la "GPL" (GNU General Public License).

7. Opcional: Si desea utilizar copias de seguridad basadas en el diario, debe compilar e instalar el componente filepath que coincide con el kernel de Linux en el sistema de cliente. Extraiga `TIVsm-filepath-source.tar.gz` y consulte el archivo README para obtener instrucciones de compilación e instalación. El módulo de kernel filepath de Linux tiene licencia en conformidad con los términos de la "GPL" (General Public License) de GNU.

Conceptos relacionados:

Desinstalación del cliente de Linux on System z

Utilice los siguientes procedimientos para desinstalar el cliente de IBM Spectrum Protect Linux on System z.

Antes de empezar

Debe haber iniciado la sesión como root para instalar el producto. Desinstale los paquetes en el orden que se muestra.

Acerca de esta tarea

Para desinstalar un paquete de cliente de IBM Spectrum Protect instalado anteriormente, entre los mandatos siguientes para eliminar los paquetes para la copia de seguridad basada en el diario, el componente de vía de acceso de archivo, el cliente de copia de seguridad y archivado, the backup-archive client, the API, and the IBM Global Security Kit (GSKit).

Consejo: Para la desinstalación no se necesita el número de versión de los paquetes.

Procedimiento

1. Para desinstalar sólo los componentes de la copia de seguridad con registro por diario, elimine ambos paquetes (vía de acceso y copia de seguridad con registro por diario). El paquete TIVsm-JBB depende del paquete filepath. Si utiliza dos mandatos **rpm -e** diferentes para desinstalar los componentes de uno en uno, desinstale antes el paquete TIVsm-JBB.

```
rpm -e TIVsm-JBB TIVsm-filepath
```

2. Desinstale los paquetes del cliente de archivado y copia de seguridad:
 - a. Si ha instalado el paquete TIVsm-BACit opcional, desinstálelo antes de desinstalar el cliente.

```
rpm -e TIVsm-BACit
```
 - b. Desinstale el cliente de archivado y copia de seguridad.

```
rpm -e TIVsm-BA
```

Nota: Si hay paquetes de idioma instalados en un cliente de la Versión 7.1.2 o anterior, debe eliminarlos antes de eliminar el paquete de API. Escriba el siguiente mandato y sustituya *xx_xx* por el código de idioma para cada idioma adicional que haya instalado. Para obtener una lista de identificadores de códigos de idioma, consulte Tabla 21.

```
rpm -e TIVsm-msg.xx_xx
```

Tabla 21. Identificadores del paquete de idioma

Idioma	Identificador de idioma
Checo	CS_CZ
Francés	FR_FR
Alemán	DE_DE
Húngaro	HU_HU
Italiano	IT_IT
Japonés	JA_JP

Tabla 21. Identificadores del paquete de idioma (continuación)

Idioma	Identificador de idioma
Coreano	KO_KR
Polaco	PL_PL
Portugués	PT_BR
Ruso	RU_RU
Español	ES_ES
Chino tradicional (EUC)	ZH_CN
Chino tradicional Big5	ZH_TW

3. Desinstale los productos que dependan de la API, como por ejemplo IBM Spectrum Protect for Databases y IBM Spectrum Protect for Mail. Cualquier producto dependiente de la API debe desinstalarse antes de desinstalar el paquete de la API. Si desinstala un producto dependiente de la API, tendrá que volver a instalarlo después de instalar una versión más reciente de los paquetes de cliente de archivado y copia de seguridad y de la API. Consulte la documentación del producto dependiente para determinar lo que necesita hacer para evitar pérdidas de datos al desinstalar y volver a instalar los productos.
 - a. Si ha instalado el paquete de inventario común de la API opcional (TIVsm-APIcit), desinstálelo antes de desinstalar el paquete de la API. Utilice el mandato siguiente para desinstalar el paquete:

```
rpm -e TIVsm-APIcit
```
 - b. Desinstale el paquete de la API mediante el mandato siguiente:

```
rpm -e TIVsm-API64
```
4. Para eliminar el paquete de GSKit de 64 bits, escriba el siguiente mandato:

```
rpm -e gskcrypt64 gskssl64
```

Tareas relacionadas:

“Instalación del cliente Linux on System z” en la página 37

Instalación del cliente Mac OS X

Puede instalar el cliente de archivado y copia de seguridad Mac OS X de IBM Spectrum Protect desde el soporte de instalación del producto.

Antes de empezar

Debe ser administrador del sistema para instalar el cliente de copia de seguridad y archivado.

Acerca de esta tarea

Este procedimiento de instalación puede utilizarse para instalar nuevas distribuciones o actualizaciones del soporte de instalación descargado. Es posible que los archivos descargados que se utilizan para instalar el cliente estén comprimidos. En función del formato de archivo de paquete, copie o extraiga los archivos en el disco y utilice estas instrucciones para instalar los componentes.

Puede descargar el archivo de paquete correspondiente de uno de los siguientes sitios web:

- Descargue el paquete de cliente de Passport Advantage o de Fix Central.

- Para obtener la información más reciente, actualizaciones y arreglos de mantenimiento, vaya a IBM Support Portal.

Para clientes de MAC OS X, puede utilizar un asistente de instalación que le solicitará información mientras se instala el producto o puede instalar el cliente desde la línea de mandatos. Cuando instala el cliente mediante el procedimiento de instalación de la línea de mandatos, la instalación se ejecuta sin la interacción del cliente. El procedimiento de la línea de mandatos es útil si desea ejecutar el script de instalación en muchos nodos o si debe instalar el software en un sistema que no tiene un monitor.

Procedimiento

Seleccione un método de instalación e instale el cliente. Utilice bien el método del asistente de instalación o instale el cliente desde la línea de mandatos.

Método de instalación	Procedimiento
Asistente de instalación	<ol style="list-style-type: none"> 1. Pulse dos veces el archivo 8.1.0.0-TIV-TSMBAC-Mac.dmg para montar la imagen de disco. 2. Pulse dos veces el icono del paquete de instalación de IBM Spectrum Protect y siga las solicitudes para completar la instalación.
Línea de mandatos	<ol style="list-style-type: none"> 1. Cambie los directorios a la ubicación del instalador de IBM Spectrum Protect. 2. Instale el paquete de instalación personalizada con el siguiente mandato: <pre>/usr/sbin/installer -pkg "/Volumes/IBM Spectrum Protect/ IBM Spectrum Protect.pkg" -target /</pre>

Qué hacer a continuación

Un ejemplo de archivo de opciones de sistema del cliente, denominado dsm.sys.smp, se crea en el directorio de instalación. Puede copiar el archivo y modificarlo para crear el archivo de opciones del sistema del cliente para su nodo. El nombre predeterminado para el archivo de opciones del cliente es dsm.sys.

Después de instalar el cliente, es posible que necesite definir las variables de entorno antes de utilizarlo. Para obtener más información sobre cómo establecer las variables de entorno, consulte “Definir variables de entorno de proceso” en la página 62.

Desinstalación del cliente Mac OS X

Puede desinstalar el cliente de IBM Spectrum Protect Mac OS X si ya no lo necesita.

Antes de empezar

Si el planificador de IBM Spectrum Protect está configurado como elemento de inicio, utilice las herramientas de IBM Spectrum Protect para la función de

administradores, o el script de shell de StopCad.sh para detener y desinstalar el planificador antes de comenzar el procedimiento.

Acerca de esta tarea

Puede utilizar el script de shell para desinstalar el cliente de archivado y copia de seguridad. El nombre del script de shell es `uninstall.sh` y está en el directorio de instalación predeterminado, que es `/Library/Application Support/tivoli/tsm/client/ba/bin`. Utilice el mandato **sudo** para ejecutar el script.

También, puede completar los siguientes pasos en lugar de utilizar el script:

Procedimiento

1. Mueva las siguientes carpetas a la papelera:
 - `/Applications/IBM Spectrum Protect`
 - `/Library/Application Support/tivoli`
2. Elimine los siguientes enlaces simbólicos:
 - `/usr/bin/dsmc`
 - `/usr/bin/dsmtca`
 - `/usr/bin/dsmcad`
 - `/usr/bin/dsmadm`
 - `/usr/bin/dsmtrace`
 - `/usr/bin/dsmagent`
 - `/usr/lib/libxmlutil-6.2.0.dylib`
 - `/usr/lib/libtsm620xerces-cl_6_0.dylib`
3. Opcional: Elimine los archivos de registro y los archivos de opciones si no quiere conservarlos. El proceso de desinstalación los deja en el disco, así que los ajustes se retienen en caso de que vuelva a instalar el producto más tarde. Es posible que el cliente de copia de seguridad y archivado haya creado archivos de registro en estas ubicaciones:
 - a. `/Library/Logs/tivoli`
 - b. `~/Library/Logs/tivoli`Los archivos de opciones del cliente (`dsm.opt` and `dsm.sys`) se encuentran en las siguientes ubicaciones:
 - a. `/Library/Preferences/Tivoli Storage Manager`
 - b. `~/Library/Preferences/Tivoli Storage Manager`

Instalación del cliente Oracle Solaris

Puede instalar el cliente de archivado y copia de seguridad de Oracle Solaris de IBM Spectrum Protect desde el soporte de instalación del producto.

Acerca de esta tarea

Si se ha instalado una versión anterior del cliente de copia de seguridad y archivado, elimínala antes de instalar una versión nueva. Para obtener más información sobre cómo eliminar los paquetes del cliente Solaris anterior, consulte “Desinstalación del cliente Oracle Solaris” en la página 46.

Se utiliza el archivo de administración de la instalación de IBM Spectrum Protect (`tsmadmin`) en lugar del archivo de administración predeterminado (`/var/sadm/install/admin`), de forma que no se le preguntan los valores de `setuid`

ni setgid, ni se le pide permiso de superusuario durante la instalación. Si desea utilizar el archivo de administración predeterminado, quite la opción -a ./tsmadmin de los mandatos que se muestran y responda a las preguntas sobre los valores setuid y setgid, o sobre el permiso de superusuario durante la instalación con Y.

Tabla 22. Nombres y descripciones de los paquetes de instalación

Paquete	Nombre del paquete	Descripción del paquete
IBM Global Security Kit (GSKit) de 64 bits	gsk8cry64.pkg y gsk8ssl64.pkg	Contiene el GSKit de IBM que proporciona cifrado de datos de 64 bits Secure Sockets Layer (SSL) entre el cliente IBM Spectrum Protect y el servidor.
Interfaz de programación de aplicaciones (API) de IBM Spectrum Protect	TIVsmCapi.pkg	Contiene los ejemplos y las bibliotecas compartidas de la API de 64 bits de IBM Spectrum Protect.
Cliente de archivado y copia de seguridad	TIVsmCba.pkg	<p>Contiene los siguientes componentes de 64 bits:</p> <ul style="list-style-type: none"> • Cliente de copia de seguridad/archivado (línea de mandatos y GUI) • Cliente de administración (línea de mandatos) • Cliente Web de copia de seguridad/archivado <p>Nota:</p> <ol style="list-style-type: none"> 1. Como métodos de comunicación, se admiten el protocolo TCP/IP y la memoria compartida. 2. El cliente web es una parte del paquete de cliente de archivado y copia de seguridad y no se puede instalar sin él.

Este procedimiento de instalación puede utilizarse para instalar nuevas distribuciones o actualizaciones del soporte de instalación descargado. Es posible que los archivos descargados que se utilizan para instalar el cliente estén comprimidos. En función del formato de archivo de paquete, copie o extraiga los archivos en el disco y utilice estas instrucciones para instalar los componentes.

Puede descargar el archivo de paquete correspondiente de uno de los siguientes sitios web:

- Descargue el paquete de cliente de Passport Advantage o de Fix Central.
- Para obtener la información más reciente, actualizaciones y arreglos de mantenimiento, vaya a IBM Support Portal.

Instale los paquetes en el orden que se muestra; algunos paquetes dependen de la presencia de otros. Por ejemplo, GSKit es un requisito previo de la API y la API es un requisito previo del paquete del cliente de archivado y copia de seguridad.

Procedimiento

1. Inicie la sesión como el usuario root.
2. Monte el volumen desde el que está realizando la instalación.
3. Cambie el directorio en el que se guardan los paquetes.
4. El GSKit IBM; es un requisito previo del paquete de la API de IBM Spectrum Protect. Instale el GSKit utilizando los siguientes mandatos:

```
pkgadd -n -a ./tsmadmin -d ./gsk8cry64.pkg gsk8cry64
pkgadd -n -a ./tsmadmin -d ./gsk8ssl64.pkg gsk8ssl64
```

Nota: En Solaris 10, estos mandatos instalan el GSKit de 64 bits en la zona global y en todas las zonas no globales en ejecución. Para instalar el cliente sólo en una zona no global esparcida-raíz, GSKit debe instalarse primero en la zona global. En Solaris 11, los paquetes sólo se instalan en la zona en la que se ejecutan estos mandatos.

5. Utilice el mandato siguiente para instalar la API de IBM Spectrum Protect:

```
pkgadd -n -a ./tsmadmin -d ./TIVsmCapi.pkg TIVsmCapi
```

Nota: En Solaris 10, este mandato instala la API de IBM Spectrum Protect de 64 bits en la zona global y en todas las zonas no globales en ejecución. Si desea instalarla sólo en la zona global, utilice el parámetro **-G** del mandato **pkgadd**. En Solaris 11, la API sólo se instala en la zona en la que se ejecuta este mandato.

6. Utilice el siguiente mandato para instalar el cliente de archivado y copia de seguridad:

```
pkgadd -n -a ./tsmadmin -d ./TIVsmCba.pkg TIVsmCba
```

Nota: En Solaris 10, este mandato instala los componentes del cliente de archivado y copia de seguridad en la zona global y en todas las zonas no globales en ejecución. Si desea instalarlos sólo en la zona global, utilice el parámetro **-G** del mandato **pkgadd**. En Solaris 11, los componentes de cliente sólo deben instalarse en la zona en la que se ejecuta este mandato.

Resultados

Importante: Para una zona no global de la raíz de archivos esparcidos de Solaris 10, el sistema de archivos /usr suele montarse como sistema de archivos de sólo lectura (LOFS) desde la zona global, y tienen aplicación las condiciones siguientes:

- Si no se ha instalado el cliente en la zona global, aparecerá un mensaje de aviso al final de la instalación. El mensaje solicitará al administrador global que cree los enlaces necesarios que se suministran como parte de los mensajes de aviso.
- Si ya se ha instalado el cliente en la zona global, no será necesario crear los vínculos. Los enlaces ya están disponibles y hacen referencia a las bibliotecas y archivos ejecutables correctos.

Conceptos relacionados:

Capítulo 2, “Configurar el cliente de IBM Spectrum Protect”, en la página 49

Desinstalación del cliente Oracle Solaris

Puede desinstalar todos los paquetes que están relacionados con el cliente de IBM Spectrum Protect Oracle Solaris, incluidos los componentes línea de mandatos, GUI, GUI web y cliente de administración.

Acerca de esta tarea

Importante: Asegúrese de desinstalar los paquetes en el orden especificado.

Se utiliza el archivo de administración de instalación de IBM Spectrum Protect (tsmadmin) en lugar del archivo de administración predeterminado (/var/sadm/install/admin), para que no se le hagan preguntas sobre el permiso de superusuario, setuid o setgid durante la instalación. Si desea utilizar el archivo de administración predeterminado, elimine la opción -a ./tsmadmin de los mandatos siguientes y haga las preguntas sobre el permiso de superusuario, setuid o setgid durante la instalación con y.

Procedimiento

1. Especifique el mandato siguiente para desinstalar el cliente de archivado y copia de seguridad:

```
pkgrm -n -a ./tsmadmin TIVsmCba
```

Este mandato desinstala todos los componentes del cliente de archivado y copia de seguridad (línea de mandatos, GUI, cliente web y el cliente administrativo). No puede desinstalar componentes individuales de este paquete (por ejemplo, el cliente de línea de mandatos).

Nota: Si se instalan uno o más paquetes de mensajes de idioma en clientes de la Versión 7.1.2 o anteriores, elimínelos antes de eliminar el paquete de API. Entre el mandato siguiente como usuario root:

```
pkgrm -n -a ./tsmadmin TIVsmCICs TIVsmCICe TIVsmCIEs TIVsmCIFr \
                    TIVsmCIHu TIVsmCIIt TIVsmCIJa TIVsmCIKo \
                    TIVsmCIPi TIVsmCIPt TIVsmCIRu TIVsmCISc TIVsmCITc
```

2. Especifique el mandato siguiente para desinstalar la API de IBM Spectrum Protect:

```
pkgrm -n -a ./tsmadmin TIVsmCapi
```

No se puede eliminar la API si está instalado el cliente de copia de seguridad y archivado. Se debe eliminar primero el cliente de archivado y copia de seguridad.

3. Especifique los siguientes mandatos para desinstalar el GSKit:

```
pkgrm -n -a ./tsmadmin gsk8ssl64
pkgrm -n -a ./tsmadmin gsk8cry64
```

Actualizaciones de software

Las actualizaciones de software deben estar disponibles periódicamente mediante IBM para su descarga.

Para obtener la información, las actualizaciones y los arreglos de mantenimiento más recientes, consulte el apartado IBM Support Portal for IBM Spectrum Protect.

Instalación del servicio de gestión de cliente para recopilar información de diagnóstico

Puede instalar los servicios de gestión de clientes de IBM Spectrum Protect para recopilar información de diagnóstico sobre el cliente de archivado y copia de seguridad. El servicio de gestión de cliente hace que la información esté disponible para IBM Spectrum Protect Operations Center, para poder realizar una supervisión básica.

Acerca de esta tarea

Tras instalar el cliente de archivado y copia de seguridad, instale el servicio de gestión de cliente en el mismo equipo, para que el administrador de Servidor de IBM Spectrum Protect puede ver la información de diagnóstico desde el Centro de operaciones.

El servicio de gestión de cliente está disponible para instalarse en sistemas de cliente de archivado y copia de seguridad de Linux.

Para ver instrucciones de instalación y más información sobre el servicio de gestión de cliente, consulte el apartado Recopilación de información de diagnóstico con los servicios de gestión de clientes de IBM Spectrum Protect.

Capítulo 2. Configurar el cliente de IBM Spectrum Protect

Tras instalar el cliente de copia de seguridad y archivado, debe configurarlo antes de empezar a llevar a cabo operaciones.

Si está actualizando el cliente de copia de seguridad y archivado, no es necesario volver a configurar el planificador, el cliente web u otros valores de configuración. Si los archivos dsm.opt y dsm.sys utilizados por la instalación del cliente anterior se encuentran en el directorio de instalación predeterminado, o en el directorio o archivo al que hacen referencia las variables de entorno DSM_CONFIG y DSM_DIR, el cliente accede a estos archivos para obtener información de configuración.

Algunas tareas de configuración son obligatorias mientras que otras son opcionales. Las siguientes tareas de configuración son obligatorias:

- “Creación y modificación del archivo opciones del sistema del cliente” en la página 56
- “Registrar la estación de trabajo en un servidor” en la página 123

Las siguientes tareas de configuración son opcionales:

- “Creación de un archivo de opciones predeterminado de usuario-cliente” en la página 58
- “Creación de un archivo de opciones del usuario cliente personalizado” en la página 60
- “Variables de entorno” en la página 61
- “Configuración del cliente web en sistemas AIX, Linux, Mac y Solaris” en la página 66
- “Configuración del planificador” en la página 66
- “Creación de una lista de inclusión/exclusión” en la página 124
- Configuración de copias de seguridad paralelas de máquinas virtuales VMware. Consulte “Copias de seguridad paralelas de máquinas virtuales” en la página 223

Tareas de usuario root y autorizado del cliente de UNIX y Linux

Un usuario autorizado es cualquier usuario no root con acceso de lectura y escritura a la contraseña almacenada (archivo TSM.PWD) o cualquiera que conozca la contraseña y la indique de forma interactiva. Los usuarios autorizados utilizan la opción passworddir para definir el directorio en el que desean guardar su copia del archivo TSM.PWD.

Tabla 23 muestra las tareas que puede y que no puede realizar el usuario root, los usuarios autorizados y los usuarios no autorizados.

Tabla 23. Tareas de usuarios root, usuarios autorizados y otros usuarios

Tarea	Usuario root	Usuario autorizado	Otros usuarios
Iniciar sesión en un servidor de IBM Spectrum Protect utilizando un servidor LDAP para autenticar las credenciales.	Sí	Sí	No

Tabla 23. Tareas de usuarios root, usuarios autorizados y otros usuarios (continuación)

Tarea	Usuario root	Usuario autorizado	Otros usuarios
Registrar nuevos nodos con el servidor IBM Spectrum Protect (si se ha definido el registro para que se abra en el servidor).	Sí	Sí	Sí, si se utiliza la opción <code>virtualnodename</code> .
Definir o recrear la contraseña de IBM Spectrum Protect para estaciones de trabajo cliente	Sí	Sí	No
Copia seguridad	<p>Sí</p> <p>Nota: El administrador de IBM Spectrum Protect puede especificar una opción en los mandatos Register Node o Update Node para especificar quién tiene permiso para realizar copia de seguridad de datos para un nodo. Definir BACKUPINITiation como root restringe las copias de seguridad de forma que solo los usuarios root o autorizados pueden realizar copias de seguridad de archivos en un nodo. El establecimiento de BACKUPINITiation en all permite a cualquier usuario realizar una copia de seguridad de datos en un nodo. Para obtener información sobre estos mandatos y opciones, consulte la documentación del servidor de IBM Spectrum Protect.</p>	Sí, si dispone de permiso de lectura, independientemente de a quién pertenezca	Sí, si es el propietario del archivo
Restore	Sí, cuando se restaura en la misma ubicación o en una nueva, se conservan los permisos y la propiedad de los archivos	Sí, pero el sistema operativo impide que se grabe en la misma ubicación si el archivo solo tiene permiso de lectura. Cuando se restaura en la misma ubicación, se conservan los permisos y la propiedad de los archivos. Cuando se restaura en una ubicación distinta, se conservan los permisos de los archivos restaurados, pero cambia la propiedad a la del usuario actual.	Sí, si es propietario del archivo o tiene acceso a él; no obstante, el sistema operativo impide que se grabe en la misma ubicación si el archivo solo tiene permiso de lectura. Cuando se restaura en la misma ubicación, se conservan los permisos y la propiedad de los archivos. Cuando se restaura en una ubicación distinta, se conservan los permisos del archivo restaurado, pero cambia la propiedad a la del usuario actual.

Tabla 23. Tareas de usuarios root, usuarios autorizados y otros usuarios (continuación)

Tarea	Usuario root	Usuario autorizado	Otros usuarios
Archive	Sí	Sí, si dispone de permiso de lectura, independientemente de a quién pertenezca	Sí, si dispone de permiso de lectura, independientemente de a quién pertenezca
Realizar una recuperación	Sí. Cuando se recupera en una nueva ubicación o en la misma ubicación, se conservan los permisos y la propiedad de archivos.	Sí. Sin embargo, el sistema operativo impide que se grabe en la misma ubicación si el archivo solo tiene permiso de lectura. La propiedad de todos los objetos recuperados pasa al usuario actual.	Sí, si ha archivado el archivo. Sin embargo, el sistema operativo impide que se grabe en la misma ubicación si el archivo solo tiene permiso de lectura. La propiedad de todos los objetos recuperados pasa al usuario actual.
Planificador cliente	Sí	Sí, si no utiliza el daemon de aceptador de cliente. Tiene que ser usuario root para gestionar el daemon de aceptador de cliente. Los usuarios autorizados no root pueden utilizar el planificador (dsmd sched).	No
Conceder acceso a los archivos del servidor de IBM Spectrum Protect	Sí	Sí	Sí, para archivos que son de su propiedad en el servidor de IBM Spectrum Protect
Suprimir espacios de archivos del servidor de IBM Spectrum Protect	Sí, si el nodo dispone de autorización para suprimir copias de seguridad o archivadas otorgada por el administrador del servidor de IBM Spectrum Protect	Sí, si el nodo dispone de autorización para suprimir copias de seguridad o archivadas otorgada por el administrador del servidor de IBM Spectrum Protect	No

En sistemas Mac OS X, un administrador de sistema es cualquier usuario que tiene permiso para administrar el sistema. Puede comprobar el tipo de su cuenta mediante la herramienta **Preferencias del sistema > Cuentas**. Los administradores del sistema tienen un tipo de cuenta de **Administrador**.

El administrador del sistema es el encargado de configurar el cliente de copia de seguridad y archivado para que los que no son administradores puedan gestionar sus propios datos. Los usuarios que no son administradores (o usuarios no autorizados) cumplen los siguientes criterios:

- No tienen un ID de usuario 0. No son el usuario root.
- Tienen una cuenta de usuario que no se ha configurado como administrador del sistema.

Cuando para completar una tarea se requiere una autorización adicional, debe utilizar la aplicación de autorizaciones para iniciar el cliente de archivado y copia de seguridad. Esto permite que el cliente se ejecute con los privilegios del sistema suficientes para completar la tarea. La tabla a continuación indica las herramientas de autorización que debe utilizar.

Tabla 24. Herramientas de autorización de Mac OS X y aplicaciones de IBM Spectrum Protect asociadas

Herramienta de autorización de Mac OS X	Aplicación de IBM Spectrum Protect asociada
IBM Spectrum Protect para administradores	IBM Spectrum Protect StartCad.sh StopCad.sh
sudo	dsmc

Habilitar usuarios que no son administradores para gestionar sus propios datos

Para permitir que los usuarios que no son administradores utilicen el cliente de copia de seguridad y archivado para gestionar sus propios datos, el administrador del sistema debe seguir varios pasos adicionales a los pasos normales de la configuración.

Además de los pasos normales de la configuración, el administrador del sistema deberá llevar a cabo los pasos siguientes:

1. Definir la opción **passwordaccess generate** en el archivo de opciones del sistema del cliente (`dsm.sys`).
2. Generar la contraseña inicial utilizando una vez el cliente de copia de seguridad y archivado.

Restricción del acceso a IBM Spectrum Protect a un grupo de usuarios

Cuando instala el cliente de archivado y copia de seguridad, cualquier usuario puede utilizar el programa cliente. Puede restringir el acceso de usuarios que no sean administradores (usuarios que no sean root) al cliente creando un grupo de usuarios y permitiendo sólo a los usuarios de dicho grupo que realicen operaciones del cliente de archivado y copia de seguridad.

Antes de empezar

Antes de utilizar este procedimiento, inicie sesión como root y establezca la opción `passwordaccess` del cliente en **generate**. El establecimiento de `passwordaccess` en **generate** almacena la contraseña localmente para que los usuarios del grupo que cree puedan iniciar sesión sin necesidad de conocer la contraseña del nodo.

Con la sesión iniciada como root, cree un grupo de usuario que contenga todos los usuarios (diferentes a root) a los que desee permitir realizar operaciones del cliente de archivado y copia de seguridad. Consulte la documentación del sistema operativo para obtener instrucciones a la hora de crear grupos de usuarios.

Este procedimiento utiliza un grupo de usuarios denominado *baclientusers* como nombre del grupo de usuarios que contiene todas las cuentas que pueden realizar operaciones de archivado y copia de seguridad. Cuando realice este procedimiento en el entorno, especifique un nombre de grupo válido.

Acerca de esta tarea

Realice los pasos siguientes para limitar el acceso a las operaciones de clientes de copia de seguridad y archivado a determinados usuarios.

Procedimiento

1. Cambie la propiedad de `dsmtca` de forma que incluya al grupo `baclientusers`. Escriba `chgrp baclientusers dsmtca`.
2. Establezca el execute (x) bit para el grupo para que nadie del grupo `baclientusers` pueda ejecutar **`dsmtca`**. Escriba `chmod 750 dsmtca`.
3. Establezca el SUID bit para `dsmtca` para que los usuarios del grupo puedan ejecutarlo con privilegios elevados. Escriba `chmod u+s dsmtca`.
4. Compruebe que el grupo tenga el execute bit establecido para el archivo `dsmtca`. Escriba `ls -l dsmtca`.
La salida de `ls -l dsmtca` debe mostrar el conjunto de SUID (s) bit para `dsmtca` en el campo de usuario y el conjunto de execute bit en el campo del grupo.
`-rwsr-x--- 1 root baclientusers 13327961 2011-05-19 08:34 dsmtca`

Resultados

Tras realizar este procedimiento, los usuarios no incluidos en el grupo de usuarios no pueden utilizar el cliente para realizar las operaciones de copia de seguridad o de archivado.

Habilitar el cifrado para usuarios cliente de copia de seguridad y archivado

Si configura el cliente de archivado y copia de seguridad para que cifre los datos durante las operaciones de archivado y copia de seguridad, y si especifica la opción de que se almacene la contraseña de la clave de cifrado (**`encryptkey save`**), de forma predeterminada sólo el usuario `root` y los usuarios autorizados de IBM Spectrum Protect pueden utilizar la contraseña almacenada para cifrar o descifrar archivos. Entre los usuarios autorizados se incluye cualquier usuario no `root` que tenga acceso de lectura y escritura al archivo `TSM.PWD`, donde se guarda la contraseña almacenada, o un usuario que sepa la contraseña y la introduzca de forma interactiva. Dispone de dos opciones para cambiar este comportamiento.

Procedimiento

Puede habilitar el cifrado para todos los usuarios o para un grupo selectivo de usuarios. Elija uno de los métodos siguientes para determinar los usuarios que pueden cifrar y descifrar archivos durante las operaciones de archivado y copia de seguridad.

Método	Descripción
Permitir a todos los usuarios acceder a la contraseña de la clave de cifrado almacenada, que es cómo funcionaba el cifrado en versiones anteriores del cliente de archivado y copia de seguridad (antes de la versión 7.1.2). Elija este método únicamente si todos los usuarios de la máquina cliente son de confianza.	<ol style="list-style-type: none">1. Utilice <code>chmod</code> para establecer los permisos del agente de cifrado (<code>dsmenc</code>) de forma que todos los usuarios puedan ejecutarlo. <code>chmod 755 dsmenc</code>2. Utilice <code>chmod</code> para establecer el SUID bit para <code>dsmenc</code>. <code>chmod +s dsmenc</code>

Método	Descripción
<p>Permitir únicamente a los miembros del grupo de usuarios acceder a la contraseña de la clave de cifrado almacenada y cifrar o descifrar archivos. En la columna de descripción de esta tabla el nombre del grupo es <i>encryptionusers</i>. Este es un nombre arbitrario para este ejemplo; puede especificar cualquier nombre de grupo de usuarios válido. Nota: En las operaciones de restauración o recuperación, los usuarios que sepan la contraseña de la clave de cifrado podrán también descifrar los archivos de los que sean propietarios, especificando la contraseña cuando el sistema se la solicite.</p>	<ol style="list-style-type: none"> 1. Utilice chgrp para cambiar la propiedad de dsmenc e incluir el grupo encryptionusers. chgrp encryptionusers dsmenc 2. Utilice chmod para establecer el execute bit para el grupo, de forma que cualquier miembro del grupo encryptionusers pueda ejecutar dsmenc. chmod 750 dsmenc 3. Utilice chmod para establecer el SUID bit para dsmenc de forma que los usuarios del grupo puedan ejecutarlo con privilegios elevados. chmod u+s dsmenc 4. Compruebe que el grupo tenga el execute bit establecido para el archivo dsmenc. Escriba <code>ls -l dsmenc</code>. La salida de este mandato muestra que se ha establecido el SUID bit (s) para dsmenc en el campo usuario y el execute bit (x) en el campo grupo. -rwsr-x--- 1 root encryptionusers 13327961 2011-05-19 08:34 dsmenc

Descripción general del archivo de opciones de cliente

Las opciones y valores del cliente se establecen (especifican) en un archivo de opciones de cliente. También puede definir opciones del cliente en un *conjunto de opciones de cliente* del servidor. Las opciones del cliente establecidas en un conjunto de opciones de cliente del servidor sustituyen a las opciones del cliente definidas en el archivo de opciones de cliente.

En sistemas AIX, Linux, Mac y Solaris, el archivo de opciones de cliente predeterminado se denomina dsm.opt. Para estos sistemas operativos, dos archivos tienen opciones del cliente de archivado y copia de seguridad:

- El archivo *opciones del usuario-cliente*. El nombre predeterminado para este archivo es dsm.opt. Por abreviar, este archivo se suele llamar *archivo de opciones de cliente*.
- El archivo *opciones sistema-cliente*. El nombre predeterminado para este archivo es dsm.sys. El archivo de opciones del sistema cliente es un archivo modificable donde se define el servidor y el método de comunicación, y proporciona la configuración de las operaciones de copia de seguridad, archivado, gestión del almacenamiento jerárquico y planificación. Por abreviar, este archivo se suele llamar *archivo de opciones del sistema*.

Puede crear varios archivos de opciones de cliente. Si su archivo de opciones de cliente no se llama dsm.opt o si dsm.opt no está en el directorio predeterminado, utilice la opción de cliente OPTFILE para indicar al cliente de archivado y copia de seguridad el archivo del que leer las opciones y parámetros, cuando se inicie el cliente de archivado y copia de seguridad.

No puede cambiar el nombre del archivo de opciones del sistema cliente. Se debe llamar dsm.sys.

Puede utilizar una aplicación de edición de texto para editar directamente el archivo de opciones de cliente. También puede establecer opciones utilizando la GUI del cliente de archivado y copia de seguridad. En la GUI, seleccione **Editar > Preferencias** y utilice el editor de preferencias para establecer las opciones de cliente. Las opciones que establezca en el editor de preferencias se almacenan en el

archivo de opciones de cliente. No todas las opciones del cliente se pueden establecer utilizando el Editor de preferencias.

Restricción: Para Mac OS X, los archivos de opciones usuario-cliente y sistema-cliente deben ser archivos de texto sin formato, con codificación Unicode (UTF-8). De forma predeterminada, TextEdit no guarda los archivos como texto sin formato. Seleccione **Formato > Convertir en texto sin formato** para guardar los archivos como archivos de texto sin formato. Seleccione **Unicode (UTF-8)** en la lista desplegable **Codificación de texto sin formato**. No añada la extensión .txt cuando guarde el archivo.

Puede utilizar el mandato **query options** para visualizar todas o parte de las opciones y sus valores actuales. Este mandato acepta un argumento para poder especificar un subconjunto de opciones. El valor predeterminado consiste en visualizar todas las opciones.

Algunas opciones constan únicamente del nombre de la opción, como por ejemplo verbose y quiet. Puede especificar el nombre de opción completo o su abreviatura. Por ejemplo, puede especificar la opción verbose de alguna de las formas siguientes:

verbose
ve

Siga estas reglas cuando añada opciones a sus archivos de opciones:

- Puede anotar valores de opción añadiendo comentarios al archivo de opciones. Empiece cada comentario con un asterisco (*) como primer carácter de la línea.
- No especifique opciones en una línea que contenga un comentario.
- Podría dar formato a las opciones con espacios o tabulaciones para que sea más sencillo ver las opciones y valores que especifique en el archivo.
- Especifique cada opción en una línea aparte y especifique todos los parámetros para una opción en la misma línea, según se muestra en los ejemplos siguientes:

```
domain /home /mfg /planning /mrketing /mgmt  
domain / /Volumes/fs2 /Volumes/fs2 /Volumes/fs3 /Volumes/fs4
```
- Para establecer una opción en este archivo, especifique el nombre de la opción y uno o varios espacios en blanco, seguidos del valor de la opción.
- Deje uno o más espacios en blanco entre los parámetros.
- La longitud de los nombres de vía de acceso y de archivo en los archivos de opciones de cliente no puede sobrepasar los límites siguientes:
 - En AIX, Mac OS y Solaris, la longitud máxima de un nombre de archivo es de 255 bytes. La longitud máxima combinada del nombre del archivo y del nombre de la vía de acceso es de 1024 caracteres. La representación Unicode de un carácter puede ocupar varios bytes, de modo que el número máximo de caracteres que un nombre de archivo contiene puede variar.
 - En Linux, la longitud máxima para un nombre de archivo es de 255 bytes. La longitud máxima combinada de la vía de acceso y el nombre es de 4096 bytes. Este valor coincide con el de **PATH_MAX** soportado por el sistema operativo. La representación Unicode de un carácter puede ocupar varios bytes, por lo tanto, el número máximo de caracteres de los que consta un nombre de vía de acceso y de archivo puede variar. La limitación es el número de bytes de los componentes de vía de acceso y archivo, que puede corresponder o no a un número de caracteres igual.
 - Para operaciones de archivado o recuperación, la longitud máxima que puede especificar para un nombre de vía de acceso y archivo, es de 1024 bytes.

Si actualiza el archivo de opciones de usuario cliente mientras hay activa una sesión, debe reiniciar la sesión para incorporar los cambios.

Referencia relacionada:

“Optfile” en la página 506

“Query Options” en la página 736

Creación y modificación del archivo opciones del sistema del cliente

El archivo opciones del sistema del cliente es un archivo modificable donde se define el servidor y el método de comunicación, y proporciona la configuración de las operaciones de copia de seguridad, archivado, gestión del almacenamiento jerárquico y planificación.

Acerca de esta tarea

La creación y modificación del archivo de opciones del sistema cliente (dsm.sys) es una tarea obligatoria.

La GUI del cliente de archivado y copia de seguridad ofrece un asistente de configuración que se puede utilizar para crear archivos de configuración básica y probar la conexión con el servidor de IBM Spectrum Protect. El asistente de configuración se inicia automáticamente si los archivos de configuración no se encuentran cuando se inicia la GUI. Si desea modificar los archivos de configuración una vez creados, pulse **Asistente para la configuración** en el menú **Herramientas** de la interfaz gráfica de usuario.

Si no utiliza el asistente para la configuración, podrá crear y modificar el archivo de opciones del cliente de forma manual.

En Mac OS X, copie el archivo dsm.sys.smp en dsm.sys de una de las siguientes ubicaciones. Las ubicaciones predeterminadas están enumeradas en el orden en el que se buscaron.

1. Una ubicación identificada por la variable de entorno DSM_DIR
2. /Library/Application Support/tivoli/tsm/client/ba/bin/
3. /Library/Preferences/Tivoli Storage Manager/

El cliente utiliza el primer archivo de opciones que se encontró. Debe utilizar el nombre dsm.sys para este archivo. El archivo dsm.sys está controlado por el administrador del sistema.

Para sistemas Oracle Solaris, no es necesario copiar dsm.sys.smp en dsm.sys. Los archivos de opciones del cliente (dsm.opt y dsm.sys) se crean automáticamente en /usr/bin, si aún no existen, y se enlazan al directorio de instalación del cliente cuando instala el cliente. Tenga en cuenta que los archivos no se eliminan si desinstala el cliente, por lo que debe reutilizar los valores si actualiza o reinstala el cliente.

Para el resto de las plataformas, como el usuario root, copie el archivo dsm.sys.smp en dsm.sys y edite dicho archivo para configurar sus valores. El cliente buscará dsm.sys en el directorio especificado por la variable de entorno **DSM_DIR** (si está definida y exportada), y en el directorio de instalación.

Importante: Si va a realizar de nuevo la instalación y desea guardar el archivo dsm.sys tal cual está, no copie el archivo dsm.sys.smp en dsm.sys.

Utilice el archivo `dsm.sys` para especificar uno o más servidores con los que desea contactar para obtener servicios y las opciones de comunicación para cada servidor. Este archivo puede incluir opciones de autorización, opciones de proceso de copia de seguridad y archivado y de planificación.

Modifique el archivo `dsm.sys` para que incluya el servidor o los servidores con los que desea establecer contacto. A continuación, se muestra un ejemplo de una stanza de un archivo de opciones del sistema cliente que contiene las opciones necesarias para un servidor con el que desea que se pongan en contacto los usuarios. Puede especificar opciones para más de un servidor:

```
Servername          server_a
COMMMethod          TCPip
TCPPort             1500
TCPServeraddress    node.domain.company.com
```

Importante: Si desea utilizar el cliente web, debe especificar además la opción `passwordaccess=generate` e iniciar sesión con el cliente para guardar la contraseña.

Como valor predeterminado, el nodo cliente contacta con el primer servidor identificado en el archivo `dsm.sys`. Puede especificar un servidor diferente con el que contactar especificando la opción `servername` en el archivo de opciones del usuario cliente (`dsm.opt`) propio o especificando dicha opción con un mandato.

Además puede especificar en el archivo `dsm.sys` un servidor predeterminado y un servidor de migración (si ha instalado el cliente HSM en la estación de trabajo).

El archivo `dsm.sys` puede contener también las siguientes categorías de opciones:

- Opciones de comunicación
- Opciones de proceso de copia de seguridad/archivado
- Opciones de proceso de restauración y recuperación
- Opciones de planificación
- Opciones de autorización
- Opciones de proceso de errores
- Opciones de proceso de transacciones
- Opciones de cliente Web

Puede modificar el archivo `dsm.sys` con uno de los siguientes métodos:

- En la ventana principal de la GUI de Java del cliente, seleccione **Edit > Client Preferences**.
- Utilice el editor de texto que prefiera.

Importante: En Mac OS X, el archivo de opciones del sistema debe ser un archivo de texto sin formato, codificado como Unicode (UTF-8). De forma predeterminada, TextEdit no guarda archivos como texto sin formato. Seleccione **Formato > Texto sin formato** para guardar el archivo de opciones del usuario como archivo de texto sin formato. Defina el **Codificación del texto sin formato**: en Unicode (UTF-8). No añada la extensión `.txt`.

Si actualiza el archivo `dsm.sys` mientras el cliente esté en ejecución, deberá reiniciar la sesión para que los cambios entren en vigor.

Conceptos relacionados:

“Descripción general del archivo de opciones de cliente” en la página 54

Capítulo 10, “Opciones de proceso”, en la página 313

Referencia relacionada:

“Defaultserver” en la página 383

“Passwordaccess” en la página 509

Creación de un archivo de opciones predeterminado de usuario-cliente

Un archivo de opciones usuario-cliente almacena las opciones de procesamiento del cliente de archivado y copia de seguridad. Cuando instala el cliente de archivado y copia de seguridad, el programa de instalación del archivo de copia de seguridad coloca un archivo de opciones de usuario-cliente de ejemplo en el disco. Un usuario root o administrador del sistema puede editar este archivo para crear un archivo de opciones de cliente predeterminado, y hace que el archivo esté accesible a los usuarios de la estación de trabajo que utilicen el cliente de archivado y copia de seguridad. Los usuarios individuales pueden crear y utilizar su propio archivo de opciones de cliente.

Antes de empezar

Para completar este procedimiento, hay que ser root o administrador del sistema.

Acerca de esta tarea

La creación de un archivo de opciones predeterminado de usuario-cliente es una tarea opcional.

De forma predeterminada, el archivo de opciones usuario-cliente se llama `dsm.opt`, y el archivo contiene los tipos de opción de cliente siguientes:

- Opciones de proceso de copia de seguridad/archivado
- Opciones de proceso de restauración y recuperación
- Opciones de planificación
- Opciones de formato
- Opciones de proceso de mandatos
- Opciones de autorización
- Opciones de proceso de errores
- Opciones de proceso de transacciones
- Opciones de cliente Web

Para clientes Mac, el programa de instalación de cliente coloca un archivo de opciones de ejemplo de usuario-cliente llamado `dsm.opt.smp` en `/Libraries/Preferences/Tivoli Storage Manager/`. Este directorio es el mismo directorio en el que el programa de instalación coloca un archivo de opciones sistema-cliente de ejemplo (`dsm.sys.smp`).

Para clientes AIX y Linux, el programa de instalación de cliente coloca un archivo de muestra de opciones de usuario-cliente denominado `dsm.opt.smp` en el directorio de instalación de cliente predeterminado. Este directorio es el mismo directorio en el que el programa de instalación coloca un archivo de opciones sistema-cliente de ejemplo (`dsm.sys.smp`).

Para clientes Solaris de Oracle, el programa de instalación coloca el archivo de opciones usuario-cliente inicial llamado `dsm.opt` en el directorio `/usr/bin`. Este directorio es el mismo directorio en el que el programa de instalación coloca un archivo de opción sistema-cliente de muestra (`dsm.sys`).

Para todos los sistemas operativos de clientes, el procedimiento siguiente le indica cómo editar el archivo de opciones usuario-cliente de ejemplo y guardarlo con el

nombre predeterminado, dsm.opt. Puede guardar el archivo con un nombre o vía de acceso distinto, si así lo prefiere, pero si cambia el nombre de archivo o si lo desplaza del directorio de instalación predeterminado, debe utilizar uno de los métodos siguientes para especificar la vía de acceso y el nombre del archivo de opciones usuario-cliente:

- Establezca la variable de entorno DSM_CONFIG para indicar la vía de acceso y nombre de archivo del archivo de opciones usuario-cliente (dsm.opt). Establezca la variable de entorno DSM_DIR para indicar la vía de acceso y nombre de archivo del archivo de opciones sistema-cliente (dsm.sys). Para obtener más información sobre las variables de entorno, consulte “Definir variables de entorno de proceso” en la página 62.
- Especifique la opción optfile del cliente de archivado y copia de seguridad para especificar la vía de acceso y nombre de archivo del archivo de opciones usuario-cliente.

Nota: Todos los usuarios del nodo deben tener acceso de lectura a la ubicación del disco en la que almacena el archivo de opciones usuario-cliente.

Procedimiento

1. Acceda al directorio que contiene el archivo de opciones usuario-cliente de ejemplo.
2. Copie en archivo a dsm.opt.
3. Añada opciones para su nodo al archivo dsm.opt. Utilice uno de los métodos siguientes para establecer las opciones usuario-cliente:
 - Edite dsm.opt con un editor de texto para añadir las opciones necesarias en el nodo.

Nota: En Mac OS X, el archivo dsm.opt se debe guardar como archivo de texto sin formato y utilizar Unicode (UTF-8) como esquema de codificación. De forma predeterminada, TextEdit no guarda los archivos como texto sin formato. Para guardar dsm.opt, en TextEdit, seleccione **Formato > Crear texto sin formato**. En la lista desplegable **Codificación de texto sin formato**, seleccione **Unicode (UTF-8)**. No añada la extensión .txt al nombre de archivo.

- Establezca las opciones de cliente utilizando el editor de preferencias. En la GUI del cliente de archivado y copia de seguridad, seleccione **Editar > Preferencias del cliente** y seleccione las opciones que quiera configurar. El editor de preferencias actualiza los archivos de configuración de cliente, dsm.opt y dsm.sys si añade, cambia o elimina opciones. Si actualiza el archivo dsm.opt mientras se ejecuta el cliente de archivado y copia de seguridad, debe reiniciar el cliente de archivado y copia de seguridad para que se reconozcan las actualizaciones.

El editor de preferencia utiliza la variable de entorno DSM_DIR para localizar el archivo de opciones (dsm.sys) y la variable de entorno DSM_CONFIG para localizar el archivo de opciones de usuario de cliente (dsm.opt). Si quiere que dsm.opt esté en una ubicación que no sea la predeterminada, establezca DSM_CONFIG antes de iniciar el cliente de archivado y copia de seguridad y luego utilice el editor de preferencia para establecer las opciones. El editor de preferencias consulta al servidor cuáles son las opciones en el servidor pero no cambia el archivo de opciones del servidor.

Conceptos relacionados:

Capítulo 10, “Opciones de proceso”, en la página 313

“Definir variables de entorno de proceso” en la página 62

Tareas relacionadas:

“Creación y modificación del archivo opciones del sistema del cliente” en la página 56

Creación de un archivo de opciones del usuario cliente personalizado

Si desea utilizar opciones diferentes de las especificadas en el archivo predeterminado de opciones del usuario cliente (dsm.opt), puede crear su propio archivo de opciones del usuario cliente.

Acerca de esta tarea

Puede establecer todas las opciones que pueden definirse en el archivo predeterminado de opciones del usuario. La creación de un archivo de opciones del usuario cliente personalizado (dsm.opt) es una tarea opcional. Para crear o modificar un archivo de opciones del usuario cliente, utilice el siguiente método:

Procedimiento

1. Póngase en contacto con el administrador de IBM Spectrum Protect de la estación de trabajo para determinar la ubicación del archivo de opciones del usuario cliente, dsm.opt.smp y para obtener la dirección TCP/IP del servidor de copia de seguridad al que se conectará y el puerto que está a la escucha.
2. Copie dsm.opt.smp en el directorio de inicio como dsm.opt o con un nombre de archivo nuevo de su elección. Almacene el archivo de opciones del usuario cliente en cualquier directorio para el que tenga acceso de grabación.
3. Establezca la variable de entorno DSM_CONFIG para que apunte al nuevo archivo de opciones del usuario cliente.
4. Edite el archivo dsm.opt según proceda para su sistema o utilice el Editor de preferencias seleccionando **Editar > Preferencias del cliente** en la GUI del cliente de copia de seguridad y archivado.

Resultados

Después de haber creado un archivo de opciones, puede realizar los siguientes pasos para editar el archivo de opciones desde la GUI.

1. Abra el menú **Editar** y seleccione **Preferencias del cliente**.
2. Realice los cambios necesarios y pulse en **Aceptar** para guardar estos cambios.

Importante: En Mac OS X, el archivo de opciones del sistema debe ser un archivo de texto sin formato, codificado como Unicode (UTF-8). De forma predeterminada, TextEdit no guarda archivos como texto sin formato. Seleccione **Formato > Texto sin formato** para guardar el archivo de opciones del usuario como archivo de texto sin formato. Defina la selección de la lista desplegable **Codificación del texto sin formato** en Unicode (UTF-8). No añada la extensión .txt.

Conceptos relacionados:

“Variables de entorno” en la página 61

“Descripción general del archivo de opciones de cliente” en la página 54

Variables de entorno

Normalmente, la definición de las variables de entorno es una tarea opcional. Si define las variables, se recomienda que utilice la línea de mandatos.

Definir variables de entorno de idioma

El cliente de copia de seguridad y archivado detecta automáticamente el idioma del entorno regional del sistema y muestra todo el programa en ese idioma.

Por ejemplo, de forma predeterminada un sistema operativo francés mostrará el cliente de copia de seguridad y archivado en francés. Si el cliente de copia de seguridad y archivado no puede cargar el catálogo de mensajes en francés, toma como valor predeterminado el idioma inglés (Estados Unidos). Por ejemplo, si el cliente se ejecuta en una combinación de entorno regional e idioma no admitida, como por ejemplo Francés/Canadá o Español/México, el cliente tomará como valor predeterminado Inglés (Estados Unidos).

Puede utilizar la variable de entorno **LANG** para especificar el idioma para los clientes UNIX y Linux.

Nota: El entorno regional del sistema operativo, el juego de caracteres del terminal y la codificación del juego de caracteres de nombre de archivo deben coincidir para que puedan visualizarse o escribirse correctamente los nombres de archivo.

Para establecer la variable de entorno **LANG** en francés, escriba la sentencia siguiente:

```
export LANG=fr_FR
```

Nota:

- Esta tarea no se aplica a Mac OS X.
- Para visualizar los menús del navegador de ayuda de IBM Spectrum Protect en el entorno regional actual de idioma, asegúrese de que la variable de entorno NLSPATH del archivo /etc/profile contiene la vía de acceso siguiente:

```
NLSPATH=/usr/dt/lib/nls/msg/%L/%N.cat:$NLSPATH
export NLSPATH
```

Si el entorno local del cliente de copia de seguridad y archivado coincide con la codificación de caracteres de los nombres de archivo, la restauración o la copia de seguridad de todos esos archivos se realiza correctamente. Si utiliza un juego de caracteres de un solo byte (SBCS), todos los nombres de archivo serán válidos y el cliente de copia de seguridad/archivado los restaurará o realizará una copia de seguridad de los mismos.

Si utiliza un entorno local DBCS o UTF-8, los nombres de archivo compuestos por caracteres que no sean válidos en estos entornos, no podrán especificarse en la línea de mandatos del cliente de copia de seguridad y archivado. Estos archivos podrán pasarse por alto cuando se ejecute una copia de seguridad en la que se utilice la especificación de comodín ("*"). A continuación, se muestra un ejemplo del mensaje de error que se emite cuando se pasan por alto los archivos:

```
ANS4042E Object name '/testData/en_US_files/file3?'
contains one or more unrecognized characters and is not valid.
```

Si no todos los directorios y archivos se han creado con el mismo entorno regional, ejecute las copias de seguridad programadas en un entorno local de juego de

caracteres de un solo byte. Esta acción asegura que no se omitan archivos porque el nombre de archivo contenga caracteres que no estén definidos en el entorno local actual. Al restaurar los archivos, hágalo en el entorno local que coincida con la codificación de entorno regional del nombre de archivo.

Por ejemplo, los nombres de archivo que consten de caracteres japoneses pueden contener caracteres de varios bytes no válidos si se visualizan en un entorno local chino. No se hará una copia de seguridad de estos archivos y tampoco se mostrarán en la interfaz gráfica de usuario. Si se encuentran estos archivos durante la copia de seguridad, el archivo `dsmerror.log` enumerará los archivos omitidos.

Consejo: Si utiliza la modalidad de planificación de cliente de copia de seguridad/archivado para realizar una copia de seguridad de todo un sistema, establezca la variable de entorno **LANG** en `en_US` (o en otro idioma SBCS) para evitar que no se omita ningún archivo.

Definir variables de entorno de proceso

En determinadas circunstancias deberá establecer variables de entorno para garantizar que las aplicaciones de IBM Spectrum Protect puedan localizar los archivos necesarios para realizar las operaciones del cliente y que las aplicaciones puedan crear archivos de registro que registren los eventos y errores que se produzcan durante operaciones del cliente.

Debe establecer las variables de entorno si se da cualquiera de las circunstancias siguientes:

- Desea invocar el cliente de copia de seguridad y archivado desde un directorio distinto del directorio de instalación del mismo.
- Desea especificar un archivo de opciones diferente para el cliente de copia de seguridad/archivado, el cliente de administración o ambos.
- Si no desea registrar los archivos que se van a grabar en el directorio de instalación predeterminado.

Consejo: También puede especificar un archivo de opciones del cliente alternativo para el cliente de línea de mandatos (no el cliente de administración) mediante la opción `optfile`.

Hay cuatro variables de entorno que puede ajustar que afectan al proceso del cliente de copia de seguridad y archivado:

PATH Incluye el directorio en el que reside el archivo ejecutable para los ejecutables del cliente (`dsmc`, `dsmadm`, `dsmj`).

DSM_DIR

Especifica el directorio en el que residen el archivo ejecutable para los ejecutables del cliente (`dsmc`, `dsmadm`, `dsmj`) los archivos de recursos y el archivo `dsm.sys`. No puede especificar el directorio raíz (`/`) para `DSM_DIR`.

Consulte la sección de instalación relativa a su sistema operativo para obtener la información referente al directorio predeterminado de instalación.

Cuando solicita una copia de seguridad de imagen, una copia de seguridad de archivos basada en instantáneas, una copia de seguridad NAS o una restauración NAS, el cliente utiliza la variable de entorno `DSM_DIR` para localizar la biblioteca de complementos correspondiente. Si no se establece `DSM_DIR`, el cliente busca la biblioteca de complementos en los siguientes directorios:

AIX /usr/tivoli/tsm/client/ba/bin/plugins

Oracle Solaris y todos los clientes Linux

/opt/tivoli/tsm/client/ba/bin/plugins

DSM_CONFIG

Especifica la vía de acceso calificada al completo y el nombre del archivo de opciones de usuario cliente para los usuarios que crean sus propios archivos de opciones personalizados. Si DSM_CONFIG no se ha establecido, o no se utiliza la opción `-optfile` del cliente, se espera que el archivo de opciones del usuario cliente cumpla estos requisitos:

1. El archivo de opciones debe denominarse `dsm.opt`.
2. Para clientes UNIX distintos de Mac OS X, si *no* se ha establecido DSM_DIR, el archivo debe residir en el directorio de instalación predeterminado. Si *sí* se ha establecido DSM_DIR, el directorio deberá residir en el directorio que especifica DSM_DIR.
3. Para Mac OS X, el archivo puede residir en cualquiera de las siguientes ubicaciones. Estos directorios se buscan en orden y se utiliza el primer archivo de opciones. `~/Library Preferences/Tivoli Storage Manager`, `/Library Preferences/Tivoli Storage Manager`, o `/Library/ Application Support/tivoli/tsm/client/ba/bin`.

Consulte la sección de instalación relativa a su sistema operativo para obtener la información referente al directorio predeterminado de instalación.

DSM_LOG

Apunta al directorio en el que desea que residan los archivos de registro de IBM Spectrum Protect. No puede especificar el directorio raíz (`/`) para DSM_LOG. Los archivos de registro contienen información sobre los errores y sucesos que se producen durante el proceso. El cliente crea los registros para ayudar al equipo de soporte técnico a diagnosticar errores graves.

Consulte la sección de instalación relativa a su sistema operativo para obtener la información referente al directorio predeterminado de instalación.

Importante: Establezca la variable de entorno DSM_LOG para asignar el nombre de un directorio donde los permisos de lectura/grabación permitan el acceso de grabación necesario para que el usuario cree y grabe información en el archivo de registro. Así se evitan anomalías en la grabación de anotaciones y terminaciones de procesos. Utilice los mandatos **chmod** o **setacl** para conceder permisos a los archivos de forma que todos los ID de usuario cliente puedan leer y grabar en ellos. Si los nombres de las anotaciones son los nombres predeterminados, bastará con establecer la variable de entorno DSM_LOG para que haga referencia al directorio en el que residen. Cuando el cliente no puede grabar en el archivo de anotaciones, se graba un mensaje de error en `stderr` y en el daemon `syslog`. El daemon `syslog` se debe estar ejecutando y debe estar configurado para procesar mensajes con una prioridad de LOG_ERR para que el mensaje de error aparezca en las anotaciones del sistema. El inicio y la configuración del daemon `syslog` es propio de cada sistema. Utilice el mandato **man syslogd** para obtener información sobre cómo iniciar el daemon `syslog`. Utilice **man syslog.conf** para obtener información sobre cómo configurar el daemon `syslog`.

Nota:

1. Las opciones `errorlogname` y `schedlogname` alteran temporalmente la variable de entorno `DSM_LOG`. Si especifica la opción del cliente `errorlogname`, el archivo se guarda en el directorio especificado por la opción `errorlogname` y no en la ubicación especificada por `DSM_LOG`. Si especifica la opción de cliente `schedlogname`, se graba en el directorio especificado por la opción `schedlogname` y no en la ubicación especificada por `DSM_LOG`.
2. Los archivos de anotaciones no pueden ser vínculos simbólicos. El cliente detecta los enlaces de este tipo, los suprime y, a continuación, sale de la operación. Esta acción evita que el cliente sobrescriba datos protegidos. Las anotaciones afectadas se crean en forma de archivos en una operación posterior.

Para utilizar programa de la GUI Java del cliente de archivado y copia de seguridad, tiene que exportar el directorio en el que haya instalado el archivo binario de Java. Por ejemplo, escriba el siguiente mandato:

```
export PATH=$PATH:java_bin_dir
```

donde: *java_bin_dir* es la vía de acceso del archivo binario de Java ejecutable en su sistema de archivos.

Referencia relacionada:

“Optfile” en la página 506

Definir variables de shell Bourne y Korn

Especifique las variables de entorno del archivo `.profile` (shell Korn) o del archivo `.bash_profile` (shell Bourne) en el directorio `$HOME`.

Lo siguiente es un ejemplo, en el que `/home/davehil/dsm.opt` es la vía de acceso y el nombre del archivo de opciones del usuario cliente y el directorio `/home/davehil` es la ubicación en la que desea almacenar el archivo `dsmerror.log`, el archivo ejecutable, los archivos de recursos y el archivo `dsm.sys`.

```
DSM_DIR=/home/davehil
DSM_CONFIG=/home/davehil/dsm.opt
DSM_LOG=/home/davehil
export DSM_DIR DSM_CONFIG DSM_LOG
```

Definir variables de shell C

En el shell C, agregue las variables `DSM_CONFIG`, `DSM_LOG` y `DSM_DIR` al archivo `.cshrc` del directorio `$HOME`.

Lo siguiente es un ejemplo, en el que `/home/davehil/dsm.opt` es la vía de acceso y el nombre del archivo de opciones del usuario cliente y el directorio `/home/davehil` es la ubicación en la que desea almacenar el archivo `dsmerror.log`, el archivo ejecutable, los archivos de recursos y el archivo `dsm.sys`.

```
setenv DSM_DIR /home/davehil
setenv DSM_CONFIG /home/davehil/dsm.opt
setenv DSM_LOG /home/davehil
```

Definir variables de entorno de la API

Si ha instalado la API de IBM Spectrum Protect, defina las siguientes variables de entorno.

DSMI_DIR

Hace referencia al directorio de instalación. Los archivos `dsmtca` y `dsm.sys` deben residir en el directorio al que apunta `DSMI_DIR`. Esta variable de entorno tiene que estar presente.

DSMI_CONFIG

Nombre completo de vía de acceso del archivo de opciones de usuario de cliente propio (`dsm.opt`).

DSMI_LOG

Vía de acceso para `dsierror.log` (esta vía de acceso no puede ser un enlace simbólico).

Nota: Los usuarios finales de las aplicaciones desarrolladas con la API pueden consultar las instrucciones de instalación de dicha aplicación para conocer los nombres de vía de acceso especiales u obtener directrices para las opciones.

Para obtener más información sobre la API de IBM Spectrum Protect, consulte Desarrollo de soluciones con la interfaz de programación de aplicaciones.

Descripción general de la configuración del cliente web

El cliente web de IBM Spectrum Protect proporciona gestión remota de un nodo de cliente desde un navegador web. Los procedimientos para configurar el cliente web varían según el sistema operativo del nodo de cliente.

Las opciones de cliente de archivado y copia de seguridad se utilizan para configurar los valores del cliente web. Estas opciones incluyen `httpport`, `managedservices`, `webports` y `revokeremoteaccess`.

En nodos de cliente AIX, Linux, Mac y Solaris, las opciones de cliente web se añaden al archivo de opciones `client-systems` (`dsm.sys`).

Para utilizar el cliente web desde la interfaz de IBM Spectrum Protect Operations Center, especifique la dirección del cliente web en el parámetro de la URL de **REGISTER NODE** o el mandato **UPDATE NODE**. La dirección web debe incluir el nombre de DNS o la dirección de IP del nodo, y el número de puerto que utiliza el cliente web. Por ejemplo, `http://node.example.com:1581`. Sustituya este nombre de host de ejemplo por la dirección IP o nombre de host de su nodo de cliente. Cuando acceda al cliente web utilizando un navegador web, especifique la misma sintaxis de URL en la barra de direcciones del explorador.

Todos los mensajes del cliente web se graban en el archivo de registro web, que se llama `dsmwebcl.log`. De forma predeterminada, el archivo `dsmwebcl.log` y el archivo de registro de errores del cliente de archivado y copia de seguridad (`dsmerror.log`) se crean en el directorio de instalación de cliente. Puede utilizar la variable de entorno `DSM_LOG` para sobrescribir las ubicaciones predeterminadas para los registros de errores. Si establece la variable de entorno `DSM_LOG`, no especifique el directorio raíz como la ubicación para los registros de errores. También puede utilizar la opción `errorlogname` del cliente de archivado y copia de seguridad para cambiar la ubicación del archivo de registro de errores. Si se especifica esta opción, sobrescribe el valor de la variable de entorno `DSM_LOG`.

Conceptos relacionados:

“Opciones de cliente Web” en la página 335

Tareas relacionadas:

Configuración del cliente web en sistemas AIX, Linux, Mac y Solaris

Para configurar el cliente web, edite el archivo de opciones del sistema cliente (dsm.sys) para especificar las opciones necesarias y, a continuación, inicie el daemon de aceptador de cliente.

Procedimiento

1. Establezca las opciones siguientes en el archivo dsm.sys: managedservices webclient schedule y passwordaccess generate.
2. Genere la contraseña IBM Spectrum Protect. Especifique dsmc query session. Cuando se le pidan las credenciales, especifique el nombre de usuario y contraseña de IBM Spectrum Protect.
En sistemas Mac OS X, también puede generar la contraseña utilizando la aplicación Herramientas de IBM Spectrum Protect para administradores. En la aplicación seleccione **IBM Spectrum Protect** para iniciar el cliente.
3. Inicie el daemon de aceptación de clientes. Especifique dsmcad.
En Mac OS X, también puede iniciar el daemon de aceptador de cliente con la aplicación Herramientas de IBM Spectrum Protect para administradores. En la aplicación, seleccione **Iniciar el daemon de aceptador de cliente**.
4. Para acceder al cliente web desde un navegador, especifique el nombre de host o dirección IP del nodo de cliente en la barra de direcciones del navegador, seguido del número de puerto del cliente web. El número de puerto predeterminado es 1581. Por ejemplo, para acceder al cliente web en el nodo myserver.example.com, especifique: http://myserver.example.com:1581
Si debe cambiar el número de puerto del cliente web predeterminado, utilice la opción httpport del cliente de archivado y copia de seguridad para asignar un número de puerto distinto.

Qué hacer a continuación

Tras configurar el cliente web, puede utilizar el IBM Spectrum Protect Operations Center o un navegador para hacer copia de seguridad y restaurar, o archivar y recuperar, datos de un nodo.

Conceptos relacionados:

“Opciones de planificación” en la página 330

“Opciones de cliente Web” en la página 335

Tareas relacionadas:

“Inicio de una sesión de cliente web” en la página 147

Referencia relacionada:

“Httpport” en la página 450

“Passwordaccess” en la página 509

Configuración del planificador

El administrador de IBM Spectrum Protect puede planificar el cliente para que realice tareas automáticamente. Para eventos planificados que deben producirse en el cliente, debe configurar el planificador del cliente para comunicarse con el servidor de IBM Spectrum Protect.

Acerca de esta tarea

Por ejemplo, puede hacer copia de seguridad automáticamente al final de cada día o archivar algunos archivos cada viernes. Este procedimiento, que se conoce como planificación central, es un esfuerzo cooperativo entre el servidor y el nodo del cliente. El administrador asocia clientes con una o varias planificaciones que forman parte del dominio de políticas mantenidas en la base de datos del servidor. Cuando el administrador de IBM Spectrum Protect ha definido la planificación central en el servidor, ya puede iniciar el planificador cliente en la estación de trabajo. Después de iniciar el planificador de cliente, ya no es necesario volver a intervenir.

Con el planificador cliente, puede realizar las tareas siguientes:

- Visualizar información sobre las planificaciones disponibles.
- Visualizar información acerca del trabajo que ha completado la planificación.
- Modifique las opciones de planificación en el archivo `dsm.sys`.

La forma más efectiva de gestionar el planificador de cliente es utilizar el servicio de aceptación de clientes. Puede obtener más información acerca de una comparación entre el aceptador de cliente y los servicios del planificador tradicional para gestionar el planificador. También puede aprender a configurar el cliente para que utilice el aceptador de cliente para gestionar el planificador.

Comparación entre servicios del gestionados por el aceptador de cliente y servicios del planificador tradicional

Puede utilizar el servicio del aceptador de cliente o el servicio del planificador tradicionales para gestionar el planificador de IBM Spectrum Protect. Se suministra una comparación de estos métodos.

La siguiente tabla muestra las diferencias entre métodos de los servicios gestionados por el aceptador de cliente y los servicios del planificador tradicional predeterminados.

Tabla 25. Servicios gestionados por el aceptador de cliente frente a servicios del planificador tradicional

Servicios gestionados por el aceptador de cliente	Servicios del planificador tradicional de IBM Spectrum Protect
Se definen utilizando la opción <code>managedservices schedule</code> y se inician con servicios del aceptador de cliente. El daemon de aceptador de cliente se inicia con el mandato dsmcad	Se inician con el mandato dsmc sched .
El servicio del aceptador de cliente inicia y detiene el proceso del planificador según resulta necesario para cada acción planificada.	Permanecen activos, incluso después de finalizar la copia de seguridad planificada.
Requiere menos recursos del sistema cuando está desocupado.	Requieren un mayor uso de los recursos del sistema cuando está desocupado.
Las opciones de cliente y las opciones de sustitución del servidor de IBM Spectrum Protect se renuevan cada vez que los servicios del aceptador de cliente inician una copia de seguridad planificada.	Las opciones de cliente y las opciones de sustitución del servidor de IBM Spectrum Protect sólo se procesan después de iniciar dsmc sched .

Tabla 25. Servicios gestionados por el aceptador de cliente frente a servicios del planificador tradicional (continuación)

Servicios gestionados por el aceptador de cliente	Servicios del planificador tradicional de IBM Spectrum Protect
No pueden utilizarse con copias de seguridad <code>SESSIONINITIATION=SERVEROnly</code> .	<p>Debe reiniciar el proceso del planificador para que las opciones de cliente surtan efecto.</p> <p>Importante: Si ejecuta el planificador del cliente en la línea de mandatos, el planificador no ejecuta el servicio en segundo plano.</p> <p>Consejo: Reinicie el planificador tradicional de forma periódica para liberar los recursos del sistema que han utilizado previamente las llamadas del sistema.</p>

Configuración del cliente para que utilice el servicio del aceptador de cliente para gestionar el planificador

Una de las formas más efectivas de gestionar el planificador de cliente es utilizar el aceptador de clientes. Debe configurar el cliente para que utilice el aceptador de clientes para gestionar el planificador.

Antes de empezar

- Si incluye archivos para cifrado, asegúrese de que la opción **encryptkey** esté establecida en `save` en el archivo de opciones. Esta opción se define seleccionando **Guardar contraseña de clave de cifrado localmente** en la pestaña Autorización del editor de preferencia. Si establece esta opción, se habilitarán los servicios planificados desatendidos. Si no se ha guardado previamente la clave de cifrado, debe ejecutar una copia de seguridad atendida de al menos un archivo de forma que pueda obtener la solicitud de cifrado para guardar la clave.
- No puede utilizar el aceptador de clientes para realizar la planificación cuando la opción **sessioninitiation** esté establecida en `serveronly`.

Acerca de esta tarea

El aceptador de clientes sirve de temporizador externo para el planificador. Al iniciar el planificador, éste realiza una consulta al servidor para saber si hay otro evento planificado. El evento se ejecuta de forma inmediata o el planificador se cierra. El aceptador de clientes reinicia el planificador cuando es el momento de ejecutar el evento planificado. Esta acción reduce el número de procesos en segundo plano en la estación de trabajo y resuelve los problemas de retención de memoria que pueden ocurrir cuando el planificador se ejecuta sin la gestión del aceptador de clientes.

El servicio del aceptador de cliente también se conoce como `daemon` de aceptador de cliente.

Procedimiento

Siga los siguientes pasos para utilizar el aceptador de clientes para gestionar el planificador de cliente:

1. En la GUI del cliente de copia de seguridad y archivado, seleccione **Editar > Preferencias**.

2. Pulse en la ficha **Cliente Web**.
3. En el campo **Opciones de servicios gestionados**, pulse **Planificar**. Si también desea que el aceptador de clientes gestione el cliente web, pulse la opción **Ambos**.
4. Inicie el daemon de aceptador de cliente ejecutando el siguiente mandato en la línea de mandatos:
`dsmcad`

Consejo:

- También puede utilizar la opción **managedservices** en el archivo de opciones de sistema del cliente (`dsm.sys`) para especificar si el aceptador de clientes debe gestionar el planificador.
- Si necesita el aceptador de clientes para gestionar el planificador en modalidad de sondeo sin abrir ningún puerto de escucha, utilice la opción **cadlistenonport** en el archivo `dsm.sys`.

Conceptos relacionados:

“Descripción general de la configuración del cliente web” en la página 65

“Activar o desactivar mandatos planificados” en la página 292

“Opciones de planificación” en la página 330

Tareas relacionadas:

“Establecimiento del proceso del planificador cliente para que se ejecute como una tarea de fondo y se inicie automáticamente al arrancar” en la página 287

Referencia relacionada:

“Cadlistenonport” en la página 362

“Managedservices” en la página 486

“Sessioninitiation” en la página 556

Iniciar el planificador cliente

Esta tarea le guía a través de los pasos necesarios para planificar sucesos utilizando la GUI y el cliente de la línea de mandato.

Planificación de sucesos mediante el cliente de línea de mandatos

Esta tarea le guía a través de los pasos necesarios para planificar sucesos utilizando el cliente de línea de mandatos.

Acerca de esta tarea

Es necesario ser administrador del sistema para configurar el cliente de copia de seguridad y archivado para que utilice la interfaz del cliente de línea de mandatos para manejar sucesos planificados. Deben instalarse las herramientas de línea de mandatos para habilitar esta función.

Nota: Si ejecuta el planificador del cliente en la línea de mandatos, el planificador no ejecuta el servicio en segundo plano.

Antes de iniciar el planificador cliente mediante el daemon de aceptación de clientes, debe realizar los siguientes pasos:

Procedimiento

1. Asegúrese de que la opción `managedservices` incluye *schedule* en el archivo de opciones del sistema cliente (`dsm.sys`).
2. Establezca la opción `passwordaccess` en *generate* en el archivo de opciones del sistema cliente (`dsm.sys`).

Resultados

Si incluye archivos para el proceso de cifrado, asegúrese de seleccionar la opción **Guardar contraseña de clave de cifrado localmente** en la ventana Preferencias de autorización para que el planificador cliente pueda realizar servicios planificados desatendidos sin solicitar al usuario la clave de cifrado. Si la clave de cifrado no se ha guardado con anterioridad, deberá realizar una copia de seguridad atendida como mínimo de un archivo para que aparezca la solicitud de cifrado y pueda guardarse la clave.

Para iniciar el planificador cliente en el nodo cliente y conectarlo al planificador del servidor:

1. Cambie al directorio de instalación del cliente de copia de seguridad y archivarlo y especifique el mandato siguiente:

```
dsmc schedule
```

Cuando inicie el planificador cliente, éste se ejecuta continuamente hasta que cierre la ventana, el sistema o la sesión del sistema.

2. Si el directorio ejecutable del cliente no está en la variable de entorno `PATH`, vaya al directorio de instalación y escriba el mandato siguiente:

```
./dsmc schedule
```

3. Para ejecutar el mandato **schedule** como proceso en segundo plano y seguir ejecutando el planificador cliente, incluso si finaliza la sesión del sistema, especifique lo siguiente:

```
nohup dsmc schedule 2> /dev/null &
```

Si se necesita una contraseña de IBM Spectrum Protect para la estación de trabajo y quiere ejecutar el mandato **schedule** en segundo plano, indique la contraseña con el mandato.

Usuario root: para iniciar automáticamente el planificador cliente, asegúrese de que la opción `passwordaccess` esté establecida en *generate* en el archivo `dsm.sys` y, a continuación, siga el procedimiento que se indica a continuación para su sistema operativo:

Para iniciar cada planificador cliente de forma automática, añada una entrada al archivo `/etc/inittab`. Por lo general, el nivel de ejecución que se utilizará es 2, 3, 4, 5 o 6, dependiendo del sistema operativo y de su configuración. Consulte la documentación correspondiente a su sistema operativo para obtener más detalles de los niveles de ejecución.

Consulte la documentación correspondiente a su sistema operativo, para verificar si la sintaxis de la entrada es correcta.

A continuación, se muestran algunos ejemplos:

En AIX, añada la siguiente entrada al archivo `/etc/inittab`:

```
itsm:2:once:/usr/bin/dsmc sched > /dev/null 2>&1 # TSM scheduler
```

En este ejemplo, el nivel de ejecución se establece como 2.

En Solaris, añada la siguiente entrada al archivo `/etc/inittab`:

```
itsm:23:once:/usr/bin/dsmc sched > /dev/null 2>&1 # TSM scheduler
```

En este ejemplo, el nivel de ejecución se establece como 2 y 3.

Nota: Debe incluir la redirección a `/dev/null` en el mandato.

Para Mac OS X:

El administrador del sistema debe generar una contraseña para que el cliente pueda almacenarla en el archivo `TSM.PWD`. Esto se puede hacer con las Herramientas de IBM Spectrum Protect para administradores o con la línea de mandatos.

Un administrador del sistema debe utilizar uno de los métodos siguientes para habilitar el daemon de aceptación de clientes para iniciar el cliente de línea de mandatos en modalidad de planificación para gestionar los eventos planificados al iniciar el sistema.

Método 1 (preferido)

- Utilice las aplicaciones Herramientas de IBM Spectrum Protect para administradores e Iniciar el daemon de aceptador de cliente. De este modo se instala el daemon de aceptación de clientes como un elemento de arranque del sistema para que el daemon de aceptación de clientes se inicie después de reiniciarse el sistema. El daemon de aceptación de clientes también se inicia inmediatamente, para que no sea necesario reiniciar el sistema para gestionar los eventos planificados.

Método 2

- Utilice el script de shell de `"/Library/Application Support/tivoli/tsm/client/ba/bin"` para instalar el daemon de aceptación de clientes como un elemento de arranque. El nombre de script es `StartCad_cad.sh`.

Realice los pasos siguientes para iniciar el daemon de aceptación de clientes manualmente y para comprobar que está en ejecución.

1. Para comprobar que el daemon de aceptación de clientes se está ejecutando, emita el mandato siguiente:

```
sudo ps -x | grep dsmcad
```

Si el daemon de aceptación de clientes está en ejecución, uno de los procesos listados tendrá la ruta `/usr/bin/dsmcad`.

2. Para iniciar el daemon de aceptación de clientes manualmente, especifique el mandato siguiente en una ventana de terminal:

```
sudo /sbin/SystemStarter start dsmcad
```

El planificador cliente puede dar errores de inicialización al iniciar el sistema porque no se ha inicializado TCP/IP completamente. Es posible que necesite retrasar el inicio del servicio del planificador para dar tiempo a la inicialización de TCP/IP.

El cliente no reconoce los cambios realizados en el archivo `dsm.opt` o `dsm.sys` mientras se ejecuta el planificador cliente. Si realiza cambios en estos archivos mientras el planificador cliente está ejecutándose y desea utilizar los nuevos valores inmediatamente, debe detener el planificador cliente y luego volverlo a

iniciar. Por ejemplo, si modifica la opción `incl excl` en el archivo `dsm.sys` para hacer referencia a un archivo de opciones de inclusión/exclusión diferente, debe detener el planificador cliente y reiniciarlo antes de que el cliente utilice el nuevo archivo.

Para detener manualmente el planificador cliente, utilice el mandato **kill** si se está ejecutando el planificador cliente en proceso de fondo o pulse **q** o **Ctrl+C** si se está ejecutando en primer plano. Para reiniciar el planificador cliente, vuelva a entrar el mandato **schedule**.

La solicitud de cintas no se produce durante el evento planificado independientemente del valor que tenga la opción `tapeprompt` del archivo de opciones.

Tareas relacionadas:

“Configuración del planificador” en la página 66

Referencia relacionada:

“Managedservices” en la página 486

“Passwordaccess” en la página 509

Configuración de las comunicaciones cliente/servidor de IBM Spectrum Protect a través de un cortafuegos

En la mayoría de los casos, el servidor y los clientes de IBM Spectrum Protect pueden operar a través de un cortafuegos.

Acerca de esta tarea

Cada cortafuegos es distinto; por eso, es posible que el administrador del cortafuegos deba consultar las instrucciones del software o del hardware del cortafuegos que se utilice.

Hay dos métodos para permitir realizar operaciones de cliente y de servidor a través de un cortafuegos:

Método 1:

Para permitir que los clientes se comuniquen con un servidor a través de un cortafuegos, el administrador de cortafuegos debe abrir los siguientes puertos en el cortafuegos:

Puerto TCP/IP

Para habilitar el cliente de copia de seguridad/archivado, el cliente de administración de línea de mandatos y el planificador de modo que se ejecuten fuera de un cortafuegos, el administrador de cortafuegos debe abrir el puerto especificado por la opción del servidor ***tcpport*** (el valor predeterminado es 1500). Este puerto se establece en el cliente y en el servidor utilizando la opción ***tcpport***. El valor debe ser el mismo en el cliente y en el servidor. Esto permite las comunicaciones del planificador de IBM Spectrum Protect tanto en modalidad de *sondeo* como en modalidad de *petición*, los planificadores gestionados por aceptador de cliente y las operaciones habituales del cliente de archivado y copia de seguridad.

Nota: el cliente no puede utilizar el puerto que especifica la opción ***tcpadminport*** (en el servidor) para una sesión del cliente. Ese puerto sólo puede utilizarse para las sesiones de administración.

Puerto HTTP

Para permitir que un cliente web se comunice con las estaciones de trabajo remotas a través de un cortafuegos, el puerto HTTP de la estación de trabajo remota debe estar abierto. Para especificar este puerto, utilice la opción *httpport* en el archivo de opciones del cliente de la estación de trabajo remota. El puerto HTTP predeterminado es 1581.

Puertos TCP/IP para la estación de trabajo remota

Los dos puertos TCP/IP para el cliente de la estación de trabajo remota deben estar abiertos. Utilice la opción *webports* en el archivo de opciones del cliente de la estación de trabajo remota para especificar estos puertos. Si no especifica los valores de la opción *webports*, el valor predeterminado, que es el cero (0), provoca que TCP/IP asigne aleatoriamente dos números de puerto libres.

Puerto TCP/IP para sesiones de administración

Especifica un número de puerto TCP/IP independiente en el que el servidor espera peticiones de sesiones de cliente de administración, lo que permite sesiones de administración seguras dentro de una red privada.

Método 2:

Para el planificador cliente en modalidad de petición, no es necesario abrir *ningún* puerto en el cortafuegos. Si establece la opción *sessioninitiation* en *serveronly*, el cliente no intentará establecer contacto con el servidor. La *planificación por petición de servidor inicia todas las sesiones* en el puerto que se ha definido en el cliente con la opción *tcpclientport*. La opción *sessioninitiation* sólo afecta al comportamiento del planificador cliente que se ejecuta en modalidad por petición.

El servidor de IBM Spectrum Protect debe establecer el parámetro SESSIONINITiation en los mandatos **register node** y **update node** para cada nodo. Si el servidor especifica SESSIONINITiation=*clientorserver*, el valor predeterminado, el cliente puede decidir qué método utilizar. Si el servidor especifica SESSIONINITiation=*serveronly*, el servidor iniciará todas las sesiones.

Nota:

1. Si *sessioninitiation* se establece en *serveronly*, el valor de la opción de cliente *tcpclientaddress* debe ser igual al valor de la opción **HLAddress** del mandato de servidor **update node** o **register node**. El valor de la opción de cliente *tcpclientport* debe ser igual al valor de la opción **LLAddress** del mandato de servidor **update node** o **register node**.
2. Si establece la opción *sessioninitiation* en *serveronly*, a excepción de los planificadores gestionados por el aceptador de cliente, el cliente de línea de mandatos, la GUI Java del cliente de archivado y copia de seguridad y la GUI del cliente web seguirán intentando iniciar las sesiones, pero se verán bloqueados por el servidor de IBM Spectrum Protect para nodos que tienen la opción *sessioninitiation* establecida en *serveronly*.
3. Al configurar el planificador en una estación de trabajo cliente por primera vez, es posible que el servicio del planificador no pueda autenticarse para el servidor cuando el servidor establece contacto con el planificador cliente para ejecutar una planificación. Esto sucede cuando se establece *passwordaccess* para que se genere y el servidor de

IBM Spectrum Protect está detrás de un cortafuegos y la contraseña cifrada no puede almacenarse localmente antes de iniciar el planificador. Para resolver este problema, es necesario ejecutar el planificador desde la línea de mandatos (`dsms schedule`), esperar a que se inicie una operación planificada y entrar la contraseña del nodo cuando se le solicite.

4. el cliente no puede solicitar la contraseña de clave de cifrado en modalidad de planificador. Si utiliza el cifrado de datos de IBM Spectrum Protect, deberá ejecutar una copia de seguridad interactiva inicial una vez para establecer la clave de cifrado abriendo la conexión TCP/IP desde la estación de trabajo cliente hasta la estación de trabajo servidor. Consulte el **Método 1** para obtener más información acerca del establecimiento de esta comunicación. Después de haberse establecido la clave de cifrado, puede utilizar sesiones iniciadas por el servidor para realizar la copia de seguridad de los archivos utilizando el cifrado.

Si establece la opción *sessioninitiation* en *client*, el cliente inicia las sesiones con el servidor (**Método 1**) comunicándose en el puerto TCP/IP definido con la opción *tcpport* en *server*. Éste es el valor predeterminado. La planificación por petición de servidor puede utilizarse para solicitar al cliente que se conecte con el servidor.

Cuando se utilice IBM Spectrum Protect a través de un cortafuegos en la modalidad de *petición*, el servidor IBM Spectrum Protect debe contactar con el cliente. Para ello, puede que sea necesario instalar software en el servidor de IBM Spectrum Protect para direccionar la solicitud por medio del cortafuegos. Este software direcciona la petición del servidor a través de un puerto socks en el cortafuegos. Este método se suele denominar *activar la comunicación por socks* de un sistema. Los proxies no se admiten puesto que sólo direccionan algunos tipos de protocolos de comunicación (HTTP, FTP, GOPHER). Las comunicaciones de IBM Spectrum Protect no se direccionan mediante proxies. Es importante tener en cuenta que el cliente crea una nueva conexión con el servidor de IBM Spectrum Protect cuando se le solicita. Esto significa que debe emplearse la configuración del cortafuegos arriba mencionada.

Tareas relacionadas:

“Configuración del planificador” en la página 66

Referencia relacionada:

“Sessioninitiation” en la página 556

“Tcpadminport” en la página 585

“Tcpport” en la página 590

“Webports” en la página 650

Configuración de las comunicaciones cliente/servidor de IBM Spectrum Protect con Secure Sockets Layer

Secure Sockets Layer (SSL) permite comunicaciones seguras estándar en el mercado basadas en SSL entre el cliente y el servidor de IBM Spectrum Protect.

Acerca de esta tarea

Los siguiente componentes del cliente admiten SSL:

- Cliente de la línea de mandatos

- Cliente de la línea de mandatos administrativo
- Interfaz gráfica de usuario de cliente
- API del cliente

Solo las conexiones de servidor/cliente de salida son compatibles con SSL. Las conexiones de entrada (por ejemplo, aceptador de cliente, conexiones de planificación iniciadas por el servidor) no admiten SSL. Las comunicaciones cliente a cliente y de la GUI web no admiten SSL.

Cada servidor de IBM Spectrum Protect que esté habilitado para SSL debe tener un certificado exclusivo. El certificado puede ser de uno de los siguientes tipos:

- Un certificado autofirmado por IBM Spectrum Protect.
- Un certificado emitido por una entidad emisora de certificados (CA). La entidad emisora de certificados puede ser una empresa, como VeriSign o Thawte, o una entidad emisora de certificados interna, mantenida dentro de la empresa.

Siga los pasos que figuran a continuación para activar una comunicación SSL con un certificado autofirmado:

1. Obtener el certificado autofirmado del servidor de IBM Spectrum Protect (cert256.arm) Utilice el archivo del certificado cert.arm cuando el servidor no esté configurado para utilizar TLS (Transport Layer Security) 1.2; de lo contrario, utilice el archivo cert256.arm. El archivo del certificado del cliente debe ser el mismo que el archivo de certificado que utiliza el servidor.
2. Configure los clientes. Para poder utilizar SSL, cada cliente debe importar el certificado de servidor autofirmado.
Utilice el programa de utilidad de línea de mandatos GSKit, gsk8capicmd_64, para importar el certificado.
3. En el caso de una recuperación tras desastre del servidor de IBM Spectrum Protect, si se ha perdido el certificado, el servidor generará de forma automática uno nuevo. Cada cliente deberá obtener e importar el nuevo certificado.

Siga los pasos que figuran a continuación para activar una comunicación SSL con un certificado firmado por una entidad emisora de certificados:

1. Obtenga el certificado raíz de la entidad emisora de certificados.
2. Configure los clientes. Para poder utilizar SSL, cada cliente debe importar el certificado de servidor autofirmado.
Utilice el programa de utilidad de línea de mandatos GSKit, gsk8capicmd_64, para importar el certificado.

Consejo: Después de completar este paso, si el servidor consigue un certificado nuevo firmado por el mismo CA, el cliente no necesita importar el certificado raíz de nuevo.

3. Si va a recuperar el cliente de copia de seguridad y archivado como parte de una recuperación tras desastre, deberá volver a instalar el certificado SSL en el servidor. Si se ha perdido el certificado, deberá obtener uno nuevo. No necesitará volver a configurar el cliente si el nuevo certificado ha sido firmado por una entidad emisora de certificados.

Si va a configurar SSL en el cliente de copia de seguridad y archivado por primera vez, tendrá que crear la base de datos de claves local del cliente, dsmcert.kdb. Para crear la base de datos de claves local del cliente, ejecute el siguiente mandato desde el directorio DSM_DIR :

```
gsk8capicmd_64 -keydb -create -populate  
-db dsmcert.kdb -pw password -stash
```

Una vez creada la base de datos de claves local, deberá importar el certificado de servidor o el certificado raíz de la entidad emisora de certificados.

Si utiliza un certificado autofirmado

Cada servidor de IBM Spectrum Protect genera su propio certificado. El certificado tiene el nombre de archivo fijo de cert.arm o cert256.arm. El archivo de certificado se almacena en la estación de trabajo del servidor en el directorio de instancias del servidor; por ejemplo, /opt/tivoli/tsm/server/bin/cert256.arm. Si el archivo de certificado no existe y especifica la opción de servidor **SSLTCPPORT** o **SSLTCPADMINPORT**, el archivo de certificado se crea cuando inicia el servidor con este conjunto de opciones. Los servidores de IBM Spectrum Protect V6.3 (y versiones posteriores) generan archivos denominados cert256.arm y cert.arm. Los servidores anteriores a la V6.3 de IBM Spectrum Protect sólo generan archivos de certificado denominados cert.arm. Debe seleccionar el certificado que se define como el predeterminado en el servidor.

Realice estos pasos para configurar una conexión SSL en un servidor:

1. Obtenga el certificado del administrador de servidor.
2. Importe el certificado a la base de datos de claves de cliente utilizando el mandato siguiente:

```
gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed  
-label "TSM server <servername> self-signed key"  
-file <path_to_cert256.arm> -format ascii
```

Si utiliza un certificado de una entidad emisora de certificados

Si el certificado lo ha emitido una entidad emisora de certificados (CA), como VeriSign o Thawte, el cliente ya estará preparado para SSL y podrá omitir los pasos que figuran a continuación.

Para obtener una lista de los certificados de raíz instalados previamente desde las autoridades de certificados externos, consulte "Certificados raíz de entidades emisoras de certificados" en la página 77.

Si el certificado no se ha emitido por una de las entidades emisoras de certificados más conocidas, siga estos pasos:

1. Obtenga el certificado raíz de la entidad emisora de certificados firmante.
2. Importe el certificado a la base de datos de claves de cliente utilizando el mandato siguiente:

```
gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed  
-label "XYZ Certificate Authority" -file <path to CA root certificate>  
-format ascii
```

Importante:

1. Se utilizará una contraseña arbitraria proporcionada por usted para cifrar la base de datos de claves. La contraseña se almacena automáticamente cifrada en el archivo stash (dsmcert.sth). El cliente de copia de seguridad y archivado utiliza el archivo stash para recuperar la contraseña de la base de datos de claves.
2. Se puede agregar más de un certificado de servidor al archivo de base de datos de claves del cliente para que el cliente se pueda conectar a distintos servidores. Distintos certificados deben tener distintas etiquetas. Los nombres de etiqueta no son importantes, pero se deben utilizar nombres significativos.

Además, se puede añadir más de un certificado raíz de entidad emisora de certificados a la base de datos de claves del cliente.

3. Si no ejecuta los mandatos anteriores desde el directorio DSM_DIR, tendrá que copiar dsmcert.kdb y dsmcert.sth en ese directorio.
4. De forma predeterminada, los archivos de la base de datos de claves local tienen permisos y propiedades raíz y no los pueden leer otros usuarios. Si tiene previsto ejecutar el cliente como un usuario no root, tendrá que actualizar los permisos. Por ejemplo, para conceder acceso de lectura a todos los usuarios y grupos, ejecute el siguiente mandato:

```
# chmod go+r dsmcert.*
```
5. Por razones de rendimiento, utilice solo SSL para las sesiones en las que sea necesario. Plántese la posibilidad de añadir recursos de procesador adicionales en el sistema servidor de IBM Spectrum Protect para gestionar la necesidad de más requisitos.
6. Para que un cliente se conecte a un servidor que está utilizando Transport Layer Security (TLS) versión 1.2, el algoritmo de la firma del certificado debe ser SHA-1 o más fuerte. Si utiliza un certificado autofirmado, debe utilizar el certificado cert256.arm. Es posible que el administrador de IBM Spectrum Protect necesite cambiar el certificado predeterminado en el servidor de IBM Spectrum Protect. Consulte el tema sobre las opciones del servidor SSLTLS12 Para obtener información detallada.

Después de agregar el certificado del servidor en la base de datos de claves del cliente, agregue la opción **ssl yes** al archivo de opciones del cliente y actualice el valor de la opción **tcpport**. Es importante entender que el servidor normalmente se configura para conexiones SSL en un puerto distinto. En otras palabras, se abren dos puertos en el servidor:

1. Un puerto acepta conexiones de cliente no SSL regulares
2. El otro puerto acepta solamente conexiones SSL

No puede conectarse a un puerto no SSL con un cliente habilitado para SSL y a la inversa.

Si el valor de la opción **tcpport** es incorrecto, el cliente no se podrá conectar al servidor. Especifique el número de puerto correcto en la opción **tcpport**.

Para inhabilitar los protocolos de seguridad que son menos seguros que TLS 1.2, añada la opción **SSLDISABLELEGACYtls yes** al archivo de opciones de cliente o, en la GUI de Java, seleccione el recuadro **Requerir TLS 1.2 o superior** en la pestaña **Comunicación** del **Editor de preferencias**. Requerir TLS 1,2 o superior ayuda a evitar ataques de programas maliciosos.

Referencia relacionada:

“Ssl” en la página 576

“Sslfipsmode” en la página 577

Certificados raíz de entidades emisoras de certificados

El cliente de archivado y copia de seguridad incluye una lista de certificados raíz para una cantidad determinada de autoridades de certificado.

La siguiente es una lista de certificados raíz para varias autoridades de certificado que se entregan con el cliente:

- Entrust.net Global Secure Server Certification Authority
- Entrust.net Global Client Certification Authority

- Entrust.net Client Certification Authority
- Entrust.net Certification Authority (2048)
- Entrust.net Secure Server Certification Authority
- VeriSign Class 3 Public Primary Certification Authority
- VeriSign Class 2 Public Primary Certification Authority
- VeriSign Class 1 Public Primary Certification Authority
- VeriSign Class 4 Public Primary Certification Authority - G2
- VeriSign Class 3 Public Primary Certification Authority - G2
- VeriSign Class 2 Public Primary Certification Authority - G2
- VeriSign Class 1 Public Primary Certification Authority - G2
- VeriSign Class 4 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G3
- VeriSign Class 2 Public Primary Certification Authority - G3
- VeriSign Class 1 Public Primary Certification Authority - G3
- Thawte Personal Premium CA
- Thawte Personal Freemail CA
- Thawte Personal Basic CA
- Thawte Premium Server CA
- Thawte Server CA
- RSA Secure Server Certification Authority

Para utilizar certificados emitidos por otras entidades emisoras de certificados, deberá instalar los certificados raíz de la entidad emisora de certificados en todos los clientes como parte de la configuración del cliente.

Configuración del sistema para copia de seguridad con registro por diario

Debe instalar y configurar el daemon de registro por diario (Linux) o el servicio de motor con registro por diario (Windows) antes de poder realizar copias de seguridad con registro por diario.

Configuración del daemon de registro por diario

La copia de seguridad con registro por diario se habilita mediante la instalación y configuración del daemon de registro por diario de IBM Spectrum Protect.

Configure el de registro por diario editando el archivo de ejemplo de configuración del daemon de registro por diario, `tsmjbbd.ini.smp`, y guardando éste como `tsmjbbd.ini`. Ambos archivos deben encontrarse en el directorio de instalación predeterminado.

Una vez que haya configurado el archivo `tsmjbbd.ini`, inicie el daemon de registro por diario iniciando el archivo ejecutable **`tsmjbbd`**.

En AIX, ejecute el archivo de script `jbbinittab` para añadir una entrada al archivo `/etc/inittab` para iniciar el daemon de registro por diario después de reiniciar el sistema. El archivo ejecutable `tsmjbbd` y el archivo de script `jbbinittab` deben estar en el directorio de instalación predeterminado.

En Linux, el instalador creará el servicio tsmjbbd en /etc/init.d. Para controlar el servicio, ejecute el mandato siguiente como raíz para que se detenga, inicie o reinicie el servicio, o para comprobar su estado:



Si el sistema operativo Linux ejecuta el servicio de inicialización systemd, siga estos pasos para iniciar el daemon de registro por diario y ejecutarlo durante el inicio del sistema:

1. Copie el archivo de unidad de systemd /opt/tivoli/tsm/client/ba/bin/tsmjbbd.service que se proporciona en el directorio /etc/systemd/system/.
2. Ejecute el siguiente mandato para renovar la lista de unidades systemd:
`systemctl daemon-reload`
3. Ejecute el mandato siguiente para iniciar el daemon de registro por diario al arrancar el sistema:
`systemctl enable tsmjbbd.service`
4. Ejecute el mandato siguiente para iniciar el daemon de registro por diario:
`systemctl start tsmjbbd.service`

Nota:

1. No se admiten sistemas de archivos de red ni extraíbles.
2. Las copias de seguridad incrementales completas periódicas deben realizarse para complementar las copias de seguridad diarias con registro por diario. La ejecución de las copias de seguridad incrementales progresivas puede llevar más tiempo que una copia de seguridad con registro por diario. Téngalo en cuenta al planificarlas, quizá planificando las copias de seguridad incrementales durante horas de baja actividad. Equilibre estas dos técnicas de copia de seguridad según sus necesidades empresariales. Por ejemplo, puede que decida planificar las copias de seguridad con registro por diario nocturnas y también planificar una copia de seguridad incremental progresiva completa semanal.
3. La copia de seguridad con registro por diario utiliza la extensión del kernel de vía de acceso para supervisar los cambios en el sistema de archivos. Para mejorar el rendimiento de las copias de seguridad con registro por diario, los directorios que no contienen archivos de usuarios no se supervisan en busca de cambios y no se incluyen en copias de seguridad con registro por diario. A continuación se listan los directorios que no se incluyen en copias de seguridad con registro por diario en sistemas AIX y Linux. Los cambios en estos directorios se procesan si se realizan copias de seguridad incrementales completas periódicas mediante el mandato **incremental** con la opción **-nojournal**.

AIX	Linux
/bin /dev /etc /lib /usr/bin /usr/lib /usr/share	/bin /boot /dev /etc /lib /proc /sbin /sys /usr/bin /usr/lib /usr/share /var

Periódicamente se comprueba el archivo de configuración del daemon de registro por diario para determinar si existen actualizaciones en la lista de sistemas de archivos de diario. Puede añadir o eliminar sistemas de archivos de la lista de sistemas de archivos supervisados sin necesidad de detener el daemon de registro por diario.

Atención: Si desactiva un sistema de archivos que se está supervisando mediante el daemon de registro por diario, se suprimirá la base de datos diaria para dicho sistema de archivos. Para conservar la base de datos, establezca `PreserveDbOnExit=1` en la stanza de los valores de los sistemas de los archivos de diario. Este valor conserva la base de datos diaria cuando se desactiva y asegura que la base de datos diaria sea válida cuando el sistema de archivos vuelva a estar activado. Para obtener más información, consulte el apartado “Sección `JournaledFileSystemSettings`” en la página 82.

La sintaxis de las stanzas y los valores de las mismas son los siguientes:

Sintaxis de stanzas:

[NombreStanza]

Sintaxis de los valores de una stanza:

ConfiguraciónStanza=valor

Nota:

1. Puede incluir comentarios en el archivo; para ello, comience la línea con un signo de punto y coma.
2. Los nombres de valor y de stanza no son sensibles a mayúsculas y minúsculas.
3. Pueden especificarse valores numéricos en formato hexadecimal, especificando `0x` delante del valor; de lo contrario, se interpretará que son valores decimales.
4. Estos valores del sistema de archivos de registro por diario no se correlacionan con ningún valor del archivo de opciones del cliente. El daemon de registro por diario es un proceso independiente; no procesa opciones del archivo del cliente.

Sección `JournalSettings`

Los valores de esta sección son globales y se aplican a todo el daemon de registro por diario.

A continuación se muestra la sintaxis para la stanza `JournalSettings`:

Sintaxis de la stanza `JournalSettings`:

[JournalSettings]

Sintaxis de los valores de una sección:
configuraciónRegistropordiario=valor

Puede especificar los siguientes valores de JournalSettings:

ErrorLog

Especifica el archivo de anotaciones en el que se graban los mensajes de error detallados que genera el daemon de registro por diario. El valor predeterminado es `jbberror.log` y se encuentra en el directorio del ejecutable del daemon. Por ejemplo:

ErrorLog=/logs/jbberror.log

JournalDir

Directorio en el que se almacenan y graban los archivos de base de datos de diario.

Si la vía de acceso especificada es un nombre de vía de acceso absoluto (por ejemplo, empieza por un delimitador `dir`), se utiliza este directorio. Si la vía de acceso especificada es un nombre de directorio relativo, esta vía de acceso se agrega a cada uno de los nombres de los sistemas de archivos y se utiliza el nombre de vía de acceso resultante.

El valor predeterminado es un directorio denominado `.tSm_JoUrNaL` (se utiliza en cada uno de los sistemas de archivos que se registran por diario).

La ventaja de tener la base de datos de diario en el sistema de archivos que se registra por diario es que la base de datos está con el sistema de archivos. La desventaja es que las actualizaciones para la base de datos deben procesarse y descartarse.

Importante: Dirigir la base de datos a un sistema de archivos sin registro por diario, a menos que el sistema de archivos se comparta en un entorno en clúster.

Este valor se aplica a todos los sistemas de archivos de diario, pero puede alterarse temporalmente con una sección de alteración temporal para cada sistema de archivos de diario.

Sección JournalExcludeList

Esta lista de sentencias de exclusión filtra los cambios que podrían registrarse en la base de datos de diario.

Los cambios realizados en objetos que coinciden con las sentencias de esta sección se pasan por alto y no se registran en la base de datos de diario.

Nota:

1. La exclusión de archivos del diario no tiene ninguna relación con la exclusión de esos archivos que realiza el cliente de copia de seguridad, aparte de impedir que los nombres de archivos se envíen al cliente de copia de seguridad para que se procesen durante la realización de la copia de seguridad con registro por diario. Un archivo que no se ha excluido del registro por diario debería excluirlo el cliente de copia de seguridad/archivado si hubiera una sentencia de exclusión coincidente en el archivo de opciones del cliente.
2. El daemon de registro por diario sólo proporciona un subconjunto de las posibilidades de la función INCLUDE/EXCLUDE que proporciona el cliente de copia de seguridad/archivado. El daemon de registro por diario no admite sentencias INCLUDE y no admite la opción *exclude.dir*.

No existe correlación entre la lista de exclusión de diario y la lista de exclusión del cliente de copia de seguridad/archivado.

Se admiten los siguientes metacaracteres de coincidencia con un patrón:

% Representa exactamente un carácter.

* representa cero o más caracteres.

%EnvVar%

Expande la variable de entorno.

A continuación se muestra un ejemplo de sintaxis de sentencia de exclusión:

```
[JournalExcludeList]
*.jbb.jbbdb
*.jbbInc.jbbdb
```

Sección JournaledFileSystemSettings

Los valores de esta stanza se aplican a cada uno de los sistemas de archivos de diario especificados, a menos que se alteren temporalmente para sistemas de archivos individuales en una stanza de alteración temporal.

Los sistemas de archivos que especifique en la stanza `JournalFileSystems.Extended` sobrescriben cualquier sistema de archivos especificado en la lista de sistemas de archivos de diario que pueda haber especificado anteriormente en la stanza `JournaledFileSystemSettings`. Cualquier otra opción que haya especificado en la stanza `JournaledFileSystemsSettings` se preservará.

La sintaxis para la stanza `JournaledFileSystemSettings` es como sigue:

Sintaxis de la stanza *JournaledFileSystemSettings* :

[JournaledFileSystemSettings]

Sintaxis de los valores de una sección:

JournaledFileSystemSetting=valor

Puede especificar los siguientes valores de *JournaledFileSystemSettings*:

JournaledFileSystems

Especifica una lista de espacio delimitado de los sistemas de archivo para registrar por diario. Se soportan las especificaciones de sistema de archivos completo y los cruces Windows. No existe un valor predeterminado. Debe especificar, como mínimo, un sistema de archivos de diario para que pueda ejecutarse el daemon de registro por diario. Pueden agregarse o eliminarse sistemas de archivos de diario mientras éstos están activados, sin tener que reiniciar el daemon. Por ejemplo:

`JournaledFileSystems=/home /other`

Importante: El registro por diario selecciona los nombres de los objetos basándose estrictamente en una coincidencia de serie de caracteres. La implicación del usuario consiste en el cuidado que debe observarse al seleccionar los sistemas de archivos que han de registrarse por diario. Por ejemplo, imaginemos que existe un sistema de archivos denominado `/jbb` y otro sistema de archivos denominado `/jbb/mnt1`. Si solicita al registro por diario que supervise sólo `/jbb`, todos los cambios para `/jbb/mnt1` también coincidirán con esta serie de caracteres y se incluirán en la base de datos. Sin embargo, cuando realiza una copia de seguridad en el cliente, éste analiza el nombre basándose en los sistemas de archivos, detecta que el registro por diario no está supervisando este sistema de archivos y, a

continuación, indica al registro por diario que elimine los archivos de /jbb/mnt1 de la base de datos. La solución es supervisar ambos o bien utilizar JournalExcludeList. Lo mismo se aplica a las opciones de punto de montaje virtual. Debe ser coherente con esta lista. Por ejemplo, si especifica /home/student1 como punto de montaje virtual en el archivo de opciones dsm.sys y desea registrar por diario /home, deberá especificar JournaledFileSystems=/home /home/student1. En este caso, se crean dos bases de datos por separado.

JournalDbSize

Especifica el tamaño máximo que puede alcanzar la base de datos de diario. El tamaño de la base de datos de diario se expresa en bytes. Un valor cero (0) indica que el tamaño de la base de datos sólo está limitado por la capacidad del sistema de archivos en el que se encuentra la base de datos de diario. El valor predeterminado es 0 (ilimitado). Por ejemplo:

```
JournalDBSize=0x10000000
```

NotifyBufferSize, DirNotifyBufferSize

Especifican tamaños de memoria intermedia de notificación de cambios para un sistema de archivos de diario. La existencia de gran cantidad de actividad relacionada con los cambios podría hacer necesario el incremento de este valor. El valor predeterminado es 0x00020000 (128 k) para los archivos y 0x00010000 (64 k) para los directorios.

```
NotifyBufferSize=0x00200000
```

Valor PreserveDbOnExit

Este valor permite que un diario siga siendo válido cuando se desactiva y se vuelve a activar un sistema de archivos con registro por diario. Esto es útil para conservar el registro por diario durante los reinicios del sistema y el traspaso de recursos.

Este valor permite que una copia de seguridad con registro por diario pueda seguir procesándose cuando se reinicia el daemon (o cuando el sistema de archivos vuelve a activarse) sin que se realice una copia de seguridad incremental completa.

Nota: No se registrará en el diario ninguna actividad de cambio que suceda mientras no se esté ejecutando el daemon de registro por diario (o el sistema de archivos esté desactivado).

El valor 1 especifica que la base de datos de diario del sistema de archivos con registro por diario no se suprime cuando se desactiva el sistema de archivos con registro por diario. La base de datos también es válida cuando se vuelve a activar el sistema de archivos con registro por diario. Este valor debe utilizarse con precaución, pues en la base de datos de diario no se refleja ninguna actividad de cambio del sistema de archivos que ocurra mientras el sistema de archivos con registro por diario esté desactivado. El valor predeterminado 0 suprime la base de datos de diario del sistema de archivos de diario.

Nota: El diario sólo se conserva cuando un sistema de archivos con registro por diario se desactiva normalmente o se desactiva cuando el recurso ya no está disponible y se especifica el valor deferFsMonStart. Si un sistema de archivos se desactiva debido a un error, como por ejemplo un desbordamiento de la memoria intermedia de notificaciones, el diario no se conservará.

Nota: Establezca `PreserveDBonExit` solamente cuando pueda asegurar que es una finalización controlada del servicio de registro por diario. El alcance de la "finalización controlada" incluye detener el servicio diario para poder volver a arrancar el sistema, sustituir un recurso de clúster o mover un recurso de clúster. La base de datos diaria puede resultar dañada si la finalización no es controlada. Por lo tanto, realice los siguientes pasos si el servicio diario no se cerró de una forma controlada o si la base de datos diaria se desactivó o no de una forma no controlada.

1. Detener el servicio diario (si se está ejecutando)
2. Eliminar las bases de datos diarias dañadas
3. Reiniciar el servicio diario
4. Realizar una copia de seguridad incremental

Un ejemplo para no suprimir la base de datos de diario al salir es:
`preserveDBonExit=1`

Valor *deferFSMonStart*

Este valor difiere un intento de iniciar la supervisión de un sistema de archivos en los casos siguientes:

- Cuando el sistema de archivos con registro por diario especificado no sea válido o no esté disponible
- Cuando no se pueda crear el directorio de diario para el sistema de archivos con registro por diario especificado o no se pueda acceder al mismo

Se comprueban los recursos en los intervalos que especifique mediante el valor *deferRetryInterval*.

1 indica que este valor está activado y 0 que está desactivado. El valor predeterminado es desactivado (0).

Valor *deferRetryInterval*

Este valor especifica el valor en segundos durante los que se comprueba la disponibilidad de los sistemas de archivos aplazados con el valor *deferRetryInterval* activado y se activan. El valor predeterminado son 5 segundos.

Valor *logFSErrors*

El valor 1 indica que deben anotarse todos los errores detectados al acceder a un sistema de archivos de diario o a un directorio de diario. El valor cero indica que se suprime la anotación de los errores detectados al comprobar los directorios de diario y los sistemas de archivos diferidos. Este valor suele utilizarse junto con el valor *deferFSMonStart* para que no se grabe un número excesivo de mensajes relacionados con la no disponibilidad del sistema de archivos en las anotaciones cuando se ha diferido la activación de un sistema de archivos de diario. El valor predeterminado es 1 (anotar todos los errores).

Conceptos relacionados:

"Modificación de stanzas" en la página 85

"Stanza `JournaledFileSystems.Extended`"

Stanza `JournaledFileSystems.Extended`:

La stanza `JournaledFileSystems.Extended` sobrescribe cualquier sistema de archivos que se incluye en la stanza `JournaledFileSystems`. También elimina la limitación de caracteres de 1023 impuesta por la stanza `JournaledFileSystem`.

Si incluye sistemas de archivos en la stanza `JournaleFileSystems`, el número total de caracteres permitidos en dicha stanza es de 1023 caracteres. Para configuraciones grandes con muchos sistemas de archivos, el límite de 1023 caracteres es demasiado pequeño para especificar todos los sistemas de archivos. Si debe utilizar más de 1023 caracteres para incluir todos los sistemas de archivos que desee incluir en copias de seguridad con registro por diario, especifique los sistemas de archivos de la stanza `JournaleFileSystems.Extended`. Esta stanza ampliada no impone la limitación de caracteres de 1023. Los valores de `JournaleFileSystems.Extended` sobrescriben cualquier valor especificado en el resto de las stanzas. Si un sistema de archivos se especifica tanto en la stanza `JournaleFileSystems` como en la stanza `JournaleFileSystems.Extended`, el sistema de archivos especificado en la stanza `JournaleFileSystems` se ignorará.

La sintaxis para `JournaleFileSystems.Extended` tiene un formato de lista simple. Sistemas de archivos que desea que se incluyan en las copias de seguridad con registro por diario editando el archivo de configuración del daemon de registro por diario (el nombre predeterminado es `tmsjbbd.ini`).

Sintaxis de la stanza `JournaleFileSystems.Extended`:
[`JournaleFileSystems.Extended`]

Sintaxis de los valores de una sección:

```
/filesystem_1  
/filesystem_2  
.  
.  
/filesystem_n
```

Liste cada sistema de archivos que desee incluir en copias de seguridad con registro por diario.

Modificación de stanzas

Cualquier valor de la stanza **`JournaleFileSystemSettings`**, a excepción de los tamaños de almacenamiento intermedio, puede alterarse temporalmente para un sistema de archivos de diario en particular creando una stanza de alteración temporal.

HookFileName

Para que el registro por diario inicie la supervisión de un sistema de archivos, debe conocer el nombre de un archivo que exista en ese sistema de archivos. Este valor especifica un archivo existente. Por lo tanto, el acceso a este archivo se utiliza para comprobar si este sistema de archivos está activado o no. (La definición del término "montado" del sistema no puede utilizarse porque, en el cliente de copia de seguridad/archivado, está permitido el uso de puntos de montaje virtuales. Esto significa que el sistema del cliente de copia de seguridad y archivado puede gestionar un directorio como si se tratara de un sistema de archivos (virtual)).

Por lo tanto, si este sistema de archivos puede montarse y desmontarse, debe proporcionarse un valor **`HookFileName`**.

Si no se especifica un valor **`HookFileName`**, el daemon de registro por diario intentará crear un archivo temporal en el directorio del primer nivel, lo utilizará para iniciar la supervisión y, a continuación, lo suprimirá.

A continuación, se muestra la sintaxis de la stanza **`JournaleFileSystemSettings`**:

Sintaxis de la sección `JournaleFileSystemSettings`:
[`JournaleFileSystemSettings.sistema de archivos`]

Sintaxis de los valores de una sección:

JournaledFileSystemSetting=alteración temporal

Por ejemplo, el nombre de la sección de alteración temporal para /home sería:

```
JournaledFileSystemSettings./home  
HookFileName=/home/doNotDeleteThisFile
```

Deduplicación de datos del lado del cliente

La *eliminación de duplicados de datos* es un método de reducción de las necesidades de almacenamiento eliminando los datos redundantes.

Visión general

Existen dos tipos de eliminación de datos redundantes: *eliminación de duplicados de datos del lado del cliente* y *eliminación de duplicados de datos del lado del servidor*.

Optimización de almacenamiento de datos del lado de cliente es una técnica de optimización de almacenamiento de datos que se utiliza en el cliente de archivado y copia de seguridad para eliminar datos redundantes durante el proceso de copia de seguridad y archivado antes de que los datos se transfieran al servidor de IBM Spectrum Protect. El uso de la eliminación de duplicados de datos del lado del cliente puede reducir la cantidad de datos que se envían a través de la red de área local.

La *eliminación de duplicados de datos del lado del servidor* es una técnica de eliminación de duplicados de datos que pone en práctica el servidor. El administrador de IBM Spectrum Protect puede especificar la ubicación de la eliminación de datos duplicados (cliente o servidor) a utilizar con el parámetro **DEDUP** en el mandato del servidor **REGISTER NODE** o **UPDATE NODE**.

Mejoras

Con una eliminación de duplicados de datos del lado del cliente, puede realizar las siguientes tareas:

- Excluir archivos específicos en un cliente de una eliminación de duplicados de datos.
- Habilitar una memoria caché de eliminación de duplicados de datos que reduzca el tráfico de la red entre el cliente y el servidor. La memoria caché contiene extensiones que se enviaron al servidor en operaciones de copia de seguridad incremental anteriores. En lugar de consultar al servidor sobre la existencia de una extensión, el cliente consulta su memoria caché.

Especificar un tamaño y una ubicación para la memoria caché de un cliente. Si se detecta una incoherencia entre el servidor y la memoria caché, la memoria caché local se elimina y se vuelve a repoblar.

Nota: Para las aplicaciones que utilizan la API de IBM Spectrum Protect, no se debe utilizar la caché de deduplicación de datos porque pueden producirse errores de copia de seguridad debido a que la caché no está sincronizada con el servidor de IBM Spectrum Protect. Si existen varias sesiones de cliente simultáneas del cliente de copia de seguridad y archivado, debe tener configurada una memoria caché independiente para cada sesión.

- Habilitar la eliminación de duplicados de datos y la compresión del lado del cliente para reducir la cantidad de datos almacenados por el servidor. Todas las extensiones se comprimen antes de ser enviadas al servidor. El equilibrio se

establece entre el ahorro en el almacenamiento y la potencia de proceso necesaria para comprimir los datos del cliente. En general, si comprime y elimina duplicados de datos del sistema cliente, está utilizando aproximadamente el doble de potencia de proceso que si sólo realizara la eliminación de duplicados de datos.

El servidor puede trabajar con datos cuyos duplicados se han eliminado y que han sido comprimidos. Además, los clientes de archivado y copia de seguridad anteriores a la V6.2 pueden restaurar datos comprimidos y con duplicados de datos eliminados.

La eliminación de duplicados de datos del lado del cliente utiliza el siguiente proceso:

- El cliente crea extensiones. Las *extensiones* son fragmentos de archivo que se comparan con otras extensiones para identificar duplicados.
- El cliente y el servidor colaboran para identificar las extensiones duplicadas. El cliente envía extensiones no duplicadas al servidor.
- Las operaciones subsiguientes de eliminación de duplicados de datos del cliente crean nuevas extensiones. Algunas o todas las extensiones pueden coincidir con las extensiones que han sido creadas en operaciones de eliminación de duplicados de datos anteriores y enviadas al servidor. Las extensiones que coinciden no se vuelven a enviar al servidor.

Ventajas

La eliminación de duplicados de datos del lado del cliente presenta las siguientes ventajas:

- Puede reducir la cantidad de datos enviados a la red de área local (LAN).
- La potencia de procesamiento necesaria para identificar datos duplicados se descarga desde el servidor a los nodos cliente. La eliminación de duplicados de datos en el lado del servidor siempre está habilitada para la agrupación de almacenamiento con la eliminación de duplicados de datos habilitada. Sin embargo, los archivos que se encuentran en la agrupación de almacenamiento habilitada para eliminación de duplicados de datos y cuyos duplicados han sido eliminados por el cliente no requieren ningún proceso adicional.
- Se elimina el poder de procesamiento necesario para eliminar datos duplicados del servidor, lo que permite ahorrar inmediatamente espacio en el servidor.

La eliminación de duplicados de datos del lado del cliente tiene una desventaja posible. El servidor no tendrá copias completas de los archivos del cliente *hasta* que haga una copia de seguridad de las agrupaciones de almacenamiento primarias que contienen extensiones de cliente en una agrupación de almacenamiento de copia sin optimización de almacenamiento. (Las *extensiones* son partes de un archivo que se crean durante el proceso de optimización de almacenamiento de datos). Durante la copia de seguridad de la agrupación de almacenamiento en una agrupación de almacenamiento sin eliminación de datos duplicados, las extensiones del cliente se vuelven a ensamblar en archivos contiguos.

De manera predeterminada, debe realizarse una copia de seguridad de las agrupaciones de almacenamiento de acceso secuencial primarias que están configuradas para la eliminación de duplicados de datos en agrupaciones de almacenamiento de copia sin eliminación de duplicados para que puedan reclamarse y para que puedan eliminarse los datos duplicados. Esta opción predeterminada garantiza que el servidor tenga copias de archivos completos en

todo momento, en una agrupación de almacenamiento primaria o en una agrupación de almacenamiento de copia.

Importante: Para obtener una reducción aún mayor de los datos, puede habilitar de forma conjunta la compresión y la eliminación de duplicados de datos del lado del cliente. Todas las extensiones se comprimen antes de ser enviadas al servidor. La compresión ahorra espacio, pero aumenta el tiempo de proceso en la estación de trabajo cliente.

En una agrupación de almacenamiento con eliminación de duplicados de datos habilitada (agrupación de archivos) solo se conserva una instancia de una extensión de datos. Otras instancias de la misma extensión de datos se sustituyen por un puntero a la instancia conservada.

Cuando está habilitada la eliminación de duplicados de datos, y el servidor se ha quedado sin almacenamiento en la agrupación de destino, pero hay una agrupación siguiente definida, el servidor detendrá la transacción. El cliente de copia de seguridad y archivado vuelve a intentar la transacción sin la eliminación de duplicados de datos del lado del cliente. En el caso de la recuperación, el administrador de IBM Spectrum Protect debe añadir más volúmenes reutilizables a la agrupación de archivos original o volver a intentar la operación con la eliminación de duplicados inhabilitada.

Para la deduplicación de datos del cliente, el servidor de IBM Spectrum Protect debe tener la Versión 6.2 o posterior.

Requisitos previos

Cuando se configura la deduplicación de datos del lado del cliente, se deben cumplir los siguientes requisitos:

- El cliente y el servidor deben tener la versión 6.2.0 o posterior. Se debe utilizar siempre la versión de mantenimiento más reciente.
- Cuando un cliente realiza una copia de seguridad o archiva archivos, los datos se graban en la agrupación de almacenamiento primaria especificada por el grupo de copia de la clase de gestión vinculada a los datos. Para eliminar duplicados de datos de cliente, la agrupación de almacenamiento primaria debe ser una agrupación de almacenamiento de disco de acceso secuencial (FILE) en la que se haya habilitado la eliminación de duplicados de datos.
- Especifique YES como valor de la opción DEDUPLICATION para el cliente. También puede establecer la opción DEDUPLICATION en el archivo de opciones del cliente, en el editor de preferencias en la GUI del cliente de copia de seguridad y archivado o en el conjunto de opciones de cliente en el servidor IBM Spectrum Protect. Utilice el mandato **DEFINE CLIENTOPT** para definir la opción DEDUPLICATION en un conjunto de la opción del cliente. Para evitar que el cliente sustituya el valor en el conjunto de opciones de cliente, especifique **FORCE=YES**.
- La eliminación de duplicación de datos del lado del cliente debe estar habilitada en el servidor. Para habilitar la optimización de almacenamiento de datos del lado del cliente, utilice el parámetro **DEDUPLICATION** en el mandato de servidor **REGISTER NODE** o **UPDATE NODE**. Establezca el valor del parámetro a **CLIENTORSERVER**.
- Asegúrese de que los archivos en el cliente no se excluyan de la deduplicación de datos del lado del cliente. De manera predeterminada, se incluyen todos los archivos. Opcionalmente, puede excluir archivos específicos de la deduplicación de datos del lado del cliente con la opción de cliente `exclude.dedup`.

- No deben cifrarse los archivos del cliente. No pueden eliminarse los duplicados de datos de los archivos cifrados y los archivos de sistemas de archivos cifrados.
- Los archivos deben superar los 2 KB y las transacciones deben estar por debajo del valor especificado en la opción CLIENTDEDUPTXNLIMIT. En los archivos de 2 KB o menos no se eliminan los datos duplicados.

El servidor puede limitar el tamaño máximo de transacción para la eliminación de duplicados de datos estableciendo la opción CLIENTDEDUPTXNLIMIT en el servidor. Para obtener más información sobre esta opción, consulte la documentación del servidor de IBM Spectrum Protect.

Las siguientes operaciones tienen preferencia sobre la eliminación de duplicados de datos del lado del cliente:

- traspaso de datos sin LAN
- Operaciones de grabación simultánea
- Cifrado de datos

Importante: No planifique ni habilite ninguna de estas operaciones durante la eliminación de duplicados de datos del lado del cliente. Si se inicia alguno de estos procesos durante la eliminación de duplicados de datos del lado del cliente, ésta se detiene y se graba un mensaje en el registro de errores.

La configuración del servidor determina en última instancia si se habilita la eliminación de duplicados de datos del lado del cliente. Consulte el apartado Tabla 26.

Tabla 26. Configuración de eliminación de duplicados de datos: cliente y servidor

Valor de la opción DEDUPLICATION de cliente	Valor en el servidor	Ubicación de eliminación de duplicados de datos
Yes	En el servidor o en el cliente	Client
Yes	Solo en el servidor	Servidor
No	En el servidor o en el cliente	Servidor
No	Solo en el servidor	Servidor

Archivos cifrados

El servidor y el cliente de archivado y copia de seguridad de IBM Spectrum Protect no pueden optimizar el almacenamiento de los archivos cifrados. Si se encuentra un archivo cifrado durante el proceso de eliminación de duplicados de datos, no se elimina el duplicado de datos del archivo y se registra un mensaje.

Consejo: No tiene que procesar los archivos cifrados y los archivos que sí son aptos para la eliminación de duplicados de datos del lado del cliente por separado. Ambos tipos de archivo pueden procesarse en la misma operación. Sin embargo, se envían al servidor en transacciones diferentes.

Como medida de seguridad, puede seguir uno o varios de los pasos que se indican a continuación:

- Habilite el cifrado del dispositivo de almacenamiento junto con la eliminación de duplicados de datos del lado del cliente.
- Utilice la eliminación de duplicados de datos del lado del cliente sólo para los nodos que crea que son seguros.

- Si no está seguro de la seguridad de la red, habilite la Capa de sockets seguros (SSL).
- Si no desea que la eliminación de duplicados de datos del lado del cliente procese ciertos objetos (por ejemplo, objetos de imagen), puede excluirlos del cliente. Si se excluye un objeto de la eliminación de duplicados de datos del lado del cliente y se envía a una agrupación de almacenamiento en la que se ha establecido la eliminación de duplicados de datos, la eliminación del duplicado de datos del objeto se lleva a cabo en el servidor.
- Utilice el mandato **SET DEDUPVERIFICATIONLEVEL** para detectar posibles ataques a la seguridad del servidor durante la eliminación de duplicados de datos del lado del cliente. Cuando utilice este mandato, puede especificar un porcentaje de extensiones de cliente para que las verifique el servidor. Si el servidor detecta un posible ataque a la seguridad, aparecerá un mensaje.

Tareas relacionadas:

“Configuración del cliente para la eliminación de duplicados de datos”

Referencia relacionada:

“Eliminación de duplicados” en la página 381

“Opciones exclude” en la página 425

“Dedupcachepath” en la página 380

“Dedupcachesize” en la página 381

“Enablededupcache” en la página 413

“Ieobjtype” en la página 452

Configuración del cliente para la eliminación de duplicados de datos

Configure el cliente para que pueda utilizar la eliminación de duplicados de datos para realizar una copia de seguridad/archivado de los archivos.

Antes de empezar

Antes de configurar el cliente para utilizar la eliminación de duplicados de datos, asegúrese de que se cumplen los requisitos enumerados en “Deduplicación de datos del lado del cliente” en la página 86:

- El servidor debe habilitar el cliente para la eliminación de duplicados de datos del lado del cliente con el parámetro **DEDUP=CLIENTORSERVER** en el mandato **REGISTER NODE** o **UPDATE NODE**.
- El destino de la agrupación de almacenamiento para los datos debe ser una agrupación de almacenamiento habilitada para la eliminación de duplicados de datos.
- Asegúrese de que los archivos están enlazados a la clase de gestión correcta.
- Los archivos deben superar los 2 KB.

Se puede excluir un archivo del proceso de eliminación de duplicados de datos del lado del cliente. De manera predeterminada, se incluyen todos los archivos. Consulte la opción `exclude.dedup` para obtener más detalles.

El servidor puede limitar el tamaño máximo de transacción para la eliminación de duplicados de datos estableciendo la opción **CLIENTDEDUPTXNLIMIT** en el servidor.

Procedimiento

Utilice uno de los siguientes métodos para habilitar la eliminación de datos duplicados en el cliente:

Opción	Descripción
Edite el archivo de opciones de cliente del cliente	<ul style="list-style-type: none">• Añada la opción deduplication yes al archivo dsm.sys.
Editor de preferencias	<ol style="list-style-type: none">1. En la ventana IBM Spectrum Protect, pulse en Editar > Preferencias de cliente.2. Pulse en Eliminación de duplicados.3. Seleccione la casilla de verificación Habilitar eliminación de duplicados.4. Pulse Aceptar para guardar las selecciones que haya realizado y cerrar el Editor de preferencias.

Resultados

Una vez configurado el cliente para eliminación de duplicados de datos, inicie una operación de copia de seguridad o de archivado. Cuando la operación finalice, el informe de copia de seguridad o archivado mostrará los datos duplicados de esta operación y el número de archivos que se han procesado mediante la eliminación de duplicados de datos del lado del cliente.

Si no dispone de suficiente espacio de disco para realizar la operación de copia de seguridad o de archivado, puede habilitar la eliminación de datos duplicados del lado del cliente sin memoria caché local de eliminación de datos duplicados en el cliente siguiendo estos pasos:

1. Añada la opción deduplication yes en el archivo de opciones de cliente del cliente.
 - Añada la opción deduplication yes al archivo dsm.sys. También puede establecer esta opción en la interfaz gráfica de usuario.
2. Desactive la memoria caché local de eliminación de datos duplicados completando uno de los siguientes pasos.
 - Añada la opción ENABLEDEDUPCACHE NO en el archivo dsm.sys.También puede definir esta opción en el editor de preferencias del cliente de archivado y copia de seguridad deseleccionando el recuadro **Habilitar memoria caché para eliminación de duplicados**.

Ejemplo

El siguiente ejemplo utiliza el mandato de sesión de consulta para mostrar el tipo de datos que se han procesado para la eliminación de duplicados de datos:

```
Protect> q sess
Información de conexión de IBM Spectrum Protect Server

Nombre de servidor.....: SERVER1
Tipo de servidor.....: Windows
Protección de archivo de retención..: "No"
Versión de servidor.....: Ver. 6, Rel. 2, Niv. 0.0
Last Access Date.....: 08/25/2009 13:38:18
Suprimir archivos copia seg.....: "No"
```

Suprimir copias archivadas.....: "Sí"
Deduplication.....: "Client Or Server"

Node Name.....: AVI
Nombre de usuario.....:

El siguiente ejemplo utiliza el mandato de clase de gestión de consulta para mostrar el tipo de datos que se han procesado para la eliminación de duplicados de datos:

```
Protect> q mgmt -det
Domain Name : DEDUP
Activated Policy Set Name : DEDUP
Activation date/time : 08/24/2009 07:26:09
Default Mgmt Class Name : DEDUP
Grace Period Backup Retn. : 30 day(s)
Grace Period Archive Retn.: 365 day(s)
```

```
MgmtClass Name : DEDUP
Description : dedup - values like standard
Space Management Technique : None
Auto Migrate on Non-Usage : 0
Backup Required Before Migration: YES
Destination for Migrated Files : SPACEMGPPOOL
Copy Group
Copy Group Name.....: STANDARD
Copy Type.....: Backup
Copy Frequency.....: 0 day(s)
Versions Data Exists...: 2 version(s)
Versions Data Deleted..: 1 version(s)
Retain Extra Versions...: 30 day(s)
Retain Only Version....: 60 day(s)
Copy Serialization.....: Shared Static
Copy Mode.....: Modified
Copy Destination.....: AVIFILEPOOL
Lan Free Destination...: NO
Deduplicate Data.....: YES
```

```
Copy Group Name.....: STANDARD
Copy Type.....: Archive
Copy Frequency.....: Cmd
Retain Version.....: 365 day(s)
Copy Serialization.....: Shared Static
Copy Mode.....: Absolute
Retain Initiation.....: Create
Retain Minimum.....: 65534 day(s)
Copy Destination.....: FILEPOOL
Lan Free Destination...: NO
Deduplicate Data.....: YES
```

El código de retorno de ANS1900I es 0.

Conceptos relacionados:

"Deduplicación de datos del lado del cliente" en la página 86

Referencia relacionada:

"Eliminación de duplicados" en la página 381

"Enablededupcache" en la página 413

"Opciones exclude" en la página 425

 Opción CLIENTDEDUPTXNLIMIT

 Mandato REGISTER NODE

 Mandato UPDATE NODE

Excluir archivos de la eliminación de duplicados de datos

Puede excluir archivos de la eliminación de duplicados de datos durante el proceso de copia de seguridad o archivado.

Acerca de esta tarea

Solo podrá excluir archivos de la eliminación de datos de archivado. Podrá excluir archivos e imágenes (cuando proceda) de la eliminación de duplicados de datos de copia de seguridad.

Procedimiento

Si no desea que la eliminación de duplicados de datos del lado del cliente procese determinados archivos, utilice la GUI para excluirlos del proceso de eliminación de duplicados de datos:

1. Pulse **Editar > Preferencias del cliente**.
2. Pulse la pestaña **Incluir/excluir**.
3. Pulse **Añadir** para abrir la ventana Definir opciones de inclusión/exclusión.
4. Seleccione una categoría para el proceso.
 - Para excluir un archivo de la eliminación de duplicados de datos durante el proceso de archivado, seleccione **Archivado** en la lista **Categoría**.
 - Para excluir un archivo de la eliminación de duplicados de datos durante el proceso de copia de seguridad, seleccione **Copia de seguridad** en la lista **Categoría**.
5. Seleccione **Exclude.Dedup** en la lista **Tipo**.
6. Seleccione un elemento de la lista **Tipo de objeto**.
 - En el caso del proceso de archivado, solo está disponible el tipo de objeto **Archivo**.
 - Para el proceso de copia de seguridad, seleccione uno de los siguientes tipos de objeto:
 - **Archivo**
 - **Imagen**
7. Especifique un archivo o patrón en el campo **Archivo o patrón**. Puede utilizar caracteres comodín. Si no desea escribir un archivo o patrón, pulse **Examinar** para abrir una ventana de selección y seleccionar un archivo. En el caso de los espacios de archivos, puede seleccionar el punto de montaje desde la ventana de selección.
8. Pulse **Aceptar** para cerrar la ventana Definir opciones de inclusión/exclusión. Las opciones de exclusión que haya definido aparecerán en una sentencia de exclusión en la parte inferior del recuadro de lista Sentencias en la pestaña **Preferencias de inclusión/exclusión**.
9. Pulse **Aceptar** para guardar las selecciones que haya realizado y cerrar el Editor de preferencias.

Qué hacer a continuación

También puede excluir archivos del proceso de eliminación de duplicados de datos editando el archivo dsm.sys:

1. Añada la opción deduplication yes.
2. Excluya los archivos de un directorio de la eliminación de duplicados de datos. Por ejemplo, para excluir los archivos del directorio /Users/Administrator/

Documents/Taxes/, añada la sentencia siguiente: EXCLUDE.dedup
/Users/Administrator/Documents/Taxes/.../*

3. Excluya la eliminación de duplicados de datos del lado del cliente de la copia de seguridad de imágenes de un sistema de archivos. Por ejemplo, para excluir el sistema de archivos /home, añada la sentencia siguiente: EXCLUDE.DEDUP
/home/*/* IEOBJTYPE=Image.

Importante: Si se envía un objeto a una agrupación de eliminación de duplicados, la eliminación de duplicados de datos se producirá en el servidor aunque el objeto se excluya de la eliminación de duplicados de datos del lado del cliente.

Conceptos relacionados:

“Deduplicación de datos del lado del cliente” en la página 86

Referencia relacionada:

“Eliminación de duplicados” en la página 381

“Enablededupcache” en la página 413

“Opciones exclude” en la página 425

Configuración y uso de la migración tras error automática del cliente

El cliente de archivado y copia de seguridad puede realizar la migración tras error en un servidor secundario para recuperar los datos cuando el servidor de IBM Spectrum Protect no está disponible. Puede configurar el cliente para la migración tras error automática o evitar que el cliente migre tras el error. También puede determinar el estado de la réplica de sus datos en servidor secundario antes de restaurar o recuperar los datos replicados.

Tareas relacionadas:

“Restaurar o recuperar datos durante una migración tras error” en la página 247

Visión general de migración tras error de cliente automatizado

Cuando hay un corte en el servidor de IBM Spectrum Protect, el cliente de archivado y copia de seguridad puede migrarse de forma automática a servidor secundario para recuperar los datos.

El servidor de IBM Spectrum Protect al que se conecta el cliente durante los procesos de producción normal se denomina *servidor primario*. Cuando los nodos del cliente de servidor primario y están configurados para la réplica del nodo, el servidor también se conoce como *source replication server*. Los datos del cliente del servidor de réplica de origen se pueden replicar en otro servidor de IBM Spectrum Protect, que es el *servidor de réplica de destino*. Este servidor también se denomina *servidor secundario*, y es el servidor sobre el que el cliente realiza la migración tras error automáticamente cuando el servidor primario falla.

Para que el cliente realice una migración tras error automáticamente en el servidor secundario, la información de conexión para el servidor secundario debe estar disponible en el cliente. Durante las operaciones normales, la información de conexión para el servidor secundario se enviará automáticamente al cliente desde el servidor primario durante el proceso de inicio de sesión. La información del servidor secundario se guardará automáticamente en el archivo de opciones del cliente. No se necesita intervención manual del cliente para añadir la información del servidor secundario.

Cada vez que el cliente inicia sesión en el servidor de IBM Spectrum Protect, el cliente intenta ponerse en contacto con el servidor primario. Si el servidor primario

no está disponible, el cliente se migra automáticamente al servidor secundario, según la información de servidor secundario disponible en el archivo de opciones del cliente. En esta modalidad de migración tras error, puede restaurar o recuperar cualquier dato del cliente replicado. Cuando el servidor primario vuelva a estar en línea, el cliente volverá automáticamente al servidor primario la próxima vez que se inicie el cliente.

Por ejemplo, el siguiente texto de ejemplo muestra la información de conexión que servidor secundario envía al cliente y guarda en el archivo de opciones del sistema del cliente (dsm.sys):

```
*** Estas opciones no se deben cambiar manualmente
REPLSERVERNAME          TARGET
REPLTCPSERVERADDRESS    192.0.2.9
REPLTCPSPORT            1501
REPLSSLPORT             1502
REPLSERVERGUID          60.4a.c3.e1.85.ba.11.e2.af.ce.00.0c.29.2f.07.d3

MYREPLICATIONServer TARGET
*** end of automatically updated options
```

Requisitos para la migración tras error automática del cliente

Antes de configurar o utilizar la migración tras error automática del cliente el cliente de archivado y copia de seguridad y el servidor de IBM Spectrum Protect debe cumplir varios requisitos.

Asegúrese de que el cliente cumpla los siguientes requisitos para la migración tras error automática del cliente:

- El servidor primario, el servidor secundario, y el cliente de archivado y copia de seguridad deben tener IBM Spectrum Protect Versión 7.1 o posterior.
- Los servidores primario y secundario deben estar configurados para la réplica del nodo.
- El nodo del cliente debe estar configurado para la réplica del nodo en el servidor de réplica de origen utilizando los mandatos del servidor REGISTER NODE REPLSTATE=ENABLED o UPDATE NODE REPLSTATE=ENABLED.
- De forma predeterminada, se habilita el cliente para la migración tras error del cliente automatizado. Sin embargo, si se especifica la opción `usereplicationfailover` no en el archivo de opciones del cliente, bien cambie el valor a `yes`, o elimine la opción.
- La información de conexión válida para el servidor secundario debe existir en el archivo de opciones del cliente. Durante las operaciones normales, esta información se enviará automáticamente al cliente desde el servidor primario.
- Para guardar la información de conexión de servidor secundario que se envía desde servidor primario, el cliente debe tener acceso de grabación al archivo `dsm.opt` en los clientes de Windows y el archivo `dsm.sys` en los clientes de AIX, Linux, Mac OS X y Oracle Solaris. Si el cliente no tiene acceso de grabación a estos archivos, la información de servidor secundario no se guarda en el archivo de opciones del cliente y se añade un error al registro de error.
- Los usuarios no raíz no pueden utilizar la ubicación predeterminada para la tabla de réplica del nodo. Debe especificar una ubicación diferente añadiendo el la opción `nrtablepath` al archivo `dsm.sys`. Para obtener más información, consulte “Nrtablepath” en la página 503.
- Los procesos siguientes se deben producir antes de la información de conexión para que se envíe el servidor secundario al archivo de opciones:
 - Se debe realizar una copia de seguridad del cliente en el servidor de réplica de origen al menos una vez.

- Se debe volver a aplicar el nodo del cliente al servidor de réplica de destino al menos una vez.
- La migración tras error ocurre en los nodos de cliente que se copian con soporte de proxy del nodo del cliente cuando tanto los nodos de destino como de agente se configuran para la réplica en servidor de réplica de destino. Cuando el nodo de destino se replica de forma explícita, el nodo del agente también se replica de forma implícita en el servidor de réplica de destino, junto con la relación de proxy.
Por ejemplo, Node_B tiene autoridad para llevar a cabo operaciones de cliente en nombre de Node_A con el siguiente mandato del servidor:
`grant proxynode target=Node_A agent=Node_B`

Si ambos nodos están configurados para la réplica con la opción `replstate=enabled` en la definición del nodo, cuando el Node_A se replica, el Node_B y la relación de proxy también se replican.

Restricciones de la migración tras error automática de cliente

Revise la siguiente información para tener un mejor conocimiento del proceso y de las restricciones que se aplican a la migración tras error automática del cliente.

Las siguientes restricciones se aplican a la migración tras error automática del cliente:

- Cuando el cliente está en modo migración tras error, no puede utilizar ninguna función que requiera que los datos se almacenen en servidor secundario, como las operaciones de archivado y copia de seguridad. Puede utilizar solo las funciones de recuperación de los datos como la restauración, recuperación u operaciones de consulta. También puede editar las opciones del cliente y cambiar la contraseña del cliente de IBM Spectrum Protect.
- Las planificaciones no se replican en el servidor secundario. Por lo tanto, las planificaciones no se ejecutan mientras servidor de servidor primario no está disponible.
- Una vez que el cliente se conecta a servidor secundario en el modo de recuperación tras error, no intenta conectarse a servidor primario hasta el siguiente inicio de sesión inicial del servidor. El cliente intenta realizar la migración tras error en el servidor secundario solo cuando falla la conexión inicial al servidor primario. La conexión inicial es la primera conexión que el cliente realiza con el servidor.

Si el servidor primario deja de estar disponible durante una operación del cliente, el cliente no realiza la recuperación tras error en el servidor secundario, y la operación falla. Debe reiniciar el cliente para que pueda realizar la migración tras error en el servidor secundario, y después ejecutar la operación del cliente de nuevo.

Las operaciones de restauración que se interrumpen cuando el servidor primario se desconecta no se pueden restaurar después de que el cliente realice la migración tras error. Debe ejecutar la operación de restauración completa de nuevo después de que el cliente realice la migración tras error al servidor secundario.

- Si la contraseña de IBM Spectrum Protect se cambia antes de que se replique el nodo del cliente, la contraseña no se sincronizará entre los servidores primarios y secundarios. Si la migración tras error se produce durante este tiempo, debe reiniciar de forma manual la contraseña en el servidor secundario y en el cliente. Cuando la servidor primario vuelve a estar disponible, la contraseña debe reiniciarse para que el cliente se conecte a servidor primario.

Si la contraseña se restaura mientras que el cliente está conectado a servidor secundario, la contraseña debe reiniciarse en el servidor primario antes de que el cliente pueda iniciar sesión en el servidor primario. Esta restricción es verdadera si la opción **passwordaccess** se define en **generate** o si la contraseña se restaura de forma manual.

- Si has realizado la copia de seguridad o archivado los datos del cliente, pero servidor primario se queda inactivo antes de replicar el nodo del cliente, la copia de seguridad o los datos de archivado más reciente no se replican en el servidor secundario. El estado de réplica del espacio de archivos no es el actual. Si intenta restaurar o recuperar los datos en el modo de migración tras error y el estado de réplica no es el actual, se muestra un mensaje que indica que los datos que está a punto de recuperar están desfasados. Puede decidir si va a seguir con la recuperación o esperar hasta que servidor primario vuelva a estar online.
- Si existe un ID de usuario administrativo con una autoridad de cliente propietario en el servidor de réplica de origen, y el ID de usuario tiene el mismo nombre que el nodo del cliente, el ID de usuario administrativo se replica durante el proceso de réplica en el servidor. Su dicho ID de usuario no existe en el servidor de réplica de origen, el proceso de réplica no crea esta definición de administrador en el servidor de réplica de destino.

Si otro ID de usuario administrativo se asigna al nodo, el administrador de IBM Spectrum Protect debe configurar de forma manual el ID de usuario administrativo en el servidor de réplica de destino. De lo contrario, el usuario administrativo no puede conectarse al servidor de réplica de destino (servidor secundario) con el cliente web de IBM Spectrum Protect.

- Si restaura un archivo desde IBM Spectrum Protect, y el sistema de archivos está gestionado por IBM Spectrum Protect for Space Management, no debe restaurar el archivo como un archivo de resguardo. Debe restaurar el archivo completo. Utilice la opción `restoremigstate=no` para restaurar el archivo completo. Si restaura el archivo como un resguardo desde el servidor de destino, se pueden producir las siguientes consecuencias:
 - No puede recuperar el archivo del servidor de origen de IBM Spectrum Protect utilizando el cliente de IBM Spectrum Protect for Space Management.
 - El proceso de reconciliación de IBM Spectrum Protect for Space Management que se ejecuta contra el servidor de origen de IBM Spectrum Protect hace caducar el archivo. Si el archivo ha caducado por un proceso de reconciliación, puede restaurar el archivo completo con el cliente de copia de seguridad/archivado y la opción `restoremigstate=no`.

Funciones de migración tras error de los componentes de IBM Spectrum Protect

Los componentes y productos de IBM Spectrum Protect se basan en el cliente de archivado y copia de seguridad o la API para realizar la copia de seguridad de los datos en el servidor primario de IBM Spectrum Protect. Cuando servidor primario deja de estar disponible, algunos de estos productos y componentes pueden migrarse tras error a servidor secundario, mientras que otros no son capaces de migrarse tras el error.

Para obtener más información sobre las funciones de migración tras error de los componentes y productos de IBM Spectrum Protect, consulte la nota técnica 1649484.

Tareas relacionadas:

“Determinación del estado los datos replicados del cliente” en la página 100

Configuración del cliente de migración automática tras error

Puede configurar de forma manual el cliente para que se migre de forma automática al servidor secundario.

Antes de empezar

Antes de iniciar la configuración:

- Asegúrese de que el nodo del cliente participa en la réplica en servidor primario.
- Asegúrese de que el cliente cumple con los requisitos de para la migración tras error automática del cliente.
- Utilice este procedimiento solo si la información de la conexión para servidor secundario no es actual o si no está en el archivo de opciones del cliente.

Acerca de esta tarea

Es posible que deba configurar el cliente para la migración tras error automática en las siguientes situaciones:

- La configuración de servidor secundario ha cambiado y el servidor primario no está disponible antes de que el cliente se registra en el servidor. Cuando añade información de conexión de forma manual, el cliente se activa para la migración tras error al servidor secundario.
- Ha eliminado de forma accidental toda la información de conexión de servidor secundario del archivo de opciones del cliente.

Consejo: En vez de configurar de forma manual el archivo de opciones del cliente, puede ejecutar el mandato **dsmc q session**, que le solicita iniciar sesión en servidor primario. La información de la conexión para servidor secundario se envía automáticamente al archivo de opciones del cliente.

Procedimiento

Para configurar de forma manual el cliente para la migración tras error automática, siga estos pasos:

1. Asegúrese de que el cliente está activado para la migración tras error automática del cliente verificando que la opción `usereplicationfailover` no está en el archivo de opciones del cliente o que está ajustada en `yes`. De forma predeterminada, el cliente está activado para la migración tras error automática, así que `usereplicationfailover` no es necesario en el archivo de opciones del cliente.
2. Obtenga la información de conexión sobre servidor secundario desde el administrador del servidor de IBM Spectrum Protect y añada la información al comienzo del archivo de opciones del cliente. Agrupe las sentencias en una stanza en la sentencia **replservername**.

Por ejemplo, añada las siguientes sentencias al archivo `dsm.sys`:

```
REPLSERVERNAME      TARGET
REPLTCPSERVERADDRESS 192.0.2.9
REPLTCPSPORT        1501
REPLSSLPORT          1502
REPLSERVERGUID       60.4a.c3.e1.85.ba.11.e2.af.ce.00.0c.29.2f.07.d3

Sservername      server_a
COMMMethod        TCPip
```

```
TCPPort 1500
TCPServeraddress server_hostname1.example.com
PASSWORDAccess prompt
MYREPLICATIONServer TARGET
```

3. Los usuarios no raíz deben especificar una ubicación para la tabla de réplica del nodo añadiendo la opción **nrtablepath** al archivo `dsm.sys`. El cliente de copia de seguridad y archivado utiliza esta tabla para almacenar la información acerca de cada operación de copia de seguridad o archivado en el servidor de IBM Spectrum Protect.

Debe especificar una ubicación a la que tu ID de usuario tenga acceso. Por ejemplo:

```
nrtablepath /Volumes/nrtbl
```

Restricción: No especifique el directorio raíz (/) para la ubicación de la tabla de réplica del nodo.

4. Guarde y cierre el archivo de opciones del cliente.
5. Reinicie la GUI del cliente de archivado y copia de seguridad o inicie sesión en el servidor de IBM Spectrum Protect desde la interfaz de la línea de mandatos. El cliente está conectado a servidor secundario.

Ejemplo

Después de configurar el cliente para la migración tras error automática, el cliente intenta iniciar sesión en el servidor y se muestra el siguiente ejemplo de salida de mandato:

```
IBM Spectrum Protect
Interfaz de línea de mandatos del cliente de copia de seguridad/archivado
Versión de cliente 8, release 1, nivel 0.0
Fecha/hora del cliente: 12/16/2016 12:05:35
(c) Copyright by IBM Corporation y otros 1990, 2016. Reservados todos los derechos.

Nombre de nodo: MY_NODE_NAME
ANS2106I Connection to primary IBM Spectrum Protect server 192.0.2.1 failed

ANS2107I Attempting to connect to secondary server TARGET at 192.0.2.9 : 1501

Nombre de nodo: MY_NODE_NAME
Session established with server TARGET: Windows
Versión de servidor 8, release 1, nivel 0.0
Fecha/hora del servidor: 12/16/2016 12:05:35 Último acceso: 12/15/2016 09:55:56

Session established in failover mode to secondary server
ANS2108I Connected to secondary server TARGET.
```

Qué hacer a continuación

Puede restaurar o recuperar cualquier dato de réplica en el modo de migración tras error.

Conceptos relacionados:

“Visión general de migración tras error de cliente automatizado” en la página 94

Tareas relacionadas:

“Restaurar o recuperar datos durante una migración tras error” en la página 247

Referencia relacionada:

“Forcefailover” en la página 445

“Myreplicationserver” en la página 497

“Nrtablepath” en la página 503

"Replserverguid" en la página 531
 "Replservername" en la página 532
 "Replsslport" en la página 534
 "Repltcpport" en la página 536
 "Repltcpserveraddress" en la página 537
 "Usereplicationfailover" en la página 602

Determinación del estado los datos replicados del cliente

Puede verificar si la copia de seguridad más reciente del cliente se replicó en el servidor secundario antes de restaurar o recuperar los datos desde servidor secundario.

Acerca de esta tarea

Puede obtener el estado de los datos de cliente replicados para determinar si la copia de seguridad del cliente más reciente se replicó en el servidor secundario.

Si la indicación de fecha y hora de la operación de copia de seguridad más reciente coincide con la indicación de fecha y hora de la copia de seguridad de servidor secundario, el estado de la réplica es actual.

Si la indicación de fecha y hora de la operación de copia de seguridad más reciente es diferente de la indicación de fecha y hora de la copia de seguridad de servidor secundario, el estado de la réplica no es corriente. Esta situación puede ocurrir si ha realizado la copia de seguridad del cliente, pero antes de que se pueda replicar el nodo del cliente, el servidor primario pasa a estar no disponible.

Procedimiento

Para determinar el estado de los datos del cliente replicado, emita el siguiente mandato en el indicador de mandatos:

```
dsmc query filespace -detail
```

El siguiente ejemplo muestra la salida de la indicación de fecha y hora en el servidor y en la réplica del cliente, por tanto, el estado de la réplica es actual:

#	Fecha último Incr	Tipo	fsID	Unicode	Réplica	Espacio archivos
1	00/00/0000 00:00:00	HFS		9	Yes	Current /
	Fecha últ. alm.	Servidor			Local	
	Backup Data :	04/22/2013 19:39:17			04/22/2013 19:39:17	
	Datos archivado:	Ninguna fecha disponible			Ninguna fecha disponible	

La siguiente salida de ejemplo muestra que la indicación de fecha hora del servidor y el cliente no coinciden, por tanto, el estado de réplica no es actual:

#	Fecha último Incr	Tipo	fsID	Unicode	Réplica	Espacio archivos
1	00/00/0000 00:00:00	HFS		9	Yes	Not Current /
	Fecha últ. alm.	Servidor			Local	
	Backup Data :	04/22/2013 19:39:17			04/24/2013 19:35:41	
	Datos archivado:	Ninguna fecha disponible			Ninguna fecha disponible	

Qué hacer a continuación

Si intenta restaurar los datos en el modo de migración tras error y el estado de réplica no es el actual, se muestra un mensaje que indica que los datos que está a punto de restaurar están desfasados. Puede decidir si va a seguir con la restaure el servidor primario esté online.

Tareas relacionadas:

“Restaurar o recuperar datos durante una migración tras error” en la página 247

Referencia relacionada:

“Nrtablepath” en la página 503

Prevención de la migración tras error automática del cliente

Puede configurar el cliente para evitar que se realice la migración tras error automática al servidor secundario.

Acerca de esta tarea

Es posible que le interese evitar la migración tras error automática, por ejemplo, si sabe que los datos del cliente no se replicaron al servidor secundario antes de que servidor primario se desconectara. En este caso, si no desea recuperar los datos replicados de es posible que el servidor secundario sea antiguo.

Procedimiento

Para impedir que el nodo del cliente migre tras error alservidor secundario, añada la siguiente sentencia al archivo de opciones del cliente:

```
usereplicationfailover no
```

Este ajuste sustituye a la configuración que proporciona el servidor de IBM Spectrum Protect en el servidor primario.

Resultados

El nodo del cliente no realiza la migración tras error de forma automática en elservidor secundario la próxima vez e intenta conectarse al servidor primario sin conexión.

Tareas relacionadas:

“Determinación del estado los datos replicados del cliente” en la página 100

Referencia relacionada:

“Usereplicationfailover” en la página 602

Forzar al cliente a la migración tras error

El cliente puede realizar la migración tras error al clienteservidor secundario si el servidor primario es operacional. Por ejemplo, puede utilizar esta técnica para verificar que el cliente va a realizar la migración al servidor secundario esperado.

Procedimiento

Para forzar al cliente a que realice la migración tras error aservidor secundario, siga estos pasos:

1. Añada la opción **forcefailover yes** al archivo de opciones del sistema del cliente (dsm.sys).

2. Conéctese al servidor secundario reiniciando la GUI del cliente de archivado y copia de seguridad o iniciando una sesión de mandatos con el mandato **dsmc**.
3. Opcional: En vez de actualizar el archivo de opciones, puede establecer una conexión con el servidor secundario si especifica la opción **-forcefailover=yes** con un mandato. Por ejemplo:

```
dsmc q sess -forcefailover=yes
```

Qué hacer a continuación

Puede verificar que está conectado a servidor secundario mediante uno de los siguientes métodos:

- Compruebe el campo **Secondary Server Information** de la ventana Connection Information de la GUI del cliente de archivado y copia de seguridad.
- Compruebe la salida del mandato cuando inicie una sesión de mandatos. El estado del servidor secundario se muestra en la salida.

Referencia relacionada:

“Forcefailover” en la página 445

Configuración del cliente para realizar una copia de seguridad y archivado de los datos de Tivoli Storage Manager FastBack

Antes de realizar una copia de seguridad o archivado de los datos del cliente de Tivoli Storage Manager FastBack, deberá completar las tareas de configuración.

Asegúrese de que ha configurado el cliente de archivado y copia de seguridad y de que ha instalado el cliente de Tivoli Storage Manager FastBack.

Instale el cliente de FastBack utilizando la información de Tivoli Storage Manager FastBack.

Después de instalar el cliente de FastBack, realice las siguientes tareas:

1. Registre un nodo para cada cliente de FastBack en el que los datos se copian o archivan. El nombre de nodo tiene que ser el nombre de host abreviado del cliente de FastBack.

Esta es una configuración única que se realiza una vez para cada cliente de FastBack cuyos volúmenes necesitan una copia de seguridad o archivado.

Este paso de registro debe realizarse de forma manual solo cuando el cliente de archivado y copia de seguridad se utiliza como una aplicación autónoma.

El Centro de administración realiza el registro de este nodo de forma automática cuando el usuario crea planificaciones para el archivado o la copia de seguridad de datos de FastBack mediante el Centro de administración. A partir de la versión 7.1, el componente del Centro de administración ya no se distribuye con Tivoli Storage Manager o IBM Spectrum Protect. Los usuarios de FastBack que tienen un Centro de administración de una versión de servidor anterior pueden seguir utilizándolo para crear y modificar planificaciones de FastBack. Si no tiene instalado el Centro de administración, puede descargar la versión anterior de <http://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/admincenter/v6r3/>. Si no tiene el Centro de administración instalado, tiene que crear y modificar planificaciones de FastBack en el servidor de IBM Spectrum Protect. Para obtener información sobre creación de planificaciones en el servidor, consulte la documentación del servidor de IBM Spectrum Protect.

2. Utilice el mandato de servidor **GRANT PROXY** para otorgar autorización de proxy al nodo actual del cliente de archivado y copia de seguridad en cada nodo que represente al cliente de FastBack creado en el paso 1. El nodo de FastBack debe ser el destino y el nodo actual del cliente debe ser el proxy. Se trata de una configuración única y la realiza el Centro de administración si es este el que inicia la copia de seguridad o archivado.
3. Ejecute el mandato **set password** para almacenar las credenciales de los repositorios de FastBack donde se conecta el cliente de archivado y copia de seguridad. Ejecute el mandato `set password -type=fastback` una vez para cada repositorio donde esté previsto que se conecte el cliente de copia de seguridad y archivado.

Las credenciales que se almacenan dependen de las siguientes configuraciones:

- Cliente de archivado y copia de seguridad del servidor de FastBack
- Cliente de archivado y copia de seguridad de FastBack Disaster Recovery Hub
- Cliente de copia de seguridad y archivado en una estación de trabajo proxy dedicada

Para obtener información sobre cómo integrar IBM Spectrum Protect y Tivoli Storage Manager FastBack, consulte Integración de Tivoli Storage Manager FastBack y IBM Spectrum Protect.

Conceptos relacionados:

“Requisitos de instalación de copia de seguridad y archivado de datos de cliente de Tivoli Storage Manager FastBack” en la página 11

Referencia relacionada:

“Establecer contraseña” en la página 784

Configuración y utilización del entorno en clúster

El término *clúster* tiene distintos significados en los distintos entornos. Puede significar alta disponibilidad, alto rendimiento, equilibrado de cargas, un entramado de sistemas informáticos o alguna combinación de estos términos.

Actualmente hay disponibles varios productos de clústeres para UNIX y Linux, y este apartado define los aspectos de un entorno en clúster que deben existir para que esta metodología de copia de seguridad funcione correctamente. Es necesario disponer de conocimientos básicos sobre las funciones de software del clúster. Las actividades relacionadas con el software de clúster, como por ejemplo el desarrollo de los scripts de inicio y detención de una aplicación, no se describen en este apartado.

Un entorno de clúster hace referencia a un entorno de UNIX o de Linux que presenta las características siguientes:

- Los discos se comparten entre estaciones de trabajo, ya sea de forma exclusiva (solamente un host accede al disco lógico cada vez) o de forma simultánea.
- Los discos parecen discos locales del host y no recursos de red.

Importante: Monte los sistemas de archivos de forma local para el sistema, no a través de un protocolo de compartición de archivos basado en una LAN, como por ejemplo el sistema de archivos de red (NFS).

- Los puntos de montaje de los discos locales son idénticos en cada host físico en el entorno (si el sistema de archivos `/group1_disk1` falla del NodoA al NodoB, se montará en el NodoB como `/grupo1_disco1`).

Visión general de entornos en clúster

Los entornos en clúster se pueden configurar de muchas formas distintas. En este apartado se describen las configuraciones de clúster más conocidas.

Activa/Activa: Agrupación de recursos de clúster

En una configuración activa/activa, cada nodo gestiona de forma activa al menos un recurso y se configura como copia de seguridad para uno o más recursos del clúster. Activa/activa es la forma más común de un entorno de clúster.

Activa/Pasiva: Tolerante a errores

En una configuración activa/pasiva, un nodo gestiona de forma activa el recurso.

El otro nodo solamente se utiliza si el nodo principal detecta un error y el recurso tiene que llevar a cabo una sustitución por anomalía. Un clúster activo/pasivo es un subtipo de un clúster activo/activo.

Acceso simultáneo

En una configuración simultánea, hay más de un nodo que gestiona un recurso. Cuando se produce un error, otros nodos continúan gestionando el recurso.

Configuración de un cliente de copia de seguridad/archivado en un entorno de clúster

El cliente de copia de seguridad/archivado de ha sido diseñado para gestionar la copia de seguridad de las unidades de clúster colocando el cliente de copia de seguridad/archivado en el contexto de los grupos de recursos del clúster.

Acerca de esta tarea

De esta forma se puede sacar partido a la acción de copia de seguridad de datos de recursos locales (en vez de tener que acceder a los datos a través de la red) para maximizar el rendimiento de la operación de copia de seguridad y para gestionar los datos de copia de seguridad relacionados con el grupo de recursos. Por consiguiente, el cliente de copia de seguridad/archivado siempre puede realizar copias de seguridad de datos en recursos de clúster como si los datos fueran datos locales y maximizar el rendimiento de copia de seguridad. De esta forma se garantiza que se realiza una copia de seguridad de los datos importantes de errores del sistema.

Por ejemplo, un entorno de clúster activo/activo tiene tres hosts físicos en el clúster denominados NodoA, NodoB y NodoC.

Los nodos tienen las siguientes calidades:

- NodeA posee el recurso de clúster con un sistema de archivos /A1 y /A2
- NodeB posee los recursos de cluster con sistemas de archivos /B1 y/B2
- NodeC posee los recursos de clúster con los sistemas de archivos /C1 y /C2

Nota: NodoA también puede tener dos volúmenes que no estén en clúster, /fs1 y /fs2, de los que se debe realizar copia de seguridad.

Para obtener el mejor rendimiento posible de la copia de seguridad, tal vez desee que todos los nodos del clúster realicen las copias de seguridad de los sistemas de archivos compartidos que poseen. Cuando se produce una sustitución por anomalía, las tareas de copia de seguridad del nodo que ha fallado pasan al nodo

en el que se ha producido la sustitución por anomalía. Por ejemplo, cuando se produce una sustitución por anomalía del NodoA al NodoB, la copia de seguridad de /A1 y de /A2 pasan al NodoB.

A continuación encontrará los requisitos previos antes de configurar el cliente de copia de seguridad/archivado para realizar una copia de seguridad de volúmenes en clúster y fuera del clúster:

- Se debe ejecutar un proceso del planificador del cliente de copia de seguridad/archivado para cada grupo de recursos que se vaya a proteger. En condiciones normales, cada nodo debería tener dos procesos del planificador: uno para los recursos del clúster y otro para los sistemas de archivo locales. Después de una anomalía, se inician procesos del planificador adicionales en un nodo para poder proteger los recursos que se han pasado a otro nodo.
- Los archivos de contraseñas del cliente de copia de seguridad/archivado se deben almacenar en discos del clúster para que después de la anomalía, la contraseña del cliente de copia de seguridad/archivado que se ha generado esté disponible para el nodo que toma el control.
- Los sistemas de archivos que se han de proteger como parte de un grupo de recursos se definen utilizando la opción del dominio del cliente de copia de seguridad/archivado. La opción del dominio se especifica en el archivo `dsm.sys`, que también debería estar almacenado en un disco del clúster para que el nodo que toma el control tenga acceso al mismo.

Lleve a cabo los pasos siguientes para configurar el cliente de copia de seguridad/archivado en un entorno de clúster.

Procedimiento

1. Registre las definiciones de nodo del cliente de archivado y copia de seguridad en el servidor IBM Spectrum Protect. Todos los nodos del clúster deben estar definidos en el servidor de IBM Spectrum Protect. Si se definen varios recursos de clúster en un entorno de clúster para la sustitución por anomalía independiente, se deben definir nombres de nodo exclusivos para cada grupo de recursos. Para la configuración de ejemplo anterior de un clúster activo/activo de tres vías, defina tres nodos (uno para cada recurso), tal como se muestra a continuación: (1) `Protect: IBM>register node nodeA nodeApw domain=standard`, (2) `Protect: IBM>register node nodeB nodeBpw domain=standard`, (3) `Protect: IBM>register node nodeC nodeCpw domain=standard`.
2. Configure el archivo de opciones del sistema del cliente de archivado y copia de seguridad. Cada nodo del clúster debe tener secciones independientes del servidor para cada grupo de recursos del clúster con el fin de realizar una copia de seguridad en cada archivo `dsm.sys` respectivo. Debe asegurarse de que las secciones del servidor sean idénticas en los archivos de opciones del sistema de cada nodo. De forma alternativa, puede colocar el archivo `dsm.sys` en una ubicación del clúster compartida. Las secciones de servidor definidas para realizar copias de seguridad de volúmenes con clústeres deben tener las siguientes características especiales:
 - La opción `nodename` debe hacer referencia al nombre del nodo del cliente registrado en el servidor de IBM Spectrum Protect. Si no se ha definido el nombre del nodo del cliente, el nombre del nodo toma de forma predeterminada el nombre del host del nodo, que entra en conflicto con otros nombres de nodo que se utilizan en el mismo sistema cliente.

Importante: Utilice la opción `nodename` para definir el nodo de cliente de forma explícita. `node`.

- La opción `tcpclientaddress` debe hacer referencia a la dirección IP de servicio del nodo del clúster.
 - La opción `passworddir` debe hacer referencia a un directorio de los volúmenes compartidos que forman parte del grupo de recursos de clúster.
 - Las opciones `errorlogname` y `schedlogname` deben hacer referencia a archivos de los volúmenes compartidos que forman parte del grupo de recursos de clúster para mantener un solo archivo de registro continuo.
 - Todas las sentencias `exclude` deben hacer referencia a archivos de los volúmenes compartidos que forman parte del grupo de recursos de clúster.
 - Si utiliza la opción `incl excl`, debe hacer referencia a una vía de acceso de archivo en los volúmenes compartidos que forme parte del grupo del clúster.
 - Los nombres de las secciones identificados con la opción `servername` deben ser idénticos en todos los sistemas.
3. Las demás opciones del cliente de copia de seguridad/archivado se pueden establecer como se desee. En el ejemplo siguiente, los tres nodos, `NodoA`, `NodoB` y `NodoC`, deben tener las siguientes tres secciones del servidor en sus archivos `dsm.sys`:

```
Servername      server1_nodeA
nodename        NodoA
commethod       tcpip
tcpport         1500
tcpserveraddress server1.example.com
tcpclientaddress nodeA.example.com
passwordaccess  generate
passworddir     /A1/tsm/pwd
managedservices schedule
schedlogname    /A1/tsm/dsmsched.log
errorlogname    /A1/tsm/errorlog.log
```

```
Servername      server1_nodeB
nodename        NodoB
commethod       tcpip
tcpport         1500
tcpserveraddress server1.example.com
tcpclientaddress nodeB.example.com
passwordaccess  generate
passworddir     /B1/tsm/pwd
managedservices schedule
schedlogname    /B1/tsm/dsmsched.log
errorlogname    /B1/tsm/errorlog.log
```

```
Servername      server1_nodeC
nodename        NodoC
commethod       tcpip
tcpport         1500
tcpserveraddress server1.example.com
tcpclientaddress nodeC.example.com
passwordaccess  generate
passworddir     /C1/tsm/pwd
managedservices schedule
schedlogname    /C1/tsm/dsmsched.log
errorlogname    /C1/tsm/errorlog.log
```

4. Configure el archivo de opciones de usuario del cliente de archivado y copia de seguridad. El archivo de opciones (`dsm.opt`) debe residir en los volúmenes compartidos del grupo de recursos del clúster. Defina la variable de entorno

DSM_CONFIG para que haga referencia a este archivo. Asegúrese de que el archivo dsm.opt tiene la siguiente configuración:

- El valor de la opción servername debe ser la sección del servidor del archivo dsm.sys que define parámetros para realizar copias de seguridad de volúmenes con clústeres.
- Defina los sistemas de archivos de clústeres para que se realicen copias de seguridad de los mismos con la opción domain.

Nota: Asegúrese de definir la opción de dominio en el archivo dsm.opt o especifique la opción en la planificación o en la línea de mandatos del cliente de copia de seguridad y archivado. Esto es para restringir las operaciones en clúster para recursos del clúster y las operaciones no en clúster para los recursos que no son del clúster.

En el ejemplo, los nodos NodoA, NodoB y NodoC tienen configurados sus respectivos archivos dsm.opt y la variable de entorno DSM_CONFIG tal como se indica a continuación:

NodoA:

1) Configure el archivo /A1/tsm/dsm.opt:

```
servername server1_nodeA
domain      /A1 /A2
```

2) Emita el mandato siguiente o inclúyalo en el perfil de usuario:

```
export DSM_CONFIG=/A1/tsm/dsm.opt
```

NodoB:

1) Configure el archivo /B1/tsm/dsm.opt:

```
servername server1_nodeB
domain      /B1 /B2
```

2) Emita el mandato siguiente o inclúyalo en el perfil de usuario:

```
export DSM_CONFIG=/B1/tsm/dsm.opt
```

NodoC:

1) Configure el archivo /C1/tsm/dsm.opt:

```
servername server1_nodeC
domain      /C1 /C2
```

2) Emita el mandato siguiente o inclúyalo en el perfil de usuario:

```
export DSM_CONFIG=/C1/tsm/dsm.opt
```

5. Configure las definiciones de planificación para cada grupo de recursos del clúster. Tras llevar a cabo la configuración básica, defina las planificaciones automáticas para que las copias de seguridad de los recursos del clúster cumplan los requisitos de copia de seguridad. El procedimiento ilustra la configuración de planificación utilizando el planificador incorporado de IBM Spectrum Protect. Si utiliza un planificador adquirido a un proveedor, consulte la documentación que le suministra el proveedor del planificador.
 - Defina una planificación en el dominio de política en el que están definidos los nodos del clúster. Asegúrese de que la ventana de inicio de la planificación es suficientemente grande para iniciar la planificación en el nodo de sustitución por anomalía si se produce un evento de anomalía o de recuperación tras error. Esto significa que la duración de la planificación

debe haberse establecido en un valor superior al tiempo que se tarda en llevar a cabo la copia de seguridad de los datos del clúster para ese nodo, en condiciones normales.

Si la reconexión se realiza en el intervalo de inicio de ese evento, se reiniciará el mandato planificado. Esta copia de seguridad incremental planificada vuelve a examinar los archivos enviados al servidor antes de la sustitución. Entonces, la copia de seguridad "vuelve" al lugar en el que se detuvo antes de la situación de sustitución.

En el ejemplo siguiente, la planificación `clus_backup` se define en el dominio estándar para iniciar la copia de seguridad cada día a las 12:30 A.M. con una duración establecida en dos horas (el tiempo normal para una copia de seguridad de los datos de cada nodo).

```
Protect: IBM>define schedule standard clus_backup action=incr  
starttime=00:30 startdate=TODAY Duration=2
```

- Asocie la planificación con todos los nodos del cliente de copia de seguridad/archivado definidos para realizar una copia de seguridad de los recursos del clúster del siguiente modo: (1) Protect: IBM>define association standard clus_backup nodeA, (2) Protect: IBM>define association standard clus_backup nodeB, (3) Protect: IBM>define association standard clus_backup nodeC.

6. Configure el servicio de planificador para realizar la copia de seguridad. En cada nodo cliente, se debe configurar un servicio de planificador para cada recursos del cual sea ese nodo responsable de realizar la copia de seguridad, en condiciones normales. La variable de entorno `DSM_CONFIG` de cada servicio de planificador de recursos debe establecerse para que haga referencia al archivo `dsm.opt` correspondiente a ese recursos. Para el ejemplo de configuración, se deben crear los siguientes scripts de shell para poder iniciar los procesos `dsmcad`, según convenga, desde cualquier nodo del clúster.

```
NodoA: /A1/tsm/startsched  
#!/bin/ksh  
export DSM_CONFIG=/A1/tsm/dsm.opt  
dsmcad  
NodoB: /B1/tsm/startsched  
#!/bin/ksh  
export DSM_CONFIG=/B1/tsm/dsm.opt  
dsmcad  
NodoC: /C1/tsm/startsched  
#!/bin/ksh  
export DSM_CONFIG=/C1/tsm/dsm.opt  
dsmcad
```

7. Defina el cliente de archivado y copia de seguridad en la aplicación del clúster. Para continuar con la copia de seguridad del recurso que ha fallado después de una condición de sustitución por anomalía, el servicio de planificador de IBM Spectrum Protect (para cada nodo del cliente del clúster) debe estar definido como recurso en la aplicación del clúster para poder participar en el proceso de sustitución por anomalía. Es necesario que sea así para poder proseguir con la copia de seguridad de los recursos anómalos desde el nodo que toma control del recurso. Si se produjera un error, la copia de seguridad del recurso que ha fallado sería incompleta. Los scripts de ejemplo del paso 5 se pueden asociar a los recursos del clúster para garantizar que se inician en los nodos del clúster mientras que los recursos de discos que se protegen pasan de un nodo a otro. Los pasos reales necesarios para configurar el servicio de planificador como recursos del clúster son específicos para el software del clúster. Consulte la documentación de su aplicación del clúster si desea información adicional.

8. Asegúrese de que se genere la contraseña de cada nodo y que se guarde en la memoria caché en la ubicación correcta que se ha especificado mediante la opción `passworddir`. Esta validación se puede realizar siguiendo estos pasos:
 - a. Compruebe que cada nodo se pueda conectar al servidor de IBM Spectrum Protect sin la solicitud de contraseña. Puede hacerlo ejecutando la interfaz de línea de mandatos del cliente de archivado y copia de seguridad y emitiendo el mandato siguiente en cada nodo:


```
#dsmc query session
```

Si se le solicita que indique su contraseña, escríbala para que el mandato se ejecute correctamente y vuelva a ejecutar el mandato. La segunda vez, el mandato se debería ejecutar sin que se le solicite la contraseña. Si se le solicita la contraseña, compruebe la configuración.
 - b. Compruebe que todos los demás nodos del clúster pueden iniciar sesiones en el servidor de IBM Spectrum Protect para el nodo que ha realizado la sustitución por anomalía. Puede hacerlo ejecutando los mismos mandatos, según se ha descrito en el paso anterior, en los nodos de copia de seguridad. Por ejemplo, para validar si el `NodoB` y el `NodoC` pueden iniciar una sesión como `NodoA` en el suceso de sustitución por anomalía sin que se le solicite la contraseña, ejecute los mandatos siguientes en el `NodoB` y en el `NodoC`

```
#export DSM_CONFIG=/A1/tsm/dsm.opt
#dsmc query session
```

La solicitud de la contraseña puede aparecer en esta ocasión, pero solo ahora. Si se le solicita la contraseña, es porque no estaba almacenada en la ubicación compartida correcta. Compruebe el valor de la opción `passworddir` que utiliza el `NodoA` y siga otra vez los pasos de configuración.
 - c. Asegúrese de que las planificaciones se ejecutan correctamente en cada nodo. Puede activar una planificación definiendo el tiempo de inicio de la planificación en `now`. Recuerde restablecer el tiempo de inicio tras finalizar la comprobación.


```
Protect: IBM>update sched standard clus_backup starttime=now
```
 - d. La sustitución por error y la recuperación tras error entre el `nodoA` y el `nodoB`, mientras el `nodoA` está en medio de la operación de copia de seguridad y la ventana de inicio de la planificación, siguen siendo válidas. Compruebe que la copia de seguridad incremental continúa ejecutándose y que finaliza correctamente tras una sustitución por anomalía y una recuperación por error.
 - e. Emita el mandato siguiente para que caduque la contraseña del nodo (`nodoA`). Asegúrese de que la copia de seguridad continúa normalmente en las operaciones normales del clúster, así como las operaciones de sustitución por anomalía y recuperación tras error:


```
Protect: IBM>update node nodeA forcep=yes
```
9. Configure el cliente de copia de seguridad/archivado para realizar una copia de seguridad de los recursos locales.
 - a. Defina nodos de cliente en el servidor de IBM Spectrum Protect. De los recursos locales nunca se debería realizar copia de seguridad ni archivado utilizando los nombres de nodo definidos para los datos del clúster de copia de seguridad. Si se hacen copias de seguridad de los volúmenes locales no definidos como recursos de clúster, se deben usar nombres de nodo independientes (e instancias de cliente independientes) tanto para los volúmenes con clústeres como para los volúmenes sin clústeres.

En el ejemplo siguiente, vamos a suponer que solamente el `NodoA` tiene sistemas de archivos locales `/fs1` y `/fs2` de los que se deba realizar copia

de seguridad. Para poder gestionar los recursos locales, registre un nodo NodeA_local en el servidor de IBM Spectrum Protect: Protect:
IBM>register node nodeA_local nodeA_localpw domain=standard.

- b. Añada una stanza independiente en cada archivo de opciones del sistema del nodo dsm.sys que tenga que hacer copia de seguridad de los recursos locales con las características especiales siguientes:
- El valor de la opción tcpclientaddress debe ser el nombre de host local o la dirección IP. Ésta es la dirección IP que se utiliza para el tráfico principal desde y hacia el nodo.
 - Si el cliente realiza copias de seguridad y restaura volúmenes sin clústeres sin estar conectado al clúster, el valor de la opción tcpclientaddress debe ser la dirección IP de arranque. Se trata de la dirección IP que se utiliza para iniciar el sistema (nodo) antes de que se una al clúster:

Sección de ejemplo para NodoA_local:

```
Servername      server1_nodeA_local
nodename        nodoA_local
commethod       tcpip
tcpport         1500
tcpserveraddress server1.example.com
tcpclientaddress nodeA_host.example.com
passwordaccess  generate
managedservices schedule
```

- c. Defina el archivo de opciones del usuario dsm.opt en una vía de acceso que esté en un recurso fuera del clúster.
- El valor de la opción servername debe ser la sección del servidor del archivo dsm.sys que define parámetros para realizar copias de seguridad de volúmenes con clústeres.
 - Utilice la opción de dominio para definir los sistemas de archivos fuera del clúster para que se realicen copias de seguridad de los mismos.

Nota: Asegúrese de definir la opción del dominio en el archivo dsm.opt o de especificar la opción en la planificación o en la línea de mandatos del cliente de copia de seguridad y archivado para restringir las operaciones de copia de seguridad/archivado a volúmenes fuera del clúster.

En el ejemplo siguiente, el nodoA utiliza el archivo /home/admin/dsm.opt siguiente y establece el entorno de DSM_CONFIG para que haga referencia a /home/admin/A1.dsm.opt.

Contenido de /home/admin/A1.dsm.opt

```
servername ibm_nodoA_local
domain      /fs1 /fs2
```

```
export DSM_CONFIG=/home/admin/A1.dsm.opt
```

- d. Defina y configure una planificación para llevar a cabo la copia de seguridad incremental para sistemas de archivos fuera del clúster.

```
Protect: IBM>define schedule standard local_backup action=incr
starttime=00:30 startdate=TODAY Duration=2
```

Asocie la planificación con todos los nodos del cliente de copia de seguridad/archivado definidos para realizar copia de seguridad de los recursos de fuera del clúster.

```
Protect: IBM>define association standard nodeA_local
```

10. Restaure los datos del sistema de archivos del clúster. Se realiza copia de seguridad de todos los volúmenes de un recurso del clúster bajo el nodo de

destino definido para ese recurso del clúster. Si tiene que restaurar los datos que residen en un volumen del clúster, puede hacerlo desde el nodo cliente que posee el recurso del clúster en el momento de la restauración. El cliente de copia de seguridad/archivado debe utilizar el mismo archivo de opciones de usuario (dsm.opt) que se utilizó durante la operación de copia de seguridad para restaurar los datos. No hay más requisitos de configuración necesarios para restaurar datos en volúmenes de clúster.

11. Restaure los datos del sistema de archivos locales. Se realiza copia de seguridad de los volúmenes fuera de clúster con un nombre de nodo independiente configurado para las operaciones fuera del clúster. Para restaurar los datos, el cliente de archivado y copia de seguridad debe utilizar el mismo archivo de opciones de usuario dsm.opt que se utilizó durante la copia de seguridad. En el ejemplo, establezca la variable de entorno DSM_CONFIG para que haga referencia a /home/admin/A1.dsm.opt antes de llevar a cabo una restauración del cliente para el nodo local nodeA_local.

Conceptos relacionados:

Capítulo 5, “Restauración de los datos”, en la página 237

Habilitación del acceso al cliente web en un entorno de clúster

Si se necesita acceso al cliente web de IBM Spectrum Protect durante una condición de migración tras error, tendrá que configurar el daemon de aceptación de clientes web asociado al clúster para poder llevar a cabo una migración tras error junto con el recurso de clúster.

Acerca de esta tarea

Tras completar los pasos de configuración que se describen en el apartado *Configuración del cliente de copia de seguridad/archivado en un entorno de clúster*, lleve a cabo los pasos adicionales que se describen a continuación para finalizar la configuración del acceso al cliente web:

Procedimiento

1. Configure el daemon de aceptación de clientes para gestionar el cliente web y el planificador. El daemon de aceptación de clientes se debe configurar para que gestione planificadores así como el acceso al cliente web. Así se reduce la cantidad de daemons que se tienen que configurar como aplicaciones de clúster y, por tanto, se simplifica la configuración y la administración. Cuando se produce una migración tras error, se inicia el aceptador de clientes en el nodo que gestiona el cambio de control.
2. Actualice la opción managedservices en el archivo de opciones del sistema dsm.sys en cada nodo para cada sección del servidor, tal como se muestra a continuación para el NodoA:

```
Servername      server1_NodoA
nodename        NodoA
commethod       tcpip
tcpport         1500
tcpserver       server1.example.com
tcpclientaddress nodeA.example.com
passwordaccess  generate
passworddir     /A1/tsm/pwd
schedlog        /A1/tsm/dsmsched.log
errorlogname    /A1/tsm/errorlog.log
managedservices webclient schedule
```

3. Configure el daemon de aceptación de clientes para que utilice un puerto HTTP conocido. De forma predeterminada, el daemon de aceptación de clientes utiliza el puerto HTTP 1581, cuando está disponible, para acceder al cliente web. Si el puerto no está disponible, el aceptador de clientes busca el primer puerto disponible, comenzando por el 1581. En una condición de migración tras error de una configuración de clúster activa-activa, probablemente haya un sistema host de clúster para la migración tras error que ejecute varias instancias del aceptador de clientes. Si se utilizan valores predeterminados para el puerto HTTP, el nodo de migración tras error utiliza cualquier puerto disponible para el aceptador de clientes que se migra, puesto que probablemente el puerto predeterminado está siendo utilizado por procesos actuales del aceptador de clientes del host de migración tras error. Esto ocasiona problemas para el cliente web asociado al aceptador de clientes que se ha migrado, puesto que los usuarios del cliente web no conocen el nuevo puerto HTTP. httpport puede utilizar la opción de especificar los puertos concretos para el acceso al cliente web de este recurso. Así podrá utilizar el mismo puerto cuando se conecte desde un navegador web, independientemente del nodo que preste servicio al recurso del clúster. Añada la opción httpport en el archivo de opciones del sistema (dsm.sys) en cada nodo para cada sección del servidor tal como se indica a continuación, asegurándose de que cada sección utilice un valor exclusivo:

```
Servername      server1_NodoA
nodename        NodoA
commethod       tcpip
tcpp            1500
tcps            server1.example.com
tcpclientaddress nodeA.example.com
passwordaccess  generate
passworddir     /A1/tsm/pwd
managedservices webclient schedule
schedlogn       /A1/tsm/dsmsched.log
errorlogname    /A1/tsm/errorlog.log
httpport        1510
```

```
Servername      server1_NodoB
nodename        NodoB
commethod       tcpip
tcpp            1500
tcps            server1.example.com
tcpclientaddress nodeB.example.com
passwordaccess  generate
passworddir     /B1/tsm/pwd
managedservices webclient schedule
schedlogn       /B1/tsm/dsmsched.log
errorlogname    /B1/tsm/errorlog.log
httpport        1511
```

```
Servername      server1_NodoC
nodename        NodoC
commethod       tcpip
tcpp            1500
tcps            server1.example.com
tcpclientaddress nodeC.example.com
passwordaccess  generate
passworddir     /C1/tsm/pwd
managedservices webclient schedule
schedlogn       /C1/tsm/dsmsched.log
errorlogname    /C1/tsm/errorlog.log
httpport        1512
```

Migración de configuraciones de AIXIBM PowerHA SystemMirror antiguas

Si actualmente utiliza el cliente de copia de seguridad y archivado en un entorno IBM PowerHA SystemMirror mediante la opción `clusternode`, debe actualizar las configuraciones actuales. La opción `clusternode` ya no está admitida.

Acerca de esta tarea

Siga estos pasos para actualizar sus configuraciones actuales:

Procedimiento

1. Actualice el archivo de opciones del sistema del cliente de archivado y copia de seguridad. Al igual que con la opción `clusternode`, cada nodo del clúster debe continuar teniendo secciones de servidor independientes para cada grupo de recursos del clúster con el fin de realizar una copia de seguridad en cada archivo `dsm.sys` respectivo. El archivo `dsm.sys` existente para `NodoA` puede parecerse al siguiente:

```
Servername      server1_nodoA
commethod       tcpip
tcpp            1500
tcps            server1.example.com
tcpclientaddress nodoA.example.com
passwordaccess  generate
passworddir     /A1
clusternode     yes
managedservices schedule
schedlogn       /A1/dsmsched.log
errorlogname    /A1/errorlog.log
```

2. Observe que en este ejemplo se utiliza la opción `nodename`. Realice los cambios siguientes en el archivo `dsm.sys` existente para `NodoA`.
 - Elimine la opción `clusternode`.
 - Especifique una opción `nodename` si todavía no lo ha hecho.
3. En nuevo archivo `dsm.sys` para `NodoA` debería parecerse al siguiente:

```
Servername      server1_nodoA
commethod       tcpip
nodename        myclus (myclus is the existing cluster name )
tcpp            1500
tcps            server1.example.com
tcpclientaddress nodoA.example.com
passwordaccess  generate
passworddir     /A1
managedservices schedule
schedlogn       /A1/dsmsched.log
errorlogname    /A1/errorlog.log
```

4. Registre los nodos del cliente de archivado y copia de seguridad en el servidor IBM Spectrum Protect. Si en el primer paso se agregan nuevos nodos del cliente de copia de seguridad/archivado para sustituir el valor actual predeterminado del nombre del nodo de clúster, registre esos nodos en el servidor de IBM Spectrum Protect.
5. Actualice las definiciones de planificación. Si se añaden nuevos nodos del cliente de copia de seguridad/archivado en el paso anterior, asegúrese de que las definiciones de planificación de copia de seguridad que se han utilizado antes de realizar la copia de seguridad de estos datos de nodo estén asociadas a los nombres de los nuevos nodos del cliente.

6. Valide la configuración. Para obtener más información detallada, consulte “Configuración de un cliente de copia de seguridad/archivado en un entorno de clúster” en la página 104.

Consideraciones para la configuración de AIX antes de realizar copias de seguridad y archivado basadas en instantáneas

Si está configurando el cliente de IBM Spectrum Protect de AIX para que realice copias de seguridad y archivado basadas en instantáneas, debe tener en cuenta algunos elementos.

- Asegúrese de que el grupo de volúmenes que contiene el sistema de archivos del que realizará la instantánea tiene espacio de disco suficiente para que se creen instantáneas externas JFS2 para el sistema de archivos.
- El cliente utiliza un tamaño predeterminado del 100 por cien del tamaño del sistema de archivos. Este valor ha demostrado ser el más adecuado para los sistemas de archivo, incluso si la actividad del sistema de archivos es moderada. Si necesita disminuir este valor según su experiencia con su propia actividad del sistema de archivos, puede utilizar la opción `snapshotcachesize` para ajustar con más precisión este valor.
- No active las instantáneas internas cuando cree nuevos sistemas de archivos JFS2 en AIX 6.1 o posterior para todos los sistemas de archivos gestionados por IBM Spectrum Protect. El cliente utiliza instantáneas externas y JFS2 no permite crear instantáneas externas e internas al mismo tiempo para el mismo sistema de archivos.

Referencia relacionada:

“`Snapshotcachesize`” en la página 567

Configuración de NetApp y IBM Spectrum Protect para copias de seguridad incrementales de diferencia de instantánea

Debe configurar información del conexión del servidor de archivos de NetApp para ejecutar el mandato de copia de seguridad incremental de diferencia de instantánea en el cliente de copia de seguridad y archivado. Debe utilizar el mandato **set password** para especificar el nombre de host del sistema de archivos y el nombre de usuario que se utiliza para acceder al servidor de archivos.

Antes de empezar

Procedimiento

1. Establezca una sesión de consola en el archivador NetApp y defina un nuevo usuario en el servidor de archivos siguiendo los pasos indicados a continuación:
 - a. Añada el ID de usuario a un grupo que permita a los usuarios iniciar sesión en el servidor de archivos con mandatos `http` y de ejecución de API.
 - b. Desde el servidor de archivos, especifique el siguiente mandato para listar el ID de usuario para verificar los valores y verificar que la salida es similar:

```
useradmin user list snapdiff_user
```

Nombre: snapdiff_user
Info:
Identificador de registro: 131077
Grupos: snapdiff_group
Nombre completo:

En los gestores de archivos 7-mode de NetApp:

Prestaciones permitidas: login-http-admin,api-*

Para los gestores de archivos ONTAP NetApp de datos en clúster, la única funcionalidad necesaria es `ontapapi` con el rol `admin`.

- c. Si la opción **`security.passwd.firstlogin.enable`** para el ID de usuario en el servidor de NetApp está definida en `on`, asegúrese de que todos los grupos tienen las prestaciones **`login-telnet`** y **`cli-passwd*`**.

Consejo: Cuando se habilita la opción **`security.passwd.firstlogin.enable`**, el ID de usuario se establece como caducado cuando se crea. El usuario no puede ejecutar ningún mandato, incluido el de seguridad incremental mediante instantáneas, hasta que se cambie la contraseña. Los usuarios en los grupos que no tienen estas prestaciones no pueden iniciar sesión en el sistema de almacenamiento. Para obtener información sobre cómo definir un ID de usuario y una contraseña en el servidor de archivos de NetApp, consulte la documentación de NetApp.

2. Configure el servidor HTTP incorporado en NetApp Data ONTAP para permitir sesiones remotas de administración en el archivador NetApp.
 - a. Si tiene previsto utilizar una conexión HTTP sencilla para las copias de seguridad diferenciales de instantáneas, active la opción **`httpd.admin.enable`** en el archivador NetApp.
 - b. Si tiene previsto utilizar una conexión HTTPS segura para las copias de seguridad diferenciales de instantáneas (especificando la opción **`-snapdiffhttps`**), active la opción **`httpd.admin.ssl.enable`** en el archivador NetApp.
 - c. Desde el nodo de cliente de IBM Spectrum Protect, compruebe la conexión entre el sistema cliente de IBM Spectrum Protect y el servidor NetApp ONTAP para asegurarse de que los cortafuegos u otras opciones de configuración de NetApp no le impiden conectarse al servidor NetApp.

Consejo: Consulte la documentación sobre NetApp ONTAP para conocer instrucciones sobre cómo comprobar la conexión.

3. Exporte los volúmenes de NetApp y tenga en cuenta los siguientes ajustes:

Consejo: Consulte la documentación de NetApp para obtener información sobre cómo exportar los volúmenes de NetApp para utilizarlos con hosts Linux.

- Correlacione los volúmenes de NetApp utilizando un montaje NFS.
- Asegúrese de que los volúmenes de NetApp tienen valores de seguridad UNIX

4. Defina el ID de usuario y la contraseña en el cliente de copia de seguridad y archivado para el ID de usuario que creó en el paso 1 en la página 114 mediante los siguientes pasos:
 - a. Inicie sesión con ID de usuario `root`.
 - b. Desde la línea de mandatos del cliente de copia de seguridad y archivado, especifique el siguiente mandato:

```
dsmc set password -type=filer my_file_server snapdiff_user newPassword
```

Sustituya los siguientes valores:

my_file_server

Este valor es el nombre de host completo del servidor de archivos NetApp.

snapdiff_user

Este valor es el ID de usuario que creó en el paso 1 en la página 114.

newPassword

Este valor es la contraseña para el ID de usuario que creó en el paso 1 en la página 114.

Tareas relacionadas:

“Protección de volúmenes de servidor de archivos ONTAP NetApp de datos en clúster”

Referencia relacionada:

“Snapdiff” en la página 561

“Snapdiffhttps” en la página 566

“Createnewbase” en la página 373

Protección de volúmenes de servidor de archivos ONTAP NetApp de datos en clúster

Puede crear una copia de seguridad incremental diferencial de instantánea de un volumen que esté en un servidor de archivos NetApp que forme parte de una configuración ONTAP de datos en clúster (servidor de archivos de modalidad-c).

Antes de empezar

- Lleve a cabo el procedimiento de “Configuración de NetApp y IBM Spectrum Protect para copias de seguridad incrementales de diferencia de instantánea” en la página 114.
- Asegúrese de que el administrador de la máquina virtual de almacenamiento NetApp haya configurado correctamente entorno ONTAP de datos en clúster.

Restricción:

- El soporte de IBM Spectrum Protect para copias de seguridad incrementales de diferencia de instantánea de volúmenes ONTAP de datos en clúster se soporta solo en NetApp ONTAP 8.2.1 y versiones posteriores.

Acerca de esta tarea

En un entorno ONTAP de datos en clúster, las máquinas virtuales de almacenamiento (también conocidas como vServers de datos) contienen volúmenes de datos que se pueden proteger mediante el cliente de copia de seguridad y archivado.

Una máquina virtual consta de un solo volumen infinito de uno o varios volúmenes flex. Se accede a los volúmenes de forma remota mediante el uso compartido de archivos (CIFS en sistemas operativos Windows, NFS en sistemas operativos Linux).

Las máquinas virtuales de almacenamiento se gestionan mediante el archivador de gestión de clústeres, que es el archivador físico (el archivador c-mode) en el que residen las máquinas virtuales de almacenamiento. El cliente de copia de seguridad está instalado en la máquina remota que accede a los volúmenes.

El cliente de archivado y copia de seguridad se tiene que configurar con credenciales para los gestores de archivos c-mode de NetApp a los que se accede para las operaciones de seguridad.

Requisitos:

- Se necesita la siguiente información para este procedimiento:
 - El nombre de host o la dirección IP del archivador de gestión de clústeres.
 - El nombre de host o la dirección IP de la máquina virtual de almacenamiento
 - El nombre de la máquina virtual de almacenamiento.
 - Las credenciales del archivador de gestión de clústeres (nombre de usuario y contraseña).
- Al usuario gestor de archivos de gestión de clústeres configurado por el cliente se le tiene que asignar la funcionalidad `ontapapi` con el rol `admin`.

La funcionalidad `ontapapi` no permite el acceso interactivo al gestor de archivos con métodos como `telnet`, `ssh` o `http/https`. No se necesita ninguna otra funcionalidad de usuario para ejecutar copias de seguridad incrementales de instantáneas.

Procedimiento

Siga los pasos siguientes en la máquina remota en la que se ha instalado el cliente de copia de seguridad y archivado:

1. Configure el cliente de archivado y copia de seguridad con las credenciales del gestor de archivos de gestión de clústeres. Utilice el mandato **`dsmd set password`** para almacenar las credenciales del gestor de archivos de gestión asociado a la máquina virtual de almacenamiento. Por ejemplo, escriba el siguiente mandato:

```
dsmd set password -type=filer management_filer_hostname  
management_filer_username management_filer_password
```

Donde:

management_filer_hostname

El nombre de host o la dirección IP del archivador de gestión de clústeres.

management_filer_username

El nombre de usuario del archivador de gestión de clústeres.

management_filer_password

La contraseña del usuario del archivador de gestión de clústeres.

Consejo: La contraseña del gestor de archivos de gestión de clústeres se cifra cuando se almacena mediante el cliente de archivado y copia de seguridad.

2. Asocie cada máquina virtual de almacenamiento con el archivador de gestión mediante el mandato **`dsmd set netappsvm`**. Por ejemplo, escriba el siguiente mandato:

```
dsmd set netappsvm management_filer_hostname  
storage_virtual_machine_hostname storage_virtual_machine_name
```

Donde:

management_filer_hostname

El nombre de host o la dirección IP del archivador de gestión de clústeres.

storage_virtual_machine_hostname

El nombre de host o la dirección IP de la máquina virtual de almacenamiento que se utiliza para montar los volúmenes que se van a copiar.

storage_virtual_machine_name

El nombre de la máquina virtual de almacenamiento.

Nota: El nombre de host o la dirección IP de la máquina virtual de almacenamiento que se utiliza para montar los volúmenes debe ser coherente con lo que se ha especificado en los mandatos **dsmc set**. Por ejemplo, si los volúmenes están montados con una dirección IP de máquina virtual de almacenamiento, se debe utilizar la dirección IP (no el nombre de host) en los mandatos **dsmc set**. De lo contrario, la autenticación de cliente con el archivador de gestión de clústeres fallará.

Solo tiene que especificar el mandato **dsmc set netappsvm** una vez para cada máquina virtual de almacenamiento. Si la máquina virtual de almacenamiento se mueva a otro archivador de gestión de clústeres, debe utilizar el mandato para actualizar el nombre de host del archivador de gestión de clústeres actualizado.

3. Monte la máquina virtual de almacenamiento en un sistema de archivos local. Por ejemplo, escriba el siguiente mandato para cada máquina virtual de almacenamiento:

```
mount storage_virtual_machine_hostname/tmp/fs1
```

Donde:

storage_virtual_machine_hostname

El nombre de host o la dirección IP de la máquina virtual de almacenamiento

/tmp/fs1

Un ejemplo de un sistema de archivos en el que montar el volumen de la máquina virtual de almacenamiento.

4. Inicie una copia de seguridad incremental progresiva de un volumen flex o infinito.

De forma predeterminada, el acceso HTTP al servidor de archivos NetApp no está habilitado. Si no ha configurado el servidor de archivos para permitir acceso utilizando HTTP, use la opción **snappdiffhttps** del cliente de archivado y copia de seguridad para permitir el acceso al servidor de gestión de clústeres con el protocolo HTTPS.

Por ejemplo, en clientes Linux, indique el mandato siguiente:

```
dsmc incr /tmp/fs1 -snappdiff -snappdiffhttps
```

Consejo: Solo tiene que ejecutar la copia de seguridad incremental progresiva completa una vez. Una vez realizada correctamente la copia de seguridad, se ejecutan copias de seguridad diferenciales en futuras operaciones de copia de seguridad.

5. Inicie una copia de seguridad diferencial de instantánea del volumen flex o infinito.

Por ejemplo, en clientes Linux, indique el mandato siguiente:

```
dsmc incr /tmp/fs1 -snappdiff -snappdiffhttps
```

Ejemplo

Un usuario cliente de copia de seguridad y archivado desea completar una copia de seguridad incremental diferencial de instantánea de los volúmenes de un servidor de archivos c-mode. El usuario utiliza el cliente de copia de seguridad y archivado de Windows para realizar la copia de seguridad y los volúmenes están montados en unidades compartidas CIFS. La configuración del archivador c-mode es la siguiente:

Archivador de gestión ONTAP 8.31

```
Hostname: netapplmgmt.example.com
User: netapplmgmt_user
Password: pass4netapplmgmt
CIFS Domain Controller: WINDC
Domain User: domainuser
```

Máquina virtual de almacenamiento de volumen flex

```
Hostname: netappl-v1.example.com
Storage virtual machine name: netappl-client1
CIFS share: demovol
Volume name: demovol
```

Máquina virtual de almacenamiento de volumen infinito

```
Hostname: netappl-v4.example.com
Storage virtual machine name: netappl-infiniteVolume1
CIFS Share: InfiniteVol
```

El usuario lleva a cabo los pasos siguientes en el cliente de copia de seguridad y archivado:

1. Configure el cliente con las credenciales del gestor de archivos de gestión emitiendo el siguiente mandato:

```
dsmc set password -type=filer netapplmgmt.example.com netapplmgmt_user
pass4netapplmgmt
```

2. Defina asociaciones de máquinas virtuales de almacenamiento para cada máquina virtual de almacenamiento con los mandatos siguientes:

```
dsmc set netappsvm netapplmgmt.example.com netappl-v1.example.com
netappl-client1
```

```
dsmc set netappsvm netapplmgmt.example.com netappl-v4.example.com
netappl-infiniteVolume1
```

3. Correlaciona volúmenes remotos con letras de unidad para cada máquina virtual:

```
net use y: \\netappl-v1.example.com\demovol WINDC\domainuser
```

```
net use z: \\netappl-v4.example.com\InfiniteVol WINDC\domainuser
```

4. Ejecuta una copia de seguridad incremental progresiva completa del volumen flex y del volumen infinito:

```
dsmc incr y: -snapdiff -snapdiffhttps
```

```
dsmc incr z: -snapdiff -snapdiffhttps
```

Solo tiene que ejecutar la copia de seguridad incremental progresiva completa una vez. Una vez realizada correctamente la copia de seguridad, se ejecutan copias de seguridad diferenciales en futuras operaciones de copia de seguridad.

5. Ejecuta una copia de seguridad diferencial de instantánea del volumen flex y del volumen infinito:

```
dsmc incr y: -snapdiff -snapdiffhttps
```

```
dsmc incr z: -snapdiff -snapdiffhttps
```

Soporte de SnapMirror para la copia de seguridad a incrementos progresivos asistida por instantáneas NetApp (snapdiff)

Puede utilizar el proceso de copia de seguridad SnapDiff de NetApp junto con la réplica SnapMirror de NetApp para realizar una copia de seguridad de volúmenes de archivos de destino u origen NetApp.

En un entorno NetApp SnapMirror, los datos que están en volúmenes asociados al centro de datos primario se copian en volúmenes asociados a un servidor remoto ubicado en un sitio de recuperación ante desastres. El archivador NetApp del centro de datos primario se denomina archivador de origen; el archivador NetApp del sitio de recuperación ante desastres se denomina archivador de destino. Puede utilizar el cliente de archivado y copia de seguridad para crear copias de seguridad diferenciales de instantánea de los volúmenes del archivador de origen o destino.

Escenario: Copia de seguridad de datos en un volumen de archivador de origen

Puede configurar el cliente de archivado y copia de seguridad para realizar copias de seguridad de los datos de volúmenes del archivador de origen. Este escenario requiere la configuración de un nodo cliente de archivado y copia de seguridad que tenga acceso a los volúmenes de archivador de origen NetApp utilizando NFS exportadas para montar los volúmenes del archivador.

Por ejemplo, suponga que tiene una configuración en la que el archivador de origen se llama ProdFiler. Suponga que existe un volumen llamado UserDataVol en el archivador ProdFiler y que el volumen es accesible utilizando NFS desde un nodo cliente de archivado y copia de seguridad. Suponga que la acción se monta como UserDataVol_Share.

Cuando inicia una copia de seguridad diferencial de instantánea, el archivador NetApp crea una nueva instantánea diferencial en el volumen que se está copiando. La instantánea diferencial se compara con la instantánea base (anterior). El nombre de la instantánea base se registró en el servidor IBM Spectrum Protect cuando se completó la copia de seguridad anterior. El contenido de la instantánea base se compara con la instantánea diferencial creada en el volumen del archivador de origen. Las diferencias entre las dos instantáneas se copian en el servidor.

Para iniciar la copia de seguridad diferencial de la instantánea se utiliza el mandato indicado a continuación. El comando se especifica en la consola de un nodo cliente configurado para acceder y proteger los volúmenes del archivador de origen. Dado que este mandato se emite para realizar copias de seguridad de volúmenes de un archivador de origen, se crea una nueva instantánea (la instantánea diferencial) y la instantánea registrada en el servidor de IBM Spectrum Protect se utiliza como instantánea base. La creación de ambas instantáneas, diferencial y base, es el comportamiento predeterminado; la opción `-diffsnapshot=create` es un valor predeterminado y no es necesario que se especifique de manera explícita en este mandato.

```
dsmc incr \\ProdFiler\UserDataVol_Share -snapdiff -diffsnapshot=create
```

Datos de copia de seguridad en un archivador de destino

Una configuración más típica consiste en descargar las copias de seguridad del archivador de origen creando copias de seguridad de los volúmenes de origen mediante el uso de instantáneas de volumen replicadas almacenadas en el

archivador de destino. Por lo general, realizar una copia de seguridad de un archivador de destino presenta un problema, ya que la creación de una copia de seguridad de instantánea diferencial requiere que se cree una nueva instantánea en el volumen del que está realizando la copia de seguridad. Los volúmenes del archivador de destino que duplican el contenido de los volúmenes de origen son volúmenes de solo lectura, por lo que no se pueden crear instantáneas en los mismos.

Para solucionar esta restricción de solo lectura, se proporcionan opciones de configuración del cliente que le permiten utilizar las instantáneas diferencial y base existentes en el volumen de destino de solo lectura para copiar los cambios en el servidor de IBM Spectrum Protect.

Al igual que en el escenario del archivador de origen, a los volúmenes del archivador de destino se accede utilizando acciones exportadas NFS.

Resumen de opciones diferenciales de instantánea

La opción `useexistingbase` hace que la instantánea más reciente del volumen se utilice como instantánea base cuando se deba establecer una instantánea base. Cuando una de las condiciones indicadas a continuación sea verdadera, se establecerá una instantánea base:

- Cuando esta copia de seguridad es la copia de seguridad inicial.
- Cuando se especifica `createnewbase=yes`.
- Cuando la instantánea base registrada por una instantánea diferencial anterior ya no existe, y no existe una instantánea más antigua que la instantánea que falta.

Si no se especifica esta opción, se crea una nueva instantánea en el volumen del que se está realizando una copia de seguridad. Dado que los volúmenes del archivador de destino son de solo lectura, se debe especificar `useexistingbase` al crear copias de seguridad diferenciales de instantánea de dichos volúmenes. Si no se especifica `useexistingbase`, las copias de seguridad diferenciales de instantánea de un volumen de archivador de destino fallan porque no se puede crear la instantánea nueva en el volumen de solo lectura.

Cuando realice una copia de seguridad de volúmenes de archivador de destino, utilice las opciones `useexistingbase` y `diffsnapshot=latest` para asegurarse de que se usan las instantáneas diferencial y base más recientes.

Utilice la opción `basesnapshotname` para especificar qué instantánea del volumen de archivador de destino desea utilizar como instantánea base. Si no especifica esta opción, se utilizará la instantánea más reciente del volumen del archivador de destino como instantánea base. Puede utilizar caracteres comodín para especificar el nombre de la instantánea base.

Utilice la opción `diffsnapshotname` para especificar qué instantánea diferencial del volumen de archivador de destino desea utilizar durante la copia de seguridad diferencial. Esta opción sólo se especifica si también se especifica `diffsnapshot=latest`. Puede utilizar caracteres comodín para especificar el nombre de la instantánea diferencial.

La opción `diffsnapshot=latest` especifica que desea utilizar la última instantánea encontrada en el servidor de archivos como instantánea de origen.

En los temas de *Referencia sobre opciones de cliente* se proporciona información adicional sobre cada una de estas opciones.

Ejemplos de mandato de copia de seguridad diferencial de instantánea

En los ejemplos indicados a continuación, se considera que se replican los volúmenes de un archivador de origen utilizando la tecnología SnapMirror de NetApp en un archivador de recuperación tras desastre (su nombre de host es DRFiler). Dado que los volúmenes de DRFiler son de solo lectura, utilice las opciones para especificar qué instantáneas replicadas desea utilizar como instantánea base y cuál como instantánea diferencial. Especificando las instantáneas que desea utilizar al crear una copia de seguridad diferencial de un archivador de destino, no se intenta crear una instantánea en volúmenes de solo lectura.

Para iniciar copias de seguridad diferenciales de instantánea se utilizan los siguientes mandatos. La mayoría de los mandatos crean copias de seguridad diferenciales utilizando instantáneas almacenadas en volúmenes del archivador de destino. Al realizar una copia de seguridad de un volumen de archivador de destino, asegúrese de incluir la opción `-useexistingbase`, ya que esta evita el intento de creación de una nueva instantánea en los volúmenes del archivador de destino de solo lectura.

Ejemplo 1: Copia de seguridad de un archivador de destino utilizando copias de seguridad nocturnas predeterminadas creadas por el planificador de instantáneas de NetApp

```
dsmc incr \\DRFiler\UserDataVol_Share -snapdiff -useexistingbase  
-diffsnapshot=latest -basesnapshotname="nightly.?"
```

Puede utilizar una interrogación (?) para que coincida con un carácter individual. En este ejemplo, `-basesnapshotname=nightly.?` se utiliza la última instantánea base, llamada "nightly.", seguida de un carácter individual (por ejemplo: `nightly.0`, `nightly.1`, etc.).

Ejemplo 2. Copia de seguridad de un archivador de destino utilizando copias de seguridad creadas manualmente (no creadas por el planificador de instantáneas de NetApp)

```
dsmc incr \\DRFiler\UserDataVol_Share -snapdiff -useexistingbase  
-diffsnapshot=latest -basesnapshotname="share_vol_base?"  
-diffsnapshotname="share_vol_diff?"
```

Este ejemplo también utiliza interrogaciones (?) como comodín para ilustrar la sintaxis si los nombres de la instantánea base y diferencial tienen números diferentes como parte de este.

Ejemplo 3. Copia de seguridad de un volumen de archivador de destino especificando que instantáneas utilizar como instantánea base y diferencial

```
dsmc incr \\DRFiler\UserDataVol_Share -snapdiff -useexistingbase  
-diffsnapshot=latest -basesnapshotname="share_vol_base"  
-diffsnapshotname="share_vol_diff_snap"
```

Ejemplo 4: Copia de seguridad de instantáneas generadas por script que utilizan la convención de nomenclatura

En este ejemplo, un script que se ejecuta en el archivador NetApp añade una indicación de fecha y hora a los nombres de las instantáneas. Por ejemplo, una instantánea creada el 3 de noviembre de 2012 a las 11:36:33 PM se llamará `UserDataVol_20121103233633_snapshot`. Puede utilizar comodines con las opciones para seleccionar las instantáneas diferencial y base más recientes. Por ejemplo:

```
dsmc incr \\DRFiler\UserDataVol_Share -snapdiff -useexistingbase
-basesnapshotname="UserDataVol_Share_*_snapshot" -diffsnapshot=latest
-diffnsnapshotname="UserDataVol_Share_*_snapshot"
```

-useexistingbase selecciona la instantánea base más reciente. Si añade un asterisco (*) a -basesnapshotname seleccionará la instantánea base más reciente que sigue la convención de nomenclatura de scripts. La opción -diffsnapshot=latest suprime la creación de una nueva instantánea diferencial y -diffsnapshotname= selecciona la instantánea diferencial más reciente que sigue la convención de nomenclatura de scripts. (El comodín asterisco coincide con cualquier serie).

Ejemplo 5: Realiza una copia de seguridad diferencial utilizando una instantánea diferencial existente en el archivador de origen

Para utilizar una instantánea diferencial existente en el archivador de origen, utilice -diffsnapshot=latest para evitar la creación de una instantánea diferencial nueva. Utilice también la opción -diffsnapshotname para especificar la instantánea diferencial existente que desea utilizar. La instantánea que especifique se compara con la instantánea base, registrada en la base de datos de servidor de IBM Spectrum Protect durante la creación de la última copia de seguridad. Por ejemplo:

```
dsmc incr \\ProdFiler\UserDataVol_Share -snapdiff -diffsnapshot=latest
-diffsnapshotname="share_vol_diff_snap"
```

Registrar la estación de trabajo en un servidor

Para poder utilizar IBM Spectrum Protect, es necesario configurar un nombre de nodo y una contraseña y el nodo debe registrarse con el servidor.

El proceso de configuración de un nombre de nodo y una contraseña se conoce como *inscripción*. Hay dos tipos de registro disponibles, *abiertos* y *cerrados*.

El administrador del servidor de IBM Spectrum Protect elige el tipo de registro del sitio.

Debe ser un usuario root o usuario autorizado para poder realizar esta tarea.

Si quiere utilizar el cliente web, necesita un ID de usuario de administración con privilegio de sistema, privilegio de política, autorización de acceso a cliente o autorización de propietario de cliente. Si se registra un nuevo nodo, el administrador del servidor tiene que crear un ID de usuario de administración que coincida con el nombre del nodo. De forma predeterminada, este nodo tiene autorización de propietario de cliente.

El administrador del servidor de IBM Spectrum Protect tiene que especificar el parámetro `userid` con el mandato de servidor **REGISTER NODE**:

```
REGISTER NODE nombre_nodo contraseña userid=ID_usuario
```

donde el nombre de nodo y el ID de usuario de administración tienen que ser iguales. Por ejemplo:

```
REGISTER NODE node_a mypassw0rd userid=node_a
```

Inscripción cerrada

Con la inscripción cerrada, el administrador de IBM Spectrum Protect debe inscribir su estación de trabajo como nodo cliente en el servidor. Si la empresa utiliza una inscripción cerrada, deberá proporcionar la información siguiente al administrador de IBM Spectrum Protect .

Acerca de esta tarea

Debe proporcionar los siguientes elementos a su administrador de IBM Spectrum Protect:

- El nombre de nodo (el valor que devuelve el mandato **hostname** , el nombre de la estación de trabajo o el nombre de nodo que especifica con la opción **nodename**). Si no especifica un nombre de nodo con la opción **nodename**, el ID de inicio de sesión predeterminado es el mismo que el que devuelve el mandato **hostname**.
- La contraseña inicial que desea utilizar, si es necesario.
- Información de contacto, como nombre, identificador de usuario y número de teléfono.

El administrador de IBM Spectrum Protect define los siguiente:

- El dominio de políticas al que pertenece el nodo cliente. Un dominio de políticas contiene juegos de políticas y clases de gestión que controlan cómo gestiona IBM Spectrum Protect los archivos de los que hace copia de seguridad y copias archivadas.
- Si se pueden comprimir los archivos antes de enviarlos al servidor.
- Si puede eliminar datos archivados y de copia de seguridad del almacenamiento del servidor.

Inscripción abierta

Con la inscripción abierta, un administrador del sistema puede inscribir la estación de trabajo como un nodo cliente con el servidor de IBM Spectrum Protect.

Acerca de esta tarea

La primera vez que se inicia una sesión, se le solicitará la información necesaria para inscribir su estación de trabajo en el servidor de IBM Spectrum Protect identificado en el archivo de opciones del cliente. Debe proporcionar el nombre de nodo, una contraseña e información de contacto.

Al utilizar la inscripción abierta:

- El nodo cliente se asigna a un dominio de políticas denominado **standard**.
- Puede suprimir copias archivadas de archivos del almacenamiento del servidor, pero no versiones de copia de seguridad de archivos.

Si es necesario, el administrador de IBM Spectrum Protect puede modificar estos valores predeterminados posteriormente.

Creación de una lista de inclusión/exclusión

Si no crea una lista de inclusión/exclusión, el cliente de copia de seguridad y archivado tiene en cuenta todos los archivos para los servicios de copia de seguridad y utiliza la clase de gestión predeterminada para los servicios de copia de seguridad/archivado.

Acerca de esta tarea

Esta es una tarea opcional, pero importante.

Puede crear una lista de inclusión/exclusión para excluir un archivo o grupo de archivos específico de los servicios de copia de seguridad, y para asignar clases de gestión específicas a los archivos. El cliente realiza una copia de seguridad de todos los archivos que no estén excluidos. Debe excluir de los servicios de copia de seguridad los directorios del cliente de IBM Spectrum Protect. Puede utilizar el mandato **query inclexcl** para visualizar una lista de sentencias de inclusión y exclusión en el orden en el que se examinan cuando determine si se debe incluir un objeto.

Especifique la lista de inclusión/exclusión en el archivo dsm.sys. Si tiene más de un servidor definido en el archivo dsm.sys, cada servidor debe tener su propia lista de inclusión/exclusión. Esta lista también puede contener sentencias de inclusión/exclusión obtenidas de los archivos de inclusión/exclusión especificados mediante la opción `inclexcl`.

Cuando el cliente procesa sentencias de inclusión/exclusión, las del archivo de inclusión/exclusión se colocan en la posición de lista ocupada por la opción `inclexcl` en dsm.sys, en el mismo orden, y se procesan en consecuencia.

Procedimiento

Puede utilizar los siguientes métodos para crear una lista de inclusión/exclusión o para especificar un archivo de inclusión/exclusión:

- Puede añadir sentencias de inclusión/exclusión en el árbol de directorios del cliente de copia de seguridad y archivado. La ayuda en línea proporciona instrucciones detalladas.
 1. Abra el menú **Editar** y seleccione **Preferencias del cliente**. En el diálogo Preferencias, seleccione el separador **Inclusión/exclusión**. Puede especificar un archivo INCLEXCL mediante el editor de preferencias. Sin embargo, no puede crear el archivo INCLEXCL mediante dicho editor.
 2. Cree la lista de inclusión-exclusión de forma manual siguiendo los pasos enumerados.
- Puede crear una lista de inclusión/exclusión manualmente, realizando los pasos siguientes:
 1. Determine las necesidades de inclusión y exclusión.
 2. Localice la stanza de servidor en el archivo dsm.sys. Cada stanza de servidor debe tener su propia lista de inclusión/exclusión.
 3. Especifique las sentencias `include` y `exclude`. El cliente evalúa *en primer lugar* todas las sentencias de `exclude.fs` y `exclude.dir` (con independencia de la posición que ocupen en la lista de inclusión/exclusión) y elimina los espacios de archivos, los directorios y los archivos excluidos de la lista de objetos que están disponibles para procesarse. Todas las demás sentencias de inclusión/exclusión se procesan de abajo a arriba, empezando por el final de la lista. Por lo tanto, es importante especificar las sentencias de inclusión/exclusión en el orden correcto. Por ejemplo, en la lista de inclusión/exclusión siguiente *no* se hace una copia de seguridad del archivo `includefile.cpp`:

```
include /Users/user01/Documents/includefile.cpp
exclude /Users/user01/Documents/.../*
```

Sin embargo, en la lista de inclusión/exclusión siguiente se hace una copia de seguridad del archivo `includefile.cpp`:

```
exclude /Users/user01/Documents/.../*
include /Users/user01/Documents/includefile.cpp
```

4. Guarde el archivo y ciérrelo.

En Mac OS X, no olvide guardar el archivo como un texto sin formato codificado como Unicode (UTF-8 o UTF-16). No añada la extensión `.txt`.

5. Reinicie el cliente para habilitar la lista de inclusión/exclusión.

Conceptos relacionados:

“Consideraciones sobre los clientes habilitados para Unicode” en la página 457

“Archivos del sistema a excluir” en la página 129

Capítulo 9, “Políticas de gestión de almacenamiento”, en la página 299

Referencia relacionada:

“Incl excl” en la página 456

Opciones de inclusión/exclusión

Este tema proporciona descripciones breves de las opciones `incluir` y `excluir` que puede especificar en el archivo de opciones del cliente, una lista mínima inclusión-exclusión que excluye a los archivos del sistema, una lista de caracteres comodín admitidos, y ejemplos de cómo se deben utilizar los caracteres comodín con patrones `incluir` y `excluir`.

Exclusión de espacios de archivos y directorios

Utilice las sentencias `exclude.dir` para excluir del proceso todos los archivos y subdirectorios del directorio especificado.

El cliente de copia de seguridad y archivado evalúa *en primer lugar* todas las sentencias `exclude.dir` (con independencia de la posición que ocupen en la lista de inclusión/exclusión), y elimina los directorios y los archivos excluidos de la lista de objetos que están disponibles para procesarse. Las sentencias `exclude.dir` modifican todas las sentencias de inclusión que coinciden con el patrón.

Tabla 27 enumera las opciones que puede utilizar para excluir los espacios de archivos y directorios del proceso.

Tabla 27. Opciones para excluir espacios de archivos y directorios

Opción	Descripción
<code>exclude.fs</code> “Opciones <code>exclude</code> ” en la página 425	Excluye los espacios de archivos que coinciden con el patrón. El cliente no ha tenido en cuenta el espacio de archivos especificado para el proceso, por lo que no se ha realizado el proceso normal de caducidad de archivos eliminados. Si se excluye un espacio de archivos que se había incluido previamente, las versiones de copia de seguridad existentes permanecen en el servidor sujetas a las reglas de retención especificadas en la definición de clase de gestión que se haya asociado.

Tabla 27. Opciones para excluir espacios de archivos y directorios (continuación)

Opción	Descripción
exclude.dir "Opciones exclude" en la página 425	<p>Excluye un directorio, sus archivos y todos sus subdirectorios y sus archivos del proceso de copia de seguridad. Por ejemplo, la sentencia <code>exclude.dir /test/dan/data1</code> excluye el directorio <code>/test/dan/data1</code>, sus archivos y todos sus subdirectorios y sus archivos. Para excluir directorios grandes con una gran cantidad de archivos de los que no desea hacer la copia de seguridad, es mejor utilizar la opción <code>exclude.dir</code> que la opción <code>exclude</code>. No puede utilizar las opciones <code>include</code> para alterar temporalmente la opción <code>exclude.dir</code>. Utilice <code>exclude.dir</code> sólo cuando se excluye toda una rama del directorio.</p> <ul style="list-style-type: none"> • Utilice las siguientes sentencias para excluir los volúmenes <code>/Volumes/disk2</code> en su conjunto del proceso de copia de seguridad. Recuerde que todavía será posible realizar la copia de seguridad del volumen (<code>/Volumes/disk2</code>), pero quedarán excluidos todos los demás directorios que se encuentren en <code>/Volumes/disk2</code>. <pre>exclude /Volumes/disk2/* exclude.dir /Volumes/disk2/*</pre> • Un método alternativo para excluir un volumen completo de la realización de la copia de seguridad incremental del dominio consiste en utilizar una sentencia de dominio para excluir el volumen. Por ejemplo: <pre>domain "-/Volumes/disk2"</pre> <p>Esta alternativa sigue permitiendo el proceso de la copia de seguridad selectiva de los archivos que se encuentran en <code>/Volumes/disk2</code>.</p>

Excluir archivos y directorios de la copia de seguridad con registro por diario

Hay dos métodos para excluir archivos y directorios de una copia de seguridad con registro por diario.

- En AIX y Linux, uno de los métodos consiste en añadir sentencias de exclusión al archivo de opciones de cliente para impedir que se realice la copia de seguridad de los archivos o directorios durante el proceso de copia de seguridad.
- En AIX y Linux, el otro método consiste en añadir sentencias de exclusión en el archivo de configuración `tsmjbbd.ini`, para evitar añadir entradas con registro por diario de los archivos o directorios, y de esta forma no procesarlos durante la copia de seguridad con registro por diario.

Si está ejecutando AIX Versión 6.1 o posterior, añada una sentencia `exclude .snapshot` al archivo `tsmjbbd.ini` para evitar que se supervisen directorios de instantáneas internos de JFS2 mediante el daemon de copia de seguridad con registro por diario.

Nota: No existe correlación entre las dos sentencias de exclusión. El lugar preferido para las sentencias de exclusión en `tsmjbbd.ini` para evitar que entren en la base de datos de diario y que sean procesados durante una copia de seguridad con registro por diario.

Controlar proceso de sentencias de exclusión

Después de que el cliente ha evaluado todas las sentencias `exclude` se evalúan las opciones siguientes con la lista restante de objetos disponibles para el proceso.

Tabla 28 enumera las opciones que puede utilizar para controlar el proceso con las sentencias de inclusión y exclusión.

Tabla 28. Opciones para controlar el proceso utilizando sentencias de inclusión y exclusión

Opción	Descripción	Página
Proceso de copia de seguridad		
exclude exclude.backup exclude.file exclude.file.backup	<i>Estas opciones son equivalentes.</i> Utilice estas opciones para excluir un archivo o un grupo de archivos de los servicios de copia de seguridad y de los servicios de gestión de espacio (si el cliente de HSM está instalado). La opción <code>exclude.backup</code> sólo excluye archivos de la copia de seguridad normal, no de HSM.	"Opciones exclude" en la página 425
include include.backup include.file	Utilice estas opciones para incluir archivos o asignar clases de gestión para el proceso de copias de seguridad.	"Opciones include" en la página 458
include.fs	Controla la forma en que el cliente procesa el espacio de archivos para las copias de seguridad incrementales.	"Opciones include" en la página 458
Proceso de archivado		
exclude.archive	Excluye un archivo o grupo de archivos de los servicios de archivado.	"Opciones exclude" en la página 425
include include.archive	<i>Estas opciones son equivalentes.</i> Utilice estas opciones para incluir archivos o asignar clases de gestión para el proceso de copias archivadas.	"Opciones include" en la página 458
Proceso de copia de seguridad de imagen		
exclude.fs.nas	Excluye sistemas de archivos del servidor de archivos NAS del proceso de copias de seguridad de imágenes cuando se utiliza con el mandato backup nas . Si no especifica un nombre de nodo NAS, el sistema de archivos identificado se aplica a todos los servidores de archivos NAS. El mandato backup nas pasa por alto todas las demás sentencias de exclusión, incluidas las sentencias <code>exclude.fs</code> y <code>exclude.dir</code> . Esta opción sólo es válida para clientes AIX y Solaris.	"Opciones exclude" en la página 425
exclude.image	Excluye sistemas de archivos montados y volúmenes lógicos RAW que coincidan con el patrón especificado de las operaciones de copia de seguridad de imágenes completas. <code>exclude.image</code> no afectará a las operaciones de copia de seguridad de imágenes incremental. Esta opción es válida para AIX, Solaris y todos los clientes Linux.	"Opciones exclude" en la página 425

Tabla 28. Opciones para controlar el proceso utilizando sentencias de inclusión y exclusión (continuación)

Opción	Descripción	Página
include.fs.nas	Utilice la opción include.fs.nas para vincular una clase de gestión a sistemas de archivos de almacenamiento conectado a red (NAS). Para especificar si el cliente debe guardar la información de la Tabla de contenido (TOC) durante una copia de seguridad de imágenes del sistema de archivos NAS, utilice la opción toc con la opción include.fs.nas en el archivo dsm.sys. Para obtener más información, consulte el apartado "Toc" en la página 596. Esta opción solo es válida para los clientes AIX y Solaris.	"Opciones include" en la página 458
include.image	Incluye un espacio de archivos o un volumen lógico o asigna una clase de gestión, o permite asignar una de las diferentes opciones de copia de seguridad de imagen en un volumen lógico cuando se utiliza con el mandato backup image . El mandato backup image ignora todas las demás opciones de inclusión. Esta opción es válida para AIX, Solaris, Linux x86_64 y Linux on POWER únicamente.	"Opciones include" en la página 458

Archivos del sistema a excluir

Hay algunos archivos del sistema que deben ubicarse en el archivo de opciones de cliente para que se puedan excluir.

Atención: Estos archivos, o los bloquea el sistema operativo, o pueden causar problemas durante la restauración. Estos son archivos del sistema que no se pueden recuperar sin correr el riesgo de dañar el sistema operativo o los archivos temporales con datos que pueden volver a crearse fácilmente.

Nota: Esta sección sólo se aplica a Mac OS X.

Las sentencias que se generan implícitamente pueden verse en las líneas de la salida del mandato **query inclexcl** con el "sistema operativo" de origen.

El cliente de copia de seguridad y archivado añade las siguientes sentencias de exclusión a la lista de inclusión-exclusión del archivo dsm.sys. No incluya ninguna de estas sentencias del archivo dsm.sys o se producirán entradas duplicadas.

```
EXCLUDE.ARCHIVE "/.../Desktop DB"
EXCLUDE.BACKUP "/.../Desktop DB"
EXCLUDE.ARCHIVE "/.../Desktop DF"
EXCLUDE.BACKUP "/.../Desktop DF"
EXCLUDE.ARCHIVE /.vol
EXCLUDE.BACKUP /.vol
EXCLUDE.ARCHIVE /automount
EXCLUDE.BACKUP /automount
EXCLUDE.ARCHIVE /Network
EXCLUDE.BACKUP /Network
EXCLUDE.ARCHIVE /dev
EXCLUDE.BACKUP /dev
EXCLUDE.BACKUP /.vol/.../*
EXCLUDE.ARCHIVE /.vol/.../*
EXCLUDE.BACKUP /automount/.../*
EXCLUDE.ARCHIVE /automount/.../*
EXCLUDE.BACKUP /Network/.../*
EXCLUDE.ARCHIVE /Network/.../*
EXCLUDE.BACKUP /dev/.../*
```

```
EXCLUDE.ARCHIVE /dev/.../*
EXCLUDE.DIR /.vol
EXCLUDE.DIR /automount
EXCLUDE.DIR /Network
EXCLUDE.DIR /dev
```

Nota:

1. No incluya puntos cuando especifique el nombre de los volúmenes (...). El cliente de copia de seguridad y archivado utiliza la secuencia de puntos como parte del proceso de inclusión/exclusión. El cliente informará de la existencia de una sentencia de inclusión/exclusión no válida si un nombre de volumen contiene puntos. *Debe* cambiarse el nombre del volumen.
2. Los objetos que tienen el tipo rhap y el creador lcmt quedarán excluidos del proceso. Por lo general, son objetos del sistema de archivos especiales aunque también pueden crearse con el mandato **mknod**, o son puntos de montaje de UNIX. Cuando se realiza una restauración completa del sistema, es necesario volver a crear manualmente los objetos o los puntos de montaje.

Debería disponer de una lista de inclusión/exclusión mínima en el archivo de opciones de inclusión/exclusión:

```
EXCLUDE    /.../dsmsched.log
EXCLUDE    /.../dsmprune.log
EXCLUDE    /.../dsmj.log
EXCLUDE    /.../dsmerror.log
EXCLUDE    /.../.hotfiles.bTree

EXCLUDE.DIR /private/tmp
EXCLUDE.DIR /private/var/vm
EXCLUDE.DIR /private/var/tmp
EXCLUDE.DIR /private/var/db/netinfo/local.nidb

EXCLUDE.DIR /.../.Trashes
EXCLUDE.DIR /.../.Spotlight-*
EXCLUDE.DIR /.../Library/Caches
EXCLUDE.DIR /.../.fseventsd
```

Incluir y excluir archivos con caracteres comodín

Debe utilizar caracteres especiales cuando incluya o excluya archivos y directorios que contengan caracteres comodín.

El cliente de copia de seguridad y archivado trata los caracteres comodín de distinta manera en diferentes plataformas.

Los nombres de los directorios y de los archivos pueden incluir diferentes símbolos. Los tipos de símbolos permitidos dependen del sistema operativo.

Por ejemplo, en AIX, los nombres de los directorios o de los archivos pueden incluir:

```
* ? : [ ]
```

Para especificar archivos y directorios en las sentencias de inclusión y exclusión, utilice el carácter de escape "\" para especificar los caracteres comodín. Sin embargo, el carácter de escape solo se puede utilizar dentro de las clases de carácter "[]".

En el siguiente ejemplo, se muestra cómo especificar archivos y directorios que contienen caracteres comodín utilizando el carácter de escape y las clases de caracteres en las sentencias de inclusión o de exclusión.

Para excluir el directorio único /usr1/[dir2] del proceso de copia de seguridad, especifique lo siguiente en el archivo dsm.sys o el archivo de inclusión-exclusión:

```
exclude.dir "/usr1/[\\[]dir2[\\]]"
```

Para excluir el archivo único /usr1/fi*le1 del proceso de copia de seguridad, especifique lo siguiente en el archivo dsm.sys o el archivo de inclusión-exclusión:

```
exclude "/usr1/fi[\\*]le1"
```

Consejo: Si utiliza el Editor de preferencias para incluir o excluir un archivo o un directorio único que contenga caracteres comodín, deberá editar de forma manual la sentencia de inclusión o de exclusión para evitar los caracteres comodín. El Editor de preferencias no evita de forma automática los caracteres comodín. Siga los ejemplos anteriores para editar las sentencias de inclusión o de exclusión en el archivo dsm.sys o el archivo de inclusión-exclusión.

Conceptos relacionados:

“Caracteres comodín” en la página 663

Inclusión y exclusión de grupos de archivos con caracteres comodín

Puede utilizar caracteres comodín para incluir o excluir grupos de archivos.

Para especificar los grupos de archivos que deben incluirse o excluirse, utilice los caracteres comodín que se indican en la siguiente tabla. Esta tabla *sólo* se aplica a las sentencias `include` y `exclude`.

una lista de inclusión/exclusión muy larga puede afectar negativamente al rendimiento de la copia de seguridad. Utilice caracteres comodín y elimine sentencias de inclusión innecesarias para que la lista sea lo más corta posible.

Tabla 29. Caracteres comodín y otros caracteres especiales

Carácter	Función
?	La coincidencia de un único carácter puede utilizarse para buscar la coincidencia con cualquier carácter individual, <i>excepto</i> el separador de directorio; no se aplica a la búsqueda de la coincidencia en el final de la serie de caracteres. Por ejemplo: <ul style="list-style-type: none"> El patrón ab? coincide con abc, pero no coincide con ab, abab ni abzzz. El patrón ab?rs coincide con abfrs, pero no coincide con abrs ni abllrs. El patrón ab?ef?rs coincide con abdefjrs, pero no coincide con abefrs, abdefrs ni abefjrs. El patrón ab??rs coincide con abcdrs, abzzrs, pero no coincide con abrs, abjrs ni abkkrs.
*	Este carácter puede coincidir con varios caracteres. Por ejemplo: <ul style="list-style-type: none"> El patrón ab* coincide con ab, abb, abxxx, pero no coincide con a, b, aa, bb. El patrón ab*rs coincide con abrs, abtrs, abrsrs, pero no coincide con ars, aabrs ni abrss. El patrón ab*ef*rs coincide con abefrs, abefghrs, pero no coincide con abefr, abers. El patrón abcd.* coincide con abcd.c, abcd.txt, pero no coincide con abcd, abcdc ni abcdtxt.
/...	Carácter de coincidencia con <i>n</i> caracteres que coincide con cero o más directorios.

Tabla 29. Caracteres comodín y otros caracteres especiales (continuación)

Carácter	Función
[El carácter de apertura de clase de caracteres inicia la enumeración de una clase de caracteres. Por ejemplo: xxx[abc] produce las coincidencias xxxa, xxxb o xxxc.
-	El rango de clase de caracteres incluye caracteres desde el primer carácter al último carácter especificado. Por ejemplo: xxx[a-z] produce las coincidencias xxxa, xxxb, xxxc... hasta xxxz.
\	Es el carácter de escape literal. Cuando se utiliza en una clase de caracteres, trata el siguiente carácter literalmente. Cuando se utiliza fuera de una clase de caracteres, éste no se trata de esta forma. Por ejemplo, si desea incluir ']' en una clase de caracteres, especifique [...\]...]. El carácter de escape no aplica el significado normal de ']' como carácter de clase de caracteres de cierre.
]	El carácter de cierre de clase de caracteres finaliza la enumeración de una clase de caracteres.

Conceptos relacionados:

“Caracteres comodín” en la página 663

Ejemplos de utilización de caracteres comodín en patrones de inclusión y exclusión

El cliente de copia de seguridad y archivado cliente acepta la opción `exclude.dir`, que se puede utilizar para excluir entradas de directorio. No obstante, las opciones `include` y `exclude.dir` no pueden utilizarse al mismo tiempo.

Nota: En el archivo `dsm.sys`, las opciones `include` y `exclude` no funcionan con vínculos simbólicos a directorios. Por ejemplo, no utilice `/u` en las sentencias de inclusión o exclusión porque `/u` es un vínculo simbólico con el directorio `/home`. En lugar de escribir:

```
include /u/tmp/save.fil
```

escriba:

```
include /home/tmp/save.fil
```

Sin embargo, la opción `exclude` sí funciona con enlaces simbólicos a directorios cuando se especifica el mandato de copia de seguridad con la vía de acceso absoluta que contiene el enlace simbólico.

Tabla 30 muestra cómo utilizar los caracteres comodín para los archivos de inclusión o exclusión.

Tabla 30. Utilización de caracteres comodín con patrones de inclusión y exclusión

Tarea	Patrón
Excluir todos los archivos que acaben por <code>.doc</code> , excepto los que se encuentren en el directorio de inicio de aleko, directorio Documents.	EXCLUDE <code>../*.doc</code> INCLUDE <code>"/home/aleko/Documents/*.doc"</code>
Excluir todos los archivos durante la operación de copia de seguridad que tengan la extensión <code>bak</code> , excepto los detectados en el sistema de archivos <code>/usr</code> en el directorio <code>dev</code> .	exclude <code>../*.bak</code> include <code>/usr/dev/*.bak</code>

Tabla 30. Utilización de caracteres comodín con patrones de inclusión y exclusión (continuación)

Tarea	Patrón
Excluir todos los archivos y directorios que pudieran existir en cualquier directorio Documents, <i>excepto</i> el archivo Current del usuario aleko.	EXCLUDE ../Documents/.../* INCLUDE "/home/aleko/Documents/Current"
Excluir todos los archivos en cualquier directorio llamado "tmp" y sus subdirectorios, <i>excepto</i> el archivo /home/tmp/save.fil.	exclude ../tmp/.../* include /home/tmp/save.fil
Excluir todos los archivos .cpp de cualquier directorio de los volúmenes Vol1, Vol2, Vol3 y Vol4.	EXCLUDE /Volumes/Vol[1-4]/.../*.cpp
Excluir todos los archivos .cpp de cualquier directorio de los volúmenes Vol1, Vol2, Vol3 y Vol4.	EXCLUDE /Volumes/Vol[1-4]/.../*.cpp
Excluir cualquier archivo .cpp de cualquier directorio de los sistemas de archivos /fs1, /fs2, /fs3 y /fs4.	EXCLUDE /fs[1-4]/.../*.cpp
Excluir los archivos .cpp que se encuentran en el directorio /fs2/source.	EXCLUDE /fs2/source/*.cpp
Excluir cualquier archivo .o de cualquier directorio de los sistemas de archivos /usr1, /usr2 y /usr3.	exclude /usr[1-3]/.../*.o
Excluir <i>sólo</i> los archivos .o detectados en el directorio raíz del sistema de archivos usr2.	exclude /usr2/*.o
Excluir cualquier archivo que resida en el directorio tmp situado en cualquier sistema de archivos.	exclude ../tmp/.../*
Excluir toda la estructura de directorios /var/spool de todo el proceso.	exclude.dir /var/spool
Excluir un único sistema de archivos del proceso de copia de seguridad.	exclude.fs /fs1 exclude.fs home:
Excluir del proceso de copia de seguridad todos los sistemas de archivos que se han montado en cualquier ubicación del árbol de directorios /test/myfs/fs01 y /test/myfs/fs02.	exclude.fs /test/myfs/fs01/.../* exclude.fs /test/myfs/fs02/*
Excluir el directorio /home/mydir/test1 y cualquier archivo y subdirectorio que contenga.	exclude.dir /home/mydir/test1
Excluir todos los directorios del directorio /home/mydir cuyo nombre empiece por test.	exclude.dir /home/mydir/test*
Excluir todos los directorios inmediatamente a continuación del directorio /mydir cuyo nombre empiece por test, en cualquier sistema de archivos.	exclude.dir ../mydir/test*
Excluir el volumen lógico RAW de la copia de seguridad de la imagen.	exclude.image /dev/hd0
Excluir todos los enlaces simbólicos o alias (los alias se aplican a Mac OS X) del proceso de copia de seguridad, <i>excepto</i> el directorio Docs de user1.	EXCLUDE.ATTRIBUTE.SYMLINK ../.../* INCLUDE.ATTRIBUTE.SYMLINK /Users/user1/Docs/*

Conceptos relacionados:

“Ejemplos de utilización de caracteres comodín en patrones de inclusión y exclusión” en la página 132

Referencia relacionada:

“Opciones exclude” en la página 425

Proceso de enlaces simbólicos y alias

El cliente de copia de seguridad y archivado evalúa todas las sentencias `exclude.fs` y `exclude.dir` y elimina los espacios de archivos y los directorios excluidos.

Después de esta evaluación inicial, el cliente evalúa todas las sentencias de inclusión/exclusión para controlar el proceso de vínculos simbólicos y alias (`exclude.attribute.symlink` e `include.attribute.symlink`) con la lista restante de objetos disponibles para su proceso.

El proceso de alias se aplica a Mac OS X.

En Tabla 31 se definen opciones para controlar el proceso de vínculos simbólicos y alias.

Tabla 31. Opciones para controlar el proceso de vínculos simbólicos y alias

Opción	Descripción	Página
<code>exclude.attribute.symlink</code>	Excluye un archivo o un grupo de archivos que son vínculos simbólicos o alias sólo del proceso de copia de seguridad.	“Opciones exclude” en la página 425
<code>include.attribute.symlink</code>	Incluye un archivo o un grupo de archivos que son vínculos simbólicos o alias dentro de un amplio grupo de archivos excluidos sólo para el proceso de copia de seguridad.	“Opciones include” en la página 458

Determinar el proceso de compresión y cifrado

El cliente de copia de seguridad y archivado evalúa `exclude.dir` y todas las demás opciones de inclusión/exclusión que controlan el proceso de copia de seguridad y archivado para determinar qué archivos se someten al proceso de compresión y cifrado compresión y cifrado.

Las siguientes opciones determinan cuáles son los archivos que se someterán al proceso de cifrado y compresión.

Tabla 32. Opciones para controlar la compresión y el cifrado

Opción	Descripción	Página
Proceso de compresión		
<code>exclude.compression</code>	Excluye archivos del proceso de compresión si se especifica <code>compression=yes</code> . Esta opción se aplica a copias de seguridad y copias archivadas.	“Opciones exclude” en la página 425

Tabla 32. Opciones para controlar la compresión y el cifrado (continuación)

Opción	Descripción	Página
include.compression	Incluye archivos en el proceso de compresión si se especifica <code>compression=yes</code> . Esta opción se aplica a copias de seguridad y copias archivadas.	"Opciones include" en la página 458
Proceso de cifrado		
exclude.encrypt	Excluye archivos del proceso de cifrado.	"Opciones exclude" en la página 425
include.encrypt	<p>Incluye archivos para el proceso de cifrado.</p> <p>Los datos que incluya se almacenarán en formato cifrado, y el cifrado no afectará a la cantidad de datos enviados o recibidos.</p> <p>Importante: el cifrado sólo puede habilitarse en el cliente de archivado y copia de seguridad mediante la opción <code>include.encrypt</code>. Si no se utiliza ninguna sentencia <code>include.encrypt</code>, no se realizará el cifrado.</p>	"Opciones include" en la página 458

Vista previa de los archivos de la lista de inclusión-exclusión

Puede realizar una previsualización de la lista de objetos de los que se va a realizar una copia de seguridad o archivado según la lista de inclusión/exclusión, antes de enviar los datos al servidor.

El árbol de directorios de la GUI web del cliente de copia de seguridad y archivado muestra información detallada sobre los objetos incluidos y excluidos. Las ventanas del árbol de directorios de la GUI web del cliente de copia de seguridad y archivado permiten seleccionar los archivos y directorios que se deben incluir o excluir. Debe utilizar el mandato **preview** para asegurarse de incluir o excluir los archivos correctos. A continuación, encontrará un ejemplo de cómo utilizar la función de previsualización de inclusión/exclusión.

Por ejemplo, siga estos pasos para realizar una copia de seguridad de los archivos del espacio de archivos `/Users/home`:

1. Inicie la GUI del cliente de copia de seguridad y archivado y abra el árbol de copias de seguridad. Puede ver todos los directorios y archivos que se han excluido mediante el archivo de opciones y mediante otras formas.
2. Avance por el árbol y observe que se realiza la copia de seguridad de todos los archivos `*.o` de `/Volumes/home/mary/myobjdir`.
3. Puesto que no desea hacer una copia de seguridad de todos los archivos `*.o`, pulse el botón derecho del ratón en un archivo `.o` y elija "Ver detalles de archivo" en el menú emergente.
4. El diálogo muestra que estos archivos están incluidos; por lo tanto, pulse el botón "Avanzado" y cree una regla para excluir todos los archivos `.o` del espacio de archivos `DATA:\home`.
5. Se habrá creado una regla en la parte final del archivo de opciones. El directorio actual se renueva en el árbol Copia de seguridad y los archivos `.o` aparecen con una 'X' de color rojo, que significa que se han excluido.

6. Cuando busque en otros directorios, mostrarán las nuevas exclusiones que se hayan agregado. Pulse en "Copia de seguridad" y realice la copia de seguridad de los archivos del espacio de archivos /home.

Referencia relacionada:

"Preview Archive" en la página 715

"Previsualizar copia de seguridad" en la página 716

Inclusión y exclusión de proceso de opciones

El servidor de IBM Spectrum Protect puede definir opciones de inclusión/exclusión mediante el parámetro `incl excl` en un archivo de opciones del cliente.

Las sentencias de inclusión/exclusión que especifica el servidor se evalúan junto con las del archivo de opciones del cliente. Las sentencias de inclusión/exclusión del servidor siempre se aplican y se colocan al final de la lista de inclusión/exclusión, evaluándose antes que las sentencias de inclusión/exclusión del cliente.

Si la lista de inclusión/exclusión del archivo `dsm.sys` contiene una o más opciones `incl excl` que especifican archivos de inclusión/exclusión, las sentencias de inclusión/exclusión de tales archivos se colocan en la posición de la lista que ocupa la opción `incl excl` y se procesan como corresponde.

una lista de inclusión/exclusión muy larga puede afectar negativamente al rendimiento de la copia de seguridad. Utilice caracteres comodín y elimine sentencias de inclusión innecesarias para que la lista sea lo más corta posible.

Cuando se realiza una copia de seguridad incremental, el cliente evalúa primero todas las sentencias `exclude.fs` y `exclude.dir` y elimina los espacios de archivos, directorios y archivos excluidos de la lista de objetos disponibles para procesarse.

Después de haber evaluado todas las sentencias `exclude.fs` y `exclude.dir`, el cliente evalúa las sentencias de inclusión/exclusión para controlar el proceso de los enlaces simbólicos o alias (`exclude.attribute.symlink` y `include.attribute.symlink`), empezando por el final y se detiene si encuentra una sentencia de inclusión o exclusión que coincide con el archivo que está procesando. Después de procesar las sentencias de inclusión/exclusión para controlar el proceso de enlaces simbólicos o alias, el cliente evalúa la lista de inclusión/inclusión restante empezando por el final y se detiene cuando encuentra una sentencia de inclusión o exclusión que coincide con el archivo que se está procesando. Por consiguiente, el orden en que se especifican las opciones de inclusión y exclusión afecta a los archivos que se incluyen y excluyen.

Para visualizar una lista de todas las sentencias de inclusión/exclusión en vigor en la estación de trabajo cliente en el orden en el que se procesan, utilice el mandato **query incl excl**.

El programa cliente procesa la lista de sentencias de inclusión/exclusión de acuerdo con las siguientes reglas:

1. Se comprueban los archivos; los directorios sólo se comprueban si se ha especificado la opción `exclude.dir`.
2. Los nombres de archivo se comparan con los patrones en la lista `include-exclude` de abajo a arriba. Cuando se detecta una coincidencia, el proceso se detiene y comprueba si la opción es `include` o `exclude`. Si la opción

es include, se realiza una copia de seguridad del archivo. Si la opción es exclude, no se realiza ninguna copia de seguridad del archivo.

Nota: Si no se encuentra ninguna coincidencia, los archivos se incluyen de forma implícita y se realiza la copia de seguridad.

3. Cuando se realiza la copia de seguridad de un archivo, se vincula con la clase de gestión predeterminada a menos que coincida con la sentencia include que especificaba un nombre de clase de gestión diferente, y en este caso se vincula con dicha clase de gestión.

En los ejemplos siguientes se muestra el proceso ascendente.

Ejemplo 1

Imaginemos que La Pomme no es el disco de arranque.

```
EXCLUDE /.../*.cpp
INCLUDE "/Volumes/La Pomme/Foo/.../*.cpp"
EXCLUDE "/Volumes/La Pomme/Foo/Junk/*.cpp"
```

El archivo que está procesándose es: /Volumes/La Pomme/Foo/Dev/test.cpp. El proceso sigue estos pasos:

1. En primer lugar se comprueba la regla 3 (la última sentencia include o exclude definida), porque se trata de un proceso ascendente. El patrón /Volumes/La Pomme/Foo/Junk/*.cpp no coincide con el nombre del archivo que está procesándose.
2. El proceso sigue con la regla 2 y realiza la comprobación pertinente. Ahora, el patrón /Volumes/La Pomme/Foo/.../*.cpp coincide con el nombre del archivo que está procesándose. El proceso se detiene, se comprueba la opción y se incluye el archivo.
3. Se realiza la copia de seguridad del archivo /Volumes/La Pomme/Foo/Dev/test.cpp.

Ejemplo 2

Imaginemos que La Pomme no es el disco de arranque.

```
EXCLUDE /.../*.cpp
INCLUDE "/Volumes/La Pomme/Foo/.../*.cpp"
EXCLUDE "/Volumes/La Pomme/Foo/Junk/*.cpp"
```

El archivo que está procesándose es: /Volumes/La Pomme/Widget/Sample File. El proceso sigue estos pasos:

1. Se comprueba la regla 3 y no se encuentra ninguna coincidencia.
2. Se comprueba la regla 2 y no se encuentra ninguna coincidencia.
3. Se comprueba la regla 1 y no se encuentra ninguna coincidencia.
4. Puesto que no se ha encontrado ninguna coincidencia, Volumes/La Pomme/Widget/Sample File se incluye implícitamente y se realiza la copia de seguridad de éste.

Ejemplo 3

Supongamos que define las sentencias siguientes para las opciones include y exclude:

```
exclude *.o
include /home/foo/.../*.o
exclude /home/foo/junk/*.o
```

El archivo que está procesándose es: /home/foo/dev/test.o. El proceso sigue estos pasos:

1. En primer lugar se comprueba la regla 3 (la última sentencia definida) porque se trata de un proceso ascendente. El patrón `/home/foo/junk/*.o` no coincide con el nombre del archivo que está procesándose.
2. El proceso sigue con la regla 2 y realiza la comprobación pertinente. Ahora, el patrón `/home/foo/.../*.o` coincide con el nombre del archivo que está procesándose. El proceso se detiene, se comprueba la opción y se advierte que se trata de `include`.
3. Se realiza la copia de seguridad del archivo `/home/foo/dev/test.o`.

Ejemplo 4

Supongamos que define las sentencias siguientes para las opciones `include` y `exclude`:

```
exclude
*.obj
include /home/foo/.../*.o
exclude /home/foo/junk/*.o
```

El archivo que está procesándose es: `/home/widg/copyit.txt`. El proceso sigue estos pasos:

1. Se comprueba la regla 3 y no se encuentra ninguna coincidencia.
2. Se comprueba la regla 2 y no se encuentra ninguna coincidencia.
3. Se comprueba la regla 1 y no se encuentra ninguna coincidencia.
4. Puesto que no se ha encontrado una coincidencia, el archivo `/home/widg/copyit.txt` se incluye implícitamente y se realiza la copia de seguridad de éste.

Ejemplo 5

Supongamos que define las sentencias siguientes para las opciones `include` y `exclude`:

```
exclude /.../*.o
include /home/foo/.../*.o
exclude /home/foo/junk/*.o
```

El archivo que se está procesando actualmente es: `/home/lib/objs/printf.o`. El proceso sigue estos pasos:

1. Se comprueba la regla 3 y no se encuentra ninguna coincidencia.
2. Se comprueba la regla 2 y no se encuentra ninguna coincidencia.
3. Se comprueba la regla 1 y se encuentra una coincidencia.
4. El proceso se detiene, se comprueba la opción y se excluye.
5. No se realiza la copia de seguridad del archivo `/home/lib/objs/printf.o`.

Ejemplo 6

Supongamos que define las sentencias siguientes para las opciones `include` y `exclude`:

```
exclude.attribute.symlink /.../*
exclude /.../*.o
include /home/foo/.../*.o
exclude /home/foo/junk/*.o
```

El archivo que está procesándose actualmente es: `/home/lib/objs/printf.o`. El proceso sigue estos pasos:

1. En primer lugar se comprueba la sentencia `exclude.attribute.symlink`. Si el archivo `printf.o` es un vínculo simbólico, se excluye. Si no lo es, vaya al paso siguiente. Tenga en cuenta que las sentencias

`exclude.attribute.symblink` siempre se procesan antes que las otras sentencias de inclusión/exclusión, independientemente de su posición en la lista de inclusión/exclusión.

2. Se comprueba la regla 3 y no se encuentra ninguna coincidencia.
3. Se comprueba la regla 2 y no se encuentra ninguna coincidencia.
4. Se comprueba la regla 1 y se encuentra una coincidencia.
5. El proceso se detiene, se comprueba la opción y se excluye.
6. No se realiza la copia de seguridad del archivo `/home/lib/objs/printf.o`.

Conceptos relacionados:

“Exclusión de espacios de archivos y directorios” en la página 126

Capítulo 10, “Opciones de proceso”, en la página 313

Referencia relacionada:

“Opciones `exclude`” en la página 425

“Query `Inclexcl`” en la página 733

Capítulo 3. Cómo empezar

Antes de poder utilizar el cliente de archivado y copia de seguridad de IBM Spectrum Protect, debe aprender a iniciar una sesión en la GUI o en la línea de mandatos, y a iniciar el planificador de cliente automáticamente. También puede aprender otras tareas frecuentes.

Antes de utilizar el cliente de archivado y copia de seguridad, complete las siguientes tareas:

- “Inicio de una sesión en la GUI Java” en la página 142
- “Inicio de una sesión de línea de mandatos” en la página 144
- “Inicio de una sesión de cliente web” en la página 147
- “Iniciar automáticamente el planificador cliente” en la página 148
- “Cambio de la contraseña” en la página 148

También puede completar las siguientes tareas:

- “Ordenación de listas de archivos mediante la GUI del cliente de copia de seguridad y archivado” en la página 150
- “Visualización de ayuda en línea” en la página 151
- “Finalización de una sesión” en la página 152

Autenticación del cliente de IBM Spectrum Protect

Si se utiliza la interfaz gráfica de usuario o la interfaz de línea de mandatos del cliente de IBM Spectrum Protect, se puede iniciar la sesión utilizando un nombre de nodo y una contraseña o un ID y una contraseña de usuario de administración.

El cliente solicita el identificador de usuario y lo compara con el nombre de nodo configurado. Si coinciden, el cliente intenta autenticar el identificador de usuario como un nombre de nodo. Si la autenticación falla o si el identificador de usuario no coincide con el nombre de nodo configurado, el cliente intenta autenticar el identificador de usuario como un identificador de usuario de administración.

Para utilizar un identificador de usuario de administración con cualquiera de los clientes de copia de seguridad/archivado, el identificador de usuario debe tener una de las autorizaciones siguientes:

Privilegio de sistema

Autorización en todo el sistema. Un administrador con privilegio de sistema pueden realizar cualquier tarea de administración.

Privilegio de política

Autorización sobre el dominio de políticas del nodo. Permite a un administrador gestionar objetos de políticas, inscribir nodos cliente y planificar operaciones de cliente para los nodos cliente.

Propietario de cliente

Autorización en el nodo cliente de IBM Spectrum Protect inscrito. Puede acceder al cliente por medio del cliente web o del cliente de archivado y copia de seguridad. Puede ser el propietario de datos y tener autorización para acceder físicamente a los datos de forma remota. Puede hacer una

copia de seguridad y restaurar archivos en el mismo sistema u otro distinto y puede suprimir espacios de archivos o datos archivados.

Acceso a cliente

Si desea utilizar el cliente web para hacer copias de seguridad y restaurar los archivos en un sistema de cliente remoto, debe disponer de un identificador de usuario de administración con autorización de acceso a cliente en el nombre de nodo para el sistema de cliente remoto. Si no desea que los administradores de IBM Spectrum Protect con autorización de acceso a cliente en el nombre de nodo puedan hacer operaciones de copia de seguridad y restauración de su sistema, especifique la opción `revokeremoteaccess` en el archivo de opciones del cliente.


La autorización de acceso a cliente sólo permite a los administradores de IBM Spectrum Protect hacer copias de seguridad y restaurar archivos en sistemas remotos. No tienen acceso físico a los datos. Es decir, no pueden restaurar en sus propios sistemas los datos que pertenecen al sistema remoto. Para restaurar en el propio sistema los datos que pertenecen a un sistema remoto, debe poseer por lo menos autorización de propietario de cliente.

Para determinar qué autorización tiene, puede utilizar uno de los siguientes métodos:

- En la ventana principal de la GUI de IBM Spectrum Protect, seleccione **Archivo** → **Información acerca de la conexión**.
- Utilice el mandato `QUERY ADMIN` del servidor de IBM Spectrum Protect desde el cliente de línea de mandatos de administración.

Referencia relacionada:

“`Revokeremoteaccess`” en la página 543

 Mandato `QUERY ADMIN`

Inicio de una sesión en la GUI Java

Los pasos que se utilizan para iniciar el programa de la interfaz gráfica de usuario del cliente de archivado y copia de seguridad depende del sistema operativo.

Procedimiento

Complete el procedimiento que sea apropiado para que su sistema operativo inicie la interfaz gráfica de usuario de Java.

Sistema operativo	Procedimiento
Mac OS X	<ul style="list-style-type: none"> • Pulse dos veces en la aplicación de IBM Spectrum Protect para iniciar el cliente de copia de seguridad y archivado sin privilegios de administrador del sistema. Cuando ejecute el cliente sin privilegios de administrador del sistema, puede gestionar los archivos que posee el usuario actual. • Pulse dos veces IBM Spectrum Protect para administradores y seleccione IBM Spectrum Protect. Después de introducir un nombre de usuario administrador del sistema y una contraseña, se inicia el cliente con privilegios de administrador del sistema. Cuando ejecuta el cliente con privilegios de administrador, puede gestionar los archivos que poseen todos los usuarios en el sistema. • También puede iniciar el cliente de copia de seguridad y archivado utilizando el mandato dsmj. Puede ejecutar el cliente como un proceso en primer plano o en segundo plano. El script dsmj está instalado en /Library/Application Support/tivoli/tsm/client/ba/bin.
AIX, Linux, Solaris	<p>En sistemas UNIX distintos a Mac OS X, la interfaz gráfica de usuario del cliente de copia de seguridad y archivado se debe ejecutar desde X Window System. Si ve el icono de IBM Spectrum Protect en el escritorio, significa que ya se está ejecutando el cliente. Efectúe una doble pulsación en el icono para abrir la ventana IBM Spectrum Protect. Si el icono IBM Spectrum Protect no se muestra en el escritorio, inicie la interfaz gráfica del cliente de copia de seguridad y archivado mediante el mandato dsmj. Puede ejecutar el cliente como un proceso en primer plano o en segundo plano.</p>

El cliente de copia de seguridad y archivado localiza y utiliza las opciones que se especifican en el archivo de opciones de sistema del cliente (dsm.sys) y en los archivos de opciones del cliente (dsm.opt).

Conceptos relacionados:

Capítulo 2, “Configurar el cliente de IBM Spectrum Protect”, en la página 49

contraseña de IBM Spectrum Protect

El administrador de IBM Spectrum Protect puede requerir que el usuario utilice una contraseña para conectarse al servidor.

El cliente de IBM Spectrum Protect le solicita la contraseña, en caso de que se necesite una. Póngase en contacto con el administrador de IBM Spectrum Protect si desconoce la contraseña.

Tareas relacionadas:

“Cambio de la contraseña” en la página 148

Asistente para la instalación

Cuando se inicia el cliente GUI, este comprueba si existe un archivo de opciones del sistema cliente.

Si no existe el archivo de opciones del cliente (lo cual suele suceder después de haber instalado el cliente por primera vez en el sistema), el asistente para la instalación se iniciará automáticamente para ayudarle a realizar todos los pasos del proceso de configuración.

El archivo de opciones del cliente es `dsm.sys`.

Inicio de una sesión de línea de mandatos

Puede iniciar una sesión de línea de mandatos por medio del mandato **dsmc** .

Nota: Si el directorio `/usr/bin` contiene un enlace simbólico al ejecutable de IBM Spectrum Protect y se han establecido todas las variables, puede especificar el mandato **dsmc** desde cualquier directorio. Sino, especifique la vía de acceso completa del mandato.

Nota: En Mac OS X, los administradores del sistema pueden utilizar el mandato **sudo** para obtener autorización adicional con el fin de que el cliente de copia de seguridad y archivado pueda acceder a los archivos de todos los usuarios del sistema.

En la línea de mandatos, especifique **dsmc** seguido del mandato (*modalidad por lotes*). Si los directorios `/usr/bin` o `opt/bin` contienen un enlace simbólico al directorio de instalación de IBM Spectrum Protect, puede especificar el mandato **dsmc** desde cualquier directorio. De lo contrario, puede especificar el nombre completo.

Solo se puede iniciar el cliente con el mandato "dsmc" en caso de que la variable de entorno `PATH` se actualice con la vía de acceso a la ubicación del cliente.

El administrador de IBM Spectrum Protect puede requerir que el usuario utilice una contraseña para conectarse al servidor. El cliente le solicita la contraseña, si se necesita. Póngase en contacto con el administrador si no conoce la contraseña.

Conceptos relacionados:

"Opciones en la modalidad interactiva" en la página 661

"Tareas de usuario root y autorizado del cliente de UNIX y Linux" en la página 49

Capítulo 11, "Utilización de los mandatos", en la página 655

Utilización de la modalidad por lotes

Utilice la modalidad *por lotes* para entrar un solo mandato de cliente. Cuando utilice la modalidad por lotes, el mandato debe ir precedido de **dsmc**.

Acerca de esta tarea

Por ejemplo, para emitir el mandato **incremental**, escriba lo siguiente en el indicador de mandatos:

```
dsmc incremental
```

Algunos mandatos requieren uno o más argumentos. Por ejemplo, para archivar un archivo:

```
dsmc archive /home/proj1/file1.txt
```

En función del valor actual de la opción `passwordaccess`, puede que el cliente le solicite la contraseña antes de procesar el comando en una sesión en modalidad por lotes.

Cuando escribe la contraseña, ésta no se visualiza en la pantalla.

Referencia relacionada:

“Passwordaccess” en la página 509

Emisión de una serie de mandatos mediante la modalidad interactiva

Utilice la modalidad *interactiva* si desea emitir una serie de mandatos.

Acerca de esta tarea

La conexión con el servidor solo se establece una vez para la modalidad interactiva, por lo que podrá procesar una serie de mandatos más deprisa en la modalidad interactiva que en la modalidad por lotes.

Para iniciar una sesión de mandatos de cliente en modalidad interactiva, entre uno de los siguientes mandatos:

- `dsmc`
- `dsmc loop`

Se visualiza el siguiente mensaje en su pantalla:

```
Protect>
```

Si está en la modalidad interactiva, no es necesario escribir **dsmc** delante de los mandatos. Por ejemplo, en lugar de escribir **dsmc archive** para archivar un archivo, escriba solamente **archive**.

Por ejemplo, para archivar un archivo, escriba el mandato con la especificación de archivo:

```
archive /home/proj1/file1.txt
```

En función del valor actual de la opción `passwordaccess`, puede que el cliente le solicite la contraseña para que pueda especificar un comando en una sesión interactiva.

Cuando escribe la contraseña, ésta no se visualiza en la pantalla.

Especificación de cadenas de entrada que contengan espacios en blanco o comillas

Debe seguir ciertas reglas cuando especifique una cadena de entrada que tenga espacios en blanco o comillas.

Siga estas reglas cuando especifique una cadena de entrada que tenga espacios en blanco o comillas:

- Si la cadena de entrada tiene uno o varios espacios, inclúyala entre comillas simples o dobles. Puede utilizar comillas simples o dobles, siempre y cuando coincidan.
- Si la cadena de entrada contiene alguna comilla simple, inclúyala entre comillas dobles, como en el siguiente ejemplo:
-description="Annual backup of the accounting department's monthly reports"
- Si la cadena de entrada contiene alguna comilla doble, inclúyala entre comillas simples, como en el siguiente ejemplo:
-description='New translations of "The Odyssey" and "The Iliad"'
- Si la cadena de entrada tiene espacios y comillas, inclúyala entre comillas. Las comillas externas no pueden ser las mismas que las comillas dentro de la cadena.

Restricción: Una cadena de entrada que contenga comillas simples y dobles no es una cadena válida.

Las siguientes reglas se aplican a estos tipos de datos:

- Nombres completos
- La opción `description` que especifique en el mandato **archive**
- Cualquier valor de opción donde la serie de caracteres incluya espacios o comillas

Importante: No podrá utilizar caracteres de escape con las cadenas de entrada. Los caracteres de escape reciben el mismo tratamiento que los demás caracteres. A continuación, se muestran algunos ejemplos en los que no se reconocen los caracteres de escape:

- Si la serie de caracteres está en un archivo de opciones
- Si la serie de caracteres está en un archivo de lista
- Si la serie de caracteres se especifica en la modalidad interactiva

Inicio: consideraciones adicionales

Puede incluir opciones en forma de argumentos para los mandatos **dsmj** y **dsmc**. Por ejemplo, puede utilizar opciones para modificar el formato que muestra fechas, horas y números o para incluir la contraseña para que el cliente de copia de seguridad y archivado no la solicite.

Acerca de esta tarea

Asimismo, si existe más de un servidor definido en `dsm.sys` y desea establecer contacto con un servidor distinto para hacer uso de los servicios de copia de seguridad/archivado (un servidor distinto del que se ha especificado en el archivo de opciones de usuario `dsm.opt`), especifique el servidor con la opción `servername`.

Por ejemplo:

```
dsmj -servername=server_b
```

La GUI Java GUI (`dsmj`) acepta parámetros de línea de mandatos como, por ejemplo, las opciones `-X` de Java. A consecuencia de ello, ahora también puede modificar el tamaño del almacenamiento dinámico de Java. Por ejemplo:

```
dsmj -Xmx512M
```

Inicio de una sesión de cliente web

El cliente web es una aplicación de inicio de Java Web que se puede iniciar y gestionar independientemente del software del navegador web. Después de instalar y configurar el cliente web en la estación de trabajo, puede utilizar el cliente web para obtener acceso remoto y poder ejecutar, de manera remota, operaciones de copia de seguridad, restauración, archivado o recuperación de datos en el nodo de cliente. El cliente web permite la utilización de dispositivos de ayuda para usuarios con discapacidades e incluye mejoras en la navegación con el teclado.

Antes de empezar

Asegúrese de configurar el cliente web antes de utilizarlo. Puede utilizar el asistente para la configuración del cliente para configurar el cliente web.

Consulte el tema de los requisitos de software para el sistema operativo y determine qué navegadores son compatibles para este software.

Para ejecutar el cliente web desde los navegadores de Firefox, la opción para **Enable JavaScript** debe estar activada. De forma predeterminada, esta opción está activada en Firefox.

Procedimiento

1. Especifique la URL de la estación de trabajo del cliente en la que ha instalado el cliente web en su navegador web. También, especifique el número de puerto HTTP que se define en la estación de trabajo del cliente para el cliente web. El número de puerto predeterminado es 1581. El siguiente ejemplo muestra la sintaxis de un URL del cliente web:

```
http://myhost.mycompany.com:1581
```

Si escribe un URL diferente o pulsa **Atrás** durante una operación, el cliente web se desconectará y la operación actual finalizará.

2. Siga las instrucciones de la página de inicio del cliente web de IBM Spectrum Protect para iniciar el cliente web.

Cada vez que inicie el cliente web, se descargará en su navegador una aplicación de inicio de Java Web (archivo .jnlp). Abra el archivo dsm.jnlp para iniciar el cliente web.

Puede cerrar el navegador web una vez iniciado el cliente web.

Consejo: El cliente web se ejecuta en el idioma de la estación de trabajo del navegador web porque utiliza el entorno de tiempo de ejecución Java instalado de manera local en la estación de trabajo. Por ejemplo, si la estación de trabajo del navegador web se está ejecutando en un entorno local en inglés y el nodo de cliente remoto está en japonés, la página de inicio del cliente web se mostrará en japonés, pero el cliente web estará en inglés.

Conceptos relacionados:

“Descripción general de la configuración del cliente web” en la página 65

Privilegios de usuario

Si tiene previsto utilizar el cliente web, asegúrese de que se le asigne un identificador de usuario de administración con privilegio de sistema, privilegio de políticas, autorización de acceso a cliente o autorización de propietario de cliente.

Cuando se inscribe un nodo nuevo en el servidor, se debe otorgar al nodo un ID de usuario de administración con el mismo nombre de nodo con autorización de propietario de cliente.

El administrador del servidor de IBM Spectrum Protect tiene que especificar el parámetro `userid` con el mandato de servidor **REGISTER NODE**:

```
REGISTER NODE nombre_nodo contraseña userid=ID_usuario
```

donde el nombre de nodo y el ID de usuario de administración tienen que ser iguales. Por ejemplo:

```
REGISTER NODE node_a mypassword userid=node_a
```

Consejo: Puede utilizar la opción `revokeremoteaccess` para impedir que los administradores de IBM Spectrum Protect con privilegio de acceso a cliente realicen operaciones de cliente en la estación de trabajo a través del cliente web. Sin embargo, los administradores de IBM Spectrum Protect con privilegio de propietario de cliente, privilegio de sistema o privilegio de política podrán seguir realizando operaciones de cliente en la estación de trabajo a través del cliente web.

Conceptos relacionados:

“Autenticación del cliente de IBM Spectrum Protect” en la página 141

Referencia relacionada:

“Revokeremoteaccess” en la página 543

Iniciar automáticamente el planificador cliente

Puede iniciar el planificador cliente automáticamente al iniciar la estación de trabajo.

Si el administrador de IBM Spectrum Protect ha definido planificaciones para el nodo, el inicio del planificador cliente permite hacer automáticamente copias de seguridad de la estación de trabajo (o realizar otras acciones planificadas).

También puede utilizar el servicio de aceptación de clientes de IBM Spectrum Protect para gestionar el planificador.

Tareas relacionadas:

“Establecimiento del proceso del planificador cliente para que se ejecute como una tarea de fondo y se inicie automáticamente al arrancar” en la página 287

Cambio de la contraseña

El administrador de IBM Spectrum Protect puede requerir que el usuario utilice una contraseña para conectarse al servidor.

Acerca de esta tarea

El cliente de copia de seguridad y archivado le solicita la contraseña, en caso de que se necesite una. Póngase en contacto con el administrador de IBM Spectrum Protect si desconoce la contraseña.

Importante: La contraseña mencionada en este tema es distinta de la que se utiliza para los archivos cifrados.

Para cambiar la contraseña desde la GUI:

Procedimiento

1. En clientes Mac OS X, inicie el cliente de copia de seguridad y archivado con las Herramientas de IBM Spectrum Protect para administradores.
2. En la ventana principal, abra el menú **Herramientas** y seleccione **Cambiar contraseña**.
3. Entre las contraseñas actual y nueva, y vuelva a entrar la contraseña nueva en el campo **Verificar contraseña**.
4. Pulse **Cambiar**.

Resultados

Para cambiar la contraseña desde el cliente de línea de mandatos, escriba este mandato:

Para clientes de UNIX, Linux, y Windows:

```
dsmc set password
```

Para clientes de Mac OS X, escriba este mandato para cambiar la contraseña desde el cliente de línea de mandatos:

```
sudo dsmc set password
```

A continuación, entre las contraseñas antigua y nueva cuando se le solicite.

Las contraseñas pueden tener una longitud máxima de 63 caracteres. Las restricciones de contraseña varían, dependiendo del lugar donde se almacenan y gestionan las contraseñas y en función de la versión del servidor IBM Spectrum Protect al que se conecta el cliente.

Si el servidor de IBM Spectrum Protect tiene la versión 6.3.3 o posterior y si usa un servidor de directorios LDAP para autenticar contraseñas:

Utilice cualquiera de los siguientes caracteres para crear una contraseña:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z  
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z  
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ( )  
| { } [ ] : ; < > , ? / ~
```

Las contraseñas son sensibles a las mayúsculas y minúsculas, y están sujetas a restricciones adicionales que puedan imponer las políticas de LDAP.

Si el servidor IBM Spectrum Protect está en la versión 6.3.3 o posterior, y si no utiliza un servidor LDAP para gestionar contraseñas

Utilice cualquiera de los siguientes caracteres para crear una contraseña:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z  
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z  
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ( )  
| { } [ ] : ; < > , ? / ~
```

Las contraseñas se almacenan en la base de datos del servidor IBM Spectrum Protect y no distinguen entre mayúsculas y minúsculas.

Si el servidor IBM Spectrum Protect es anterior a la versión 6.3.3

Utilice cualquiera de los siguientes caracteres para crear una contraseña:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z  
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z  
0 1 2 3 4 5 6 7 8 9  
_ - & + .
```

Las contraseñas se almacenan en la base de datos del servidor IBM Spectrum Protect y no distinguen entre mayúsculas y minúsculas.

Recuerde:

En la línea de mandatos, escriba entre comillas todos los parámetros que contengan uno o varios caracteres especiales. Sin las comillas, los caracteres especiales se pueden interpretar como caracteres de escape, caracteres de redirección de archivos u otros caracteres que tienen importancia para el sistema operativo.

En sistemas AIX, Linux y Solaris:

Escriba los parámetros de mandato entre comillas simples (').

Ejemplo de línea de mandatos:

```
dsmc set password -type=vmguest 'Win 2012 SQL'
'tsm12dag\administrator' '7@#$$%^&7'
```

Las comillas no son necesarias cuando escribe una contraseña con caracteres especiales en el archivo de opciones.

Conceptos relacionados:

“Iniciar automáticamente el planificador cliente” en la página 148

Tareas relacionadas:

“Inicio: consideraciones adicionales” en la página 146

Referencia relacionada:

“Contraseña” en la página 507

“Establecer contraseña” en la página 784

Ordenación de listas de archivos mediante la GUI del cliente de copia de seguridad y archivado

Puede utilizar la interfaz gráfica de usuario del cliente de copia de seguridad y archivado para mostrar, ordenar o seleccionar archivos.

Acerca de esta tarea

Tabla 33. Trabajar con archivos mediante la GUI del cliente de copia de seguridad y archivado

Tarea	Procedimiento
Visualización de archivos	Para visualizar los archivos de un directorio, pulse en el icono de la carpeta situado junto al nombre de directorio. Los archivos aparecen en el cuadro Lista de archivos de la derecha.
Clasificar la lista de archivos	<ul style="list-style-type: none">• Pulse la cabecera de la columna que corresponda en el cuadro Lista de archivos.
Visualizar versiones de copia de seguridad activas e inactivas	<ul style="list-style-type: none">• Pulse la opción Visualizar archivos activos/inactivos en el menú Ver.• Pulse la herramienta Visualizar archivos activos e inactivos en la barra de herramientas.
Visualizar sólo versiones de copia de seguridad activas	Pulse la opción Visualizar sólo archivos activos en el menú Ver .

Tabla 33. Trabajar con archivos mediante la GUI del cliente de copia de seguridad y archivado (continuación)

Tarea	Procedimiento
Seleccionar archivos para restaurar o recuperar	<ul style="list-style-type: none"> • Pulse la casilla situada junto al nombre de directorio o archivo que desea restaurar o recuperar. • Resalte los archivos que desea restaurar o recuperar y pulse la herramienta Seleccionar elementos en la barra de herramientas. • Resalte los archivos que desea restaurar o recuperar y pulse la opción Seleccionar elementos en el menú Editar.
Deseleccionar archivos	<ul style="list-style-type: none"> • Pulse la casilla marcada situada junto al nombre de directorio o archivo. • Resalte los archivos que desea deseleccionar y pulse la herramienta Deseleccionar elementos en la barra de herramientas. • Resalte los archivos que desea deseleccionar y pulse la opción Deseleccionar elementos en el menú Editar.
Visualizar información de archivo	<ul style="list-style-type: none"> • Resalte el nombre de archivo y pulse el botón Ver detalles de archivo en la barra de herramientas. • Resalte el nombre de archivo y seleccione Detalles de archivo en el menú Ver.

Nota:

1. A menos que se indique algo distinto, las tareas y procedimientos de la tabla de arriba se aplican a todas las GUI de cliente.
2. Con las GUI de cliente, puede clasificar una lista de archivos en función de varios atributos, como por ejemplo, nombre, directorio, tamaño o fecha de modificación. La clasificación de archivos en función de la fecha de la última copia de seguridad puede ser útil para determinar la fecha y la hora que se debe utilizar en la función de instante específico.
3. Un archivo *activo* es la versión de copia de seguridad más reciente de un archivo que existía en la estación de trabajo cuando se ejecutó la última copia de seguridad. El resto de versiones de copia de seguridad del archivo están *inactivas*. Sólo se visualizan las versiones de copia de seguridad activas de los archivos, a menos que seleccione la opción de menú **Visualizar archivos activos/inactivos**. Si suprime el archivo de la estación de trabajo, la versión activa pasa a estar inactiva la siguiente ocasión en que se ejecute una copia de seguridad incremental.

En el cliente de línea de mandatos, puede utilizar los mandatos **query** con la opción **inactive** para visualizar los objetos activos e inactivos. Puede utilizar los mandatos **restore** con las opciones **pick** e **inactive** para generar la lista de copias de seguridad activas e inactivas para realizar selecciones.

Referencia relacionada:

“Inactive” en la página 456

“Pick” en la página 512

Visualización de ayuda en línea

Puede visualizar la ayuda en línea de cualquiera de los siguientes modos: en la GUI del cliente de copia de seguridad y archivado, desde el cliente web, o desde la línea de mandatos de **dsmsc**.

Acerca de esta tarea

- En la GUI del cliente de copia de seguridad y archivado:
 - Abra el menú Ayuda. Pulse en **Help** o pulse en F1.
 - Pulse el botón **Ayuda** en la ventana actual.
 - En sistemas de Mac, pulse en la interrogación de la GUI(?), que muestra la información online sobre la operación actual.
- Desde la línea de mandatos de **dsmc**: escriba el mandato **help**. Se visualiza la tabla de contenidos completa para el texto de ayuda que está disponible.

Referencia relacionada:

“Help” en la página 703

Finalización de una sesión

Puede terminar una sesión de cliente desde la GUI del cliente de copia de seguridad y archivado o desde la línea de mandatos **dsmc**.

Acerca de esta tarea

- Desde la GUI de cliente de copia de seguridad y archivado:
 - Abra el menú **File** (Archivo) y seleccione **Quit** (Salir).
 - Pulse Command+Q.
 - Abra el menú **Archivo** y seleccione **Salir**.
 - Abra el menú **Sistema** y seleccione **Cerrar**.
 - Para el cliente web: abra otro URL o cierre el navegador.
- En la línea de mandatos de DSMC:
 - En la modalidad de proceso por lotes, cada mandato **dsmc** que introduce es una sesión completa. El cliente finaliza la sesión cuando acaba de procesar el mandato.
 - Para finalizar una sesión interactiva, escriba **quit** en el indicador Protect>.
 - Para interrumpir un mandato **dsmc** antes de que el cliente haya terminado el proceso, especifique QQ en la consola de IBM Spectrum Protect. En la mayoría de los casos, no en todos, ello interrumpirá el mandato. Si no se puede interrumpir el mandato, utilice el mandato **kill -9** de UNIX desde un indicador de mandatos disponible. No pulse Control-C ni utilice el mandato **kill -15** de UNIX ya que podría producir resultados inesperados.

Referencia relacionada:

“Loop” en la página 712

Foros en línea

Para participar en debates de usuarios de IBM Spectrum Protect puede inscribirse en el servidor de listas ADSM-L.

Acerca de esta tarea

Se trata de un foro de usuarios administrado por Marist College. Aunque IBM no le da soporte de forma oficial, los desarrolladores del producto y otros miembros del personal de soporte de IBM también participan de forma informal. Dado que no se trata de un canal oficial de soporte de IBM deberá ponerse en contacto con el servicio de soporte de IBM si necesita obtener una respuesta específica de IBM. De lo contrario, no tiene ninguna garantía de que IBM responda a la pregunta en el servidor de listas.

Puede inscribirse enviando un mensaje a la siguiente dirección de correo electrónico:

`listserv@vm.marist.edu`

El cuerpo del mensaje debe contener la siguiente información:

`SUBSCRIBE ADSM-L mi_nombre mi_apellido`

El servidor de listas le enviará un mensaje solicitando que confirme la solicitud de suscripción. Una vez confirmada la solicitud de suscripción, el servidor de listas le enviará nuevas instrucciones. A continuación, podrá enviar mensajes al servidor de listas escribiendo un correo electrónico a:

`ADSM-L@vm.marist.edu`

Si posteriormente desea borrarse de ADSM-L, puede enviar un mensaje a la siguiente dirección de correo electrónico:

`listserv@vm.marist.edu`

El cuerpo del mensaje debe contener la siguiente información:

`SIGNOFF ADSM-L`

También puede leer y buscar los archivos ADSM-L, participar en foros de debates y acceder a otros recursos en el siguiente URL:

<http://www.adsm.org>

Capítulo 4. Copia de seguridad de los datos

Utilice el cliente de copia de seguridad/archivado para almacenar versiones de copia de seguridad de los archivos en un servidor de IBM Spectrum Protect. Estas versiones de copia de seguridad se pueden restaurar en caso de que los archivos originales se pierdan o resulten dañados.

Todos los procedimientos de copia de seguridad y restauración de cliente también se aplican al cliente web.

Restricción: El cliente web no dispone de un Editor de preferencias para configurar las opciones del cliente.

A continuación se muestra una lista de las principales tareas de copia de seguridad.

- “Planificación de las copias de seguridad”
- “Consideraciones previas a la copia de seguridad (UNIX y Linux)” en la página 157
- “Realización de una copia de seguridad incremental selectiva o incremental por fecha (UNIX y Linux)” en la página 170
- “Supresión de datos de copia de seguridad” en la página 185
- “Copia de seguridad de archivos desde uno o varios espacios de archivos para una copia de seguridad de grupo (UNIX y Linux)” en la página 187
- “Copia de seguridad de imagen” en la página 194
- “Realice la copia de seguridad de los sistemas de archivos NAS utilizando el Protocolo de gestión de datos de redes” en la página 208

Planificación de las copias de seguridad

Si es la primera vez que utiliza este producto o si solo realiza copias de seguridad de los archivos de forma ocasional, puede utilizar la tabla que figura en este tema como lista de comprobación de los pasos previos que deben tenerse en cuenta antes de realizar una copia de seguridad.

Lea la lista de tareas para determinar si está preparado para realizar una copia de seguridad de los datos.

- Debe decidir si desea realizar una copia de seguridad o una copia archivada. Consulte “Cuándo realizar copias de seguridad y cuándo archivar copias” en la página 156 para obtener más información.
- En el apartado “Consideraciones previas a la copia de seguridad (UNIX y Linux)” en la página 157 encontrará información importante que debe tenerse en cuenta antes de hacer la copia de seguridad de los archivos y directorios.
- ¿Debe excluir archivos de los servicios de copia de seguridad? Consulte el apartado “Opciones de inclusión/exclusión para controlar el proceso” en la página 160 para obtener más información.

Conceptos relacionados:

Capítulo 1, “Instalación de los clientes de archivado y copia de seguridad de IBM Spectrum Protect”, en la página 1

Los archivos de los que se hace copia de seguridad

Cuando se solicita una copia de seguridad, el cliente realiza una copia de seguridad de un archivo si se cumplen algunos de los requisitos siguientes.

Para hacer copia de seguridad de un archivo, el cliente debe cumplir los siguientes requisitos:

- La clase de gestión seleccionada contiene un grupo de copia de seguridad.
- El archivo cumple con los requisitos de serialización que se definen en el grupo de copia de seguridad. Si el parámetro de serialización del grupo de copia es `static` o `shrstatic` y el archivo cambia durante la copia de seguridad, no se ha realizado la copia de seguridad del archivo.
- El archivo cumple con los requisitos de **mode** que se definen en el grupo de copia de seguridad. Si el parámetro **mode** del grupo de copia es `modified`, el archivo debe haber cambiado desde la última copia de seguridad. Si **mode** es `absoluta`, puede realizarse una copia de seguridad del archivo aunque este no haya cambiado.
- El archivo cumple con los requisitos de frecuencia que se definen en el grupo de copia de seguridad. El número mínimo especificado de días desde la última copia de seguridad que deben transcurrir antes de que se realice la copia de seguridad del archivo.
- El archivo no se excluye de la copia de seguridad por una sentencia de exclusión.
- El archivo no se excluye de la copia de seguridad por un sistema operativo. Estos archivos excluidos se pueden encontrar en la subclave de registro `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup`.

Los archivos que son parte del estado del sistema de Windows se pueden elegir para realizar la copia de seguridad solo cuando se ha realizado una copia de seguridad del estado del sistema. Puede realizar una copia de seguridad del estado del sistema únicamente como una sola entidad debido a las dependencias entre los componentes de Estado del sistema. No puede realizar la copia de seguridad o restaurar los archivos de forma individual. Por ejemplo, ya que `C:\windows\system32\ntoskrnl.exe` es parte del estado del sistema de Windows, no se realiza la copia de seguridad durante la copia de seguridad incremental o selectiva de la unidad `C:\`.

Conceptos relacionados:

Capítulo 9, “Políticas de gestión de almacenamiento”, en la página 299

“Clases de gestión y grupos de copia” en la página 300

Referencia relacionada:

“Absolute” en la página 345

Cuándo realizar copias de seguridad y cuándo archivar copias

Cuando el cliente de copia de seguridad/archivado realiza una copia de seguridad o una copia archivada de un archivo, envía una copia de este archivo y sus atributos asociados al servidor. Sin embargo, las operaciones de copia de seguridad y archivado tienen objetivos distintos.

Utilice las copias de seguridad como protección en caso de que los archivos se dañen de forma súbita y utilice las copias archivadas para conservar las versiones de los archivos de forma más permanente.

Los datos de copia de seguridad se gestionan por versiones mediante la política predeterminada basada en reglas. Utilizando estas reglas, el administrador de IBM Spectrum Protect puede controlar los procesos siguientes:

- El número de versiones que se mantienen en el servidor de IBM Spectrum Protect
- El número de días que se conserva cada copia adicional de la copia de seguridad
- Lo que ocurre con las versiones de copia de seguridad cuando se suprime el archivo del sistema cliente

Cada copia del archivo se almacena en el servidor se considera una versión independiente y única del archivo.

El archivado es un mecanismo potente y flexible para guardar datos a largo plazo. Los datos archivados, denominados copias de archivado, se guardan durante un número determinado de días. La función de archivado no tiene un concepto o soporte para las versiones. El usuario o el administrador son los responsables de determinar qué archivos se agregan a las copias archivadas.

Consejo: Si se archiva un archivo varias veces mediante la misma descripción de archivo, se añade una copia nueva del archivo al archivado cada vez que se ejecuta la operación. Para simplificar la operación de recuperación, guarde solo una copia de un archivo en cada archivado.

Las copias de seguridad se protegen contra el daño de los archivos o la pérdida que puede ocurrir a través de la supresión accidental, corrupción o anomalías en el discos. El servidor conserva una o varias versiones de copia de seguridad de cada archivo del que se ha realizado una copia de seguridad. Las versiones antiguas se eliminan a medida que se van creando versiones nuevas. El administrador se encarga de establecer el número de versiones de copia de seguridad que el servidor debe conservar.

Las copias archivadas se guardan para su almacenamiento a largo plazo. Los administradores pueden limitar el período de tiempo que estas copias deben conservarse. El servidor puede almacenar un número ilimitado de versiones de copias archivadas de un archivo. Las copias de archivado son útiles si desea volver a una versión particular de sus archivos, o si desea suprimir un archivo desde la estación de trabajo y recuperarla más tarde si fuese necesario. Por ejemplo, es posible que deba guardar hojas de cálculo para los impuestos, pero, puesto que no las utiliza, puede que no desee dejarlas en su estación de trabajo.

Conceptos relacionados:

Capítulo 6, “Archivar y recuperar datos (UNIX y Linux)”, en la página 269

“Restauración de datos desde un conjunto de copias de seguridad” en la página 240

Consideraciones previas a la copia de seguridad (UNIX y Linux)

Diversos factores en el sistema o el entorno pueden afectar la manera en que el cliente de archivado y copia de seguridad procesa los datos. Revise estas consideraciones antes de realizar la copia de seguridad de los datos.

traspaso de datos sin LAN

El traspaso de datos fuera de la LAN desplaza el traspaso de datos de cliente desde la red de comunicaciones hasta una red de área de almacenamiento (SAN). De esta forma se reduce la carga en el servidor de IBM Spectrum Protect.

La SAN proporciona una vía de acceso que permite realizar una copia de seguridad, restaurar, archivar y recuperar datos en un dispositivo de almacenamiento conectado a la SAN y desde el mismo. Los datos del cliente se traspasan por la SAN hasta llegar al dispositivo de almacenamiento utilizando el agente de almacenamiento de IBM Spectrum Protect. El agente de almacenamiento debe estar instalado en el mismo sistema que el cliente.

Los clientes de AIX, Linux y Solaris admiten el movimiento de datos sin LAN.

Requisitos previos del soporte para fuera de la LAN

Para habilitar el soporte sin LAN, debe instalar y configurar el agente de almacenamiento de IBM Spectrum Protect for SAN en la estación de trabajo cliente.

IBM Spectrum Protect for SAN es un producto separado.

Para obtener más información sobre cómo instalar y configurar el agente de almacenamiento, consulte la documentación de IBM Spectrum Protect for SAN.

Opciones de traspaso de datos fuera de la LAN

Para habilitar el traspaso de datos fuera de la LAN, puede utilizar varias opciones del cliente. Antes debe instalar y configurar el agente de almacenamiento de IBM Spectrum Protect for SAN en la estación de trabajo cliente.

Utilice las opciones siguientes para habilitar el traspaso de datos fuera de la LAN:

enablelanfree

Especifica si se activa una ruta disponible fuera de la LAN para un dispositivo de almacenamiento conectado a SAN.

lanfreecommmethod

Especifica un protocolo de comunicaciones entre el cliente y el agente de almacenamiento.

lanfreeshmport

Especifica el número exclusivo que el cliente y el agente de almacenamiento utilizarán para identificar el área de memoria compartida utilizada para las comunicaciones.

lanfreetcpport

Especifica el número de puerto TCP/IP en el que está conectado el agente de almacenamiento.

lanfreetcpserveraddress

Especifica la dirección TCP/IP del agente de almacenamiento.

Referencia relacionada:

“Enablelanfree” en la página 416

“Lanfreecommmethod” en la página 478

“Lanfreeshmport” en la página 480

“Lanfreessl” en la página 481

“Lanfreetcpport” en la página 481

“Lanfreetcpserveraddress” en la página 482

Copias de seguridad incrementales en sistemas con restricción de memoria

El rendimiento de la copia de seguridad incremental se ve afectado negativamente si la cantidad de memoria disponible en el sistema es baja antes de iniciarse la copia de seguridad.

Si el sistema tiene restricciones de memoria, especifique la opción `memoryefficientbackup yes` en el archivo de opciones de cliente. Esta opción da lugar a que el cliente de copia de seguridad y archivado sólo procese un único directorio cada vez, lo que reduce el consumo de memoria pero incrementa el tiempo necesario para la realización de la copia de seguridad. Cuando especifica `yes`, el cliente sólo analiza un único directorio cada vez para la realización de la copia de seguridad. Si el rendimiento sigue siendo bajo, compruebe los valores del búfer de comunicación y el enlace de comunicación existente entre el sistema y el servidor de IBM Spectrum Protect. Si el sistema no tiene restricciones de memoria, el establecimiento de la opción `memoryefficientbackup` en `yes` afectará negativamente al rendimiento de la copia de seguridad.

Referencia relacionada:

“`Memoryefficientbackup`” en la página 491

Copias de seguridad incrementales en sistemas con un gran número de archivos

El cliente puede utilizar grandes cantidades de memoria para ejecutar las operaciones de copia de seguridad incremental, en especial en los sistemas de archivos que contienen gran cantidad de archivos.

El término *memoria* tal como se utiliza aquí hace referencia a la memoria direccionable que está disponible para el proceso del cliente. La memoria direccionable es una combinación de la RAM física y de la memoria virtual.

Como término medio, el cliente utiliza aproximadamente 300 bytes de memoria para cada objeto (archivo o directorio). De esta forma, para un sistema de archivos que tenga un millón de archivos y directorios, el cliente necesita, como promedio, 300 MB de memoria aproximadamente. La cantidad exacta de memoria que se utiliza para cada objeto varía en función de la longitud de la vía de acceso del objeto y de la longitud del nombre o de la profundidad de anidamiento de los directorios. El número de bytes de datos no es un factor importante para la determinación del requisito de memoria del cliente de copia de seguridad.

El número máximo de archivos puede determinarse dividiendo la cantidad máxima de memoria virtual disponible para un proceso entre la cantidad media de memoria necesaria para cada objeto.

El requisito de memoria total puede reducirse aplicando cualquiera de los métodos siguientes:

- Utilice la opción del cliente de `memoryefficientbackup diskcachemethod`. Esta opción reduce la utilización de memoria a un mínimo, lo cual se obtiene a expensas del rendimiento y de un incremento significativo del espacio de disco necesario para la realización de la copia de seguridad. Los datos de descripción de archivo del servidor se almacenan en una base de datos temporal que reside en el disco, no en la memoria. A medida que se exploran los directorios de la estación de trabajo, se consulta la base de datos para determinar si ha de

realizarse una operación de copia de seguridad, de actualización o de caducidad para cada objeto. Cuando se ha completado la copia de seguridad, el archivo de base de datos se suprime.

- Utilice la opción del cliente **memoryefficientbackup yes**. El promedio de memoria que utiliza el cliente equivaldrá entonces a 300 bytes multiplicados por el número de directorios más 300 bytes por cada archivo del directorio que está procesándose. Para los sistemas de archivos con números grandes (millones) de directorios, puede que el cliente no pueda alojar suficiente memoria para llevar a cabo la copia de seguridad incremental con **memoryefficientbackup yes**.
- Los clientes UNIX y los clientes Linux pueden utilizar la opción de cliente **virtualmountpoint** para definir varios puntos de montaje virtuales dentro de un único sistema de archivos, lo que permitirá que el cliente pueda realizar la copia de seguridad de cada uno de estos independientemente.
- Si la opción de cliente **resourceutilization** se establece en un valor mayor que 4 y se desea realizar la copia de seguridad de varios sistemas de archivos, la reducción del valor de la opción **resourceutilization** a 4 o un valor inferior limita el proceso de la copia de seguridad incremental a un único sistema de archivos cada vez. Este ajuste reduce los requisitos de memoria. Si, por razones de rendimiento, debe realizarse la copia de seguridad de varios sistemas de archivos en paralelo, y los requisitos de memoria combinados exceden los límites del proceso, pueden utilizarse varias instancias del cliente de copia de seguridad para realizar la copia de seguridad de varios sistemas de archivos en paralelo. Por ejemplo, si desea realizar la copia de seguridad de dos sistemas de archivos al mismo tiempo, pero los requisitos de memoria de éstos exceden los límites de un único proceso, inicie una instancia del cliente para que realice la copia de seguridad de uno de los sistemas de archivos e inicie una segunda instancia del cliente para que realice la copia de seguridad del otro sistema de archivos.
- Utilice la opción de cliente - **incrbydate** para realizar una copia de seguridad "incremental por fecha".
- Utilice la opción **exclude.dir** del cliente para impedir que el cliente recorra los directorios y realice la copia de seguridad de los directorios cuya copia de seguridad no es necesario realizar.
- Excepto para Mac OS X, utilice la función de copia de seguridad de imágenes del cliente para realizar la copia de seguridad del volumen completo. Es posible que una copia de seguridad de imagen que utilice menos recursos del sistema y ejecute más rápidamente que la copia de seguridad incremental de algunos sistemas de archivos con un gran número de pequeños archivos.
- Reduzca el número de archivos por sistema de archivos distribuyendo los datos entre varios sistemas de archivos.

Referencia relacionada:

"Snapdiff" en la página 561

"Opciones exclude" en la página 425

"Incrbydate" en la página 474

"Memoryefficientbackup" en la página 491

"Resourceutilization" en la página 539

"Virtualmountpoint" en la página 606

Opciones de inclusión/exclusión para controlar el proceso

Puede que tenga archivos en los sistemas de archivos cuya copia de seguridad no desee realizar. Estos archivos podrían ser archivos del núcleo, cachés locales de los sistemas de archivos de red, archivos del sistema operativo o de aplicaciones que

podrían recuperarse fácilmente si se volviera a instalar el programa o cualquier otro archivo que pueda volver a crearse con facilidad.

Puede utilizar las opciones `exclude` e `include` de la lista de opciones de inclusión/exclusión para especificar los archivos que deben excluirse del proceso de copia de seguridad.

Utilice las opciones `include` y `exclude` de `dsm.sys` para definir qué archivos deben incluirse o excluirse del proceso de copia de seguridad incremental o selectiva. Un archivo es elegible para la copia de seguridad salvo que se excluya por una opción `exclude`. No es necesario utilizar una opción `include` para incluir archivos específicos para la copia de seguridad, a menos que estos archivos estén en un directorio que contenga otros archivos que desea excluir.

IBM Spectrum Protect utiliza clases de gestión para determinar cómo se deben gestionar las copias de seguridad en el servidor. Cada vez que efectúe una copia de seguridad de un archivo, se asignará al archivo una clase de gestión. La clase de gestión es una clase de gestión predeterminada que selecciona personalmente o bien una clase de gestión que asigna al archivo mediante la utilización de la opción `include` en la lista de inclusión/exclusión. Si asigna una clase de gestión, ésta deberá contener un grupo de copia de seguridad para el archivo cuya copia de seguridad desea realizarse.

Tareas relacionadas:

“Creación de una lista de inclusión/exclusión” en la página 124

“Establecimiento del proceso del planificador cliente para que se ejecute como una tarea de fondo y se inicie automáticamente al arrancar” en la página 287

Cifrado de datos durante una operación de copia de seguridad o archivado

La manera de garantizar la seguridad de datos consiste en cifrar los datos. Utilice el cifrado de datos para proteger los datos durante una operación de copia de seguridad o archivado. El cifrado AES (Advanced Encryption Standard - Estándar de cifrado avanzado) de 128 bits es la opción de cifrado predeterminada. Para obtener el nivel más alto de cifrado de datos, utilice el cifrado de datos AES (Estándar de cifrado avanzado) de 256 bits especificando la opción **encryptontype**.

Los datos que incluya se almacenarán en formato cifrado, y el cifrado no afectará a la cantidad de datos enviados o recibidos.

El cifrado sólo puede habilitarse en el cliente de copia de seguridad/archivado mediante la opción **include.encrypt**. Si no se utilizan sentencias `include.encrypt`, no se puede producir el cifrado.

El cifrado no es compatible con las copias de seguridad de la máquina virtual de VMWare que utilizan los modos de copia virtual incremental para siempre (**MODE=IFIncremental** y **MODE=IFFull**). Si el cliente se configura para el cifrado, no se puede utilizar la copia de seguridad siempre incremental.

Utilice las opciones **include** y **exclude** en `dsm.sys` para definir qué archivos incluir o excluir del proceso de copias de seguridad incrementales o selectivas. Un archivo es elegible para la copia de seguridad salvo que se excluya por una opción **exclude**. No es necesario utilizar una opción **include** para incluir archivos específicos para la copia de seguridad, a menos que estos archivos estén en un directorio que contenga otros archivos que desea excluir.

Para cifrar datos de archivos, debe seleccionar una contraseña de clave de cifrado, que el cliente utiliza para generar la clave de cifrado para cifrar y descifrar los datos de archivos. Guarde la contraseña de clave de cifrada para utilizarla posteriormente. Puede especificar si se debe guardar la contraseña de clave de cifrado en un archivo que se denomina TSM.PWD utilizando la opción **encryptkey**.

El cifrado del cliente de IBM Spectrum Protect permite especificar un valor que tenga un máximo de 63 caracteres de longitud. Esta contraseña de cifrado debe confirmarse al cifrar el archivo para la copia de seguridad y también debe especificarse cuando se realizan restauraciones de archivos cifrados.

Al restaurar el archivo cifrado, el cliente solicitará al usuario la contraseña de clave para descifrar el archivo en los casos siguientes:

- La opción **encryptkey** se ha establecido en Prompt.
- La clave proporcionada por el usuario en el caso anterior no coincide.
- La opción **encryptkey** se ha establecido en Save y la contraseña de clave guardada localmente no coincide con el archivo cifrado.

Referencia relacionada:

“Encryptiontype” en la página 417

“Encryptkey” en la página 418

“Options exclude” en la página 425

“Options include” en la página 458

Soporte para sistemas de archivos y ACL

Los sistemas de archivos especiales contienen información dinámica generada por el sistema operativo; no contienen datos ni archivos. Los clientes UNIX y Linux pasan por alto los sistemas de archivos especiales y su contenido.

Los sistemas de archivos especiales incluyen los siguientes tipos:

- El sistema de archivos /proc en la mayoría de las plataformas UNIX
- El sistema de archivos /dev/fd en Solaris
- El /dev/pts en Linux

El cliente de copia de seguridad y archivado puede trabajar en tipos de sistema de archivos específicos que se utilizan habitualmente. Para obtener una lista de los tipos de sistemas de archivos admitidos, consulte la Tabla 34.

Restricción: La tabla muestra el soporte completo de NFS en AIX, incluida la conservación de ACL y atributos ampliados. En otros sistemas operativos, se admiten las copias de seguridad de NFS, pero dichas copias de seguridad sólo incluyen metadatos POSIX estándares (permisos de acceso, fecha de creación, etc.). Para obtener más información sobre cómo realizar copias de seguridad de sistemas NFS, consulte “Copia de seguridad de sistemas de archivos de red” en la página 213.

Tabla 34. Sistemas de archivos admitidos y soporte para ACL

Plataforma	Sistema de archivos	Soporte de ACL
AIX	GPFS	yes
	JFS	yes
	JFS2	yes
	JFS2 NFSV4	yes
	VxFS	yes

Tabla 34. Sistemas de archivos admitidos y soporte para ACL (continuación)

Plataforma	Sistema de archivos	Soporte de ACL
Linux x86_64	Btrfs	yes
	XFS	yes
	EXT2	yes
	EXT3	yes
	EXT4	yes
	ReiserFS GPFS	yes
	JFS	yes
	VxFS	no
	NSS	no
		yes
Linux en servidores de Power Systems	Btrfs	yes
	XFS	yes
	EXT2	yes
	EXT3	yes
	EXT4	yes
	ReiserFS	yes
	JFS GPFS	no
		yes
Linux en z Systems	Btrfs	yes
	EXT2	yes
	EXT3	yes
	EXT4	yes
	ReiserFS	yes
	JFS	no
	GPFS	yes
macOS	HFS estándar (HFS)	yes
	HFS extendido (HFS+)	yes
	HFS extendido y sensible a mayúsculas/minúsculas (HFSX+)	yes
	Xsan (XSAN)	yes
	Formato de disco universal (UDF)	yes
	ISO9660	yes
Solaris	UFS	yes
	VxFS	yes
	QFS	no
	ZFS	yes

En los sistemas de archivos en los que se han definido y utilizado las ACL NFS (Solaris ZFS y AIX JFS2 Versión 2), incluso si sólo se han modificado los permisos de UNIX estándar o las ACL, por ejemplo, con el mandato CHMOD, se vuelve a realizar una copia de seguridad completa del archivo o del directorio. Con el resto de sistemas de archivos, este tipo de cambio sólo hace que se actualice un atributo en el servidor de IBM Spectrum Protect.

Para poder procesar todos los demás sistemas de archivos, utilice la opción `virtualmountpoint` para habilitar el soporte de los siguientes elementos:

- Para realizar una copia de seguridad, restaurar, archivar y recuperar datos de archivos
- Permisos básicos de UNIX y Linux
- Para cambiar, acceder y modificar indicaciones de fecha y hora y la estructura del árbol de directorio

No son válidos los atributos específicos de sistema de archivos, como ACL. El tipo de sistema de archivos para dichos sistemas de archivos debe establecerse en "UNKNOWN".

Por ejemplo, si el sistema de archivos /media/abc/DATA1 no es compatible con el cliente, añada la siguiente sentencia a dsm.sys para realizar la copia de seguridad o archivar los datos en este sistema de archivos:

```
VIRTUALMOUNTPOINT /media/abc/DATA1
```

Este soporte sólo está disponible si el sistema de archivos puede utilizar llamadas al sistema POSIX, como el proceso de lectura o de grabación en el sistema.

No se admite la copia de seguridad entre plataformas ni la restauración. Por ejemplo, los datos cuya copia de seguridad ha realizado un cliente AIX no están disponibles para que los restaure un cliente Windows y viceversa.

Nota: Los datos copiados o archivados mediante el cliente de Mac OS X no pueden restaurarse mediante otro cliente. Además, el cliente de Mac OS X no puede restaurar ni recuperar datos de otros clientes.

Podrá utilizar el método de restauración o recuperación de la información de ACL en sistemas de archivos distintos solo si tanto el sistema de archivos original como el de destino admiten listas ACL compatibles. Por ejemplo, en Solaris, la información de ACL cuya copia de seguridad se ha realizado desde un sistema de archivos VxFS se restaura en un sistema de archivos UFS porque estos sistemas de archivos admiten listas ACL compatibles. La información de ACL no se restaura durante las operaciones de restauración o recuperación en sistemas de archivos distintos si el sistema de archivos original y el de destino no admiten listas ACL.

El paquete autónomo LSCqfs 3.5.0 es la única versión admitida de QFS. Asimismo, el sistema de archivos QFS tendrá las siguientes restricciones:

- No se admite la copia de seguridad de imagen en los sistemas de archivos QFS.
- El cliente de copia de seguridad/archivado de Solaris no admite la combinación de QFS y SAM que es necesaria para archivar copias en almacenamiento subordinado terciario, como por ejemplo cintas. En su lugar, recupera automáticamente archivos de cinta a disco, si encuentra archivos migrados mientras realiza una copia de seguridad.
- Un sistema de archivos QFS contiene dos archivos de sistema ocultos y un directorio de sistema del que no se puede realizar una copia de seguridad; y es aceptable porque no se necesita una copia de seguridad de estos archivos. Contienen datos internos para gestionar el sistema de archivos. Los datos internos se excluyen de forma automática desde una copia de seguridad y se recrean de forma automática mediante el sistema de archivos en sí mismo si se completa una restauración de archivos en ese sistema de archivos.

En AIX se admiten la copia de seguridad incremental, la copia de seguridad selectiva, la copia de seguridad de lista de archivos, la operación de archivado, la restauración y el proceso de recuperación del sistema de archivos de Veritas y sus ACL. La restauración de un volumen de Veritas en un volumen del gestor de volúmenes lógicos, y viceversa, está admitida siempre que ambos tengan el mismo tipo de sistema de archivos.

La siguiente información solo pertenece a sistemas Mac OS:

- En sistemas Mac OS X, los sistemas de archivos UFS y HFSX son sensibles a mayúsculas mientras que el sistema de archivos HFS+ no distingue entre

mayúsculas y minúsculas pero las preserva. Es posible que las copias de seguridad de archivos de un sistema de archivos UFS o HFSX (sensible a mayúsculas/minúsculas) no se restauren correctamente en un sistema de archivos HFS+ (no sensible a mayúsculas/minúsculas). Por ejemplo, en un sistema de archivos UFS, los archivos `Afile` y `afile` se consideran archivos distintos. Sin embargo, en un sistema de archivos HFS+ los dos archivos se ven como idénticos.

- En Mac OS X, si se utilizan los sistemas de archivos HFS+ o UFS sensibles a mayúsculas, es importante que la copia de seguridad de los datos del sistema de archivos HFSX o UFS no se realice en un sistema de archivos HFS+ en el servidor de IBM Spectrum Protect. Debe utilizarse un nombre nuevo en el sistema o bien renombrar el espacio de archivos existente en el servidor de IBM Spectrum Protect. Por ejemplo, imagine un sistema que tiene un sistema de archivos llamado `/Volumes/fs2` y que éste se reparticiona con un sistema de archivos HFS+ que distingue entre mayúsculas y minúsculas. Bien el sistema de archivos `/Volumes/fs2` en el servidor de IBM Spectrum Protect debe cambiarse de nombre, bien el nombre nuevo debe utilizarse en el sistema local. De lo contrario, los datos que distinguen entre mayúsculas y minúsculas de HFSX se combinarán con los datos que no distinguen entre mayúsculas y minúsculas de HFS+ ya almacenados en el servidor de IBM Spectrum Protect.
- En Mac OS X, se realiza una copia de seguridad de los alias y de los enlaces simbólicos. Sin embargo, el cliente no lleva a cabo copias de seguridad de los datos a los que hacen referencia los enlaces simbólicos.
- En Mac OS X, cuando se realiza la copia de seguridad de los archivos desde un volumen HFS se restauran a un volumen UFS, los resource forks no se asignan al propietario correcto. Corrija este problema utilizando el mandato **chown** en el archivo del resource fork para cambiar el propietario. El almacén de archivos del resource fork almacena los datos estructurados en un archivo.

En Linux enPOWER y Linux en System z, debe instalar `libacl.so` para que el cliente realice copias de seguridad de ACL.

Importante: Si está ejecutando GPFS para AIX, GPFS para Linux x86_64 o GPFS para Linux en z Systems en un clúster multinodo y todos los nodos comparten un sistema de archivos GPFS montado, el cliente procesa este sistema de archivos como un sistema de archivos local. El cliente realiza copias de seguridad del sistema de archivos en cada nodo durante una copia de seguridad incremental. Para evitar esto, puede realizar una de las siguientes tareas:

- Configure explícitamente la sentencia `domain` en el archivo de opciones de usuario de cliente (`dsm.opt`) para enumerar los sistemas de archivos de los que desea que dicho nodo realice una copia de seguridad.
- Establezca la opción `exclude.fs` en el archivo `dsm.sys` para excluir el sistema de archivos GPFS de los servicios de copia de seguridad.

Si el clúster GPFS contiene diferentes plataformas, debe utilizar los clientes de copia de seguridad y archivado sólo en una plataforma para proteger un solo sistema de archivos. No utilice clientes de copia de seguridad y archivado en más de una plataforma para proteger un sistema de archivos GPFS que se comparta entre más de una plataforma.

Por ejemplo, supongamos que un clúster contiene nodos en sistemas AIX, Linux x86 y Linux zSeries. Puede proteger el sistema de archivos A con clientes de copia de seguridad y archivado AIX y el sistema B con clientes de copia de seguridad y archivado Linux zSeries. También puede proteger el sistema de archivos A y el sistema de archivos B con clientes de copia de seguridad y archivado AIX. Si

protege el sistema de archivos A con un cliente de copia de seguridad y archivado AIX, no debe proteger el sistema de archivos A con un cliente de copia de seguridad y archivado de ninguna plataforma que no sea AIX.

Tamaño máximo de archivo para operaciones

El tamaño máximo de archivo depende del tipo de sistema de archivos. El cliente de copia de seguridad y archivado no comprueba ningún límite de tamaño de archivo durante las operaciones de copia de seguridad, archivado, restauración o recuperación

Si el sistema de archivos permite crear el archivo, el cliente realiza la copia de seguridad o el archivado de dicho archivo.

En la tabla siguiente se especifican los tamaños máximos de archivos para sistemas de archivos nativos en las plataformas cliente UNIX y Linux.

Tabla 35. Tamaño máximo de archivo

Plataforma	Tamaño máximo de archivo (en bytes)
Limitaciones de tamaño para AIX 6.1 (JFS2)	Tamaño máximo del sistema de archivos JFS2: 32 TB Tamaño máximo del sistema de archivos JFS2: 16 TB Tamaño mínimo del sistema de archivos JFS2: 16 MB
Todos los clientes Linux	9.223.372.036.854.775.807 (8 EB-1)
Mac OS X	HFS - 2.147.485.648 (2GB) HFS+, HFSX, XSAN y UFS - 9.223.372.036.854.775.808 (8EB)
Solaris	1.099.511.627.775 (1 TB-1)
Solaris (ZFS)	18.446.744.073.709.551.616 (16 EB)

Nombres de usuario y de grupo largos

El cliente de archivado y copia de seguridad puede gestionar sin problemas nombres de usuario y de grupo con hasta 64 caracteres. Sin embargo, los nombres de más de 64 caracteres requieren un manejo especial por parte de IBM Spectrum Protect.

Importante: No exceda el límite de 64 caracteres para los nombres de usuario y de grupo. Si lo hace, el cliente acorta el nombre para que se ajuste a este límite mediante la utilización de las transformaciones siguientes: se tomarán los 53 primeros caracteres y se añadirán una barra inclinada (/) y, a continuación, el ID numérico como serie de caracteres.

Se anota un mensaje de error que contiene el nombre largo y la serie de caracteres acortada resultante. Para ejecutar la mayoría de las funciones no será necesario que conozca el nombre abreviado. Las excepciones son:

- El mandato **set access**
- La opción **fromowner**
- Las opciones **users y groups** (autorización)

En cada uno de estos casos, cuando tenga que especificar un nombre, deberá buscar el mensaje de error que contiene la transformación o bien construir el nombre utilizando la regla que se describe aquí.

Nombres de volumen en Mac OS X

El cliente de copia de seguridad y archivado hace copias de seguridad de los volúmenes en función de su nombre de punto de montaje UNIX.

IBM Spectrum Protect mantiene cada uno de los nombres de un volumen como una restauración aparte o volumen rescatado. Estos nombres de volumen se convierten en los nombres de los espacios de archivo en un servidor.

Si se cambia el nombre de un volumen del que ya se ha efectuado copia de seguridad, el cliente la considera como un volumen nuevo y no lo relaciona con el anterior. Cualquiera copia de seguridad de un volumen hace copia de seguridad de los archivos con un nombre nuevo. Se puede producir una discrepancia si cambia el nombre de los volúmenes, o si accede a IBM Spectrum Protect desde una estación de trabajo distinta de la utilizada para realizar la copia de seguridad de los archivos.

Precauciones respecto a la asignación de nombres de volumen en Mac OS X

IBM Spectrum Protect crea todos los espacios de archivos nuevos en el servidor con el punto de montaje UNIX del volumen.

Si hay dos volúmenes que se llaman "La Pomme" y "la pomme", se crearán dos puntos de montaje UNIX únicos.

Los ejemplos siguientes muestran los dos puntos de montaje que se crean:

```
/Volumes/La Pomme  
/Volumes/la pomme
```

Si existen volúmenes duplicados en su escritorio, es posible que los puntos de montaje UNIX no sean los mismos que la última vez que el cliente realizó una copia de seguridad. El cliente podría no hacer copia de seguridad de los datos en el sistema de archivos correcto en el servidor de IBM Spectrum Protect.

Puede comprobar el sistema de archivos en el que el cliente realiza una copia de seguridad de los datos:

1. En la ventana de copia de seguridad, seleccione un sistema de archivos.
2. Pulse **Archivo** → **Mostrar Info**.

El punto de montaje de UNIX está en el diálogo de Información.

La mejor manera de evitar problemas potenciales con la asignación de nombres es asegurarse de que los nombres de volumen sean únicos.

Importante:

- El cliente continuará utilizando los nombres de espacio de archivos existentes en el servidor de IBM Spectrum Protect. Solo los nuevos espacios de archivos utilizarán el punto de montaje UNIX para el nombre.
- No incluya puntos cuando especifique el nombre de los volúmenes (...). El cliente utiliza la secuencia de puntos como parte del proceso de

inclusión/exclusión. El cliente informará de la existencia de una sentencia de inclusión/exclusión no válida si un nombre de volumen contiene puntos. *Debe* cambiarse el nombre del volumen.

Precauciones respecto a la asignación de nombres de volumen en Mac OS X en sistemas de arranque dual

Si dispone de más de una versión de Mac OS X que utiliza de manera alternativa, es fundamental que comprenda cómo el cliente utiliza las vías de acceso de montaje de UNIX con los nombres de espacios de archivos del servidor de IBM Spectrum Protect.

Por ejemplo, supongamos que dispone de un sistema de arranque dual con dos volúmenes, El Capitan y Sierra. El buscador y la GUI del cliente de archivado y copia de seguridad los muestran como El Capitan y Sierra. Sin embargo, los puntos de montaje de UNIX dependen de la versión de Mac OS que se esté ejecutando. Si El Capitan es el disco de inicio, las vías de acceso de UNIX serán:

```
/
/Volumes/Sierra
```

Si Sierra es el disco de inicio, las vías de acceso de UNIX serán:

```
/
/Volumes/El Capitan
```

Cuando se ejecute una operación de copia de seguridad o de archivado, los nombres de espacios de archivos dependerán también de la versión de Mac OS X que se esté ejecutando.

Las dos versiones de Mac OS X realizarán una copia de seguridad en el sistema de archivos / del servidor de IBM Spectrum Protect. Si esto sucede, los archivos de sistema se entremezclan.

Para evitar posibles problemas con los sistemas de arranque dual, realice una de las siguientes tareas:

1. Seleccione una versión de Mac OS X para instalar y ejecutar IBM Spectrum Protect. De este modo se asegura de que los puntos de montaje de UNIX son los mismos cada vez que el cliente realiza una copia de seguridad.
2. Configure cada una de las versiones de Mac OS X con un nombre de nodo de IBM Spectrum Protect único. A continuación, excluya la otra versión de Mac OS X del proceso de copia de seguridad con una sentencia de dominio en el archivo de opciones del sistema. Por ejemplo, si el volumen Sierra es el disco de inicio, añada esta opción al archivo de opciones del sistema:

```
DOMAIN -/Volumes/El Capitan
```

Si el volumen El Capitan es el disco de inicio, añada esto al archivo de opciones del sistema:

```
DOMAIN -/Volumes/Sierra
```

Habilitación de Unicode para Mac OS X

El cliente Mac OS X está habilitado para Unicode. Los clientes nuevos que almacenen datos en el servidor por primera vez no requieren una configuración especial.

El servidor almacena automáticamente archivos y directorios activados para Unicode. Sin embargo, si desea actualizar al cliente activado para Unicode, tiene que planificar la migración de los espacios de archivos existentes para que puedan admitir Unicode.

Se tiene que cambiar el nombre de los espacios de archivos que ya están en el servidor para que se puedan crear espacios de archivos activados para Unicode. Utilice la opción `autofsrename` para cambiar el nombre a los espacios de archivos existentes.

Referencia relacionada:

“Autofsrename” en la página 356

Disco de copia de seguridad Time Machine de Mac OS X

Time Machine es la aplicación de copia de seguridad disponible con Mac OS X.

IBM Spectrum Protect se puede utilizar al mismo tiempo que la aplicación Mac OS X Time Machine. Debido a la forma única en que Time Machine de Mac OS X realiza copias de seguridad de los datos, tenga en cuenta algunas cuestiones antes de utilizar el cliente de copia de seguridad y archivado para realizar una copia de seguridad de los datos de Time Machine de Mac OS X:

- El disco de copia de seguridad de Time Machine de Mac OS X hace un uso amplio de los enlaces fijos de directorio y de archivo para minimizar la utilización del disco. Por ejemplo, si el disco objeto de la copia de seguridad con Time Machine de Mac OS X tiene 5 GB, la primera copia de seguridad copiará los 5 GB de datos en el disco de copia de seguridad de Time Machine de Mac OS X.

Las copias de seguridad subsiguientes copiarán únicamente los archivos que hayan cambiado desde la copia de seguridad anterior. Todos los archivos y directorios que no hayan cambiado se enlazarán de forma fija con la versión que se ha copiado durante la copia de seguridad anterior.

El Finder mostrará cada copia de seguridad como de 5 GB, para un tamaño total de 10 GB. Sin embargo, debido al uso de enlaces fijos, el uso total del disco será ligeramente superior a 5 GB.

Se realiza una copia de seguridad de todos los objetos enlazados de forma fija que no se encuentren en el servidor de IBM Spectrum Protect.

Por ejemplo, se enviarían 10 GB de datos al servidor de IBM Spectrum Protect.

- Cuando los archivos que están restaurados son enlaces fijos, el cliente vuelve a crear el enlace fijo original. La recreación del enlace fijo original solo se puede hacer si *todos* los archivos que están enlazados de forma fija se restauran al mismo tiempo. La restauración de todos los archivos con enlaces fijos no es un método práctico para un disco de copias de seguridad grande que utiliza la aplicación Time Machine de Mac OS X.
- Cuando Time Machine de Mac OS X copia los archivos en el disco de copia de seguridad, se añaden ACL a los archivos para evitar que puedan eliminarse. El cliente de copia de seguridad y archivado puede realizar copias de seguridad de los archivos y restaurarlos con las listas de control de acceso (ACL). Sin embargo, todos los archivos que se restauren seguirán teniendo estas ACL restrictivas.

Sugerencia: Para obtener mejores resultados, excluya los datos de la copia de seguridad de la aplicación Time Machine. Todos los datos de Time Machine se encuentran en un directorio denominado `Backups.backupdb`.

Conceptos relacionados:

Realización de una copia de seguridad incremental selectiva o incremental por fecha (UNIX y Linux)

Es posible que el administrador haya establecido planificaciones para realizar automáticamente copias de seguridad de archivos de la estación de trabajo. En los apartados siguientes se indica cómo realizar copias de seguridad sin utilizar una planificación.

Existen dos tipos de copia de seguridad incremental: *incremental completa* e *incremental parcial*.

Tareas relacionadas:

“Establecimiento del proceso del planificador cliente para que se ejecute como una tarea de fondo y se inicie automáticamente al arrancar” en la página 287

Copia de seguridad incremental completa y parcial

Una copia de seguridad incremental sólo copia los archivos nuevos y modificados. El tipo de copia de seguridad incremental depende de los objetos que selecciona para realizar la copia de seguridad.

Si selecciona los sistemas de archivos completos, la copia de seguridad es una copia de seguridad incremental completa. Si selecciona un árbol de directorio o archivos individuales, la copia de seguridad es una copia de seguridad incremental parcial.

La primera vez que se ejecuta una copia de seguridad incremental completa, el cliente de copia de seguridad y archivado realiza una copia de seguridad de todos los archivos y directorios que especifique. La operación de copia de seguridad puede llevar mucho tiempo si el número de archivos es grande o si uno o más archivos grandes deben copiarse. Las posteriores copias de seguridad incrementales completas sólo realizan copias de seguridad de los archivos nuevos y modificados. El servidor de copia de seguridad mantiene las versiones actuales de sus archivos sin tener que perder tiempo o espacio realizando la copia de seguridad de los archivos que existen en el almacenamiento del servidor de IBM Spectrum Protect.

Dependiendo de las políticas de gestión de almacenamiento, es posible que el servidor de IBM Spectrum Protect tenga más espacio que una versión de sus archivos en el almacenamiento. Las últimas copias de seguridad realizadas son versiones de copia de seguridad activas. Las copias de archivos más antiguas son versiones inactivas. Sin embargo, si suprime un archivo de la estación de trabajo, la siguiente copia de seguridad incremental completa hace que la versión de copia de seguridad activa del archivo pase a ser inactiva. Puede restaurar la versión inactiva de un archivo. El número de versiones inactivas que mantiene el servidor y cuánto tiempo se gobiernan mediante las políticas de gestión definidas por el administrador del servidor de IBM Spectrum Protect. Las versiones activas representan los archivos que existían en el sistema de archivos cuando se realizó la última copia de seguridad.

Para iniciar una copia de seguridad incremental completa o parcial mediante la GUI del cliente, seleccione **Backup**, y después seleccione la opción **Incremental (complete)**. Desde la línea de mandatos, utilice el mandato **incremental** y

especifique los sistemas de archivos, los árboles del directorio o los archivos individuales que se incluyen en la copia de seguridad.

Durante una copia de seguridad incremental, el cliente consulta al servidor o la base de datos de diario para determinar cuál es el estado exacto de los archivos desde la última copia de seguridad incremental realizada. El cliente utiliza esta información para las siguientes tareas:

- Realizar copias de seguridad de archivos nuevos.
- Realizar copias de seguridad de archivos cuyo contenido ha cambiado desde la última copia de seguridad.

Se realiza la copia de seguridad de los archivos cuando cualquiera de los siguientes atributos cambia:

- Tamaño del archivo
- Fecha u hora de la última modificación
- Atributos ampliados
- La lista de control de accesos.

Si los siguientes atributos cambian, los atributos se actualizan en el servidor de IBM Spectrum Protect, pero no se realiza la copia de seguridad del archivo:

- Propietario del archivo
- Permisos del archivo
- Inodo
- ID de grupo
- Tiempo de cambio (ctime). Consulte la opción **updatectime** para obtener los detalles.
- Ubicación del icono (sólo Mac OS X)
- Tipo o creador (sólo Mac OS X)

- Realizar copias de los directorios.

Se realiza una copia de seguridad de un directorio en cualquiera de las siguientes circunstancias:

- No se ha realizado una copia de seguridad previa del directorio
- Los permisos del directorio han cambiado desde la última copia de seguridad
- El directorio de la lista de control de acceso ha cambiado desde la última copia de seguridad
- El directorio de atributos ampliados ha cambiado desde la última copia de seguridad
- La indicación de fecha y hora de la modificación del directorio ha cambiado desde la última copia de seguridad

Los directorios se enumeran de acuerdo con el número de objetos de copia de seguridad. Para excluir directorios y el contenido de los mismos del proceso de copia de seguridad, utilice la opción `exclude.dir`.

- Hacer caducar las versiones de copia de seguridad de los archivos del servidor que no tienen archivos correspondientes en la estación de trabajo. El resultado es que los archivos que ya no existen en la estación de trabajo no tienen versiones de copia de seguridad activas en el servidor. Sin embargo, las versiones inactivas se conservan en función de las reglas definidas por el administrador de IBM Spectrum Protect.
- Volver a vincular las versiones de copia de seguridad si han cambiado las asignaciones de clase de gestión. Sólo volverán a enlazarse los objetos que tengan versiones de copia de seguridad activas. Los objetos para los que sólo existan versiones de copia de seguridad inactivas no volverán a enlazarse.

Durante una operación de copia de seguridad incremental, los objetos se vuelven a enlazar o caducan de la siguiente manera:

Si la especificación de archivo coincide con todos los archivos en una vía de acceso:

El reenlace y la caducidad se produce para todas las versiones de copia de seguridad seleccionables que coinciden con la especificación de archivo. Éste sería el caso de un mandato incremental como `dsmc incr c:\mydir* -subdir=yes`.

Si la especificación de archivo no coincide con todos los archivos en una vía de acceso:

El reenlace y la caducidad se produce para todas las versiones de copia de seguridad seleccionables que coinciden con la especificación de archivo. Sin embargo, las versiones de copia de seguridad seleccionables no caducan ni se vuelven a enlazar si se encuentran en un directorio que ya no existe en el sistema de archivos del cliente.

Pongamos por ejemplo un mandato incremental como `dsmc incr c:\mydir*.txt -subdir=yes`. Supongamos que algunos archivos en `c:\mydir\` no tienen el tipo de archivo `txt`. El reenlace y la caducidad sólo se produce para archivos que coinciden con la especificación `*.txt` y cuyos directorios aún existen en el sistema de archivos del cliente.

Puede utilizar la opción `preservelastaccessdate` para especificar si va a modificar la última fecha de acceso después de realizar una operación de copia de seguridad o archivado. De forma predeterminada, la fecha de acceso cambia después de una operación de copia de seguridad o archivado predeterminada.

Conceptos relacionados:

Capítulo 9, “Políticas de gestión de almacenamiento”, en la página 299

Referencia relacionada:

“Opciones exclude” en la página 425

“Preservelastaccessdate” en la página 519

“Updatectime” en la página 601

Copia de seguridad basada en el diario en AIX y Linux

La copia de seguridad con registro por diario es un método alternativo de copia de seguridad que utiliza un diario de cambios mantenido por el proceso del daemon de registro por diario de IBM Spectrum Protect.

En AIX, se admite la copia de seguridad basada en el diario en sistemas de archivos JFS y JFS2.

En Linux, la copia de seguridad basada en el diario se admite en Ext2, Ext3, Ext4; XFS, ReiserFS, JFS, VxFS y NSS, y en un sistema de archivos locales compartidos a través de NFS. GPFS no se admite para las copias de seguridad basadas en el diario.

Para dar soporte a la copia de seguridad con registro por diario, debe instalar y configurar el daemon de registro por diario de IBM Spectrum Protect.

Una copia de seguridad de un sistema de archivos en particular será una copia de seguridad con registro cuando el daemon de registro por diario se haya instalado y configurado para registrar por diario el sistema de archivos en particular y cuando se haya establecido un diario válido para el sistema de archivos. La copia de seguridad con registro por diario se habilita al finalizar satisfactoriamente una copia de seguridad incremental completa.

La principal diferencia entre la copia de seguridad incremental tradicional y la copia de seguridad con registro por diario es el método que se utiliza con los candidatos para copia de seguridad o para caducidad.

La copia de seguridad incremental tradicional obtiene la lista de candidatos para copia de seguridad o para caducidad creando listas integrales de objetos locales y listas de objetos de servidor activos para el sistema de archivos del que se está realizando una copia de seguridad. Las listas locales se obtienen explorando el sistema de archivos local completo. La lista de servidores se obtiene consultando todos los objetos activos en el inventario completo del servidor.

Los dos listas se comparan y los candidatos se seleccionan en función de los siguientes criterios:

- Un objeto se selecciona como candidato para copia de seguridad si existe en la lista local, pero no existe en la lista de servidores. El objeto es también un candidato para copia de seguridad si existe en ambas listas, pero difiere según los criterios incrementales (por ejemplo, cambios en los atributos o cambios en la fecha y el tamaño).
- Un objeto se selecciona como candidato para caducidad si existe en la lista de servidores, pero no existe en la lista local.

La copia de seguridad con registro por diario obtiene la lista de objetos candidatos para copia de seguridad y caducidad consultando el daemon de registro por diario acerca del contenido del diario de cambios del sistema de archivos del que se está realizando una copia de seguridad.

Las entradas del diario de cambios se borran (se marcan como libres) una vez que han sido procesadas por el cliente de copia de seguridad y confirmadas en el servidor de IBM Spectrum Protect.

Puede utilizar la copia de seguridad con registro por diario cuando realice una copia de seguridad de sistemas de archivos con un número pequeño o moderado de cambios entre ciclos de copia de seguridad. Si tiene muchos cambios en archivos entre ciclos de copia de seguridad, tendrá diarios de cambios enormes. Los diarios de cambios enormes pueden crear problemas de memoria y de rendimiento que pueden anular las ventajas de la copia de seguridad con registro por diario. Por ejemplo, la creación, la eliminación, el cambio de nombre o la transferencia de grandes árboles de directorio pueden también invalidar las ventajas del uso de una copia de seguridad con registro por diario en lugar de una copia de seguridad incremental normal.

La copia de seguridad con registro por diario no está pensada para ser un sustituto completo de la copia de seguridad incremental tradicional. Debe complementar la copia de seguridad con registro por diario con una copia de seguridad incremental progresiva completa de forma periódica. Por ejemplo, realice copias de seguridad con registro por diario todos los días y copias de seguridad incrementales completas todas las semanas.

A continuación, se muestran algunas limitaciones de la copia de seguridad con registro por diario:

- Los atributos de servidor individuales no están disponibles durante una copia de seguridad con registro por diario. Es posible que no se apliquen determinadas configuraciones de política, como la frecuencia de copia y la modalidad de copia.

- Otros comportamientos específicos de plataforma podrían evitar que los objetos se procesen de forma correcta. Otro software que cambie el comportamiento predeterminado del sistema de archivos podría evitar que se detectaran los cambios en el sistema de archivos.
- Si el sistema de archivos está muy activo cuando está en curso una copia de seguridad con registro por diario, es posible que no haya caducado un pequeño número de archivos eliminados.
- Si restaura archivos en un sistema de archivos que tiene un registro por diario activo, se puede realizar copia de seguridad de algunos de los archivos restaurados de nuevo cuando se de la siguiente copia de seguridad con registro por diario, aunque los archivos no hayan cambiado desde que se restauraran.
- La opción “Skipaclupdatecheck” en la página 560 no tendrá efecto durante las copias de seguridad con registro por diario. Sin importar cómo esté establecida esta opción, al realizar copias de seguridad con registro por diario de un sistema de archivos, el cliente siempre realiza una copia de seguridad de un archivo si su ACL o atributos ampliados se han cambiado desde la última copia de seguridad.

Debe realizar copias de seguridad incrementales completas periódicas y copias de seguridad con registro por diario más frecuentes. La copia de seguridad incremental tradicional compara el inventario de archivos completo del servidor con la totalidad del sistema de archivos local. Por lo tanto, la copia de seguridad incremental es siempre el método de copia de seguridad más completo.

Nota: Es posible que una copia de seguridad con registro por diario no se realice como la copia de seguridad incremental tradicional si el dominio de políticas de su nodo se ha modificado en el servidor. Esto depende de cuándo se ha actualizado por última vez el juego de políticas de su dominio y de la fecha de la última copia de seguridad incremental. En este caso, deberá forzar una copia de seguridad incremental completa del modo tradicional para volver a vincular los archivos con el dominio nuevo. Utilice la opción `nojournal` con el mandato **incremental** para especificar que desea realizar una copia de seguridad incremental completa tradicional en lugar de la copia de seguridad con registro por diario predeterminada.

Proceso de restauración con copias de seguridad basadas en el diario (AIX y Linux):

El servicio de diario intenta identificar los cambios realizados en un archivo como resultado de una operación de restauración. Si no se ha modificado un archivo desde que se restauró, no se vuelve a hacer una copia de seguridad del mismo durante la siguiente copia de seguridad registrada por diario. Se supone que se está restaurando un archivo porque contiene los datos que necesita, de modo que no tiene sentido hacer de nuevo una copia de seguridad del archivo cuando se produce la siguiente copia de seguridad de diario. Los cambios en archivos restaurados que se producen tras la restauración de los archivos se deben reconocer como nuevos cambios y el archivo se procesa en la siguiente copia de seguridad basada en el diario.

Cuando existe un diario activo para un sistema de archivos concreto, el cliente de archivado y copia de seguridad notifica al daemon de diario si se va a restaurar un archivo. Todos los cambios que se produzcan en el archivo en un periodo corto de tiempo tras la notificación al daemon de diario se consideran resultado de la restauración del archivo. Estos cambios no se registran y el archivo no se incluye en la siguiente copia de seguridad basada en el diario.

En la mayoría de los casos, el proceso de diario identifica correctamente los cambios en los archivos generados como resultado de la restauración del archivo y evita que se copie el archivo en la siguiente copia de seguridad basada en el diario.

Los retardos sistémicos en el sistema, causados por una E/S intensiva o por la latencia del sistema de archivos, pueden impedir que una operación de restauración se inicie en el periodo de tiempo asignado por el daemon de diario una vez que recibe la notificación de que se va a producir la restauración. Si se produce dicho retardo, los cambios realizados en el archivo se consideran nuevos cambios implementados tras la restauración del archivo. Estos cambios se registran y el archivo se incluye en la siguiente copia de seguridad basada en el diario. Circunstancias como los retardos de procesos sistémicos o la latencia del sistema de archivos están fuera del control del cliente de copia de seguridad y archivado y simplemente son limitaciones reconocidas de las copias de seguridad basadas en el diario.

Copia de seguridad incremental por fecha

Para que un sistema de archivos sea elegible para copias de seguridad incrementales por fecha, debe haberse realizado como mínimo una copia de seguridad incremental completa de todo el sistema de archivos. Si ejecuta una copia de seguridad incremental de sólo una rama de directorios o un archivo individual, el sistema de archivos no será elegible para realizar copias de seguridad incrementales por fecha.

El cliente realiza una copia de seguridad sólo de aquellos archivos cuya fecha y hora de modificación es posterior a la fecha y hora de la última copia de seguridad incremental del sistema de archivos en el que se encuentra el archivo. Los archivos que agregue el cliente después de la última copia de seguridad incremental, pero cuya fecha de modificación sea anterior a la última copia de seguridad incremental, no se incluyen en la operación de copia de seguridad.

Los archivos cuyo nombre se ha cambiado después de la última copia de seguridad incremental, pero que no se han modificado, no se incluirán en la copia de seguridad. El cambio de nombre de un archivo no hace cambiar la fecha ni la hora de modificación del archivo. No obstante, si se cambia el nombre de un archivo sí se cambia la fecha de modificación del directorio en el que se encuentra. En este caso, se hace la copia de seguridad del directorio, pero no de los archivos que contiene.

Si ejecuta una copia de seguridad incremental por fecha de todo un sistema de archivos, el servidor actualiza la fecha y hora de la última copia de seguridad incremental. Si efectúa una copia de seguridad incremental por fecha sólo en una parte de un sistema de archivos, el servidor no actualiza la fecha de la última copia de seguridad incremental completa. En este caso, la siguiente copia de seguridad incremental por fecha vuelve a copiar estos archivos.

Nota: A diferencia de la copia de seguridad incremental, la copia de seguridad incremental por fecha no hace caducar los archivos suprimidos o vuelve a vincular las versiones de copia de seguridad a una nueva clase de gestión si ésta se ha modificado.

Tareas relacionadas:

“Copia de seguridad de datos mediante la GUI Java” en la página 181

Comparación de copias de seguridad incrementales por fecha, con registro por diario y copias de seguridad diferenciales de instantánea de NetApp con las copias de seguridad incrementales completas y parciales

Los métodos incrementales por fecha, con registro por diario y diferenciales de instantánea de NetApp son alternativas a los métodos de copia de seguridad incremental completa y parcial.

Copia de seguridad incremental por fecha

Una copia incremental por fecha tarda menos tiempo en procesarse que una copia incremental completa y requiere menos memoria.

Puede ser que una copia de seguridad incremental por fecha no coloque exactamente los mismos archivos de copia de seguridad en el almacenamiento del servidor, ya que la copia de seguridad incremental por fecha:

- No hace caducar las versiones de copia de seguridad de aquellos archivos que se han suprimido de la estación de trabajo.
- No vuelve a vincular las versiones de copia de seguridad a una nueva clase de gestión si ésta se ha modificado.
- No efectúa copias de seguridad de archivos cuyos atributos cambian, a menos que también se hayan modificado la fecha y la hora de modificación.
- No tiene en cuenta el atributo de frecuencia de grupo de copia de las clases de gestión (las copias de seguridad con registro por diario tampoco tienen en cuenta este atributo).

Copia de seguridad con registro por diario

Los requisitos de memoria para un entorno de registro por diario inicial son los mismos que los requisitos de memoria necesarios para una copia de seguridad incremental de espacio de archivos completa, pues las copias de seguridad con registro por diario deben completar la copia de seguridad incremental de espacio de archivos completa para poder establecer la base de datos de diario como válida y para poder establecer la línea de base para el registro por diario.

Los requisitos de memoria para las posteriores copias de seguridad con registro por diario serán mucho menores. Las sesiones de copia de seguridad con registro por diario se ejecutan en paralelo y las rige la opción de cliente *resourceutilization*, de la misma forma que las sesiones de copia de seguridad normales. El tamaño del archivo de base de datos de diario vuelve a adquirir un tamaño mínimo (menos de 1 KB) cuando se ha suprimido la última entrada del diario. Puesto que las entradas se suprimen del diario a medida que el cliente las procesa, el tamaño de disco que ocupa el diario debería ser el mínimo después de haberse realizado una copia de seguridad con registro por diario completa. Una copia de seguridad incremental completa con el registro por diario activo necesita menos tiempo para procesarse que una copia de seguridad incremental por fecha.

En AIX y Linux, la copia de seguridad con registro por diario tiene algunas limitaciones. Para obtener más información, consulte el apartado “Copia de seguridad basada en el diario en AIX y Linux” en la página 172.

Diferencial de instantánea de NetApp

Para servidores de archivos NAS y N-Series que se ejecuten en ONTAP 7.3.0, o superior, puede utilizar la opción `snapdiff` para invocar la copia de seguridad de diferencia de instantáneas NetApp cuando se realice una copia incremental de volumen completa. Esta opción reduce el uso de memoria y es más rápida.

Tenga en cuenta las siguientes limitaciones cuando ejecute una copia de seguridad incremental de volúmenes completos mediante la opción `snapdiff` para garantizar que se realiza una copia de seguridad de los datos en el momento adecuado.

- Un archivo se excluye debido a una regla de exclusión en el archivo de inclusión/exclusión. El cliente realiza una copia de seguridad de la instantánea actual con la regla de exclusión en vigor. Esto ocurre cuando no se han realizado cambios en el archivo, pero se ha eliminado la regla que excluía el archivo. NetApp no detecta este cambio de inclusión/exclusión, porque sólo detecta los cambios de los archivos entre dos instantáneas.
- Si ha añadido una sentencia de inclusión en el archivo de opciones, esta opción de inclusión solo entra en vigor cuando NetApp detecta que el archivo se ha modificado. El cliente no inspecciona cada uno de los archivos del volumen durante la copia de seguridad.
- Si ha utilizado el mandato **`dsmdc delete backup`** para suprimir explícitamente un archivo del inventario de IBM Spectrum Protect, NetApp no puede detectar que se ha eliminado manualmente un archivo del almacenamiento de IBM Spectrum Protect. Por consiguiente, el archivo sigue sin protección en el almacenamiento de IBM Spectrum Protect hasta que se cambia en el volumen y NetApp detecta el cambio, señalando al cliente que vuelva a hacer una copia de seguridad del mismo.
- Los cambios de políticas como, por ejemplo, de **`mode=modified`** a **`mode=absolute`** no se detectan.
- El espacio de archivo entero se suprime del inventario IBM Spectrum Protect. Esta acción provoca que la opción `snapdiff` cree una instantánea para utilizar como origen y una copia de seguridad incremental completa para ejecutarse.

El software de NetApp determina qué es un objeto cambiado, no IBM Spectrum Protect.

Si ejecuta una copia de seguridad de volumen completa de un NFS-mounted NetApp o N-Series, es posible que también se realice una copia de seguridad de todas las instantáneas del directorio de instantáneas. Para evitar realizar la copia de seguridad de todas las instantáneas del directorio de instantánea realice una de las siguientes acciones:

- Ejecutar copias de seguridad NDMP
- Ejecutar copias de seguridad utilizando la opción `snapshotroot`
- Ejecutar copias de seguridad incrementales utilizando la opción `snapdiff`

Consejo: Si ejecuta una copia de seguridad incremental mediante la opción `snapdiff` y planifica copias de seguridad incrementales periódicas, utilice la opción `createnewbase=yes` junto con la opción `snapdiff` para crear una instantánea base y utilizarla como origen para ejecutar una copia de seguridad incremental.

- Excluir el directorio de instantáneas desde las copias de seguridad.
En sistemas Linux, el directorio de instantáneas está en `.snapshot`.

Nota: En algunas versiones de Red Hat Linux, no se realiza una copia de seguridad del directorio `.snapshot`, por lo que no necesita excluirlo.

Copia de seguridad diferencial de la instantánea con una conexión HTTPS

Puede utilizar una conexión segura HTTPS para que el cliente de archivado y copia de seguridad se comuniquen con un archivador NetApp durante una copia de seguridad diferencial de una instantánea.

El protocolo HTTPS está habilitado en los archivadores NetApp de forma predeterminada y no puede desactivarse.

Cuando ejecuta una copia de seguridad diferencial de instantánea, el cliente de archivado y copia de seguridad establece una sesión administrativa con un archivador NetApp. Las credenciales del archivador, como el nombre de host del archivador o la dirección IP, el nombre de usuario que se utiliza para conectar el archivador y la contraseña del archivador se almacenan localmente en el cliente de archivado y copia de seguridad. Esta información debe transmitirse al archivador para establecer la sesión administrativa autenticada. Es importante utilizar una conexión segura porque autenticar la sesión del archivador administrativo requiere que el cliente transmita la contraseña del archivador en texto claro.

Para establecer una conexión segura mediante el protocolo de comunicación HTTPS, debe utilizar la opción **snappdiffhttps** cuando ejecuta una copia de seguridad de diferencial de instantánea. Sin la opción **snappdiffhttps**, el cliente de archivado y copia de seguridad puede establecer sesiones de gestor de archivos solo con el protocolo HTTP, que requeriría acceso administrativo HTTP para habilitarse en el gestor de archivos. Con la opción **snappdiffhttps**, puede establecer una sesión de administración segura con el archivador NetApp independientemente de si está habilitado o no el acceso de administración de HTTP en el archivador NetApp.

Restricciones:

Las siguientes restricciones se aplican a copias de seguridad diferencias instantáneas con HTTPS:

- La conexión HTTPS sólo se utiliza para transmitir datos de forma segura a través de la sesión de administración entre el cliente de archivado de copia de seguridad y el archivador de NetApp. Los datos de la sesión de administración incluyen información como credenciales del archivador, información de instantánea y los nombres de archivo y los atributos que se generan mediante el proceso de diferenciación de instantáneas. La conexión HTTPS no se utiliza para transmitir datos de archivos normales a los que se accede en el archivador mediante el cliente a través del compartimiento de archivos. La conexión HTTPS tampoco se aplica a los datos de archivos normales transmitidos mediante el cliente al servidor de IBM Spectrum Protect a través del protocolo cliente/servidor de IBM Spectrum Protect normal.
- La opción **snappdiffhttps** no se aplica a vFilers porque el protocolo HTTPS no está admitido en NetApp vFiler.
- La opción **snappdiffhttps** sólo está disponible utilizando la interfaz de línea de mandatos. No está disponible para su utilización con la GUI del cliente de archivado de copia de seguridad.

Tareas relacionadas:

“Configuración de NetApp y IBM Spectrum Protect para copias de seguridad incrementales de diferencia de instantánea” en la página 114

“Ejecutar una instantánea de la copia de seguridad diferencial con una conexión HTTPS”

Referencia relacionada:

“Snapdiffhttps” en la página 566

“Snapdiff” en la página 561

Ejecutar una instantánea de la copia de seguridad diferencial con una conexión HTTPS

Cuando ejecuta una copia de seguridad diferencial de una instantánea, puede utilizar la opción **snapdiffhttps** para crear una conexión HTTPS segura entre el cliente de archivado y copia de seguridad y el archivado NetApp.

Antes de empezar

Antes de comenzar a realizar una copia de seguridad diferencial de una instantánea a través de una conexión HTTPS, asegúrese de que ha configurado el cliente como se describe en “Configuración de NetApp y IBM Spectrum Protect para copias de seguridad incrementales de diferencia de instantánea” en la página 114.

Este método está disponible solo en la interfaz de línea de mandatos.

Procedimiento

Para iniciar una operación de copia de seguridad diferencial de una instantánea a través de una conexión HTTPS, especifique el mandato **incremental** con las opciones **snapdiff** y **snapdiffhttps** en la interfaz de línea de mandatos.

Por ejemplo, imagine que está utilizando un sistema de Linux con un sistema de archivos montado en NFS /vol/vol1 alojado en el servidor de archivos homestore.example.com. El directorio /net/home1 es el punto de montaje de /vol/vol1. Emita el siguiente mandato:

```
dsmc incr /net/home1 -snapdiff -snapdiffhttps
```

Conceptos relacionados:

“Copia de seguridad diferencial de la instantánea con una conexión HTTPS” en la página 178

Referencia relacionada:

“Snapdiffhttps” en la página 566

Copia de seguridad selectiva

Utilice la copia de seguridad selectiva para realizar copias de seguridad de archivos específicos o directorios independientemente de si ya existe una copia de seguridad de dichos archivos en el servidor.

Las copias de seguridad incrementales suelen formar parte de un sistema automatizado para hacer copia de seguridad de todos los sistemas de archivos. Por el contrario, las copias de seguridad selectivas permiten seleccionar manualmente un juego de archivos de los que se debe realizar una copia de seguridad, independientemente de si dichos archivos han cambiado desde la última copia de seguridad incremental.

A diferencia de la copia de seguridad incremental, una copia de seguridad selectiva:

- No provoca que el servidor actualice la fecha y la hora de la última copia incremental.
- Realiza copias de seguridad de entradas de archivos y directorios aunque el tamaño, indicación de la hora de modificación o los permisos no hayan cambiado.
- No hace caducar los archivos suprimidos.
- No vuelve a vincular las versiones de copia de seguridad a una nueva clase de gestión si ésta se ha modificado.

Tareas relacionadas:

“Copia de seguridad de datos mediante la GUI Java” en la página 181

Referencia relacionada:

“Selective” en la página 775

Zona global Solaris y copias de seguridad de zonas no globales

Para zonas de Solaris, realice copias de seguridad selectivas e incrementales de sistemas de archivos dentro de la zona en la que se han creado dichos sistemas de archivos.

Trate cada zona no global como un sistema independiente que tiene su propio nombre de nodo de IBM Spectrum Protect y que ejecuta copias de seguridad desde dentro de cada una de las zonas.

Si ejecuta copias de seguridad incrementales o selectivas de zonas no globales desde la zona no global, el administrador de la zona global debe decidir qué archivos de la zona no global deben incluirse o excluirse de las copias de seguridad. Por ejemplo, los archivos kernel, de sistema o dispositivo de las zonas no globales no se excluyen automáticamente de las copias de seguridad, pero no debe realizarse ninguna copia de seguridad de los mismos. La restauración de tales archivos puede inutilizar una zona no global.

Cómo guardar permisos de acceso

Al realizar copias de seguridad de archivos, el cliente de copia de seguridad y archivado también guarda los permisos de acceso UNIX estándar asignados a los archivos.

En función del sistema operativo, también guarda permisos ampliados. Por ejemplo, para archivos de una estación de trabajo AIX, el cliente guarda listas de control de accesos.

Un usuario autorizado puede realizar copias de seguridad para otro usuario, sin que ello provoque conflictos de propiedad. El servidor de copia de seguridad registra que el archivo pertenece al propietario original. No es necesario que el usuario autorizado conceda al usuario original acceso a las versiones de copia de seguridad.

Establecimiento de un punto de montaje virtual

Si es un usuario autorizado y desea realizar copias de seguridad de archivos que empiecen por un directorio específico del sistema de archivos, puede definir dicho directorio como punto de montaje virtual.

Al definir un punto de montaje virtual en un sistema de archivos, se proporciona una vía de acceso directa a los archivos de los que se desea realizar una copia de seguridad, lo que ahorra tiempo de proceso. Es más eficaz que definir el sistema de archivos con la opción `domain` y utilizar posteriormente una opción `exclude` para excluir los archivos que no desea que se tengan en cuenta para la copia de seguridad. También permite almacenar copias de seguridad y copias archivadas de directorios específicos en espacios de archivos de almacenamiento separados.

Referencia relacionada:

“Virtualmountpoint” en la página 606

Copia de seguridad de datos mediante la GUI Java

Puede realizar copias de seguridad de archivos específicos, de directorios enteros o de sistemas de archivos enteros del árbol de directorios.

Acerca de esta tarea

Puede localizar los archivos de los que desea realizar una copia de seguridad mediante las operaciones de búsqueda y filtrado. El filtrado muestra sólo los archivos que coinciden con los criterios de filtrado de la operación de copia de seguridad.

Utilice la GUI Java del cliente de copia de seguridad y archivado para realizar copias de seguridad de los datos tal como se indica a continuación:

Procedimiento

1. Pulse **Copia de seguridad** en la ventana IBM Spectrum Protect. Aparecerá la ventana Copia de seguridad.
2. Expanda el árbol de directorios si es preciso. Pulse las casillas situadas junto al objeto u objetos de los que desea realizar la copia de seguridad. Para buscar o filtrar archivos, pulse el icono **Buscar** de la barra de herramientas.
3. Escriba los criterios de búsqueda en la ventana Buscar archivos (Copia de seguridad).
4. Pulse el botón **Buscar**. Aparecerá la ventana Archivos coincidentes (Copia de seguridad).
5. Pulse las casillas situadas junto a los archivos de los que desea realizar la copia de seguridad y cierre la ventana Archivos coincidentes (Copia de seguridad).
6. Escriba los criterios de filtrado en la ventana Buscar archivos (Copia de seguridad).
7. Pulse el botón **Filtrar**. La ventana Copia de seguridad muestra los archivos filtrados.
8. Pulse las casillas situadas junto a los archivos o directorios filtrados de los que desea realizar la copia de seguridad.
9. Seleccione uno de los tipos de copia de seguridad siguientes del menú desplegable: (1) Para efectuar una copia de seguridad incremental, pulse **Incremental (completa)**, (2) Para ejecutar una copia de seguridad incremental por fecha, pulse **Incremental (sólo por fecha)**, (3) Para efectuar una copia de seguridad selectiva, pulse **Hacer siempre copia de seguridad**.
10. Pulse **Copia de seguridad**. La ventana **Lista de tareas** de copia de seguridad muestra el estado del proceso de la copia de seguridad.

Resultados

Tenga en cuenta los siguientes elementos cuando haga copia de seguridad de sus datos mediante la GUI de Java .

- Si desea modificar opciones de copia de seguridad específicas, pulse el botón **Opciones**. Las opciones que seleccione estarán en vigor *únicamente* durante la sesión actual.
- IBM Spectrum Protect utiliza clases de gestión para determinar cómo se deben gestionar las copias de seguridad en el servidor. Cada vez que efectúe una copia de seguridad de un archivo, se asignará al archivo una clase de gestión. La clase de gestión utilizada es una clase de gestión predeterminada seleccionada o la que el usuario asigne al archivo con la opción *include* en la lista de opciones de inclusión/exclusión. Seleccione **Programas de utilidad** → **Ver información de políticas** en la GUI Java del cliente de copia de seguridad/archivado o en la GUI del cliente web para ver las políticas de copia de seguridad definidas por el servidor de IBM Spectrum Protect para su nodo cliente.
- Para realizar una copia de seguridad incremental automática del dominio predeterminado, seleccione **Acciones** → **Copia de seguridad del dominio**. El dominio predeterminado tiene establecida la opción *domain* en el archivo de opciones del usuario cliente (dsm.opt). Si la opción *domain* no está establecida, el dominio predeterminado comprende *todos los sistemas de archivos locales*.
- Puede utilizar el editor de preferencias para excluir del proceso de copia de seguridad sistemas de archivos del dominio predeterminado.

Conceptos relacionados:

Capítulo 9, “Políticas de gestión de almacenamiento”, en la página 299

Referencia relacionada:

“Domain” en la página 394

Copia de seguridad de datos mediante la línea de mandatos

Puede utilizar los mandatos **incremental** o **selective** para realizar copias de seguridad.

En la siguiente tabla se muestran ejemplos de utilización de estos mandatos para realizar diferentes tareas.

Tabla 36. Ejemplos de copia de seguridad desde la línea de mandatos

Tarea	Mandato	Consideraciones
<i>Copias de seguridad incrementales</i>		
Realizar una copia de seguridad incremental del dominio del cliente.	dsmc incremental	Consulte el apartado “ Incremental ” en la página 704 para obtener más información sobre el mandato incremental .
Realizar una copia de seguridad de los sistemas de archivos /fs1 y /fs2 además de los sistemas de archivos /home, /usr, y /datasave definidos en el dominio de cliente.	dsmc incremental -domain="/fs1 /fs2"	Consulte el apartado “Domain” en la página 394 para obtener más información sobre la opción domain.

Tabla 36. Ejemplos de copia de seguridad desde la línea de mandatos (continuación)

Tarea	Mandato	Consideraciones
Realizar una copia de seguridad de los sistemas de archivos /Volumes/fs1 y /Volumes/fs2 además de los volúmenes definidos en el dominio de cliente.	<code>dsmc incremental -domain="/Volumes/fs1 /Volumes/fs2"</code>	Consulte el apartado "Domain" en la página 394 para obtener más información sobre la opción domain.
Realizar una copia de seguridad de todos los sistemas de archivos locales definidos en el dominio de cliente salvo el sistema de archivos /home.	<code>dsmc incremental -domain="all-local -/home"</code>	No es posible utilizar el operador (-) delante de la palabra clave de dominio all-local. Para obtener más información, consulte el apartado "Domain" en la página 394. Para Los clientes Windows también pueden excluir el dominio del estado del sistema del proceso de copia de seguridad de este modo.
Realizar la copia de seguridad de los sistemas de archivos /fs1 y /fs2.	<code>dsmc incremental /fs1 /fs2</code>	Ninguna
Realizar una copia de seguridad de los archivos del directorio /home y todos sus subdirectorios.	<code>dsmc incremental /home/ -subdir=yes</code>	Consulte el apartado "Subdir" en la página 581 para obtener más información sobre la opción subdir.
Realizar una copia de seguridad de todos los archivos del directorio /Users y todos sus subdirectorios.	<code>dsmc incremental /Users/ -subdir=yes</code>	Consulte el apartado "Subdir" en la página 581 para obtener más información sobre la opción subdir.
Ejecutar una copia de seguridad incremental, dándose por supuesto que ha iniciado una instantánea del sistema de archivos /usr y que ha montado la instantánea como /snapshot/day1, de todos los archivos y directorios de la instantánea local y gestionar éstos en el servidor de IBM Spectrum Protect, en el nombre de espacio de archivos /usr.	<code>dsmc incremental /usr -snapshotroot=/snapshot/day1</code>	El cliente de copia de seguridad y archivado considera el valor de snapshotroot como el nombre del espacio de archivos. Para obtener más información, consulte el apartado "Snapshotroot" en la página 571.
<i>Copia de seguridad incremental por fecha</i>		
Realizar una copia de seguridad incremental por fecha del dominio de cliente predeterminado.	<code>dsmc incremental -incrbydate</code>	Utilice la opción incrbydate con el mandato incremental para hacer una copia de seguridad de los archivos nuevos y modificados con una fecha de modificación posterior a la de la última copia de seguridad incremental almacenada en el servidor. Consulte el apartado "Incrbydate" en la página 474 para obtener más información sobre la opción incrbydate.

Copias de seguridad selectivas

Tabla 36. Ejemplos de copia de seguridad desde la línea de mandatos (continuación)

Tarea	Mandato	Consideraciones
Realizar una copia de seguridad del directorio /home/proj o /Users/van/Documents.	dsmc selective /home/proj/ o dsmc selective /Users/van/Documents/	Utilizar el mandato selective para hacer copia de seguridad de archivos o directorios específicos sin tener en cuenta si han cambiado desde la última copia de seguridad incremental. Puede utilizar caracteres comodín para realizar una copia de seguridad de varios archivos a la vez. Consulte el apartado “ Selective ” en la página 775 para obtener más información sobre el mandato selective .
Realizar una copia de seguridad de todos los archivos del directorio /home/proj y todos sus subdirectorios.	dsmc selective /home/proj/ -subdir=yes	<p>Si especifica -subdir=yes al realizar una copia de seguridad de un ruta y archivo específico, el cliente realiza la copia de seguridad de todos los subdirectorios de esta ruta y de todas las instancias del archivo especificado que existan bajo cualquiera de estos subdirectorios.</p> <p>Si un subdirectorio es un sistema de archivos montado, el cliente no realiza la copia de seguridad de los archivos de dicho subdirectorio si se utiliza la opción subdir=yes. Consulte el apartado “Subdir” en la página 581 para obtener más información sobre la opción subdir.</p>
Realizar una copia de seguridad de todos los archivos del directorio /Users/van/Documents y todos sus subdirectorios.	dsmc selective /Users/van/Documents/ -subdir=yes	<p>Si especifica -subdir=yes al realizar la copia de seguridad de una vía de acceso y archivo específicos, el cliente realiza una copia de seguridad de forma recursiva de todos los subdirectorios de esa vía de acceso, y todas las instancias del archivo especificado que existen en todos esos subdirectorios.</p> <p>Si un subdirectorio es un sistema de archivos montado, el cliente no realiza la copia de seguridad de los archivos de dicho subdirectorio si se utiliza la opción subdir=yes. Consulte el apartado “Subdir” en la página 581 para obtener más información sobre la opción subdir.</p>
Realizar una copia de seguridad de los archivos /home/dir1/h1.doc y/home/dir1/test.doc.	dsmc selective /home/dir1/h1.doc /home/dir1/test.doc	Si especifica la opción removeoperandlimit con los mandatos incremental o selective , no se aplicará el límite de 20 operandos, y las únicas restricciones serán los recursos disponibles u otros límites del sistema operativo. Esto permite especificar más de 20 archivos en un único mandato. Consulte el apartado “Removeoperandlimit” en la página 528 para obtener más información acerca de esta opción.

Tabla 36. Ejemplos de copia de seguridad desde la línea de mandatos (continuación)

Tarea	Mandato	Consideraciones
Realizar una copia de seguridad de los archivos /Users/ann/Documents/h1.doc y /Users/ann/Documents/test.doc.	dsmc selective /Users/ann/Documents/h1.doc /Users/ann/Documents/test.doc	Si especifica la opción <code>removeoperandlimit</code> con los mandatos incremental o selective , no se aplicará el límite de 20 operandos, y las únicas restricciones serán los recursos disponibles u otros límites del sistema operativo. Esto permite especificar más de 20 archivos en un único mandato. Consulte el apartado “ <code>Removeoperandlimit</code> ” en la página 528 para obtener más información acerca de esta opción.
Realizar una copia de seguridad de una lista de archivos del archivo /home/filelist.txt.	selective -filelist=/home/filelist.txt	Utilice la opción <code>filelist</code> para procesar una lista de archivos. Para obtener más información, consulte el apartado “ <code>Filelist</code> ” en la página 439.
Realizar una copia de seguridad de todos los archivos indicados en el archivo /Users/filelist.txt.	dsmc selective -filelist=/Users/filelist.txt	Utilice la opción <code>filelist</code> para procesar una lista de archivos. Para obtener más información, consulte el apartado “ <code>Filelist</code> ” en la página 439.
Suponiendo que ha iniciado una instantánea del sistema de archivos /usr y ha montado la instantánea como /snapshot/day1, ejecute una copia de seguridad selectiva del árbol de directorios /usr/dir1/sub1 desde la instantánea local y gestiónelo en el servidor de IBM Spectrum Protect debajo del nombre de espacio de archivos /usr.	dsmc selective /usr/dir1/sub1/-subdir=yes -snapshotroot=/snapshot/day1	El cliente considera el valor de <code>snapshotroot</code> como el nombre del espacio de archivos. Para obtener más información, consulte el apartado “ <code>Snapshotroot</code> ” en la página 571.

Referencia relacionada:

“**Incremental**” en la página 704

“**Selective**” en la página 775

Supresión de datos de copia de seguridad

Si el administrador le ha otorgado autorización, puede suprimir copias de seguridad individuales del servidor de IBM Spectrum Protect sin suprimir todo el espacio de archivos. Para determinar si tiene esta autorización, seleccione **Archivo** > **Información de conexión** en la GUI de cliente de copia de seguridad y archivado o en el menú principal del cliente web. El estado de la autorización se proporciona en el campo **Suprimir archivos de copia de seguridad**.

Acerca de esta tarea

Importante: si suprime archivos de copia de seguridad, *no podrá restaurarlos*. Antes de suprimirlos, verifique que los archivos de copia de seguridad ya no sean necesarios. El cliente le solicitará si desea continuar con la operación de supresión. Si especifica *Sí*, los archivos de copia de seguridad especificados se suprimirán inmediatamente y se eliminarán del almacenamiento del servidor de IBM Spectrum Protect.

Para suprimir copias de seguridad mediante la GUI de cliente de copia de seguridad y archivado o el cliente web:

Procedimiento

1. Seleccione **Suprimir datos de copia de seguridad** en el menú **Herramientas**. Aparecerá la ventana Supresión de copia de seguridad.
2. Expanda el árbol de directorios pulsando en el signo más (+) o en el icono de carpeta situado junto al objeto que desea expandir.
3. Pulse en las casillas que se encuentran junto a los objetos que desee suprimir.
4. Seleccione un elemento de la lista desplegable que hay junto a la parte superior de la ventana **Supresión de copia de seguridad** para especificar el tipo de supresión de copia de seguridad que desea realizar. Puede suprimir las versiones de copia de seguridad activas, las versiones de copia de seguridad inactivas o todos los objetos que haya seleccionado en el árbol.

Resultados

Nota:

1. Un directorio solo se suprimirá si selecciona **Suprimir todos los objetos**.
2. Para suprimir copias de seguridad mediante el cliente de línea de mandatos, utilice el mandato **delete backup**.

Referencia relacionada:

“Delete Backup” en la página 694

Supresión de espacios de archivos

Si el administrador de IBM Spectrum Protect le concede autorización, puede suprimir espacios de archivos completos del servidor. Cuando se suprime un espacio de archivos, está suprimiendo todos los archivos y las imágenes, tanto las versiones de copia de seguridad como las de copias archivadas que hay en ese espacio de archivos. Por ejemplo, si suprime el espacio de archivos /tmp, está suprimiendo todas las copias de seguridad de cada uno de los archivos de ese sistema de archivos y de cada uno de los archivos que ha archivado desde ese sistema de archivos. Considere detenidamente si desea suprimir un espacio de archivos.

Acerca de esta tarea

También puede suprimir un espacio de archivos con el mandato **delete filespace**. Utilice la opción `class` con el mandato **delete filespace** para suprimir espacios de archivos NAS.

Puede suprimir las versiones individuales de copia de seguridad utilizando el mandato **delete backup**.

Puede suprimir espacios de archivos mediante la GUI del cliente de copia de seguridad y archivado o mediante clientes de línea de mandatos. Para suprimir espacios de archivos NAS, utilice el cliente web o el cliente de línea de mandatos.

Para suprimir un espacio de archivos mediante la GUI, siga estos pasos:

Procedimiento

1. Seleccione **Herramientas > Suprimir espacios de archivos** en la ventana principal.

2. Pulse en las casillas que se encuentran junto a los espacios de archivos que desea eliminar.
3. Pulse el botón **Suprimir**. El cliente le pedirá una confirmación antes de eliminarlos.

Referencia relacionada:

"Class" en la página 364

"Delete Backup" en la página 694

"Delete Filespace" en la página 698

Copia de seguridad de archivos desde uno o varios espacios de archivos para una copia de seguridad de grupo (UNIX y Linux)

Puede utilizar el mandato **backup group** para crear y realizar la copia de seguridad de un grupo que contenga una lista de archivos desde uno o más orígenes de espacio de archivos en un espacio de archivos virtual en el servidor de IBM Spectrum Protect.

Restricción: el mandato **backup group** no se aplica a Mac OS X.

Una *copia de seguridad de grupo* permite crear una copia de seguridad de instante específico coherente de un grupo de archivos que se gestiona como si se tratara de una entidad lógica única:

- Todos los objetos del grupo se asignan a la misma clase de gestión.
- Las sentencias *exclude* existentes que se aplican a cualquier archivo del grupo se pasan por alto.
- Todos los objetos del grupo se exportan juntos.
- Todos los objetos del grupo caducan al mismo tiempo, tal como se ha especificado en la clase de gestión. Ninguno de los objetos de un grupo caduca hasta que caducan los demás objetos del grupo, incluso cuando caduque otro grupo al que pertenecen.

Se puede añadir una copia de seguridad de grupo a un conjunto de copias de seguridad.

Puede realizar una copia de seguridad completa o diferencial mediante la opción **mode**.

Por ejemplo, para realizar una copia de seguridad completa de todos los archivos indicados en el archivo `/home/dir1/filelist1` en el espacio de archivos virtual `/virtfs` que contiene el archivo de líder de grupo `/home/group1`, especifique:

```
dsmc backup group -filelist=/home/dir1/filelist1 -groupname=group1 -virtualfsname=/virtfs -mode=full
```

Conceptos relacionados:

"Restauración de datos desde un conjunto de copias de seguridad" en la página 240

Referencia relacionada:

"Backup Group" en la página 672

"Opciones include" en la página 458

"Mode" en la página 492

Copia de seguridad con soporte de proxy de nodo cliente (UNIX y Linux)

Las copias de seguridad de varios nodos que comparten almacenamiento se puede agrupar en un nombre de nodo de destino común en el servidor de IBM Spectrum Protect.

Acerca de esta tarea

La consolidación de copias de seguridad de varios nodos en un nombre de nodo de destino común en el servidor es útil en configuraciones en las que la estación de trabajo responsable de realizar las copias de seguridad pudiera cambiar con el tiempo, como dentro de un clúster.

Un nodo de agente es un nodo cliente al que se otorga autorización para realizar operaciones de cliente en nombre de un nodo de destino.

Un nodo de destino es un nodo cliente que otorga autorización a uno o varios nodos de agente para realizar operaciones en nombre de éste.

Utilice la opción `asnodename` con el mandato adecuado para hacer una copia de seguridad, archivar restaurar y recuperar datos bajo el nombre del nodo de destino del servidor.

La opción `asnodename` también permite restaurar datos desde un sistema distinto del que se utilizó para realizar la copia de seguridad.

Tenga en cuenta las siguientes características cuando utilice un nodo proxy para realizar una copia de seguridad o una restauración de datos en otros nodos:

- Una operación de proxy utiliza los valores del nodo de destino (como `maxnummp` y `deduplication`) y las planificaciones definidas en el servidor de IBM Spectrum Protect. Los valores del nodo de servidor de IBM Spectrum Protect y las planificaciones del nodo de agente se ignoran.
- Todos los nodos agente del entorno de varios nodos deberían ejecutar el mismo tipo de sistema operativo.
- No utilice nodos de destino como nodos tradicionales, especialmente si cifra los archivos antes de hacerles una copia de seguridad en el servidor.
- No puede acceder a otro nodo (ya sea desde el desplegable de la GUI o mediante la opción `fromnode`).
- No se puede llevar a cabo una copia de seguridad o una restauración de NAS.

Procedimiento

1. Instale el cliente de copia de seguridad/archivado en todos los nodos de un entorno de datos compartido.
2. Registre cada nodo con el servidor IBM Spectrum Protect. Registre el nombre de nodo de destino común que vaya a compartir cada uno de los nodos agente utilizado en el entorno de datos compartido.
3. Registre cada uno de los nodos en el entorno de datos compartido con el servidor de IBM Spectrum Protect. Registre el nombre de nodo agente que se utiliza con fines de autenticación. Los datos no se almacenan en el servidor, bajo dicho nombre de nodo, cuando se utiliza la opción `asnodename`.

4. El administrador del servidor IBM Spectrum Protect debe otorgar autoridad de proxy a todos los nodos del entorno compartido para el acceso al nombre de nodo de destino, con el mandato GRANT PROXYNODE.
5. Utilice el mandato QUERY PROXYNODE del cliente administrativo para mostrar los nodos de cliente del usuario autorizado al que se le ha otorgado permiso mediante el mandato GRANT PROXYNODE.

Referencia relacionada:

“Asnodename” en la página 349

Habilitación de varias operaciones de nodos desde la GUI

Para habilitar operaciones multinodo en la GUI, utilice el editor Preferencias para especificar el nombre del nodo de destino al que se ha otorgado autoridad de proxy.

Procedimiento

1. Compruebe que el nodo cliente dispone de una autorización de proxy a un nodo de destino (o que está autorizado para actuar como nodo de destino) mediante el uso del mandato de cliente de administración **QUERY PROXYNODE**.
2. Seleccione **Editar > Preferencias de cliente** para abrir la venta de preferencias.
3. Seleccione la ficha **General** y rellene el campo **Como nombre de nodo** con el nombre de nodo de destino.
4. Pulse **Aplicar** y, a continuación, **Aceptar** para cerrar la ventana de preferencias.

Qué hacer a continuación

Realice uno de estos pasos para comprobar que el nodo cliente acceda ahora al servidor como nodo de destino:

- Abra la ventana de árbol y compruebe que aparece el nombre de nodo de destino especificado por el campo **Como nombre de nodo**.
- Compruebe el nombre de nodo de destino del campo **Acceder como nodo** de la ventana **Información de conexión**.

Para volver a la operación de nodo único, suprima **Como nombre de nodo** desde el campo **Acceso como nodo** en el separador **General > Preferencias**.

Configuración del cifrado

En este tema se enumeran los pasos que debe seguir para configurar el cifrado con la opción encryptkey.

Procedimiento

1. Especifique **encryptkey=save** en el archivo de opciones.
2. Realice la copia de seguridad de un archivo como mínimo con **asnode=ProxyNodeName** para crear una clave de cifrado local en cada nodo agente del entorno de varios nodos.

Resultados

Efectúe estos pasos para configurar el cifrado con la opción **encryptkey=prompt**:

1. Especifique **encryptkey=prompt** en el archivo de opciones.
2. Asegúrese de que los usuarios de los nodos agente del entorno de varios nodos utilicen la misma clave de cifrado.

Importante:

- Si cambia la clave de cifrado, deberá repetir los pasos anteriores.
- Utilice la misma clave de cifrado para todos los archivos de los que se haya realizado una copia de seguridad en el entorno de nodos compartido.

Copias de seguridad de planificación con soporte de proxy de nodo cliente

Se pueden utilizar varios nodos para realizar operaciones de copia de seguridad mediante un planificador.

Acerca de esta tarea

Cuando se otorga autorización de proxy a los nodos agente, estos efectúan las operaciones de copia de seguridad programada en nombre del nodo de destino. Cada nodo agente debe utilizar la opción `asnodename` en su planificación para realizar copias de seguridad de varios nodos para el nodo agente.

Inicie las planificaciones mediante el mandato del cliente `dsmc sched`:

En los siguientes ejemplos se muestran los mandatos del servidor de clientes de administración mediante el uso del planificador en varios nodos.

- El administrador registra todos los nodos que van a utilizarse emitiendo los siguientes mandatos:
 - `register node NODE-A`
 - `register node NODE-B`
 - `register node NODE-C`
- El administrador concede autoridad de proxy a cada nodo de agente utilizando los siguientes mandatos:
 - `grant proxynode target=NODE-Z agent=NODE-A`
 - `grant proxynode target=NODE-Z agent=NODE-B`
 - `grant proxynode target=NODE-Z agent=NODE-C`
- El administrador define las planificaciones utilizando los siguientes mandatos:
 - `define schedule standard proxy1 description="NODE-A proxy schedule" action=incremental options="-asnode=NODE-Z" objects=/Volumes/Xsan1 startdate=05/21/2005 starttime=01:00`
 - `define schedule standard proxy2 description="NODE-B proxy schedule" action=incremental options="-asnode=NODE-Z" objects=/Volumes/Xsan2 startdate=05/21/2005 starttime=01:00`
 - `define schedule standard proxy3 description="NODE-C proxy schedule" action=incremental options="-asnode=NODE-Z" objects=/Volumes/Xsan3 startdate=05/21/2005 starttime=01:00`

Nota: Coloque la opción `asnodename` únicamente en la definición de la planificación. No la coloque en el archivo de opciones del cliente, en la línea de mandatos, ni en ninguna otra ubicación.

También puede utilizar el daemon de aceptación del cliente (**dsmcad**), con `managedservices` definida como **schedule** en el archivo de opciones del sistema.

Nota:

- Cada planificación se puede iniciar desde una LPAR o estación de trabajo distinta.
- Tras ejecutar las planificaciones, cualquier cliente con proxy puede solicitar y restaurar todos los datos con copia de seguridad.
- Una operación de proxy utiliza los valores del nodo de destino (por ejemplo, **maxnumppy deduplication**) y las planificaciones que se definen en el servidor de IBM Spectrum Protect. Los valores del nodo de servidor de IBM Spectrum Protect y las planificaciones del nodo de agente se ignoran.

Referencia relacionada:

“Asnodename” en la página 349

“Valores de sesión y planificaciones de una operación de proxy” en la página 350

 Mandato DEFINE SCHEDULE

Ejemplos de cómo planificar una copia de seguridad de un clúster de IBM PowerHA SystemMirror

Esta sección muestra algunos ejemplos de cómo realizar una copia de seguridad de un clúster de IBM PowerHA SystemMirror.

Acerca de esta tarea

Siga estos pasos para activar la planificación de varios nodos:

1. Asegúrese de que todos los nodos agente tengan una autorización de proxy sobre el nodo de destino común
2. Asegúrese de que todos los nodos agente tengan una planificación definida en el servidor:

```
def sched domain_name sched_name options='-asnode=target'
```
3. Asegúrese de que cada nodo agente tenga la planificación asociada con un nodo:

```
def association domain_name schedule_name <agentnodename>
```

En los ejemplos siguientes, IBM PowerHA SystemMirror está configurado para dos hosts de AIX, host_a y host_b. Junto con sus propios datos locales, los hosts comparten el almacenamiento de disk, que tiene dos espacios de archivos: /disk1 y /disk2.

En el ejemplo del CLUSTERNODE se muestra cómo la opción clusternode se utiliza en un entorno IBM PowerHA SystemMirror actual.

- El administrador define 3 nodos en el servidor IBM Spectrum Protect: host_a, host_b, cluster_group, mediante los mandatos siguientes: (1) REGISTER NODE host_a mysecretpa5s, (2) REGISTER NODE host_b mysecretpa5s, (3) REGISTER NODE cluster_group mysecretpa5s.
- El administrador define un archivo dsm.opt en host_a y host_b (tenga en cuenta que los archivos opt son distintos en cada host), utilizando los siguientes mandatos: (1) NODENAME host_a (la opción se puede dejar como valor predeterminado), (2) DOMAIN /home /usr ... etc..
- El administrador define un archivo dsm.opt ubicado en algún sitio de uno de los grupos de disco de clúster, p.ej. /disk1/tsm/dsm.opt, utilizando los siguientes mandatos: (1) NODENAME cluster_group, (2) DOMAIN /disk1 /disk2, (3) CLUSTERNODE YES.
- El administrador define una planificación en el servidor de IBM Spectrum Protect, utilizando el mandato DEFINE SCHEDULE STANDARD CLUSTER_BACKUP.

- El administrador define asociaciones para cada uno de los 3 nodos, utilizando el mandato `DEFINE ASSOC STANDARD CLUSTER_BACKUP host_a,host_b,cluster_group`. En un momento dado, se ejecutan tres instancias de la planificación del cliente de archivado y copia de seguridad. (El planificador para `cluster_group` formará parte de los recursos del clúster que se sustituyen siempre que se sustituyan los recursos de disco del grupo de clúster. Por lo tanto, se ejecutará en el `host_a` o el `host_b`, pero no en los dos a la vez.)
- Los tres nombres de nodo contienen datos en el servidor de IBM Spectrum Protect.

En el ejemplo de `ASNODE` se muestra cómo se puede configurar sin utilizar `CLUSTERNODE`; se trata de una solución global que se podría aplicar a las soluciones de clúster de UNIX a las que no damos soporte, p.ej. Veritas Cluster Server for Solaris.

- El administrador define 3 nodos en el servidor de IBM Spectrum Protect, `host_a`, `host_b`, `cluster_group`:

```
REGISTER NODE host_a mysecretpa5s
REGISTER NODE host_b mysecretpa5s
REGISTER NODE cluster_group mysecretpa5s
```
- El administrador define una relación de nodo proxy entre `host_a` y `host_b` con `hacmp_cluster`

```
GRANT PROXYNODE TARGET=cluster_group AGENT=host_a,host_b
```
- El administrador define un archivo `dsm.opt` en `host_a` y `host_b` para manejar los sistemas de archivos locales:

```
NODENAME host_a (la opción se puede dejar como valor predeterminado)
DOMAIN /home /usr ... etc.

NODENAME host_b (la opción se puede dejar como valor predeterminado)
DOMAIN /home /usr ... etc.
```
- El administrador define un archivo `dsm.opt` en el recurso de clúster para gestionar la copia de seguridad de los recursos en clúster, por ejemplo: `/disk1/tsm/dsmcluster.opt` (el nombre de nodo es el nombre de nodo predeterminado, que es `host_a` o `host_b`, según la máquina que contenga el grupo de clúster en cada momento):

```
DOMAIN /disk1 /disk2
ASNODE cluster_group
```
- El administrador define una planificación en el servidor de IBM Spectrum Protect:

```
DEFINE SCHEDULE STANDARD CLUSTER_BACKUP
```
- El administrador define asociaciones para cada uno de los 3 nodos.

```
DEFINE ASSOC STANDARD CLUSTER_BACKUP host_a,host_b,cluster_group
```
- En un momento dado, se ejecutarán tres instancias de la planificación del cliente copia de seguridad/archivado estando en ejecución el planificador para el nodo `hacmp_cluster` del `host_a` o el `host_b`, pero no en ambos (se incluye en los recursos de clúster que se sustituirían por anomalía). Este planificador indicaría al archivo `dsmcluster.opt` que está definido en cada host. Las tres instancias se iniciarían como:

```
[host_a] dsmc sched
[host_b] dsmc sched
[cluster_group] dsmc sched -optfile=/disk/tsm/dsmcluster.opt
```
- Los tres nombres de nodo contienen datos en el servidor de IBM Spectrum Protect.

Para obtener más información sobre los mandatos del planificador del servidor, consulte la documentación del mismo.

Planificar una copia de seguridad de un sistema de archivos de GPFS

Utilice el planificador y las relaciones de proxy para realizar la copia de seguridad de un sistema de GPFS.

Acerca de esta tarea

Supongamos que los tres nodos de un clúster GPFS participan en la operación de copia de seguridad. Los nodos `node_1`, `node_2` y `node_3` se utilizan solo para autenticación. Se realiza la copia de seguridad de los espacios de archivo que pertenecen al nodo `node_gpfs`.

Procedimiento

1. Defina cuatro nodos en el servidor de IBM Spectrum Protect.

```
REGISTER NODE node_1 mysecretpa5s  
REGISTER NODE node_2 mysecretpa5s  
REGISTER NODE node_3 mysecretpa5s  
REGISTER NODE node_gpfs mysecretpa5s
```
2. Defina una relación de proxy entre los nodos.

```
GRANT PROXYNODE TARGET=node_gpfs AGENT=node_1,node_2,node_3
```
3. Defina una planificación.

```
DEFINE SCHEDULE STANDARD GPFS_SCHEDULE ACTION=incremental  
OBJECTS="/gpfs"  
  
DEFINE ASSOCIATION STANDARD GPFS_SCHEDULE node_gpfs
```
4. Elija uno de los sistemas GPFS para ejecutar la planificación. Especifique las opciones **nodename** y **asnodename** en el archivo de opciones `dsm.sys` en todos los sistemas del clúster de GPFS. El valor para la opción **asnodename** debe ser el mismo en todos los sistemas.

Definiciones en el archivo de opciones `dsm.sys` en el nodo 1:

```
nodename node_1  
asnodename node_gpfs
```

Definiciones en el archivo de opciones `dsm.sys` en el nodo 2:

```
nodename node_2  
asnodename node_gpfs
```




Definiciones en el archivo de opciones `dsm.sys` en el nodo 3:

```
nodename node_3  
asnodename node_gpfs
```

5. Inicie el planificador en el sistema que se elige para ejecutar la planificación.

```
DSMC SCHED
```

Información relacionada:

-  Mandato `mmbackup`: Requisitos de IBM Spectrum Protect
-  Orientación para integrar IBM Spectrum Scale AFM con IBM Spectrum Protect
-  Utilización de las opciones de inclusión y exclusión de IBM Spectrum Protect con el mandato `mmbackup` de IBM Spectrum Scale

Asociar una instantánea local con un espacio de archivos del servidor (UNIX y Linux)

Utilice la opción `snapshotroot` con los mandatos **incremental** y **selective** junto con una aplicación de otro proveedor de software independiente que proporcione una instantánea de un volumen lógico para asociar los datos de la instantánea local con los datos del espacio de archivos reales que se almacenan en el servidor de IBM Spectrum Protect.

La opción `snapshotroot` no proporciona ningún recurso para tomar una instantánea de volumen, sólo para gestionar los datos que ha creado una instantánea de volumen.

Referencia relacionada:

“Snapshotroot” en la página 571

Copia de seguridad de imagen

Desde la estación de trabajo local puede hacer una copia de seguridad de un volumen lógico como un solo objeto (copia de seguridad de imagen) del sistema.

La copia de seguridad de imagen estática tradicional impide que durante la operación otras aplicaciones del sistema accedan con permiso de escritura al volumen.

Debe ser usuario root para realizar esta tarea y la copia de seguridad de imágenes no se aplica a Mac OS X.

Una copia de seguridad de imagen proporciona las ventajas siguientes:

- La copia de seguridad de sistemas de archivos que contienen un gran número de archivos es más rápida que la copia de seguridad incremental completa de un sistema de archivos.
- Mejora la velocidad con la que el cliente restaura los archivos del sistema que contienen muchos archivos pequeños.
- Conserva los recursos del servidor durante las copias de seguridad ya que solamente es necesaria una entrada para la imagen.
- Proporciona una imagen de un instante específico del volumen lógico, que puede resultarle útil si la empresa debe recuperar esta información.
- Restaura un sistema de archivos corrupto o un volumen lógico RAW. Los datos se restauran en el mismo estado que estaban cuando se realizó la última copia de seguridad de volúmenes lógicos.

La copia de seguridad de imagen estática tradicional impide que durante la operación otras aplicaciones del sistema accedan con permiso de escritura al volumen. Utilice la opción `dynamicimage` para realizar una copia de seguridad del volumen tal cual sin volver a montarlo como de sólo lectura. La copia de seguridad se puede dañar si las aplicaciones siguen grabando en el mismo volumen mientras que se está ejecutando la copia de seguridad. Al grabar en un volumen mientras que se está ejecutando una copia de seguridad puede provocar que los datos no sean consistentes y la pérdida de datos después de ejecutar una operación de restauración. La opción `dynamicimage` sustituye el valor de serialización de la copia en la clase de gestión para llevar a cabo una copia de seguridad de una imagen. Después de restaurar una copia de seguridad de una imagen llevada a cabo con la opción `dynamicimage`, siempre debe ejecutar el programa de utilidad `chkdsk`.

Para poder restaurar una copia de seguridad de imágenes de un volumen, el cliente de copia de seguridad y archivado debe ser capaz de obtener un bloque exclusivo en el volumen que está restaurándose.

Restricción: No utilice copias de seguridad de imágenes dinámicas para sistemas de archivos, ya que el diseño interno del sistema de archivos podría dar lugar a datos incoherentes, incluso cuando no exista actividad de grabación. Asimismo, la copia de seguridad de imágenes dinámicas puede causar una imagen difusa, que podría no ser válida o estar completa al restaurarse.

Si el cliente de copia de seguridad y archivado no consigue montar el sistema de archivos después de restaurar una imagen, ejecute **fsck**. Sin embargo, la ejecución de **fsck** puede afectar a la integridad de grandes cantidades de datos. No utilice la copia de seguridad de imágenes dinámicas con sistemas de archivos JFS2 AIX. El cliente de copia de seguridad y archivado no admite copias de seguridad de imágenes dinámicas con sistemas de archivos JFS2 AIX. Si especifica `dynamicimage=yes` en un sistema de archivos JFS2, el cliente realiza una copia de seguridad de imágenes basada en instantánea. Si por alguna razón no puede crearse la instantánea, el cliente realiza una copia de seguridad de imágenes estática.

Atención: Para evitar perder datos, procure no utilizar la opción `dynamicimage` y asegúrese de que no exista ningún tipo de actividad de grabación en el volumen mientras se esté ejecutando la copia de seguridad.

En los sistemas de archivos AIX JFS2 la cantidad de datos de los que se hace copia de seguridad en el servidor IBM Spectrum Protect durante la copia de seguridad de imágenes estáticas o de instantánea se reduce porque sólo se copian los bloques que utiliza el sistema de archivos o los que tengan un valor menor de la opción `imagegapsize`. Este método de copia de seguridad de los datos mejora el rendimiento de las copias de seguridad de imágenes. Para obtener más información, consulte “Imagegapsize” en la página 454.

Solo para clientes AIX: de manera predeterminada, el cliente realiza una copia de seguridad de imágenes de instantánea en línea de los sistemas de archivos JFS2, durante la cual el volumen queda disponible para otras aplicaciones del sistema.

Para clientes de Linux solo: de forma predeterminada, el cliente realiza una copia de seguridad de una imagen de instantánea de los sistemas de archivos que hay en un volumen lógico creado por Linux Logical Volume Manager. El volumen está disponible en otras aplicaciones del sistema, mientras que se realiza la copia de seguridad.

En el cliente de Linux: no se admiten las copias de seguridad de imágenes de dispositivos DASD con modalidad de acceso de seguimiento raw en Linux on z Systems.

Atención: Los sistemas de archivos gestionados por IBM Spectrum Protect for Space Management no se habilitan para la copia de seguridad.

Tareas relacionadas:

“Copia de seguridad y archivado de archivo basada en instantánea y copia de seguridad de imágenes basada en instantánea” en la página 203

Realización de tareas de requisitos previos antes de crear una copia de seguridad de imágenes

En este tema se indican algunas de las consideraciones que deben tenerse en cuenta al realizar una copia de seguridad de imágenes.

Acerca de esta tarea

A continuación, se indican las consideraciones que deberá tener en cuenta cuando realice una copia de seguridad.

- Asegúrese de que ninguna otra aplicación utiliza el volumen cuando ejecute una copia de seguridad de imágenes estática. Para garantizar una imagen coherente durante el proceso de copia de seguridad, si se detecta un espacio de archivos en el volumen, el cliente desmonta y vuelve a montar el volumen en modo de sólo lectura, de manera que ninguna otra aplicación pueda acceder a él. Si el volumen se encuentra en uso cuando el cliente intenta desmontarlo, la copia de seguridad da un error. Si el cliente no puede desmontar y volver a montar el volumen en modalidad de sólo lectura porque está utilizándose y no hay disponible una copia de seguridad de instantánea, puede utilizar la opción `dynamicimage` para obligar al cliente a realizar una copia de seguridad de imagen sin desmontar y volver a montar el volumen en modalidad de sólo lectura. Establezca la opción `dynamicimage` en la sentencia `include.image` o desde la línea de mandatos. La copia de seguridad puede resultar dañada si las aplicaciones graban en el volumen mientras la operación de copia de seguridad se encuentra en proceso. Esto puede corregirse ejecutando `fsck` después de una operación de restauración para solucionar los bloques que se hayan dañado.

Si no se detecta ningún sistema de archivos en el volumen del que se está haciendo la copia de seguridad, asegúrese de que todas las aplicaciones que escriben en los volúmenes estén detenidas. El cliente de copia de seguridad/archivado utiliza la tabla del sistema de archivos y la tabla de montaje para detectar los sistemas de archivos soportados.

No incluya archivos del sistema en una copia de seguridad de imagen, ya que los archivos del sistema que se utilizan de forma activa no se pueden desmontar.

Sólo para AIX y Linux: si realiza una copia de seguridad de imágenes de un sistema de archivos que se ha montado en otro punto de montaje y se ha especificado en la tabla de sistemas de archivos, después de llevar a cabo la copia de seguridad de imágenes, se perderán la mayoría de opciones de montaje de este sistema, salvo el estado de lectura/grabación.

Importante: si un sistema de archivos tiene puntos de montaje anidados, desmóntelos antes de intentar realizar una copia de seguridad. De lo contrario, el cliente no puede desmontar el volumen. El sistema de archivos estará *ocupado* si contiene montajes.

- Utilice la opción `include.image` para asignar una clase de gestión a la imagen del volumen. Si no la asigna, se utilizará la clase de gestión predeterminada para la imagen.
- Puede excluir un volumen de la copia de seguridad de imagen utilizando la opción `exclude.image`.
- Debe utilizar el punto de montaje para el volumen del sistema de archivos en el que desee realizar una copia de seguridad de imágenes. El cliente no realizará una copia de seguridad del volumen del sistema de archivos sin utilizar un punto de montaje. Realice una copia de seguridad de sistemas de archivos utilizando el nombre montado. Por ejemplo, si `/dev/lv01` se formatea como un sistema de archivos montado en `/home`, escriba este mandato para realizar una copia de seguridad de imagen de este volumen:


```
dsmc backup image /home
```

Realizar una copia de seguridad de volúmenes RAW utilizando el nombre del dispositivo. Por ejemplo, si /dev/lv02 es un volumen RAW, escriba este mandato para realizar una copia de seguridad de imagen de este volumen:

```
dsmc backup image /dev/lv02
```

Si realiza una copia de seguridad de un volumen RAW formateado como sistema de archivos, asegúrese de que el sistema de archivos no está montado y no tiene ninguna entrada en /etc/filesystems.

Conceptos relacionados:

Capítulo 9, “Políticas de gestión de almacenamiento”, en la página 299

Referencia relacionada:

“Opciones exclude” en la página 425

“Opciones include” en la página 458

Soporte de tipo de dispositivo de volumen para una copia de seguridad de imagen

En este tema se enumeran los diferentes dispositivos admitidos por el mandato **backup image**.

La tabla siguiente lista los dispositivos admitidos cuando se utiliza el mandato **backup image**. Un dispositivo RAW puede ser una porción de disco, una partición o un volumen lógico.

Tabla 37. Soporte de tipo de dispositivo de volumen para una copia de seguridad de imagen

Gestor de volúmenes lógicos	Tipos de dispositivo RAW	Nombre de dispositivo de ejemplo	Soporte del mandato Backup image
Gestor de volúmenes lógicos de AIX	Volúmenes lógicos	/dev/lv00	AIX
Gestor de volúmenes Sun Solstice DiskSuite	Metadispositivos	/dev/md/dsk/dl	Solaris
Gestor de volúmenes Solaris	Metadispositivos	/dev/md/dsk/dl	Solaris
Gestor de volúmenes de Veritas	Volúmenes lógicos	/dev/vx/dsk/rootdg/vol01 - AIX /dev/vg00/lvol01 - Solaris	Solaris AIX
Disco RAW	Particiones	/dev/hda1, /dev/sda3	Linux x86_64, Linux en POWER
Disco RAW	Dispositivos de disco	/dev/sda /dev/mapper/mpathX	Linux x86_64
Disco RAW	Particiones	/dev/dasdx	Linux on System z
Gestor de volúmenes lógicos de Linux	Volúmenes lógicos	/dev/myvolgroup/ mivolumen	Linux en general
Disco RAW	Porciones de disco	/dev/dsk/c0tld0s0	Solaris

Para dispositivos en bruto, el cliente de copia de seguridad y archivado realiza copias de seguridad del volumen tal cual. Es decir, no se realiza ninguna instantánea y las aplicaciones pueden continuar escribiendo en el volumen mientras se lleva a cabo la copia de seguridad. IBM Spectrum Protect no puede garantizar la coherencia de los datos al realizar copias de seguridad a nivel del

disco físico; si los datos del volumen cambian mientras la realización de la copia de seguridad está en curso, estos podrían corromperse.

El cliente debe admitir el tipo de dispositivo RAW de la plataforma específica para poder realizar una copia de seguridad de imagen de un dispositivo RAW. Si se desea realizar una copia de seguridad de imágenes de un sistema de archivos montado en un dispositivo RAW, debe darse soporte a dicho dispositivo. Recuerde que debe especificar los dispositivos RAW según el nombre de dispositivo del bloque.

Para los clientes Linux, la copia de seguridad de imágenes sólo se admite en las particiones que tienen el ID 0x83 o en los volúmenes lógicos creados con el gestor de volúmenes lógicos de Linux. La realización de la copia de seguridad de otras particiones, como las particiones ampliadas que contienen datos de base de datos o sistemas de archivos montados, podría generar datos de copia de seguridad incoherentes si los datos cambian durante la operación de copia de seguridad de imagen.

Para AIX y Solaris: puede realizar operaciones de imágenes en volúmenes creados con el gestor de volúmenes de Veritas. Inicialmente, el cliente admite tipos de imágenes estáticas (opción predeterminada) y dinámicas para la copia de seguridad.

En los clientes de Solaris 10, utilice la copia de seguridad de imagen solo para los sistemas de archivos que se han asignado desde la zona global hasta la zona no global exportando el dispositivo y especificando agregar dispositivo y establecer coincidencia. No utilice la copia de seguridad de imagen para otros sistemas de archivos de las zonas no globales, pues la zona no global no dispone de autorización para montar o desmontar el sistema de archivos. Asimismo, en los clientes de Solaris 10, no utilice el dispositivo de superposición del disco de la raíz (c0t0d0s2) para la copia de seguridad de dispositivo RAW. Debe evitarse utilizar esta función en los discos o porciones que se utilizan como dispositivos de intercambio.

Los metadispositivos que ha creado el gestor de volúmenes de Veritas, incluido el grupo de discos de /etc/vfstab, deben listarse para que el cliente de archivado y copia de seguridad pueda reconocerlos para realizar una copia de seguridad de imágenes de los sistemas de archivos. Los sistemas de archivos deben estar sin montar. Los dispositivos RAW no deben encontrarse en /etc/vfstab. Por ejemplo, a continuación se muestra el nombre del metadispositivo correcto que debe utilizarse en el archivo /etc/vfstab:

```
/dev/vx/dsk/<grupo_discos>/<nombre_metadispositivo>
```

La especificación de /dev/vx/dsk/ no se reconocerá correctamente y recibirá un error (ANS1134E).

No debe realizarse la copia de seguridad o restauración de las porciones de disco que contienen el cilindro 0. En este caso, se graba encima del VTOC. Si debe realizar la copia de seguridad de la primera porción del disco, excluya el cilindro 0 iniciando la porción del disco desde el cilindro 1 (utilice la herramienta de formato). El cliente de archivado y copia de seguridad no comprueba si el cilindro 0 está o no contenido en el dispositivo sobre el que se graba durante un proceso de restauración.

Utilización de las copias de seguridad de imagen para realizar copias de seguridad incrementales del sistema de archivos

En este tema se enumeran los métodos y los pasos necesarios para utilizar las copias de seguridad de imágenes para realizar copias de seguridad incrementales eficaces del sistema de archivos.

Estos métodos de copia de seguridad permiten realizar una restauración a un instante específico de los sistemas de archivos y mejorar el rendimiento de las operaciones de copia de seguridad y restauración. La copia de seguridad sólo la puede realizar en volúmenes con formato y no en volúmenes lógicos RAW.

Puede utilizar uno de los siguientes métodos para realizar copias de seguridad de imagen de volúmenes con sistemas de archivos montados:

Método 1: Uso de las copias de seguridad de imagen con la copias de seguridad incrementales de sistemas de archivos

En este tema figuran los pasos necesarios para realizar copias de seguridad de imágenes con copias de seguridad incrementales de sistemas de archivos.

Acerca de esta tarea

Procedimiento

1. Realizar una copia de seguridad de imágenes del sistema de archivos. De este modo se establece una base para las copias de seguridad incrementales futuras.
2. Realice una copia de seguridad de imagen del mismo sistema de archivos para posibilitar la restauración de la imagen.
3. Realice periódicamente copias de seguridad incrementales del sistema de archivos para garantizar que las adiciones y las supresiones se registran de forma precisa en el servidor.
4. Realice una copia de seguridad de imagen periódicamente para garantizar una restauración más rápida.
5. Restaure los datos realizando una restauración incremental. Asegúrese de seleccionar las opciones **Imagen más directorios y archivos incrementales** y **Suprimir archivos inactivos de sistema local** en la ventana Opciones de restauración antes de iniciar el proceso de restauración. Durante la restauración, el cliente realiza lo siguiente:

Resultados

- Restaure la imagen más reciente en el servidor.
- Suprime todos los archivos restaurados en el paso anterior que están desactivados en el servidor. Éstos son los archivos que existían en el momento de realizar la copia de seguridad de imágenes pero que después se suprimieron y grabaron en una copia de seguridad incremental.
- Restaure los archivos nuevos y modificados a partir de las copias de seguridad incrementales.

Nota: Si una copia de seguridad incremental se realiza varias veces después de haberse realizado una copia de seguridad de una imagen, asegúrese de que el grupo de copias de seguridad del servidor de IBM Spectrum Protect dispone de suficientes versiones de los archivos existentes y suprimidos en el servidor para que la posterior restauración de imagen con las opciones incremental y deletefiles pueda suprimir correctamente los archivos.

Tareas relacionadas:

“Copia de seguridad de datos mediante la GUI Java” en la página 181

“Realización de una copia de seguridad de imagen mediante la GUI” en la página 201

“Restauración de una imagen mediante la GUI” en la página 239

Método 2: Uso de las copias de seguridad de imagen con las copias de seguridad de imagen incremental por fecha

En este tema figuran los pasos necesarios para realizar copias de seguridad de imágenes con copias de seguridad de imagen incremental por fecha.

Procedimiento

1. Realice una copia de seguridad de imagen del sistema de archivos.
2. Realice una copia de seguridad de imágenes incremental por fecha del sistema de archivos. Con ello solamente se envían al servidor los archivos que se han añadido o modificado desde la copia de seguridad de imágenes más reciente.
3. Periódicamente, realice copias de seguridad completas.
4. Restaure el volumen realizando una restauración incremental. Asegúrese de seleccionar la opción **Imagen más directorios y archivos incrementales** en la ventana Opciones de restauración antes de iniciar el proceso de restauración. Con ello se restaura primero la imagen más reciente y después todas las copias de seguridad incrementales realizadas desde esa fecha.

Resultados

Nota: Debe realizar copias de seguridad de imagen completas periódicamente en los casos siguientes:

- Cuando un sistema de archivos cambie notablemente (más del 40%), tal como se indica en el paso 4 del método 1 y en el paso 3 del método 2. Al realizar la restauración, se proporcionará una imagen del sistema de archivos similar a la que existía en el momento de la última copia de seguridad de imagen incremental por fecha, y además se mejorará el tiempo de restauración.
- Según sea adecuado en su entorno.

De este modo se reduce el tiempo necesario para la restauración, ya que se aplican menos cambios de las copias de seguridad incrementales.

Cuando se utiliza el método 2 se aplican las restricciones siguientes:

- El sistema de archivos no puede tener copias de seguridad incrementales completas anteriores.
- La copia de seguridad de imagen incremental por fecha no desactiva los archivos en el servidor, por lo tanto, cuando restaure una imagen que tenga la opción incremental, los archivos que se hayan suprimido después de la copia de seguridad de imagen original estarán presentes después de la restauración.
- Si se trata de la primera copia de seguridad de imágenes del sistema de archivos, se realiza una copia de seguridad de imágenes completa.
- Si los sistemas de archivos están funcionando completos o casi completos, puede provocarse una condición de falta de espacio durante la restauración.

Tareas relacionadas:

“Realización de una copia de seguridad de imagen mediante la GUI” en la página 201

“Restauración de una imagen mediante la GUI” en la página 239

Comparación de los métodos 1 y 2

En este tema se muestra una comparación de los métodos 1 y 2: (1) Uso de la copia de seguridad de imágenes con la copia de seguridad incremental del sistema de archivos o (2) Uso de la copia de seguridad de imágenes con la copia de seguridad de imágenes incremental por fecha.

Para ayudarle a determinar el método más adecuado para su entorno, en la siguiente tabla se muestra una comparación de los métodos 1 y 2.

Tabla 38. Comparación de métodos de copia de seguridad de imagen incremental

Método 1: Uso de la copia de seguridad de imagen con la copia de seguridad incremental de sistemas de archivos	Método 2: Uso de la copia de seguridad de imagen con la copia de seguridad de imagen incremental por fecha
Los archivos caducan en el servidor cuando se suprimen del sistema de archivos. Al restaurarlos, tiene la opción de suprimir los archivos que caduquen en la imagen del servidor.	Los archivos no caducan en el servidor. Una vez finalizada la restauración de imagen incremental, todos los archivos suprimidos en el sistema de archivos después de la copia de seguridad de imágenes están presentes después de la restauración. Si los sistemas de archivos están funcionando completos o casi completos, puede provocarse una condición de falta de espacio.
El tiempo de copia de seguridad incremental es el mismo que en las copias de seguridad incrementales normales.	La copia de seguridad de imagen incremental es más rápida porque el cliente no consulta en el servidor cada archivo copiado.
La restauración es mucho más rápida que una restauración incremental completa del sistema de archivos.	La restauración es mucho más rápida que una restauración incremental completa del sistema de archivos.
Los directorios suprimidos del sistema de archivos después de la última copia de seguridad de imagen no caducan.	Los directorios y archivos suprimidos del sistema de archivos después de la última copia de seguridad de imagen completa no caducan.

Realización de una copia de seguridad de imagen mediante la GUI

Si la característica de copia de seguridad de imágenes está configurada, puede crear una copia de seguridad de imágenes durante la cual el volumen queda disponible para las otras aplicaciones del sistema.

Acerca de esta tarea

Durante el proceso de copia de seguridad de imágenes, se mantiene una imagen constante del volumen.

Cuando realice una copia de seguridad de imagen con la opción `image backup` de la GUI del cliente de archivado y copia de seguridad, la operación de copia de seguridad se ejecuta según el valor de la opción `snapshotproviderimage`. La opción `snapshotproviderimage` toma como valor predeterminado una instantánea AIX JFS2 para AIX y una instantánea Linux LVM para Linux. Puede sustituir el valor predeterminado utilizando la pestaña Instantánea del Editor de preferencias y Preferencias de instantánea de imagen.

En el caso de clientes Solaris, al seleccionar la opción `image backup` se ejecuta una copia de seguridad de imágenes estáticas de forma predeterminada. En una copia

de seguridad de imagen estática, el cliente desmonta y vuelve a montar el volumen en modo de sólo lectura, de manera que ninguna otra aplicación pueda acceder a él. Puede sustituir el valor predeterminado utilizando la opción `include.image` y seleccionando `dynamicimage yes`. En una copia de seguridad de imagen dinámica, el cliente realiza la copia de seguridad de imagen, durante la cual el sistema de archivos no será de sólo lectura.

Para crear una copia de seguridad de imagen del sistema de archivos o del volumen lógico RAW, lleve a cabo los pasos siguientes:

Procedimiento

1. Pulse el botón **Copia de seguridad** en la ventana principal de IBM Spectrum Protect. Aparecerá la ventana Copia de seguridad.
2. Expanda el árbol de directorios y seleccione los objetos de los que desee hacer una copia de seguridad. Para realizar una copia de seguridad de un volumen lógico RAW, localice y expanda el objeto de árbol de directorios RAW.
3. Pulse en **Copia de seguridad**. La ventana **Lista de tareas** de copia de seguridad muestra el estado del proceso de la copia de seguridad. Aparecerá la ventana Informe de copia de seguridad.

Resultados

- Para realizar una copia de seguridad de imagen estática, seleccione **Copia de seguridad de imagen** en la lista desplegable.
- *Sólo* en clientes AIX y Linux : para realizar una copia de seguridad de imagen de instantánea, utilice la opción `snapshotproviderimage`.
- Para realizar una copia de seguridad de imagen incremental por fecha, seleccione **Incremental de imagen (sólo por fecha)** en la lista desplegable.

A continuación, figuran algunas cuestiones que deberá tener en cuenta cuando realice una copia de seguridad de imagen basada en instantánea:

- Si desea modificar opciones de copia de seguridad específicas, pulse el botón **Opciones**. Las opciones que seleccione estarán en vigor únicamente durante la sesión actual.
- Si desea modificar opciones de copia de seguridad específicas, pulse el botón **Opciones**. Las opciones que seleccione estarán en vigor únicamente durante la sesión actual.

Solo Linux: el cliente IBM Spectrum Protect versión 5.4 (y posteriores) no reconocerá ningún volumen LVM1 para operaciones de imagen. Sin embargo, permite la restauración de las copias de seguridad de imagen anteriores de los volúmenes LVM1 en volúmenes LVM2. En la Tabla 39 se muestran las combinaciones que implican a los niveles de cliente anteriores y nuevos que gestionan volúmenes LVM1 y LVM2 para distintas operaciones de imagen.

Tabla 39. Comparaciones de las operaciones de imagen de LVM1 y LVM2

Versión del cliente IBM Spectrum Protect	Copia de seguridad y restauración de LVM1	Copia de seguridad y restauración de LVM2	Volúmenes combinados	
			Copia de seguridad: LVM1. Restauración: LVM2	Copia de seguridad: LVM2. Restauración: LVM1
V5.3 y anteriores	SÍ	Sólo imagen estática para el sistema de archivos	NO	NO: no se admiten los volúmenes RAW

Tabla 39. Comparaciones de las operaciones de imagen de LVM1 y LVM2 (continuación)

Versión del cliente IBM Spectrum Protect	Copia de seguridad y restauración de LVM1	Copia de seguridad y restauración de LVM2	Volúmenes combinados	
			Copia de seguridad: LVM1. Restauración: LVM2	Copia de seguridad: LVM2. Restauración: LVM1
V5.4 y posteriores	NO Se visualiza el mensaje de error ANS1090E	SÍ	SÍ La copia de seguridad del volumen LVM1 debe haberse realizado utilizando el cliente anterior	NO La restauración en el volumen LVM1 falla

Referencia relacionada:

“Snapshotproviderimage” en la página 570

Realización de una copia de seguridad de imagen mediante la línea de mandatos

Utilice los mandatos **backup image** y **restore image** para realizar las operaciones de copia de seguridad de imagen y las operaciones de restauración en un solo volumen.

Utilice la opción **mode** con el mandato **backup image** para realizar una copia de seguridad de imágenes incremental por fecha que únicamente realice una copia de seguridad de los archivos nuevos y de los que se han modificado desde la copia de seguridad de imágenes completa más reciente. Sin embargo, de este modo solamente realizará una copia de seguridad de los archivos cuya fecha se haya modificado y no de los archivos cuyos permisos se hayan modificado.

Referencia relacionada:

“Backup Image” en la página 674

“Mode” en la página 492

“Restore Image” en la página 758

Copia de seguridad y archivado de archivo basada en instantánea y copia de seguridad de imágenes basada en instantánea

Para clientes de copia de seguridad y archivado que se ejecutan en AIX 5.3 o sistemas de archivos JFS2 posteriores como usuario root, la copia de seguridad de imágenes basada en instantánea se crea mediante las instantáneas predeterminadas.

Acerca de esta tarea

Opcionalmente puede habilitar las operaciones de copia de seguridad y archivado de nivel de archivo basadas en instantánea; para ello especifique la opción **snapshotproviderfs**. Si por alguna razón no puede tomarse una instantánea, el cliente intenta realizar una copia de seguridad de imágenes estática o una copia de seguridad de archivos normal.

Si desea especificar una operación de copia de seguridad y archivado de archivo basada en instantánea, defina la opción `snapshotproviderfs` con el valor `JFS2`. Este será aplicable a todos los sistemas de archivos JFS2 para ese cliente.

Importante: Utilice una copia de seguridad y archivado basada en instantánea y una copia de seguridad de imágenes basada en instantánea para todos los sistemas de archivos AIX JFS2.

Por ejemplo, para *activar* la copia de seguridad y archivado de archivo basada en instantánea para todos los sistemas de archivos JFS2 del cliente, especifique lo siguiente en la sección del servidor del archivo `dsm.sys`:

```
snapshotproviderfs JFS2
```

Para *desactivar* de manera explícita la copia de seguridad y archivado de archivo basada en instantánea para todos los sistemas de archivos JFS2 del cliente, especifique lo siguiente en la sección del servidor del archivo `dsm.sys`:

```
snapshotproviderfs NONE
```

Para *activar* de manera explícita la copia de seguridad y archivado de archivo basada en instantánea sólo para un sistema de archivos JFS2 determinado del cliente, especifique lo siguiente en la sección del servidor del archivo `dsm.sys`:

```
snapshotproviderfs NONE
```

```
include.fs /kalafs1 snapshotproviderfs=JFS2
```

Para *desactivar* de manera explícita la copia de seguridad y archivado de archivo basada en instantánea sólo para un sistema de archivos JFS2 determinado del cliente, especifique lo siguiente en la sección del servidor del archivo `dsm.sys`:

```
snapshotproviderfs JFS2
```

```
include.fs /kalafs2 snapshotproviderfs=NONE
```

Para *activar* de manera explícita la copia de seguridad y archivado de archivo basada en instantánea sólo para una operación determinada en el cliente, especifique lo siguiente en la línea de mandatos:

```
dsmc incr -snapshotproviderfs=JFS2 /kalafs1
```

Para *desactivar* la copia de seguridad y archivado de archivo basada en instantánea sólo para una operación determinada en el cliente, especifique lo siguiente en la sección del servidor del archivo `dsm.sys`:

```
snapshotproviderfs JFS2
```

Luego ejecute el mandato `backup`. Por ejemplo:

```
dsmc incr -snapshotproviderfs=NONE /kalafs2
```

Referencia relacionada:

“`Snapshotproviderfs`” en la página 569

Protección de los sistemas de archivos Btrfs

El sistema de archivos Btrfs debe incluirse como las especificaciones de los archivos para emitir los mandatos de copia de seguridad y restauración, los mandatos de archivado y recuperación y en los mandatos de **backup image** y **restore image**. También puede especificar los subvolúmenes Btrfs como la especificación del archivo para realizar la copia de seguridad y restauración y las

funciones de archivado y recuperación. No puede utilizar la imagen del cliente de archivado y copia de seguridad o los mandatos de restauración de la imagen en un subvolumen Btrfs.

Los sistemas de archivos Btrfs son compatibles en SLES 11 SP2 o posterior, en IBM System x, System p y System z.

Si desea crear una copia de seguridad de imagen estática del sistema de archivos Btrfs completo, debe desmontar todos los subvolúmenes para que el cliente de archivado y copia de seguridad se puede desmontar o montar el sistema de archivos Btrfs durante el proceso de copia de seguridad. Puede evitar los requisitos de montaje y desmontaje si lleva a cabo una copia de seguridad de imagen de instantánea del sistema de archivos Btrfs en vez de una copia de seguridad de una imagen estática.

La función de copia de seguridad y restauración de la imagen no está disponible para los subvolúmenes Btrfs. Si intenta realizar la copia de seguridad de un subvolumen utilizando **image backup**, se muestra el siguiente mensaje:

```
ANS1162E Filesystem could not be mounted
```

Puede montar un subvolumen Btrfs mediante el nombre del subvolumen o el ID del subvolumen.

En sistemas de archivos Btrfs, la copia de seguridad diaria se puede realizar en el sistema de archivos y a nivel del subvolumen. Si lleva a cabo copias de seguridad basadas en diario en un sistema de archivos Btrfs, el diario que se crea es para el sistema de archivos completo; no hay un diario individual para cada subvolumen.

Restricción: En sistemas Linux, algunos sistemas de archivos como ext2, ext3, ext4, btrfs y xfs utilizan un UUID (universally unique identifier) para que se identifiquen con el sistema operativo. Si crea una copia de seguridad de imagen de tal volumen y la restaura en una ubicación distinta, es posible que tenga dos volúmenes con el mismo UUID. Si utiliza UUID para definir los sistemas de archivos en `/etc/fstab`, tenga en cuenta que es posible que el cliente de copia de seguridad y archivado no pueda montar correctamente el sistema de archivos restaurado debido al conflicto de UUID. Para evitar esta situación, restaure la imagen a su ubicación original. Si debe restaurarla a una ubicación distinta, cambie el UUID de cualquier volumen original o restaurado antes de montar el sistema de archivos restaurado. Consulte la documentación de Linux para obtener instrucciones sobre cómo cambiar un UUID. También es posible que deba editar manualmente el archivo `/etc/fstab` para que se pueda montar el volumen original, el volumen restaurado, o ambos volúmenes.

Realizar la copia de seguridad y la restauración de los sistemas de archivos Btrfs

Puede realizar la copia de seguridad o restauración o el archivado y la recuperación de los sistemas de archivos Btrfs utilizando los mandatos del cliente de archivado y copia de seguridad **incremental**, **selective**, **restore**, **archive**, and **retrieve**.

Acerca de esta tarea

Si ha utilizado una versión del cliente de archivado y copia de seguridad anterior a la Versión 7.1 para realizar la copia de seguridad del sistema de archivos Btrfs, el tipo de sistema de archivos se ha listado como Unknown, en el servidor de GUI de

IBM Spectrum Protect y en la salida del mandato. El tipo de archivo del sistema Unknown se desplaza antes por IBM Spectrum Protect 7.1, los sistemas de archivos Btrfs no son compatibles formalmente. Si utiliza el cliente de archivado y copia de seguridad V7.1 (o posterior) para realizar la copia de seguridad al mismo sistema de archivos de Btrfs, se vuelve a realizar la copia de seguridad de todos los archivos que tienen listas de control de acceso (ACLs) y atributos extendidos (XATTRs), incluso si su contenido no ha cambiado desde la última copia de seguridad que se creó mediante la versión anterior del cliente. Además, después de realizar la copia de seguridad de un sistema de archivos Btrfs mediante el cliente con V7.1 (o posterior), el tipo de sistema se muestra correctamente como Btrfs en la GUI del servidor de IBM Spectrum Protect y en la salida del mandato.

Incluso con un cliente de V7.1 o posterior, copiar un archivo en un sistema de archivos Btrfs podría hacer que el archivo se incluyera en la siguiente operación de copia de seguridad. Por ejemplo, si copia un archivo utilizando el mandato **cp** con las opciones **-p** o **-preserve** (modos "preserve, ownership, y time stamps"), y si se cambian los atributos del archivo, el acceso al atributo ampliado ACL (system.posix_acl_access) también cambia. Ya que cambia el atributo ampliado, el cliente realiza la copia de seguridad del archivo completo en vez de solo actualizar los atributos para el archivo.

Procedimiento

1. Monte el sistema de archivos que desea proteger o recuperar. Por ejemplo, utilice la siguiente sintaxis para montar un sistema de archivos: `mount /dev/sdb1 on /btreefs1 type btrfs (rw)`
2. Proteja o recupere el sistema de archivos realizando una de las siguientes operaciones:

Operación	Mandato
Copia de seguridad del sistema de archivos	<code>dsmc incr /btreefs1</code>
Restauración del sistema de archivos	<code>dsmc restore /btreefs1/ -subdir=yes -replace=yes</code>
Archivado del sistema de archivos	<code>dsmc archive /btreefs1/ -subdir=yes</code>
Recuperación del sistema de archivos	<code>dsmc retrieve /btreefs1/ -subdir=yes -replace=yes</code>
Copia de seguridad de una instantánea de sistema de archivos	<p>Cree una instantánea del sistema de archivos. Utilice el mandato btrfs subvolume snapshot. El directorio de instantánea que se especifica en este ejemplo es el directorio <code>btreefs1_snap</code> del sistema de archivos denominado <code>/btreefs1</code>.</p> <pre>btrfs subvolume snapshot /btreefs1/ /btreefs1/btreefs1_snap</pre> <p>Emita el mandato del cliente de archivado y copia de seguridad incremental. Especifique la opción snapshotroot y la ubicación de la instantánea Btrfs.</p> <pre>\$DSM_DIR/dsmc incr /btreefs1 -snapshotroot=/btreefs1/btreefs1_snap</pre>

Operación	Mandato
Realización de una copia de seguridad de imagen	<p>Todos los subvolumenes deben estar desmontados antes de crear una copia de seguridad de la imagen.</p> <pre>dsmc backup image /btreefs1 -snapshotproviderimage=none</pre> <p>Para evitar tener que desmontar los subvolumenes, cree una copia de seguridad de imagen basada en instantánea.</p> <pre>dsmc backup image /btreefs1</pre>
Restauración de la copia de seguridad de la imagen	<p>Todos los subvolumenes deben estar desmontados antes de restaurar una copia de seguridad de la imagen.</p> <pre>dsmc restore image /btreefs1</pre>

Copia de seguridad y restauración de los subvolumenes Btrfs

Puede realizar una copia de seguridad o restauración o archivar y restaurar volúmenes de Btrfs utilizando los mandatos del cliente de archivado y copia de seguridad **incremental**, **selective**, **restore**, **archive** y **retrieve**.

Procedimiento

1. Liste los subvolumenes y determine sus identificadores.

```
btrfs subvolume list /btreefs1
ID 256 top level 5 path @
ID 262 top level 5 path @/btreefs1_sub1
```
2. Seleccione el directorio que se utilizará como punto de montaje en el subvolumen.

```
mkdir /btreefs1_sub1
```
3. Monte el subvolumen. Por ejemplo, para montar el subvolumen en un dispositivo sdb1 en /btreefs1_sub1, utilice la siguiente sintaxis: `mount -t btrfs -o subvolid=262 /dev/sdb1 /btreefs1_sub1`
Proteja o recupere el subvolumen utilizando una o más de las siguientes operaciones:

Operación	Mandato
Realizar la copia de seguridad de un subvolumen	<p>Se admiten tanto las copias de seguridad incrementales como las selectivas.</p> <pre>dsmc incr /btreefs1_sub1 dsmc sel /btreefs1_sub1/ -subdir=yes</pre>
Restaurar un subvolumen	<pre>dsmc restore /btreefs1_sub1/ -subdir=yes -replace=yes</pre>
Archivar un subvolumen	<pre>dsmc archive /btreefs1_sub1/ -subdir=yes</pre>
Recuperar un subvolumen	<pre>dsmc retrieve /btreefs1_sub1/ -subdir=yes -replace=yes</pre>

Operación	Mandato
Realizar una instantánea de un subvolumen Btrfs	<p>Cree una instantánea de subvolumen. Utilice el mandato btrfs subvolume snapshot. El directorio de la instantánea que se especifica en este ejemplo es el directorio <code>/btreefs1/btreefs1_sub1_snap</code> para el volumen llamado <code>btreefs1_sub1</code>.</p> <pre>btrfs subvolume snapshot /btreefs1/btreefs1_sub1 /btreefs1/btreefs1_sub1_snap</pre> <p>Emita el cliente de archivado y copia de seguridad del mandato incremental. Especifique la opción raíz de la instantánea y la ubicación de la instantánea Btrfs.</p> <pre>dsmc incr /btreefs1_sub1 -snapshotroot=/btreefs1 /btreefs1_sub1_snap</pre>

Realice la copia de seguridad de los sistemas de archivos NAS utilizando el Protocolo de gestión de datos de redes

Los clientes de archivado y copia de seguridad de Windows, AIX y Solaris pueden utilizar NDMP (Network Data Management Protocol - Protocolo de gestión de datos de redes) para realizar copias de seguridad de imágenes de sistema de archivo de almacenamiento conectado a la red (NAS) y restaurar dichas imágenes de forma eficiente. Las imágenes de sistema de archivo se pueden copiar en, o restaurar desde, bibliotecas o unidades de cinta automatizadas que están conectadas localmente a servidores de archivos NAS de EMC Celerra o de dispositivos de red, o se pueden copiar en, o restaurar desde, unidades de cinta o bibliotecas conectadas de forma local al servidor de IBM Spectrum Protect.

El soporte de NDMP solo está disponible en IBM Spectrum Protect Extended Edition.

Para clientes de Linux x86_64, se puede utilizar también la copia de seguridad incremental para realizar copias de seguridad de instantáneas de sistemas de archivos de NAS. Consulte el mandato **incremental** y las opciones `snapshotroot`, `snapdiff`, `createnewbase` y `diffsnapshot` para obtener más información.

Después de configurar el soporte de NDMP, el servidor se conecta al dispositivo NAS y utiliza NDMP para iniciar, controlar y supervisar cada operación de copia de seguridad y de restauración. El dispositivo NAS realiza la transferencia de datos externos hacia y desde el sistema de archivos NAS a una biblioteca asociada localmente.

La transferencia de datos de archivador a servidor se encuentra disponible para los dispositivos NAS que admitan NDMP versión 4.

Entre las ventajas de realizar copias de seguridad utilizando el soporte de NDMP se incluyen las siguientes:

- La transferencia de datos fuera de la LAN.
- Un alto rendimiento y copias de seguridad y restauraciones escalables.
- La copia de seguridad de dispositivos de cintas locales sin tráfico en la red.

Se proporciona el soporte siguiente:

- Copia de seguridad de imagen del sistema de archivos completa de todos los archivos de un sistema de archivos NAS.
- Copia de seguridad de imagen de archivos diferencial de todos los archivos que se han modificado desde la última copia de seguridad de imagen completa.
- Operaciones de copia de seguridad y restauración paralelas al procesar varios sistemas de archivos NAS.
- Opción de interfaces para iniciar, supervisar o cancelar operaciones de copia de seguridad y de restauración:
 - cliente Web
 - Interfaz de mandatos de cliente de archivado y copia de seguridad
 - Interfaz de línea de mandatos de cliente administrativo (se pueden programar operaciones de copia de seguridad y restauración utilizando el programador de mandatos administrativos)
 - Cliente web de administración

Las siguientes funciones *no* se admiten:

- Archivar y recuperar
- Planificación de cliente. Utilice los mandatos del servidor para planificar una copia de seguridad NAS.
- Detección de imágenes dañadas.
- Operaciones de transferencia de datos para datos NAS almacenados por IBM Spectrum Protect:
 - Migración
 - Reclamación
 - Exportación
 - Generación de juegos de copias de seguridad

Conceptos relacionados:

“Requisitos de soporte para NDMP (sólo Extended Edition)” en la página 11

Referencia relacionada:

“Diffsnapshot” en la página 387

“Incremental” en la página 704

“Snapdiff” en la página 561

“Snapshotroot” en la página 571

Copia de seguridad de los sistemas de archivos NAS con la GUI del cliente web utilizando el Protocolo de gestión de datos de redes NDMP

Para tanto la GUI del cliente web como la interfaz de línea de mandatos del cliente, debe especificar `passwordaccess=generate` (que es una restricción del cliente web actual para el nodo de cliente) y `set authentication=on` en el servidor.

Siempre se le solicitará un identificador de usuario y una contraseña. Para visualizar nodos NAS y llevar a cabo funciones NAS, debe entrar un identificador de usuario y una contraseña de administración autorizados. El ID de usuario de administración debe tener como mínimo autorización de propietario de cliente sobre el nodo NAS y sobre el nodo de la estación de trabajo cliente que están utilizando tanto desde la línea de mandatos como desde la Web.

Puede utilizar la opción `toc` con la opción `include.fs.nas` en el archivo de opciones del cliente para especificar si el cliente guarda la información de la tabla de contenido (TOC) para cada copia de seguridad del sistema de archivos. Si guarda la información de la TOC, puede utilizar el cliente web de Windows para examinar todo el árbol del sistema de archivos y seleccionar los archivos y directorios que deben restaurarse. Para crear una TOC, debe definir el atributo `TOCDESTINATION` en el grupo de copias de seguridad para la clase de gestión a la que se vincula esta imagen de copia de seguridad. Tenga en cuenta que, para crear una tabla de contenido, se necesitan un proceso adicional, recursos de red, espacio de agrupación de almacenamiento y, posiblemente, un punto de montaje durante la operación de copia de seguridad.

Para realizar una copia de seguridad de sistemas de archivos NAS utilizando la GUI del cliente web:

1. Pulse **Copia de seguridad** en la ventana principal. Se muestra la ventana Backup.
2. Expanda el árbol de directorios si es preciso.

Nota:

- a. El nodo raíz denominado **Nodos** no se puede seleccionar. Este nodo sólo aparece si hay un complemento NAS presente en la estación de trabajo cliente.
 - b. Los nodos NAS se muestran en el mismo nivel que el del nodo de la estación de trabajo cliente. Sólo aparecen los nodos para los que tiene autorización el administrador.
 - c. Puede expandir los nodos NAS hasta mostrar los espacios de archivos, aunque es la expansión máxima (no muestra nombres de archivo).
3. Pulse las casillas situadas junto a los nodos o los sistemas de archivos de los que desea realizar la copia de seguridad.
 4. Pulse el tipo de copia de seguridad que desee realizar en el menú desplegable de tipo de copia de seguridad. La lista de tipos de copia de seguridad NAS está activa sólo cuando se selecciona por primera vez los objetos de copia de seguridad NAS. **Copia de seguridad completa** realiza una copia de seguridad de todo el sistema de archivos. **Diferencial** realiza una copia de seguridad de los cambios realizados desde la copia de seguridad completa más reciente.
 5. Pulse en **Copia de seguridad**. La ventana Lista de tareas de copia de seguridad NAS muestra el estado del proceso y la barra de progreso de la copia de seguridad. El número que aparece junto a la barra de progreso indica la cantidad de bytes de los que se ha realizado copia de seguridad hasta ese momento. Cuando la copia de seguridad finaliza, la ventana NAS Backup Report muestra los detalles de proceso, incluido el tamaño actual de la copia de seguridad, incluidos los bytes totales de los que se ha realizado la copia de seguridad.

Nota: Si es necesario cerrar la sesión del navegador web, las operaciones NAS continúan después de la desconexión. Puede utilizar el botón **Descartar** situado en la ventana Lista de tareas de la copia de seguridad NAS para salir del proceso de supervisión sin finalizar la operación actual.

6. (Opcional) Para procesar la supervisión de una operación desde la ventana principal de la GUI, abra el menú **Actions** y seleccione **IBM Spectrum Protect Activities**. Durante una copia de seguridad, la barra de estado indica el estado del proceso. No aparece ningún porcentaje de aproximación para las copias de seguridad diferencial.

A continuación, figuran algunas cuestiones que deberá tener en cuenta cuando realice una copia de seguridad de los sistemas de archivo NAS mediante la GUI del cliente web.

- Las copias de seguridad de estaciones de trabajo y remotas (NAS) se excluyen mutuamente en una ventana Copia de seguridad. Tras haber seleccionado un elemento para realizar una copia de seguridad, el siguiente elemento que seleccione deberá ser del mismo tipo (NAS o no NAS).
- No se mostrarán detalles en el marco derecho de la ventana Copia de seguridad correspondientes a los nodos o sistemas de archivos NAS. Para ver información sobre los objetos en el nodo de NAS, resalte el objeto y seleccione **View > File Details** en el menú.
- Para suprimir espacios de archivo NAS, seleccione **Utilities > Delete Filespaces**.
- Las opciones de copia de seguridad no son válidas para los espacios de archivos NAS y se pasan por alto durante una operación de copia de seguridad de NAS.

Conceptos relacionados:

“Descripción general de la configuración del cliente web” en la página 65

“Restaurar sistemas de archivos NAS” en la página 254

Referencia relacionada:

“Toc” en la página 596

Copia de seguridad de sistemas de archivos NAS mediante la línea de mandatos

La copia de seguridad incremental también puede utilizarse para realizar copias de seguridad de instantáneas de sistemas de archivos de NAS.

Tabla 40 enumera los mandatos y opciones que puede utilizar para realizar una copia de seguridad de las imágenes del sistema de archivos NAS desde la línea de mandatos.

Tabla 40. Opciones y mandatos NAS

Opción o mandato	Definición	Página
<code>domain.nas</code>	Utilice la opción <code>domain.nas</code> para especificar los volúmenes que se incluirán en el dominio predeterminado para las copias de seguridad NAS.	“Domain.nas” en la página 400
<code>exclude.fs.nas</code>	Utilice la opción <code>exclude.fs.nas</code> para excluir sistemas de archivos del servidor de archivos NAS del proceso de copia de seguridad de imágenes cuando se utiliza con el mandato backup nas . Esta opción <i>sólo</i> es válida para clientes AIX y Solaris.	“Opciones exclude” en la página 425

Tabla 40. Opciones y mandatos NAS (continuación)

Opción o mandato	Definición	Página
<code>include.fs.nas</code>	<p>Utilice la opción <code>include.fs.nas</code> para vincular una clase de gestión a sistemas de archivos de almacenamiento conectado a red (NAS). También puede especificar si se debe guardar la información de la tabla de contenidos (TOC) durante una copia de seguridad de imagen del sistema de archivos NAS mediante la opción <code>toc</code> con la opción <code>include.fs.nas</code> en el archivo de opciones del cliente.</p> <p>Esta opción <i>sólo</i> es válida para clientes AIX y Solaris.</p>	"Opciones include" en la página 458
<code>query node</code>	Utilice el mandato query node para mostrar todos los nodos en los que un identificador de usuario de administración determinado dispone de autorización para realizar operaciones. El ID de usuario de administración debe tener como mínimo autorización de propietario de cliente sobre el nodo NAS y sobre el nodo de la estación de trabajo cliente que están utilizando.	"Query Node" en la página 735
<code>backup nas</code>	Utilice el mandato backup nas para crear una copia de seguridad de imagen de uno o varios sistemas de archivos pertenecientes a un servidor de archivos NAS (almacenamiento conectado a red).	"Backup NAS" en la página 680
<code>toc</code>	Utilice la opción <code>toc</code> con el mandato backup nas o la opción <code>include.fs.nas</code> para especificar si se debe guardar la información de la Tabla de contenido (TOC) para cada copia de seguridad del sistema de archivos.	"Toc" en la página 596
<code>monitor process</code>	Utilice el mandato monitor process para mostrar los procesos actuales de copia de seguridad y restauración de todos los nodos NAS sobre los que un usuario de administración tiene autorización. El usuario de administración puede seleccionar el proceso que desea supervisar.	"Monitor Process" en la página 714
<code>cancel process</code>	Utilice el mandato cancel process para mostrar los procesos actuales de copia de seguridad y restauración de todos los nodos NAS sobre los que un usuario de administración tiene autorización. Desde la lista, el usuario de administración puede seleccionar el proceso que desea cancelar.	"Cancel Process" en la página 691
<code>query backup</code>	Utilice el mandato query backup con la opción <code>class</code> para mostrar información sobre las imágenes de sistema de archivos de las que se ha realizado una copia de seguridad para un servidor de archivos NAS.	"Query Backup" en la página 720

Tabla 40. Opciones y mandatos NAS (continuación)

Opción o mandato	Definición	Página
query filesystem	Utilice el mandato query filesystem con la opción class para visualizar una lista de espacios de archivos pertenecientes a nodo NAS.	"Query Filespace" en la página 727
delete filesystem	Utilice el mandato delete filesystem con la opción class para que se visualice una lista de los espacios de archivos que pertenecen a un nodo NAS y para seleccionar el que desea suprimir.	"Delete Filespace" en la página 698

- Los nodos NAS representan un nuevo tipo de nodo. El nombre de nodo NAS identifica de forma exclusiva un servidor de archivos NAS y sus datos en IBM Spectrum Protect. Puede añadir un prefijo de nombre de nodo NAS en la especificación de archivo para indicar el servidor de archivos al que se aplica la sentencia de inclusión. Si no especifica un nombre de nodo NAS, el sistema de archivos que especifique se aplica a todos los servidores de archivos NAS.
- Independientemente de la plataforma del cliente, las especificaciones del sistema de archivos NAS utilizan como separador la barra inclinada (/), como en el ejemplo siguiente: /vol/vol0.

Nota: Cuando se inicia una copia de seguridad de NAS utilizando la interfaz de línea de mandatos, la GUI de cliente o el cliente web, el servidor empieza un proceso para iniciar, controlar y supervisar la operación. Es posible que tarde unos cuantos minutos en observar el progreso en la interfaz de línea de mandatos porque el servidor debe realizar el montaje, y otras tareas necesarias, antes de que se produzca el traspaso de datos.

Referencia relacionada:

"Toc" en la página 596

Copia de seguridad de sistemas de archivos de red

Puede configurar el cliente de archivado y copia de seguridad para proteger archivos a los que se accede con el protocolo NFS (Network File System) o con el protocolo CIFS (Common Internet File System).

Si bien es posible conseguir un mejor rendimiento de copia de seguridad gracias a la instalación del cliente de archivado y copia de seguridad donde existe físicamente el sistema de archivos. Pero a veces es necesario acceder a los sistemas de archivos utilizando NFS o CIFS para hacer copias de seguridad o recuperar datos en unidades compartidas remotas. El cliente de archivado y copia de seguridad en sistemas operativos AIX, Linux, Mac OS X y Solaris puede realizar copias de seguridad, archivar, restaurar y recuperar datos de archivos en una unidad compartida montada en NFS o CIFS. Estas operaciones son válidas en todas las versiones del protocolo NFS, incluyendo NFS versión 2, NFS versión 3 y NFS versión 4.

El cliente de copia de seguridad y archivado puede hacer copia de seguridad y restaurar listas de control de acceso cuando está configurado para utilizar NFS versión 4.

Se aplican las siguientes restricciones cuando el cliente de archivado y copia de seguridad protege datos en volúmenes de sistemas de archivos de red:

- Los clientes de archivado y copia de seguridad no pueden completar copias de seguridad de imagen de volúmenes de sistemas de archivos de red.
- Los clientes de copia de seguridad y archivado de AIX no pueden completar copias de seguridad de archivos basadas en instantáneas ni archivar archivos en volúmenes del sistema de archivos de la red.
- Los clientes de archivado y copia de seguridad no pueden completar copias de seguridad basadas en registro diario de volúmenes de sistemas de archivos de red.
- Es posible que los clientes de archivado y copia de seguridad no puedan realizar copias de seguridad de instantáneas de volúmenes de NetApp si se accede a ellas utilizando el protocolo NFS. Si el archivador NetApp proporciona identificadores de dispositivos distintos para sus instantáneas de volúmenes, dichas instantáneas se pueden excluir de las copias de seguridad. El comportamiento depende de la versión del SO, de la versión del archivador NetApp y de su configuración.

Copia de seguridad de sistemas de archivos NFS con la función de espacio de nombres global

Los clientes de NFS V4 pueden realizar una copia de seguridad de los sistemas de archivos NFS se montan mediante la función del espacio de nombres global, llamado *referencia*. La copia de seguridad de todos los sistemas de archivos del espacio de nombres global se realiza en un único espacio de archivos.

Los siguientes ejemplo muestran los sistemas de archivos en el espacio de nombres global del que se realiza la copia de seguridad en un espacio de archivos individual:

```
el servidor
'publications' tiene el sistema de archivos /doc
el servidor 'projects' tiene el sistema de archivos /projects
el servidor 'data' tiene el sistema de archivos /data
```

El servidor 'account1' es el servidor NFS principal que exporta todos estos sistemas de archivos utilizando la referencia y es el servidor que reconocen todos los clientes. El directorio /etc/exports en account1 tiene el siguiente aspecto:

```
/doc -vers=4,refer=/doc@publications
/projects -vers=4,refer=/projects@projects
/data -vers=4,refer=/data@data
```

El sistema de archivos 'payroll' del cliente monta directorios del servidor account1 y puede acceder a los tres sistemas de archivos:

```
payroll:/#mount -o vers=4 account1:/ /mnt
payroll:/#ls /mnt
doc/ projects/ data/
```

El cliente 'payroll' puede realizar una copia de seguridad del archivo /mnt como un único sistema de archivos NFS, el cual realiza una copia de seguridad de todos los demás sistemas de archivos.

Importante: El uso de la opción `virtualmountpoint` puede mejorar el rendimiento del sistema cuando realiza una copia de seguridad de sistemas de archivos NFSV4 mediante el espacio de nombres global. Añada las siguientes entradas de una stanza en `dsm.sys` para realizar una copia de seguridad de cada directorio montado como si se tratara de un espacio de archivos por separado:

```
VIRTUALMOUNTPOINT /doc
VIRTUALMOUNTPOINT /projects
VIRTUALMOUNTPOINT /data
```

Copia de seguridad de los sistemas de archivos con partición de carga de trabajo de AIX

Mediante la utilización del cliente de archivado y copia de seguridad en AIX, puede realizar la copia de seguridad y restaurar los datos del archivo de partición local dentro de la partición global utilizando el espacio de nombres disponible dentro de la partición global.

Cada partición de carga de trabajo (WPAR) tiene su propio dominio de seguridad, por lo que el usuario raíz global tiene garantizado el acceso a todos los datos.

Las WPAR son particiones que se crean por completo en el software de una sola imagen del sistema AIX, con los atributos siguientes:

- Normalmente la WPAR parece un sistema AIX autónomo completo
- No hay asistencia ni configuración de hardware de ningún tipo

Las particiones de carga de trabajo proporcionan un entorno seguro y aislado para aplicaciones de empresa en términos de proceso, señal y espacio de sistemas de archivos. El software que se ejecuta en el contexto de una partición de carga de trabajo tiene su propia instancia de AIX.

El ejemplo siguiente muestra una configuración de WPAR a partir de la WPAR global:

Global partition:

Nombre del sistema: shimla

Nombre del archivo: /home /opt

WPAR #1 configuration:

Nombre: wpar1

Sistema de archivos: /home; name in global WPAR: /wpars/wpar1/home

WPAR #2 configuration:

Nombre: wpar2

Sistema de archivos: /data; name in global WPAR: /wpars/wpar2/data

Hay dos formas de realizar copia de seguridad de los datos de la WPAR. Estos son:

- Realice una copia de seguridad de todos los sistemas de archivos WPAR como espacios de archivo en la partición global. El nombre de espacio de archivos se debe utilizar para identificar el WPAR al cual pertenece. Todos los datos se gestionan en un nodo mediante una planificación. Si utiliza la configuración de ejemplo, aquí encontrará un archivo de ejemplodsm.sys con una stanza del servidor para todos los archivos, tanto global como local:

```
SErvername shimla
TCPPort      1500
TCPSeveraddress servidor.ejemplo.com
nodename     shimla
PasswordAccess generate
Domain       /wpars/wpar1/home /wpars/wpar2/data /home /opt
```

- Realice una copia de seguridad de cada sistema de archivos de la WPAR bajo un nombre de nodo distinto. De esta forma se proporciona la segregación del

nombre de espacios de archivos para cada WPAR. Cada WPAR debe tener un nombre de nodo independiente y un planificador en ejecución en la partición global. Además, se han de configurar los tres servicios del planificador, utilizando para cada uno de ellos un archivo `dsm.opt` distinto correspondiente al nombre de la stanza del servidor. Este método permite que cada operación de copia de seguridad de WPAR se pueda gestionar de forma independiente de las demás. Aquí encontrará un archivo de ejemplo, `dsm.sys`, que utiliza la configuración de ejemplo, con tres secciones de servidor: una para `wpar1`, otra para `wpar2` y otra para la partición global `shimla`:

```
SErvername  shimla_wpar1
TCPPort    1500
TCPSeveraddress  servidor.ejemplo.com
nodename    wpar1
PasswordAccess  generate
Domain      /wpars/wpar1/home

SErvername  shimla_wpar2
TCPPort    1500
TCPSeveraddress  servidor.ejemplo.com
nodename    wpar2
PasswordAccess  generate
Domain      /wpars/wpar2/data

SErvername  shimla
TCPPort    1500
TCPSeveraddress  servidor.ejemplo.com
nodename    shimla
PasswordAccess  generate
Domain      /home /opt
```

Realizar la copia de seguridad de sistemas de archivos Solaris Zettabyte

En los sistemas Solaris SPARC y Solaris x86, puede hacer copia de seguridad de los sistemas de archivos Zettabyte (ZFS -Zettabyte file systems), utilizando instantáneas ZFS. La ventaja de este método frente a una copia de seguridad incremental o selectiva ordinaria es que los archivos y carpetas de una instantánea siempre están en estado de sólo lectura, de forma que no se pueden modificar durante una copia de seguridad.

Acerca de esta tarea

Puede crear una instantánea ZFS con mandatos de Oracle Solaris ZFS. Por ejemplo:

```
zfs snapshot tank/myZFS@mySnapshot
```

En este ejemplo, el nombre de la agrupación ZFS es `tank` y el nombre del sistema de archivos ZFS es `myZFS`. Los archivos que pertenecen a esta instantánea ZFS se encuentran en el subdirectorío denominado `tank/myZFS/.zfs/snapshot/mySnapshot/`.

Procedimiento

Utilice uno de los dos métodos siguientes para hacer copia de seguridad de una instantánea ZFS.

- Realizar una copia de seguridad de cada archivo de la instantánea con la opción `snapshotroot`. Por ejemplo:

```
dsmc inc -snapshotroot=/tank/myZFS/.zfs/snapshot/mySnapshot /tank/myZFS
```

Esta opción permite al administrador sustituir la vía de acceso de instantánea actual por la vía de acceso del sistema de archivos ZFS de forma que se hace la copia de seguridad de los archivos y carpetas bajo el sistema de archivos original.

- Hacer una copia de seguridad de la instantánea completa con mandatos de Oracle Solaris ZFS. Por ejemplo:

```
zfs send tank/myZFS@mySnapshot > /tmpdir/mySnapshotFile
```

La ventaja de realizar una copia de seguridad de la instantánea completa es que se puede realizar una restauración de todo el sistema de archivos en un escenario de recuperación tras desastre.

Conceptos relacionados:

“Restauración de sistemas de archivos ZFS de Solaris” en la página 263

Referencia relacionada:

“Snapshotroot” en la página 571

Copia de seguridad del sistema de archivos cifrado de JFS2 de AIX

Utilice el sistema de archivos cifrados (EFS) de JFS2 de AIX para realizar una copia de seguridad de los archivos en formato de texto legible o sin formato (RAW). Con el formato de texto legible, el archivo se descifra mediante EFS a medida que se va leyendo. Si no se aplica formato, los datos no se descifran. El valor predeterminado es no aplicar formato, pero cuando establece la opción `efsdecrypt` en `yes`, obtiene copias de seguridad de texto legible.

Acerca de esta tarea

Importante: siempre que ejecute una copia de seguridad que incluya archivos cifrados en un EFS, debe asegurarse de que utiliza la especificación correcta de la opción `efsdecrypt`. Si el valor de la opción `efsdecrypt` cambia entre las dos copias de seguridad incrementales, se volverá a realizar una copia de seguridad de todos los archivos cifrados de los sistemas de archivos EFS, incluso si no se han modificado desde la última copia de seguridad. Por ejemplo, si ejecuta una copia de seguridad incremental de archivos cifrados de los que anteriormente había hecho una copia de seguridad como `raw`, debe asegurarse de que `efsdecrypt` se ha especificado como `no`. Si cambia el valor de `efsdecrypt` a `yes`, se volverá a realizar una copia de seguridad de todos los archivos en texto legible incluso si no se han modificado; por lo tanto, asegúrese de utilizar esta opción cuidadosamente.

Si intenta restaurar un archivo cifrado en una estación de trabajo que no admite EFS o en un sistema de archivos en el que EFS no esté activo, se escribirá un mensaje de error y el archivo se pasará por alto.

Estos son algunos de los motivos para realizar una copia de seguridad de EFS utilizando el cifrado de texto legible:

- Este tipo de descifrado es útil si desea utilizar el cifrado del cliente de archivado y copia de seguridad de IBM Spectrum Protect u otro tipo de cifrado de hardware (para los sistemas de cintas, por ejemplo).
- Puede utilizar el texto en formato legible para el archivado de datos a largo plazo, debido a que los datos se almacenan independientemente de la plataforma o del esquema de cifrado.

Estos son algunos de los puntos a tener en cuenta cuando se realiza una copia de seguridad de un archivo en texto legible:

- El usuario que ha invocado el cliente de copia de seguridad y archivado debe poder descifrarlo.
- El usuario puede tener acceso de lectura a un archivo, pero puede no tener acceso a la clave.

En los casos siguientes se emite un mensaje de error:

Procedimiento

1. El usuario está en modalidad de salvaguarda root y EFS reconoce el concepto de dos tipos de usuario root. El administrador root es la modalidad tradicional. Con una modalidad de salvaguarda root no se tendrá acceso a los datos no cifrados, a menos que el usuario sea el propietario o un miembro del grupo de archivos.
2. El usuario trabaja con un ID de usuario no root y está intentando archivar un archivo para el que tiene acceso de lectura, pero el usuario no es propietario o miembro del grupo de archivos. EFS no permitirá que los datos se descifren.

Resultados

Estos son algunos de los puntos que se han de tener en cuenta cuando se realiza una copia de seguridad de los datos sin formato de EFS:

- El cliente de copia de seguridad y archivado no respetará la configuración de cifrado del cliente, que impide el doble cifrado, sino sólo en el cliente. El servidor no sabe que los datos están cifrados, por lo que el cifrado que realice una unidad de cinta, por ejemplo, seguirá teniendo lugar.
- El cliente no respetará la configuración de compresión, por lo que el cliente ni intentará comprimir los datos.
- El cliente no hace copia de seguridad ni restaura de forma automática los archivos del almacén de claves. Cuando restaure archivos cifrados, puede que tenga que restaurar los almacenes de claves para poder descifrar los datos.

Sugerencias:

1. Para proteger el almacén de claves, asegúrese de que el contenido de /var/efs se incluya en las copias de seguridad periódicas.
 2. Para los datos del almacén de claves, utilice la política de almacenamiento de IBM Spectrum Protect con un número de versiones ilimitado.
- La copia de seguridad de los archivos EFS (sistema de archivos cifrado) que se ha realizado en modalidad sin formato (valor predeterminado) no se puede restaurar mediante un cliente de copia de seguridad y archivado anterior a la versión 5.5 o mediante un cliente de otra plataforma UNIX.

Copia de seguridad de los atributos ampliados de AIX


El sistema de archivos de AIX JFS2 (Enhanced Journal File System) proporciona el proceso de copia de seguridad de los atributos ampliados para todos los sistemas de archivos que admiten atributos ampliados con nombre.

Se hace copia de seguridad de estos atributos ampliados de forma automática con cada objeto que dispone de datos de atributos ampliados y no se exige ninguna otra acción.

Cuando el sistema de archivos se define con el formato v2, el único sistema de archivos que admite atributos ampliados con nombre es JFS2. Puede utilizar JFS2 para los atributos ampliados de archivos y directorios, pero no para los atributos ampliados de enlaces simbólicos.

Realización de copia de seguridad de máquinas virtuales VMware

Puede utilizar el cliente de archivado y copia de seguridad para realizar copias de seguridad y restaurar una máquina virtual (VM) a VMware. Las copias de seguridad completas de la máquina virtual operan a nivel de una imagen de disco. Las copias de seguridad incrementales solo copian los datos modificados desde la última copia de seguridad completa.

 Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

La Tabla 41 lista las prestaciones de copia de seguridad y restauración para máquinas virtuales VMware que el cliente de archivado y copia de seguridad puede realizar modificaciones en las plataformas Linux.

Tabla 41. Prestaciones de copia de seguridad y restauración para máquinas virtuales VMware en plataformas Linux

Prestación	Observación
Copia de seguridad de máquina virtual incremental-constante completa:	<p>Una copia de seguridad de máquina virtual completa es necesaria antes de poder crear copias de seguridad incrementales. Si planifica copias de seguridad incrementales, constantes, este tipo de copia de seguridad se selecciona automáticamente para la primera copia de seguridad si una copia de seguridad completa no se hubiera creado todavía. Los datos de copias de seguridad incrementales se combinan con datos de la copia de seguridad completa para crear una imagen sintética de la copia de seguridad completa. Las copias de seguridad incrementales, constantes subsiguientes leen todos los bloques utilizados y los copian en el servidor IBM Spectrum Protect. Cada copia de seguridad completa, incremental, constante, de máquina virtual lee y copia todos los bloques utilizados, tanto si han cambiado los bloques o no, desde la copia de seguridad anterior. Aún puede planificar una copia de seguridad completa de la máquina virtual, aunque una copia de seguridad completa ya no sea necesaria. Por ejemplo, puede ejecutar una copia de seguridad completa de máquina virtual para crear una copia de seguridad a un nodo con otro nombre, con los valores de retención diferentes.</p> <p>No puede utilizar esta modalidad de copia de seguridad para realizar la copia de seguridad de la máquina virtual de VMware si el cliente se configura para cifrar los datos de copia de seguridad.</p>

Tabla 41. Prestaciones de copia de seguridad y restauración para máquinas virtuales VMware en plataformas Linux (continuación)

Prestación	Observación
Copia de seguridad de máquina virtual incremental-constante-incremental:	<p>Requiere que cree una copia de seguridad completa de la máquina virtual una única vez. La copia de seguridad completa de la máquina virtual copia todos los bloques de disco utilizados propiedad de una máquina virtual en el servidor de IBM Spectrum Protect. Después de completarse la copia de seguridad completa inicial, todas las copias de seguridad posteriores de la máquina virtual son copias incrementales, constantes, incrementales. Cada copia de seguridad incremental, contante, incremental copia únicamente los bloques que se han modificado desde la copia de seguridad anterior, independientemente del tipo de la copia de seguridad anterior. El servidor utiliza una tecnología de agrupación que asocia los bloques cambiados a partir de la copia de seguridad más reciente con datos ya almacenados en el servidor de copias de seguridad anteriores. Una copia de seguridad completa nueva se crea, entonces, cada vez que los bloques cambiados se copian en el servidor mediante una copia de seguridad incremental, constante, incremental.</p> <p>La modalidad de copia de seguridad incremental, constante, incremental proporciona las ventajas siguientes:</p> <ul style="list-style-type: none"> • Mejora la eficacia de la realización de copias de seguridad de máquinas virtuales. • Simplifica las operaciones de restauración de datos. • Optimiza las operaciones de restauración de datos. <p>Durante una operación de restauración, puede especificar opciones para la hora de instante específico y la fecha de instante específico para recuperar los datos. Los datos se restauran a partir de la copia de seguridad completa original y todos los bloques cambiados asociadas con los datos.</p> <p>No puede utilizar esta modalidad de copia de seguridad para realizar la copia de seguridad de la máquina virtual de VMware si el cliente se configura para cifrar los datos de copia de seguridad.</p>
Elemento de recuperación para archivos y carpetas a partir de una copia de seguridad completa de la máquina virtual:	Ofrece la posibilidad de recuperar archivos y carpetas a partir de una copia de seguridad completa de una máquina virtual. La recuperación de elementos solo está disponible con el IBM Spectrum Protect Recovery Agent.
Restauración completa de la máquina virtual:	Restaura todos los sistemas de archivos, discos virtuales y la configuración de la máquina virtual.

Conceptos relacionados:

“Copias de seguridad paralelas de máquinas virtuales” en la página 223

Tareas relacionadas:

“Preparación del entorno para copias de seguridad paralelas de máquinas virtuales VMware”

“Creación de copias de seguridad completas de máquinas virtuales VMware” en la página 222

Preparación del entorno para copias de seguridad paralelas de máquinas virtuales VMware

Utilice los siguientes pasos para preparar el entorno VMware para realizar copias de seguridad de máquinas virtuales VMware completas. El servidor de seguridad de vStorage puede ejecutar un cliente de Windows o de Linux.

Antes de empezar



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Procedimiento

1. Para configurar el entorno de almacenamiento para copias de seguridad, complete los pasos siguientes:
 - a. Configure el entorno de almacenamiento para que el servidor de copias de seguridad de vStorage pueda acceder a los volúmenes de almacenamiento que están en el conjunto de servidores ESX.
 - b. Si utiliza almacenamiento conectado a red (NAS) o almacenamiento conectado de forma directa, asegúrese de que el servidor de seguridad vStorage accede a los volúmenes con transporte basado en red.
 - c. Opcional: Para el acceso a datos, haga lo siguiente:
 - Cree zonas de red de área de almacenamiento (SAN) que su servidor de seguridad vStorage pueda utilizar para acceder a las unidades lógicas de almacenamiento (LUN) en las que se encuentran sus almacenes de datos VMware.
 - Configure sus correlaciones de host de subsistema de discos para que todos los servidores ESX y el proxy de copia de seguridad puedan acceder a los mismos volúmenes de disco.
2. Para configurar el servidor de seguridad vStorage, complete los pasos siguientes:
 - a. Configure y exporte la variable de entorno **LD_LIBRARY_PATH** para que apunte al directorio de instalación del cliente. Por ejemplo:
export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
 - b. Añada el directorio de instalación del cliente a la ruta de cada cuenta que utiliza los mandatos del cliente de archivado y copia de seguridad, por ejemplo, **dsmc**, **dsmcad** o **dsmj**.
3. Para modificar IBM Spectrum Protect, complete los pasos siguientes:
 - a. Acceda a la línea de mandatos de administración del cliente de copia de seguridad y archivado.
 - b. Desde el cliente de copia de seguridad y archivado del servidor de seguridad vStorage, escriba el siguiente comando para registrar el nodo:
`register node my_server_name my_password`

Donde *my_server_name* es el nombre completo del sistema del servidor de seguridad vStorage y *my_password* es la contraseña para acceder a él.

Tareas relacionadas:

“Creación de copias de seguridad completas de máquinas virtuales VMware” en la página 222

Referencia relacionada:

“Backup VM” en la página 683

“Query VM” en la página 741

“Restore VM” en la página 764

“Vmchost” en la página 612

“Vmcpw” en la página 613

“Vmcuser” en la página 615

Creación de copias de seguridad completas de máquinas virtuales VMware

Una copia de seguridad completa de una máquina virtual VMware es una copia de la totalidad de la máquina virtual, incluidos los discos virtuales y el archivo de configuración de la máquina virtual. Este tipo de copia de seguridad es parecido a una copia de seguridad de imágenes de imagen. Para crear una copia de seguridad completa, configure el cliente de archivado y copia de seguridad en el servidor de seguridad vStorage. El servidor de seguridad vStorage debe ejecutarse en un cliente Windows o Linux.

Antes de empezar



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Procedimiento

1. Para preparar el entorno, complete los pasos del siguiente tema:
“Preparación del entorno para copias de seguridad paralelas de máquinas virtuales VMware” en la página 220
2. Para configurar el cliente de archivado y copia de seguridad en un servidor de seguridad vStorage, complete los pasos siguientes:
 - a. Desde la página de bienvenida de la GUI del cliente de copia de seguridad y archivado, pulse **Editar > Preferencias del cliente**.
 - b. Seleccione la ficha **Copia de seguridad de máquina virtual**.
 - c. Seleccione **Máquina virtual completa de VMWare**.
 - d. En la lista de **Tipos de copia de seguridad de dominio**, seleccione **Máquina virtual de dominio**.
 - e. En el campo **Host**, especifique un nombre de host para cada servidor ESX o el nombre de host del centro virtual. Si especifica el centro virtual, puede realizar la copia de seguridad de las máquinas virtuales desde cualquier servidor VMware gestionado por dicho centro virtual.
 - f. Escriba la información de contraseña y de ID de usuario para el host que ha especificado en el campo **Host**.
 - g. Opcional: Si desea sobrescribir la clase de gestión predeterminada para las copias de seguridad de la máquina virtual completa, especifique la clase de gestión que desee utilizar.
 - h. En el campo **Ubicación del almacén de datos**, especifique la ruta al directorio donde se almacenarán los archivos.
 - i. Pulse **Aceptar** para guardar los cambios.
3. Para crear una copia de seguridad de las máquinas virtuales, complete los pasos siguientes:
 - a. En la línea de mandatos del servidor de seguridad vStorage, ejecute el siguiente mandato:

```
dsmc backup vm my_vm_name -mode=iffull -vmbackuptype=fullvm
```

Donde *my_vm_name* es el nombre de su máquina virtual.

- b. Compruebe que el mandato se completa sin errores. El siguiente mensaje indicará una terminación correcta:

```
Mandato de copia de seguridad de la máquina virtual completo
Número total de máquinas virtuales que se han copiado con éxito: 1
máquina virtual vmname copiada a nodename NODE
Número total de máquinas virtuales que han fallado: 0
Número total de máquinas virtuales procesadas: 1
```

4. Para verificar si puede restaurar los archivos para la máquina virtual, complete los pasos siguientes:
- En la interfaz de línea de mandatos del servidor de seguridad vStorage, ejecute el mandato siguiente:
`dsmc restore vm my_vm_name`
 - Si se produce algún error en el proceso de restauración, consulte el archivo de registro de errores para obtener más información.

Consejo: El archivo de registro se guarda en `/opt/ibm/Tivoli/TSM/baclient/dsmerror.log`

Conceptos relacionados:

“Copias de seguridad paralelas de máquinas virtuales”

Tareas relacionadas:

“Preparación del entorno para copias de seguridad paralelas de máquinas virtuales VMware” en la página 220

Referencia relacionada:

“Backup VM” en la página 683

“Domain.vmfull” en la página 401

“Query VM” en la página 741

“Restore VM” en la página 764

“Mode” en la página 492

“Vmchost” en la página 612

“Vmcpw” en la página 613

“Vmcuser” en la página 615

“Vmmc” en la página 631

“Vmvstortransport” en la página 648

Copias de seguridad paralelas de máquinas virtuales

Con un proceso de copia de seguridad paralela, puede utilizar un único nodo de transportador de datos para realizar la copia de seguridad de varias máquinas virtuales (VM) al mismo tiempo y así optimizar el rendimiento de las copias de seguridad.



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Para obtener información sobre las operaciones de copia de seguridad paralela, consulte el apartado Realización de copias de seguridad de varias máquinas virtuales en paralelo.

Copia de seguridad y archivado de los datos de Tivoli Storage Manager FastBack

Utilice Tivoli Storage Manager FastBack para realizar copias de seguridad y archivado de las instantáneas más recientes para retención a corto plazo.

Utilice los mandatos **archive fastback** y **backup fastback** para archivar y realizar una copia de seguridad de volúmenes especificados mediante las opciones **fbpolicyname**, **fbclientname** y **fbvolumename** para retención a largo plazo.

Conceptos relacionados:

“Requisitos de instalación de copia de seguridad y archivado de datos de cliente de Tivoli Storage Manager FastBack” en la página 11

“Configuración del cliente para realizar una copia de seguridad y archivado de los datos de Tivoli Storage Manager FastBack” en la página 102

Referencia relacionada:

“Fbclientname” en la página 432

“Fbpolicyname” en la página 434

“Fbvolumename” en la página 438

Visualización del estado del proceso de copia de seguridad

Durante una copia de seguridad, de forma predeterminada, el cliente de copia de seguridad y archivado muestra el estado de cada archivo del que intenta realizar una copia de seguridad.

El cliente informa del tamaño, la ruta, el nombre del archivo, el número total de bytes transferidos y de si el intento de copia de seguridad se ha realizado correctamente. Estos datos también se registran en el archivo `dsmsched.log` para los mandatos planificados.

El cliente web y la GUI de Java del cliente de copia de seguridad/archivado proporcionan una ventana denominada **Lista de tareas** en la que se visualiza información acerca de los archivos durante el proceso. Cuando finaliza una tarea, la ventana **Informe de copia de seguridad** muestra los detalles del proceso. Pulse el botón **Ayuda** en la ventana **Informe de copia de seguridad** para obtener la ayuda contextual.

En la línea de mandatos de copia de seguridad y archivado, el nombre de cada archivo se visualiza después de enviarlo al servidor. En el indicador de progreso se muestra el progreso general.

Tabla 42 enumera algunos mensajes informativos y significados.

Tabla 42. Mensajes informativos de la línea de mandatos del cliente

Mensaje informativo	Significado
Directory-->	Indica el directorio del que se debe hacer una copia de seguridad.
Normal File-->.	Cualquier archivo que no sea un directorio, un vínculo simbólico o un archivo especial.

Tabla 42. Mensajes informativos de la línea de mandatos del cliente (continuación)

Mensaje informativo	Significado
Special File-->	Los archivos especiales definen dispositivos para el sistema o archivos temporales creados por procesos. Existen tres tipos básicos de archivos especiales: FIFO (el primero en entrar es el primero en salir), de bloques y de caracteres. Los archivos FIFO también se denominan conductos. Los pipes los crea un proceso para permitir temporalmente la comunicación con otro proceso. Estos archivos dejan de existir cuando finaliza el primer proceso. Los archivos de bloques y de caracteres definen dispositivos. El cliente sólo procesa archivos especiales de dispositivos y conductos con nombre. Los archivos especiales de socket no se procesan.
Symbolic Link-->	Indica que el cliente realiza una copia de seguridad de un enlace simbólico.
Updating-->	Indica que solamente se envían metadatos del archivo, no el propio archivo.
Expiring-->	Indica que un objeto (archivo o directorio) del servidor que ya no existe en el cliente pasa a estar caducado e inactivo en el servidor.
Total objetos inspeccionados:	Según se indica. Cuando se utiliza la copia de seguridad con registro por diario, el número de objetos inspeccionados podría ser menor que el número de objetos cuya copia de seguridad se ha realizado. Cuando se utiliza la copia de seguridad incremental de diferencias de instantáneas, el número de objetos que se inspeccionan es cero. El número es cero porque el cliente realiza una copia de seguridad incremental de los archivos que NetApp marca como un cambio. El cliente no explora el volumen en busca de archivos que han cambiado.
Total objetos con copia de seguridad:	Según se indica.
Número total de objetos cifrados:	Se trata de un recuento de los objetos que se han cifrado durante el proceso de copia de seguridad o de archivo.
Tipo de cifrado de datos:	Especifica el tipo de algoritmo de cifrado (por ejemplo, AES de 256 bits), si se han cifrado uno o varios objetos durante el proceso de copia de seguridad o de archivo.
Total objetos actualizados:	Son los archivos cuyos atributos como, por ejemplo, el propietario o los permisos del archivo, han cambiado.
Total objetos vueltos a vincular:	Para obtener más información, consulte el apartado “Vincular clases de gestión a archivos” en la página 308.
Total objetos suprimidos:	Es un recuento de los objetos que se suprimen de la estación de trabajo cliente después de haberse archivado correctamente en el servidor. El recuento es cero para todos los mandatos de copia de seguridad.
Total objetos caducados:	Para obtener más información, consulte la sección acerca de las copias de seguridad incrementales completas y parciales.
Total objetos no restaurados:	Los objetos pueden fallar por diversas razones. Consulte el archivo dsmerror.log para obtener más detalles.
Número total de objetos de diferencia de instantánea:	Para copias de seguridad incrementales de diferencia de instantánea, ello representa el número total de objetos a los que se ha realizado una copia de seguridad y el número total de objetos caducados.
Total de objetos con optimización de almacenamiento:	Especifica el número de archivos cuyas duplicaciones se han eliminado.
Número total de bytes inspeccionados:	Especifica el tamaño total de los archivos que se han seleccionado para la operación. Por ejemplo, el número total de bytes inspeccionados para este mandato es el número de bytes que se utilizan en el volumen /Volumes/BUILD: dsmc INCREMENTAL /Volumes/BUILD/* -SU=Yes

Tabla 42. Mensajes informativos de la línea de mandatos del cliente (continuación)

Mensaje informativo	Significado
Bytes totales antes de la optimización de almacenamiento:	Especifica el número de bytes que se enviarán al servidor de IBM Spectrum Protect y si el cliente no elimina datos redundantes. Compare esta cantidad con Total de bytes después de la optimización de almacenamiento. Incluye el tamaño de metadatos y puede ser superior a los bytes inspeccionados.
Total de bytes después de la optimización de almacenamiento	Especifica el número de bytes que se envían al servidor de IBM Spectrum Protect después de la deduplicación de los archivos en el sistema cliente. Incluye el tamaño de metadatos y puede ser superior a los bytes procesados.
Número total de bytes procesados:	Especifica el tamaño total de los archivos que se han procesado para la operación.
Tiempo de transferencia de datos:	El tiempo total para transferir datos a través de la red. Las estadísticas de la transferencia podrían no coincidir con las estadísticas del archivo si ha vuelto a intentarse ejecutar la operación debido a una anomalía en las comunicaciones o a la pérdida de la sesión. Las estadísticas de transferencia muestran el número de bytes que se intentó transferir durante todos los intentos realizados con el mandato.
Velocidad de transferencia de datos en red:	La velocidad media a la que la red transfiere datos entre el cliente y el servidor. La velocidad se calcula dividiendo el número total de bytes transferidos por el tiempo que ha sido preciso para transferir los datos por la red. El tiempo que el cliente necesita para procesar los objetos no se incluye en la velocidad de transferencia de la red. Por lo tanto, la velocidad de red es superior a la velocidad compuesta.
Velocidad de transferencia de datos compuesta:	<p>La velocidad media a la que IBM Spectrum Protect y la red transfieren datos entre el cliente y el servidor. La velocidad se calcula dividiendo el número total de bytes transferidos por el tiempo que transcurre desde el principio hasta el final del proceso. En la velocidad de transferencia compuesta se incluyen el tiempo de proceso de IBM Spectrum Protect y el tiempo de la red. Por lo tanto, la velocidad de transferencia compuesta es inferior a la velocidad de transferencia de red.</p> <p>Nota: A veces, la velocidad de transferencia de datos agregados puede ser más alta que la velocidad de transferencia de datos de red. Esto es debido a que el cliente de copia de seguridad/archivado puede tener varias sesiones simultáneas con el servidor de copia de seguridad. Si establece la opción <code>resourceutilization</code>, el cliente intenta mejorar el rendimiento y el equilibrio de carga utilizando varias sesiones cuando realiza una copia de seguridad de un espacio de archivos u otros juegos de archivos. Si hay varias sesiones abiertas durante la operación de copia de seguridad, el tiempo de transferencia de datos representa la suma de los tiempos de todas las sesiones. En este caso, el tiempo de transferencia de datos compuesta se visualizará incorrectamente con un valor mayor. Sin embargo, si se ejecuta una sola sesión, la velocidad de transferencia de datos compuesta siempre se visualizará con un valor menor que la velocidad de transferencia de datos en red.</p>
Comprimido:	Especifica el porcentaje de datos enviados por la red dividido por el tamaño original del archivo en el disco. Por ejemplo, si los bytes de datos enviados por la red son 10 K y el archivo tiene 100 K, el valor de compresión será: $((1 - (10240/102400)) \times 100) = 90\%$.
Total number of objects grew:	El número total de archivos que han aumentado como resultado de la compresión.

Tabla 42. Mensajes informativos de la línea de mandatos del cliente (continuación)

Mensaje informativo	Significado
Reducción de optimización de almacenamiento:	Especifica el tamaño de las extensiones duplicadas que se han encontrado, dividido por el tamaño inicial de los datos o del archivo. Por ejemplo, si el tamaño de objeto inicial es de 100 MB, tras la optimización de almacenamiento, será de 25 MB. La reducción sería: $(1 - 25/100) * 100 = 75\%$.
Proporción de reducción de datos en total:	Añade efectos de compresión e incrementales. Por ejemplo, si los bytes inspeccionados son 100 MB y los bytes enviados son 10 MB, la reducción sería: $(1 - 10/100) * 100 = 90\%$
Tiempo del proceso:	El tiempo de proceso activo que requiere completar un mandato. Esto se calcula restando la hora de inicio del proceso de un mandato a la hora final de la finalización del proceso del mandato.
Total bytes transferidos:	Según se indica.
Número total de bytes transferidos fuera de la LAN:	Número total de bytes de datos transferidos durante una operación fuera de la LAN. Si la opción <code>enablelanfree</code> se establece en <i>no</i> , esta línea no aparecerá.
Número total de bytes inspeccionados:	El tamaño total de los archivos seleccionados para la operación.
Número total de reintentos:	El número total de reintentos durante una operación de copia de seguridad. Según los valores del atributo de serialización y la opción changingretries , es posible que no se haga copia de seguridad de un archivo abierto por otro proceso durante el primer intento de copia de seguridad. Es posible que el cliente de copia de seguridad intente hacer copia de seguridad de un archivo varias veces durante una operación de copia de seguridad. Este mensaje indica el número total de reintentos para todos los archivos incluidos en la operación de copia de seguridad.

Copia de seguridad(UNIX y Linux): Consideraciones adicionales

Hay algunas situaciones especiales que debe tener en cuenta antes de realizar una copia de seguridad de los datos.

Archivos almacenados

Al realizar copias de seguridad y copias archivadas de archivos, IBM Spectrum Protect almacena estas copias en un espacio de archivos del almacenamiento que tiene el mismo nombre que el sistema de archivos o el punto de montaje virtual en el que se crearon los archivos.

Por ejemplo, si tiene un sistema de archivos denominado `/home` y ha realizado una copia de seguridad de un archivo llamado `doc1` en el directorio `/home/monnett`, IBM Spectrum Protect almacena el archivo en un espacio de archivos llamado `/home`. Si posteriormente define `/home/monnett` como un punto de montaje virtual, cualquier archivo del que realice una copia de seguridad del directorio `/home/monnett`, como por ejemplo `doc2`, se almacena en un espacio de archivos denominado `/home/monnett`. Si especifica este mandato:

```
dsmc query backup "/home/monnett/*"
```

IBM Spectrum Protect busca archivos en el espacio de archivos `/home/monnett`. Siempre busca un archivo en el espacio de archivos con el nombre más largo que coincida con la especificación de archivo que incluya en el mandato. Encuentra el archivo denominado `doc2` cuya copia de seguridad es posterior a la definición del punto de montaje virtual. Sin embargo, no encuentra el archivo denominado `doc1`

porque la copia de seguridad de dicho archivo se realizó antes de definir el punto de montaje virtual y la copia de seguridad se almacenó en el espacio de archivos /home.

Para listar o restaurar el archivo doc1 mediante un mandato, debe especificar explícitamente el nombre de espacio de archivos delimitándolo entre llaves. Por ejemplo:

```
dsmc query backup "{/home}/monnett/*"  
dsmc restore {/home}/monnett/doc1
```

Si elimina posteriormente el punto de montaje virtual /home/monnett y realiza copias de seguridad de más archivos del directorio /home/monnett, las copias de seguridad se volverán a almacenar en el espacio de archivos /home. Por ejemplo, si realiza una copia de seguridad de un archivo denominado doc3 del directorio /home/monnett, se almacena en el espacio de archivos /home. No se almacena en el espacio de archivos /home/monnett.

Sin embargo, puesto que el espacio de archivos /home/monnett ya existe, cuando intente consultar o restaurar el archivo doc3, IBM Spectrum Protect buscará este archivo en el espacio de archivos /home/monnett a menos que especifique el nombre del espacio de archivos correcto. Por ejemplo:

```
dsmc query backup "{/home}/monnett/*"  
dsmc restore {/home}/monnett/doc2
```

Nota: Debe especificar explícitamente el nombre del espacio de archivos sólo cuando puede haber más de una resolución de la especificación del archivo.

Por ejemplo, si existen los espacios de archivos siguientes en el almacenamiento:

```
/home  
/home/monnett  
/home/monnett/project1  
/home/monnett/project1/planning
```

y, a continuación, especifique:

```
dsmc query backup "/home/monnett/project1/planning/*"
```

IBM Spectrum Protect busca archivos sólo en el espacio de archivos /home/monnett/project1/planning, aunque uno o varios espacios de archivos contengan una vía de acceso con el mismo nombre. Sin embargo, si especifica una de estas opciones:

```
dsmc query backup "{/home}/monnett/project1/planning/*"  
dsmc query backup "{/home/monnett}/project1/planning/*"  
dsmc query backup "{/home/monnett/project1}/planning/*"
```

IBM Spectrum Protect busca archivos sólo en el espacio de archivos /home, el espacio de archivos /home/monnett o el espacio de archivos /home/monnett/project1, dependiendo del formato que utilice.

Sistemas de archivos especiales

Los sistemas de archivos especiales contienen información dinámica generada por el sistema operativo; no contienen datos ni archivos. El cliente de copia de seguridad y archivado pasa por alto los sistemas de archivos especiales y su contenido.

Los sistemas de archivos especiales son los siguientes:

- el sistema de archivos /proc en la mayoría de las plataformas UNIX

- el sistema de archivos /dev/fd en Solaris
- el sistema de archivos /dev/pts en Linux

NFS o puntos de montaje virtuales

Cuando se realiza una copia de seguridad de los archivos y se archivan desde un sistema de archivos o punto de montaje virtual, el cliente no sigue los puntos de montaje NFS o virtuales anidados (si se ha definido alguno en un sistema de archivos). No se realizará copia de seguridad ni se archivarán los puntos de montaje NFS o virtuales anidados.

Clases de gestión

IBM Spectrum Protect utiliza clases de gestión para determinar cómo se deben gestionar las copias de seguridad en el servidor.

Cada vez que efectúe una copia de seguridad de un archivo, se asignará al archivo una clase de gestión. La clase de gestión utilizada es una clase de gestión predeterminada seleccionada o la asignada al archivo con la opción `include` en la lista de opciones de inclusión/exclusión. La clase de gestión seleccionada debe contener un grupo de copia de seguridad para que se realice la copia de seguridad del archivo.

Seleccione **Programas de utilidad** → **Ver información de políticas** en la GUI Java o en el cliente web para ver las políticas de copia de seguridad definidas por el servidor de IBM Spectrum Protect para su nodo cliente.

Conceptos relacionados:

Capítulo 9, “Políticas de gestión de almacenamiento”, en la página 299

Copias de seguridad de enlaces simbólicos

El cliente de copia de seguridad y archivado realiza una copia de seguridad de los enlaces simbólicos de manera diferente a los archivos y directorios normales.

La manera en la que el cliente realiza una copia de seguridad de los enlaces simbólicos depende de la configuración de las opciones, de la posibilidad de acceder o no al directorio de destino y de la forma de especificación de los objetos.

Un *enlace simbólico UNIX* es un archivo que contiene un puntero a otro archivo o directorio. El objeto al que señala el enlace simbólico se denomina objeto de destino.

Se puede realizar una copia de seguridad de un enlace simbólico como información de la vía de acceso a un directorio de destino o como un directorio. Si se realiza una copia de seguridad del enlace simbólico como un directorio, también se podrá hacer una copia de seguridad de los archivos y carpetas de ese directorio de destino.

Nota: el proceso de los vínculos simbólicos que se describe en este apartado no es aplicable a Mac OS X. La copia de seguridad de los vínculos simbólicos se hace siempre como archivos y nunca se siguen.

Referencia relacionada:

“Archsymlinkasfile” en la página 348

“Followsymbolic” en la página 444

“Virtualmountpoint” en la página 606

Ejemplos: copia de seguridad incremental o selectiva de enlaces simbólicos

El modo en el que el cliente realiza copias de seguridad de un enlace simbólico depende de si su destino es un archivo o un directorio, y de cómo se especifique en el mandato de copia de seguridad incremental o selectiva.

Si un enlace simbólico dirige a un archivo, el cliente solamente realiza una copia de seguridad de la información de la vía de acceso. El cliente no realiza copias de seguridad del archivo de destino del enlace simbólico.

Si un enlace simbólico dirige a un directorio, la copia de seguridad depende de cómo se especifique el directorio en el mandato.

Si se especifica con una barra inclinada final en un mandato de copia de seguridad selectiva o incremental, el cliente guarda el enlace simbólico como directorio y realiza una copia de seguridad del contenido del directorio de destino.

Si el enlace simbólico se especifica sin barra inclinada final, o si no se indica ningún enlace simbólico explícitamente en una especificación de archivo de la copia de seguridad, el cliente solamente realiza una copia de seguridad de la información de la vía de acceso del directorio de destino. No se realiza ninguna copia de seguridad del contenido del directorio de destino.

En el siguiente ejemplo, suponga que `symdir` es un enlace simbólico al directorio de destino `/fs1/guest/`. `/fs1/guest/` contiene estos objetos:

```
/fs1/guest/file (un archivo)
/fs1/guest/dir1 (un directorio)
/fs1/guest/dir1/file1 (un archivo)
```

Ejemplo 1

```
dsmc incr /home/gillis/symdir/
```

En este ejemplo, el cliente realiza una copia de seguridad del enlace simbólico como directorio y del contenido del directorio de destino `/fs1/guest/`. Si especifica la opción `subdir=yes`, el cliente realiza una copia de seguridad de los subdirectorios de `/fs1/guest/`.

Ejemplo 2

```
dsmc incr /home/gillis/symdir/dir1
```

Ejemplo 3

```
dsmc incr /home/gillis/symdir/dir1/
```

En los ejemplos 2 y 3, el cliente realiza una copia de seguridad del enlace simbólico como directorio y del subdirectorio `/dir1/` del directorio de destino. La barra inclinada final solamente es relevante en el enlace simbólico y es irrelevante en subdirectorios del enlace simbólico. Si especifica la opción `subdir=yes`, el cliente realiza una copia de seguridad de los subdirectorios de `/fs1/guest/dir1/`. Las copias de seguridad almacenadas en el servidor de IBM Spectrum Protect tienen una ruta similar a `/home/gillis/symdir/dir1/file1`.

Ejemplo 4

```
dsmc incr /home/gillis/symdir
```

En el ejemplo 4, dado que no hay barra inclinada final tras el enlace simbólico, el cliente solamente realiza una copia de seguridad de la vía de acceso del directorio

de destino. El cliente no realiza copias de seguridad del enlace simbólico como directorio ni de los archivos o carpetas del directorio de destino.

Ejemplo 5

```
dsmc incr /home/gillis/
```

En el ejemplo 5, dado que no se ha indicado explícitamente el enlace simbólico en la especificación de archivo de la copia de seguridad, el cliente solamente realiza una copia de seguridad de la vía de acceso del directorio de destino. El cliente no realiza copias de seguridad del enlace simbólico como directorio ni de los archivos o carpetas del directorio de destino.

Restricción: Si realiza una copia de seguridad de un enlace simbólico como directorio y después lleva a cabo una copia de seguridad incremental que no lo copie también como directorio, el enlace simbólico caduca como directorio, así como los archivos y directorios dentro de él.

Por ejemplo, suponga que primero realiza una copia de seguridad del enlace simbólico `symdir` como directorio, y realiza una copia de seguridad del contenido del directorio de destino. El mandato del ejemplo 1 anterior hace esto. El cliente crea copias de seguridad con una vía de acceso de alto nivel `/home/gillis/symdir/`. En el siguiente ejemplo, el cliente crea copias de seguridad con estas vías de accesos:

```
/home/gillis/symdir/  
/home/gillis/symdir/file  
/home/gillis/symdir/dir1  
/home/gillis/symdir/dir1/file1
```

Se hace una copia de seguridad del contenido de `/home/gillis` mediante el siguiente mandato:

```
dsmc inc /home/gillis/ -subdir=yes
```

Este mandato procesa `symdir` como un enlace simbólico y no procesa ninguno de los objetos a los que apunta el enlace simbólico. Por lo tanto, el cliente hará que caduquen las copias de seguridad del directorio `/home/gillis/symdir/` que se crearon en la copia de seguridad del ejemplo 1.

Copia de seguridad incremental de un dominio solamente

El cliente hace copias de seguridad de un enlace simbólico durante una copia de seguridad incremental del dominio, si el enlace simbólico está definido como punto de montaje virtual y la opción `followsymbolic` está configurada como `yes`.

El cliente hará copias de seguridad de un enlace simbólico y de un directorio de destino cuando todo lo que viene a continuación sea verdad:

- El cliente realiza una copia de seguridad incremental del dominio.
- El enlace simbólico se define como punto de montaje virtual por medio de la opción `virtualmountpoint`.
- `followsymbolic=yes`

Las opciones `virtualmountpoint` y `followsymbolic` añaden el enlace simbólico al dominio. El mandato **Incremental** hace una copia de seguridad del dominio, que incluye el destino del enlace simbólico.

Referencia relacionada:

“`Followsymbolic`” en la página 444

“Virtualmountpoint” en la página 606

Enlaces fijos

Cuando hace copia de seguridad de archivos que tienen un enlace fijo, el cliente de copia de seguridad y archivado hará una copia de seguridad de cada instancia del archivo enlazado.

Por ejemplo, si hace una copia de seguridad de dos archivos que tienen un enlace fijo, el cliente hace dos copias de seguridad de los datos de los archivos.

Cuando se restauren archivos con vínculo fijo, el cliente intentará restablecer los vínculos. Por ejemplo, si se había establecido un enlace fijo entre dos archivos y solo se encuentra uno en su estación de trabajo, al restaurar ambos archivos habrá un enlace fijo entre los dos. También se aplicarán enlaces fijos a los archivos aunque ninguno de los archivos exista en el momento de la restauración si ambos archivos se restauran conjuntamente mediante la ejecución de un único mandato. La única excepción de este procedimiento se da cuando se realizan copias de seguridad dos archivos entre los que hay un vínculo fijo y se interrumpe la conexión entre éstos en la estación de trabajo. Si restaura los dos archivos desde el servidor con el proceso de restauración estándar (o clásico), el cliente respeta el sistema de archivos actual y no vuelve a establecer el enlace fijo.

Importante: Si no realiza la copia de seguridad y la restauración al mismo tiempo de todos los archivos que tienen enlaces fijos, se producirán problemas. Para garantizar que los archivos unidos mediante vínculos fijos permanecen sincronizados, realice una copia de seguridad de todos los archivos que están conectados entre sí mediante vínculos fijos al mismo tiempo y, a continuación, restaure estos mismos archivos juntos.

Archivos dispersos

Los archivos esparcidos no tienen espacio de disco asignado para cada bloque en todo el espacio de direcciones, lo que provoca la aparición de espacios vacíos en los archivos. Los espacios vacíos se detectan por su contenido, que siempre está formado por ceros, y estos ceros ocupan espacio.

El valor predeterminado consiste en restaurar el archivo esparcido sin los espacios vacíos, con lo que se obtiene más espacio de disco libre. El cliente de copia de seguridad y archivado detecta los archivos esparcidos durante una operación de copia de seguridad y los marca como esparcidos en el servidor de IBM Spectrum Protect.

Nota: Los archivos dispersos no se aplican a Mac OS X.

El cliente de copia de seguridad y archivado hace copia de seguridad de un archivo esparcido si la compresión del cliente está desactivada.

Referencia relacionada:

“Compression” en la página 370

“Makesparsefile” en la página 484

Montajes de hard y soft de NFS

Cuando el cliente de copia de seguridad y archivado se conecta a un sistema de archivos NFS, puede utilizar un montaje por hardware o un montaje por software.

El cliente utiliza el valor de la opción **nfstimeout** para determinar el tiempo de espera de una llamada de un sistema NFS para responder antes de que exceda el tiempo de espera; este valor se aplica a montajes por hardware y software. El valor predeterminado es 0 segundos. Esto significa que el cliente utiliza el comportamiento predeterminado de llamadas de sistema NFS.

Tenga en cuenta las consecuencias de los montajes por hardware y software si el montaje queda obsoleto (por ejemplo, si el servidor del sistema de archivos no está disponible).

Montaje por hardware

Si el sistema de archivos NFS está montado por hardware, los daemons NFS intentan repetidamente establecer contacto con el servidor. Los reintentos de los daemons de NFS no excederán el tiempo de espera, afectan al rendimiento del sistema y no pueden interrumpirse. Sin embargo, el control vuelve al cliente cuando se alcanza el valor **nfstimeout**.

Montaje por software

Si el sistema de archivos NFS está montado por software, NFS intenta repetidamente establecer contacto con el servidor hasta que:

- Se establezca una conexión
- Se alcance el umbral de reintentos de NFS
- Se alcance el valor **nfstimeout**

Cuando se produce uno de estos eventos, el control vuelve al programa que ha efectuado la llamada.

Nota: En sistemas de UNIX y Linux, la opción **nfstimeout** puede fallar si el montaje de NFS es duro. Si se cuelga el proceso, desactive la opción **nfstimeout** y monte el sistema de archivos NFS montado por software de este modo:

```
mount -o soft,timeo=5,retry=5 machine:/filesystem /mountpoint
```

Los parámetros son los siguientes:

soft Genera un montaje por software del sistema de archivos NFS. Si se produce un error, la función **stat()** devuelve un error. Si ha utilizado la opción **hard** **stat()**, nunca vuelve hasta que el sistema de archivos está disponible.

timeo=n

Establece el tiempo de espera para un error de montaje de tipo **soft** en *n* décimas de segundo.

retry=n

Establece el número de veces que se puede intentar el montaje, donde *n* es un entero; la opción predeterminada es 10000.

Sistemas de archivos suprimidos

Cuando se ha suprimido un sistema de archivos o una unidad, o dejan de hacerse copias de seguridad de los mismos mediante el cliente de copia de seguridad y archivado, las versiones de copia de seguridad existentes de cada archivo se gestionan según los siguientes atributos de política: Número de días que se deben mantener inactivas las versiones de copia de seguridad y número de días que se debe mantener la última versión de copia de seguridad (si no hay ninguna versión activa)

Si no lleva a cabo ninguna otra acción, las versiones de copia de seguridad activas se conservan indefinidamente. Si no necesita guardar de manera indefinida las versiones activas, utilice el mandato **expire** para desactivar las versiones activas.

Si no necesita guardar ninguna de las versiones de copia de seguridad, utilice el mandato **delete backup** para suprimir todas las versiones de copia de seguridad del espacio de archivos. El administrador del servidor de IBM Spectrum Protect deberá otorgarle autorización para suprimir copias de seguridad antes de utilizar estos mandatos. Utilice el mandato **query session** para determinar si tiene autorización de supresión de copia de seguridad. Como alternativa, solicite al administrador del servidor IBM Spectrum Protect que suprima por usted el espacio de archivos.

Conceptos relacionados:

Capítulo 9, “Políticas de gestión de almacenamiento”, en la página 299

Archivos abiertos

El cliente de copia de seguridad y archivado busca archivos que se han modificado entre el inicio y la finalización de la copia de seguridad del archivo.

Puede que algunos archivos del sistema estén utilizándose o estén abiertos mientras intenta realizar la copia de seguridad de éstos. Puesto que un archivo abierto puede cambiar, puede que una acción de copia de seguridad no refleje el contenido correcto del archivo en un momento determinado.

Plantéese si el archivo es importante y si puede volver a crearlo. Si no es importante, puede que no desee realizar una copia de seguridad de él. Si el archivo es importante, un usuario root en la estación de trabajo puede garantizar que el archivo esté cerrado antes de realizar la copia de seguridad.

Si las copias de seguridad se ejecutan según una planificación, un usuario root puede utilizar la opción `preschedulecmd` para especificar un mandato que cierre el archivo. Por ejemplo, si el archivo abierto es una base de datos, utilice el mandato **quiesce** de la base de datos para cerrarla. Un usuario root puede utilizar la opción `postschedulecmd` para reiniciar la aplicación que utiliza el archivo una vez finalizada la copia de seguridad. Si no sigue ninguna planificación para la copia de seguridad, asegúrese de cerrar la aplicación que utiliza el archivo antes de iniciar la copia de seguridad.

El cliente puede realizar una copia de seguridad de un archivo aunque esté abierto y se modifique durante la operación de copia de seguridad. Esto es útil sólo si el archivo está utilizable incluso aunque cambie durante la operación de copia de seguridad. Para efectuar copias de seguridad de estos archivos, asigne a los archivos una clase de gestión con serialización *dinámica* o *dinámica compartida*.

Conceptos relacionados:

“Visualizar información sobre clases de gestión y grupos de copia” en la página 301

“Seleccionar una clase de gestión para los archivos” en la página 305

Caracteres comodín

Puede utilizar los caracteres comodín del sistema operativo en las especificaciones de archivo con el cliente de copia de seguridad y archivado. Estos caracteres permiten seleccionar grupos de archivos que tienen nombres similares.

En un mandato, los caracteres comodín sólo pueden utilizarse en el nombre o la extensión del archivo. No pueden utilizarse para especificar archivos, sistemas de archivos ni directorios de destino. Cuando utilice caracteres comodín en la modalidad de no bucles, como en `dsmd sel "/home/ledger.*"`, incluya entre comillas el parámetro que contiene el asterisco para asegurarse de que el sistema no interprete el carácter comodín y genera resultados inesperados. En la tabla siguiente se incluye información sobre el carácter comodín.

Importante: Utilice un asterisco (*) en lugar de una interrogación (?) como carácter comodín cuando intente buscar la coincidencia de un patrón en una página de códigos de varios bytes con el fin de evitar que se produzcan resultados no esperados.

En esta tabla se muestran algunos patrones comodín y cómo especificarlos.

<i>* (Asterisco)</i>	Ninguno o varios caracteres que coinciden con todos los archivos:
*.cpp	Con la extensión cpp
hm*.*	Empieza por hm, independientemente de la extensión, pero debe tener el carácter '.'
hm*	Empieza por hm, independientemente de si existe una extensión
h.*	Con una h en algún lugar del nombre de archivo, independientemente de la extensión, pero debe tener un .
<i>? (Signo de interrogación)</i>	Un carácter que coincide con todos los archivos con:
?.*	La extensión cpp con un único carácter en el nombre del archivo
hm?.*	Nombres de tres caracteres que empiezan por hm y que tienen la extensión cpp
<i>* ? (Asterisco y signo de interrogación)</i>	Combinaciones de asterisco y signos de interrogación que coinciden con:
??hm.*	Todos los nombres de archivo de cuatro caracteres que acaban en hm., independientemente de su extensión

En un nombre de vía de acceso de una especificación de archivo, no se puede especificar un directorio cuyo nombre contenga un asterisco (*) o un signo de interrogación (?). El cliente únicamente reconoce estos caracteres como caracteres comodín.

Capítulo 5. Restauración de los datos

Utilice IBM Spectrum Protect para restaurar versiones de copia de seguridad de archivos específicos, de un grupo de archivos con nombres similares o de directorios completos.

Estas versiones de copia de seguridad se pueden restaurar en caso de que los archivos originales se pierdan o resulten dañados. Seleccione los archivos que desea restaurar utilizando una especificación de archivo (vía de acceso, nombre y extensión de archivo), una lista de directorios o una vía de acceso de subdirectorios en un directorio y sus subdirectorios.

Todos los procedimientos de copia de seguridad y restauración de cliente que aparecen en este tema también se aplican al cliente web. Sin embargo, el cliente web no dispone de un Editor de preferencias para configurar las opciones del cliente.

Atención: No restaure archivos del sistema operativo como directorios base del sistema, módulos de kernel o parches a su ubicación original mientras el sistema de archivos esté en ejecución. El sistema operativo se podría colgar o bloquear.

Estas son las principales tareas de restauración:

- “Restauración de una imagen”
- “Restauración de datos mediante la GUI” en la página 258
- “Ejemplos de restauración desde la línea de mandatos” en la página 258
- “Restauración de datos desde un conjunto de copias de seguridad” en la página 240
- “Restauración de datos a un instante específico” en la página 251
- “Restaurar sistemas de archivos NAS” en la página 254
- “Cómo autorizar a otro usuario para que restaure o recupere archivos” en la página 264
- “Restauración o recuperación de archivos de otro nodo cliente” en la página 265
- “Restaurar o recuperar archivos en otra estación de trabajo” en la página 266
- “Restauración de un disco en caso de pérdida del mismo” en la página 266
- “Supresión de espacios de archivos” en la página 267

Consulte *IBM Spectrum Protect para Space Management para UNIX y Linux* para obtener detalles sobre la restauración de archivos migrados y sobre la opción `restoremigstate`.

Tareas relacionadas:

“Inicio de una sesión de cliente web” en la página 147

Restauración de una imagen

Existen algunos puntos que debe tener en cuenta antes de comenzar a restaurar imágenes en el sistema.

Para poder restaurar una imagen (desactivada o activada), debe tener autorización de administrador del sistema.

A continuación, se muestra una lista de los puntos que debe tener en cuenta antes de restaurar una imagen:

- Al restaurar la imagen de un volumen, los datos se restaurarán al mismo estado en el que estaban cuando se realizó la última copia de seguridad de imagen. Asegúrese por completo de que necesita restaurar una imagen, puesto que sustituirá todo el sistema de archivos o volumen RAW por la imagen del servidor.
- Asegúrese de que el volumen al que está restaurando la imagen tiene como mínimo el mismo tamaño que la imagen que se está restaurando.
- En sistemas Linux, algunos sistemas de archivos como ext2, ext3, ext4, btrfs y xfs utilizan un UUID (universally unique identifier) para que se identifiquen con el sistema operativo. Si crea una copia de seguridad de imagen de tal volumen y la restaura en una ubicación distinta, es posible que tenga dos volúmenes con el mismo UUID. Si utiliza UUID para definir los sistemas de archivos en `/etc/fstab`, tenga en cuenta que es posible que el cliente de copia de seguridad y archivado no pueda montar correctamente el sistema de archivos restaurado debido al conflicto de UUID. Para evitar esta situación, restaure la imagen a su ubicación original. Si debe restaurarla a una ubicación distinta, cambie el UUID de cualquier volumen original o restaurado antes de montar el sistema de archivos restaurado. Consulte la documentación de Linux para obtener instrucciones sobre cómo cambiar un UUID. También es posible que deba editar manualmente el archivo `/etc/fstab` para que se pueda montar el volumen original, el volumen restaurado, o ambos volúmenes.
- El sistema de archivos o volumen que está restaurando tiene que ser del mismo tipo que el original.
- Asegúrese de que el volumen de destino de la restauración no está utilizándose. El cliente bloquea el volumen antes de iniciar la restauración. El cliente desbloquea el volumen cuando finaliza la restauración. Si el volumen se está utilizando cuando el cliente intenta bloquear el sistema de archivos, la restauración da un error.
- No es posible restaurar una imagen en la ubicación de instalación del programa de cliente de IBM Spectrum Protect.
- Si ejecuta copias de seguridad incrementales de forma progresiva y copias de seguridad de imagen del sistema de archivos, puede realizar una restauración de imagen incremental del sistema de archivos. El proceso restaura los archivos individuales una vez restaurada la imagen completa. Los archivos individuales restaurados son los archivos de los que se ha hecho una copia de seguridad después de la imagen original. Opcionalmente, si los archivos se hubieran suprimido después de la copia de seguridad original, la restauración incremental puede suprimir estos archivos de la imagen base.

La supresión de archivos se realizará correctamente si el grupo de copia de seguridad del servidor de IBM Spectrum Protect cuenta con suficientes versiones para los archivos existentes y suprimidos. Las copias de seguridad y restauraciones incrementales solamente se pueden realizar en sistemas de archivos montados y no en volúmenes lógicos RAW.

- Si por algún motivo se daña una imagen restaurada, puede utilizar la herramienta `fcsk` para intentar repararla.
Puede utilizar la opción `verifyimage` con el mandato **restore image** para especificar que desea activar la detección de sectores defectuosos en el volumen de destino. Si se detectan sectores defectuosos en el volumen de destino, el cliente emite un mensaje de aviso en la consola y en el registro de errores.
Si existen sectores defectuosos en el volumen de destino, puede utilizar la opción `imagnetofile` con el mandato **restore image** para especificar que desea

restaurar la imagen de origen en un archivo. Más tarde, puede utilizar el programa de utilidad de copia de datos que elija para transferir la imagen del archivo a un volumen de disco.

Referencia relacionada:

“Imagetofile” en la página 455

“Verifyimage” en la página 605

Restauración de una imagen mediante la GUI

Puede utilizar la GUI para restaurar una imagen del sistema de archivos o un volumen lógico RAW.

Acerca de esta tarea

Realice estos pasos para restaurar una imagen del sistema de archivos o volumen lógico RAW:

Procedimiento

1. Pulse **Restaurar** en la ventana principal. Aparecerá la ventana Restaurar.
2. Expanda el árbol de directorios.
3. Localice el objeto del árbol que tiene el nombre **Imagen** y amplíelo. Pulse en las casillas que hay junto a la imagen que desea restaurar. Si desea obtener información detallada sobre el objeto, resáltelo y seleccione **Ver → Detalles de archivo** en la ventana principal, o bien pulse el botón **Ver detalles de archivo**.
4. **Opcional:** para realizar una restauración de imagen incremental, pulse el botón **Opciones** para abrir la ventana Opciones de restauración y seleccione la opción **Imagen más directorios y archivos incrementales**. Si desea suprimir archivos inactivos del sistema de archivos local, seleccione la casilla **Suprimir archivos inactivos de sistema local**. Pulse el botón **Aceptar**.
5. Pulse **Restaurar**. Aparecerá la ventana Destino de restauración. La imagen se puede restaurar en el volumen con el punto de montaje desde el que se ha hecho originalmente la copia de seguridad. Alternativamente, se puede seleccionar un volumen diferente como ubicación de la restauración.
6. Pulse el botón **Restaurar** para iniciar la restauración. Aparecerá la ventana **Lista de tareas**, en la que se muestra el progreso de la restauración. Aparecerá la ventana Informe de restauración.

Resultados

A continuación, figuran algunas cuestiones que deberá tener en cuenta cuando realice una operación de restauración de imagen mediante la GUI:

- Puede seleccionar **Ver → Detalles de archivo** en la ventana principal o pulsar el botón **Ver detalles de archivo** para visualizar las imágenes del sistema de archivos de las que el cliente ha realizado una copia de seguridad:
 - Tamaño de imagen - Es el tamaño del volumen del que se ha realizado la copia de seguridad.
 - Tamaño almacenado - Es el tamaño de la imagen real que se ha almacenado en el servidor. La imagen almacenada en el servidor de IBM Spectrum Protect tiene un tamaño que equivale a la capacidad del volumen.
 - Tipo de sistema de archivos
 - Fecha y hora de la copia de seguridad
 - Clase de gestión asignada a la copia de seguridad de imagen

- Si la copia de seguridad de imágenes es una copia activa o inactiva
- Si desea modificar opciones de restauración específicas, pulse el botón **Opciones**. Las opciones que modifique *sólo* estarán en vigor durante la sesión actual.
- En la ventana Opciones de restauración, puede elegir restaurar sólo la imagen o la imagen y los archivos de los directorios de datos de copia incremental. Si elige **Sólo la imagen**, solo se restaurará la imagen de la última copia de seguridad. Éste es el valor predeterminado.

Si ha ejecutado una copia de seguridad de imagen incremental por fecha en un volumen o copias de seguridad de imagen en un volumen con datos de copia incremental, puede elegir la opción **Imagen más directorios y archivos incrementales**. Si elige **Imagen más directorios y archivos incrementales**, también puede seleccionar **Suprimir archivos inactivos de sistema local** para suprimir los archivos inactivos que se restauren en el sistema de archivos local. Si el único tipo de copia de seguridad que ha realizado en el sistema de archivos ha sido la copia de seguridad de imagen incremental por fecha, no se suprimirán los archivos.

Importante: Debe asegurarse por completo de que necesita realizar una restauración incremental, puesto que se sustituirá todo el sistema de archivos por la imagen del servidor y, a continuación, se restaurarán los archivos de los que ha hecho copia de seguridad con la operación de copia de seguridad de imagen incremental.

Restauración de una imagen mediante la línea de mandatos

Utilice el mandato **restore image** para restaurar una imagen mediante el cliente de línea de mandatos de IBM Spectrum Protect.

Referencia relacionada:

“Imagetofile” en la página 455

“Verifyimage” en la página 605

Restauración de datos desde un conjunto de copias de seguridad

El administrador de IBM Spectrum Protect puede generar un conjunto de copias de seguridad, que es una colección de los archivos que residen en el servidor, en soportes portables creados en un dispositivo utilizando un formato compatible con el dispositivo de cliente.

Puede restaurar datos de un juego de copias de seguridad del servidor de IBM Spectrum Protect o cuando el juego de copias de seguridad esté disponible localmente como un archivo o en un dispositivo de cinta.

Puede restaurar conjuntos de copias de seguridad desde las siguientes ubicaciones:

- Desde el servidor de IBM Spectrum Protect
- Desde medios portables de un dispositivo conectado a la estación de trabajo cliente
- Desde un archivo de conjunto de copias de seguridad en la estación de trabajo cliente

Los conjuntos de copias de seguridad pueden proporcionarle las funciones de archivado instantáneo y recuperación rápida, como se describe a continuación.

Archivado instantáneo

Esta función permite al administrador crear un juego de copias archivadas a partir de las versiones de copia de seguridad ya almacenadas en el servidor.

Recuperación rápida con conjuntos de copias de seguridad locales

Normalmente, las restauraciones se realizan a partir de copias de seguridad de archivos normales almacenados en el servidor de IBM Spectrum Protect fuera de los juegos de copias de seguridad. Este enfoque le ofrece la posibilidad de restaurar la versión de copia de seguridad más reciente de cada archivo. Es posible que un conjunto de copias de seguridad no contenga la versión de copia de seguridad más reciente de los archivos.

En algunos casos, la restauración de datos desde un juego de copias de seguridad puede ser una opción más adecuada que la restauración desde archivos de copia de seguridad normales del servidor de IBM Spectrum Protect. La restauración desde juegos de copias de seguridad puede ser más adecuada por los siguientes motivos:

- Un conjunto de copias de seguridad puede contribuir a una recuperación más rápida porque todos los archivos necesarios para la restauración están dentro de un menor número de volúmenes de almacenamiento.
- Los juegos de copias de seguridad permiten la colección de instante de los archivos. Puede restaurar en un instante específico en vez de restaurar lo que está disponible en ese momento en una restauración a nivel de archivo normal desde el servidor.

Restaurar un conjunto de copias de seguridad del servidor de IBM Spectrum Protect ofrece un conjunto mayor de opciones de restauración que restaurar a partir de un conjunto de copias de seguridad local. Sin embargo, en algunos casos puede ser preferible restaurar a partir de un conjunto de copias de seguridad local:

- Es posible que tenga que restaurar los datos cuando no haya una conexión de red disponible con el servidor de IBM Spectrum Protect. Esto puede suceder en una situación de recuperación ante siniestro.
- La restauración local puede ser más rápida que la restauración a través de una conexión de red con el servidor de IBM Spectrum Protect.

Un juego de copias de seguridad puede restaurarse desde el servidor de IBM Spectrum Protect mientras los volúmenes de juego de copias de seguridad estén disponibles en dicho servidor, o pueden haberse cambiado al sistema del cliente para una restauración de juego de copias de seguridad local. Puede generarse un conjunto de copias de seguridad con o sin una tabla de contenidos (TOC), y éste puede contener datos de archivos o imágenes.

La posibilidad de restaurar datos de conjuntos de copias de seguridad está restringida por la ubicación del conjunto de copias de seguridad y el tipo de datos de que contiene. El cliente de línea de mandatos puede restaurar algunos datos que la GUI no puede, pero la GUI le permite examinar y elegir los objetos que desea restaurar. Por lo general, los conjuntos de copias de seguridad del servidor con una tabla de contenido ofrecen más opciones durante la restauración. Sin embargo, los juegos de copias de seguridad locales ofrecen opciones que a veces son preferibles a restaurar a partir del servidor de IBM Spectrum Protect.

Las limitaciones para restaurar datos de juegos de copias de seguridad mediante la GUI se resumen en la siguiente tabla. Cada celda interior representa una combinación de tipo de datos y ubicación del conjunto de copias de seguridad. En cada situación, la celda indica si puede utilizar la GUI para restaurar únicamente el conjunto de copias de seguridad completo, seleccionar objetos del conjunto de copias de seguridad o si no puede utilizarla para restaurar el conjunto de copias de seguridad.

Tabla 43. Restricciones de restauración del conjunto de copias de seguridad de la GUI

Tipo de datos del conjunto de copias de seguridad	Ubicación del conjunto de copias de seguridad		
	Local (location=file o location=tape)	Servidor de IBM Spectrum Protect (tabla de contenidos disponible)	Servidor de IBM Spectrum Protect (tabla de contenidos no disponible)
archivo	Sólo restauración del conjunto de copias de seguridad completo.	Restauración del conjunto de copias de seguridad completo o de objetos seleccionados.	Sólo restauración del conjunto de copias de seguridad completo.
imagen	No se puede restaurar.	Restauración del conjunto de copias de seguridad completo o de objetos seleccionados.	No se puede restaurar.
estado del sistema	Sólo restauración del conjunto de copias de seguridad completo.	Restauración del conjunto de copias de seguridad completo o de objetos seleccionados.	Sólo restauración del conjunto de copias de seguridad completo.

Las restricciones para restaurar datos de conjuntos de copias de seguridad mediante el cliente de la línea de mandatos se resumen en la tabla que se encuentra a continuación. Cada celda interior representa una combinación de tipo de datos y ubicación del conjunto de copias de seguridad. En cada situación, la celda contiene los mandatos de restauración que puede utilizar. Salvo lo indicado, puede restaurar objetos específicos dentro de un conjunto de copias de seguridad así como el conjunto de copias de seguridad completo.

Tabla 44. Restricciones de restauración de los conjuntos de copias de seguridad de la línea de mandatos

Tipo de datos del conjunto de copias de seguridad	Ubicación del conjunto de copias de seguridad		
	Local (location=file o location=tape)	Servidor de IBM Spectrum Protect (tabla de contenidos disponible)	Servidor de IBM Spectrum Protect (tabla de contenidos no disponible)
archivo	Mandatos: restauración restore backupset	Mandatos: restauración restore backupset	Mandatos: restore backupset
imagen	No se puede restaurar	Mandato: restore image	No se puede restaurar
estado del sistema	Mandato: restore backupset	Mandatos: restore backupset restore systemstate	Mandato: restore backupset

Restricción: Cuando restaura datos del estado del sistema mediante el mandato **restore backupset**, no puede especificar objetos individuales. Sólo puede restaurar el estado del sistema completo.

Referencia relacionada:

“Localbackupset” en la página 484

“Query Backupset” en la página 723

“Query Image” en la página 731

“Restore” en la página 744

“Restore Backupset” en la página 749

“Restore Image” en la página 758

Restauración de conjuntos de copias de seguridad: consideraciones y restricciones

Existen algunas consideraciones y restricciones que debe tener en cuenta cuando restaure conjuntos de copias de seguridad.

Consideraciones de restauración del conjunto de copias de seguridad

Al restaurar conjuntos de copias de seguridad, tenga en cuenta lo siguiente:

- Si el objeto que desea restaurar se ha generado desde un nodo cliente cuyo nombre es distinto del nodo actual, especifique el nombre del nodo original con el parámetro **filespace**name en cualquiera de los mandatos restore.
- Si no puede restaurar un conjunto de copias de seguridad desde el medio portable, póngase en contacto con el administrador de IBM Spectrum Protect para asegurarse de que el medio portable se creó en un dispositivo con un formato compatible con el suyo.
- Si utiliza el mandato **restore backupset** en la línea de mandatos inicial con el parámetro **-location=tape** o **-location=file**, el cliente no intenta ponerse en contacto con el servidor de IBM Spectrum Protect.
- Cuando restaure un grupo a partir de un conjunto de copias de seguridad:
 - Se restaurará todo el grupo, o todos los grupos, del espacio de archivos virtual. Si hay varios grupos en el mismo espacio de archivos virtual, no podrá restaurar un solo grupo especificando el nombre de grupo. No puede restaurar una parte de un grupo especificando una vía de acceso de archivo.
 - Especifique un grupo utilizando los valores siguientes:
 - Especifique el nombre de espacio de archivos individual con el parámetro **filespace**name.
 - Utilice la opción **subdir** para incluir subdirectorios.
- Se proporciona soporte limitado para la restauración de conjuntos de copias de seguridad desde dispositivos de cinta conectados al sistema cliente. Se debe utilizar siempre un controlador de dispositivo nativo proporcionado por el fabricante del dispositivo. El controlador de dispositivo proporcionado por IBM para que lo utilice el servidor de IBM Spectrum Protect no se puede utilizar en el sistema cliente para restaurar juegos de copias de seguridad locales.
- Si un conjunto de copias de seguridad contiene archivos de distintos propietarios, el propio conjunto de copias de seguridad será propiedad del ID de usuario root y los ID de usuarios que no sean root no verán el conjunto de copias de seguridad. En tal caso, los ID de usuario que no son root pueden restaurar sus archivos si el administrador de IBM Spectrum Protect les

proporciona el nombre del juego de copias de seguridad. Los usuarios que no sean root sólo podrán restaurar sus propios archivos.

- Para permitir que la GUI del cliente restaure un conjunto de copias de seguridad de un dispositivo local, sin que sea necesaria una conexión al servidor, utilice la opción `localbackupset`.

Consideraciones de restauración del conjunto de copias de seguridad

Al restaurar conjuntos de copias de seguridad, tenga en cuenta las siguientes restricciones:

- No es posible restaurar ni utilizar los datos de los conjuntos de copias de seguridad de los que se ha hecho una copia de seguridad mediante la API.
- No puede restaurar datos de imagen de un conjunto de copias de seguridad mediante la utilización del mandato **restore backupset**. Sólo puede restaurar datos de imagen de un conjunto de copias de seguridad con el mandato **restore image**.
- No puede restaurar datos de imagen de un conjunto de copias de seguridad local (`location=tape` o `location=file`). Sólo puede restaurar datos de imagen de un juego de copias de seguridad del servidor de IBM Spectrum Protect.

Referencia relacionada:

“**Localbackupset**” en la página 484

“**Restore**” en la página 744

“**Restore Image**” en la página 758

“**Restore Backupset**” en la página 749

Restauración del conjunto de copias de seguridad

IBM Spectrum Protect interpreta que un juego de copias de seguridad es un objeto que contiene una estructura de archivos completa. Puede restaurar todo el conjunto de copias de seguridad o, en algunos casos, puede seleccionar partes de él. Los medios del conjunto de copias de seguridad son autodescriptivos y contienen toda la información necesaria para realizar correctamente una restauración.

Si está conectado a un servidor de Tivoli Storage Manager Versión 5.4 o posterior, el administrador del servidor podrá crear conjuntos de copias de seguridad apiladas. Los juegos de copias de seguridad apilados pueden contener datos de varios nodos y distintos tipos de datos para un nodo cliente en particular. Los tipos de datos pueden ser datos de archivo o datos de imagen.

Restricción: El proceso de restauración de datos de imagen y datos de aplicación solo está disponible cuando la restauración se realiza desde el servidor. No puede restaurar datos de imagen y datos de aplicación de la restauración de un conjunto de copias de seguridad de un cliente local.

Cuando un juego de copias de seguridad se ha apilado, sólo puede restaurar los datos de su propio nodo. Los datos de todos los demás nodos se pasan por alto. Cuando restaure datos desde un juego de copias de seguridad apilado de un dispositivo local, sólo podrá restaurar los datos de archivo de su propio nodo cliente. Es importante que la opción `nodename` se configure para que coincida con el nombre de nodo utilizado para generar el conjunto de copias de seguridad de uno de los nodos de la pila.

Importante: Debido a la portabilidad de los conjuntos de copias de seguridad locales, deben realizarse pasos adicionales para proteger los conjuntos de copias de seguridad locales de los medios portables. Los medios del conjunto de copias de seguridad deben protegerse físicamente, porque el conjunto de copias de seguridad puede restaurarse localmente sin autenticarse con el servidor. Todos los usuarios disponen de acceso a todos los datos del juego de copias de seguridad apilado, lo que significa que los usuarios disponen de acceso a los datos que no son de su propiedad, cambiando el nombre de nodo o visualizando el juego de copias de seguridad en el formato RAW de éste. Los únicos métodos que garantizan la protección de los datos son la protección física o el cifrado de los medios.

Si desea restaurar datos del conjunto de copias de seguridad desde el servidor, puede restaurar archivos individuales, directorios o los datos del conjunto de copias de seguridad completo en una única operación desde la GUI o desde la línea de mandatos. Si desea restaurar datos del conjunto de copias de seguridad localmente, la GUI sólo podrá visualizar y restaurar un conjunto de copias de seguridad completo. La línea de mandatos se puede utilizar para restaurar archivos o directorios individuales que están almacenados en un conjunto de copias de seguridad localmente.

Restauración de conjuntos de copias de seguridad mediante la GUI

La GUI de cliente puede restaurar datos desde un conjunto de copias de seguridad del servidor, desde un archivo local o desde un dispositivo de cinta local. Puede utilizar la GUI para restaurar archivos individuales de un juego de copias de seguridad del servidor de IBM Spectrum Protect con una tabla de contenidos, pero no de un juego de copias de seguridad local ni de un juego de copias de seguridad del servidor sin una tabla de contenidos.

Acerca de esta tarea

Importante: antes de iniciar una operación de restauración, tenga en cuenta que los conjuntos de copias de seguridad pueden contener datos para varios espacios de archivos. Si especifica un destino distinto de la ubicación original, los datos de *todos* los espacios de archivos se restauran en la ubicación especificada.

Para restaurar un conjunto de copias de seguridad de la GUI, siga los pasos a continuación:

1. Pulse **Restaurar** en la ventana principal de la GUI. Aparecerá la ventana Restaurar.
2. Localice el objeto de árbol de directorios **Juegos de copias de seguridad** y amplíelo pulsando en el signo más (+) que aparece junto a éste.
 - Para restaurar el conjunto de copias de seguridad de un dispositivo local, expanda el objeto **Local** y aparecerá la ventana para especificar la ubicación de conjunto de copias de seguridad. En la ventana, seleccione **Nombre de archivo:** o **Nombre de cinta:** en la lista desplegable y, a continuación, especifique la ubicación del archivo o la cinta. También puede pulsar el botón **Examinar** para que se abra una ventana de selección de archivos y seleccionar un conjunto de copias de seguridad.
 - Para restaurar datos del conjunto de copias de seguridad desde el servidor, amplíe primero el objeto **Servidor** y, a continuación, **Nivel de archivo** o **Imagen**, en función del tipo de restauración solicitada.

3. Realice una pulsación en el recuadro que se encuentra junto al conjunto de copias de seguridad o al directorio o archivo del conjunto de copias de seguridad que desea restaurar.
Puede seleccionar archivos de un conjunto de copias de seguridad si el conjunto de copias de seguridad se encuentra en el servidor y tiene una tabla de contenido.
4. Pulse **Restaurar**. Aparecerá la ventana Destino de restauración. Entre la información pertinente.
5. Pulse **Restaurar**. La ventana Lista de tareas mostrará el estado del proceso de restauración.

Nota:

- Si el objeto que desea restaurar forma parte de un juego de copias de seguridad generado en un nodo y se cambia el nombre de nodo en el servidor, los objetos del juego de copias de seguridad generados antes del cambio de nombre no coincidirán con el nuevo nombre de nodo. Asegúrese de que el nombre del nodo es el mismo que el nodo para el que se generó el juego de copias de seguridad.
- El cliente puede utilizarse para restaurar un conjunto de copias de seguridad en un dispositivo conectado, con o sin una conexión de servidor. Si no puede establecerse conexión con el servidor, se visualizará un mensaje preguntándole si desea continuar con la restauración de un conjunto de copias de seguridad locales. Asimismo, también puede utilizarse la opción `localbackupset` para indicar al cliente que no intente establecer conexión con el servidor.
- Algunos dispositivos locales, como los dispositivos de cinta (los dispositivos de cinta no se aplican a Mac OS X), requieren la instalación de controladores de dispositivo antes de realizarse la restauración. Consulte el manual del dispositivo para obtener ayuda para realizar esta tarea. También necesita conocer la dirección del dispositivo para llevar a cabo la restauración.
- Las siguientes funciones de una restauración de conjunto de copias de seguridad desde el servidor no están disponibles cuando la restauración se realiza localmente:
 1. Restaurar una imagen.
 2. Visualización y restauración de la GUI de archivos y directorios individuales. Para restaurar un directorio o archivo individual desde un conjunto de copias de seguridad locales puede utilizarse la línea de mandatos.

Restauraciones de los conjuntos de copia de seguridad utilizando una interfaz de línea de mandatos

La interfaz de línea de mandatos puede restaurar datos de un conjunto de copias de seguridad, desde un archivo local o de un dispositivo de cinta local. Puede utilizar el cliente de interfaz de línea de mandatos para restaurar archivos individuales de los conjuntos de copias de seguridad local y de conjuntos de copia de seguridad configurados sin TOC.

Para restaurar la interfaz de línea de mandatos del cliente, utilice el mandato **query backupset** para visualizar qué datos del conjunto de copias de seguridad están disponibles, a continuación utilice los mandatos de restauración de los datos.

Puede utilizar los mandatos siguientes para restaurar datos de sus conjuntos de copias de seguridad:

- **restore**
- **restore backupset**

- **restore image**

Utilice el mandato adecuado para la ubicación del conjunto de copias de seguridad y de los datos del conjunto de copias de seguridad. Para obtener más información, consulte el apartado Tabla 44 en la página 242.

Referencia relacionada:

“Query Backupset” en la página 723

“Query Image” en la página 731

“Restore” en la página 744

“Restore Backupset” en la página 749

“Restore Image” en la página 758

Restaurar o recuperar datos durante una migración tras error

Cuando el cliente se migra a servidor secundario, puede restaurar o recuperar los datos replicados desde servidor secundario.

Antes de empezar

Antes de empezar a restaurar o recuperar los datos durante una operación de migración tras error:

- Asegúrese de que el cliente está configurado para la migración tras error automática.
- Asegúrese de estar conectado a un servidor de IBM Spectrum Protect que replique los nodos de cliente. Para obtener más información sobre los requisitos de la migración tras error, consulte “Requisitos para la migración tras error automática del cliente” en la página 95.

Restricción: En la modalidad de migración tras error, no puede realizar la copia de seguridad o archivar los datos en servidor secundario.

Procedimiento

Para restaurar o recuperar los datos durante una migración tras error, siga estos pasos:

1. Compruebe el estado de réplica de los datos del cliente de servidor secundario. El estado de réplica indica si la copia de seguridad más reciente se ha replicado en el servidor secundario.
2. Restaure o recupere los datos como lo haría normalmente desde la GUI del cliente o desde la interfaz de línea de mandatos.

Consejo: La función de operaciones de restauración reinicializable funcionan como se esperaba cuando está conectado a servidor secundario. Sin embargo, las operaciones de restauración que se interrumpen cuando el servidor primario se desconecta no se pueden restaurar después de que el cliente realice la migración tras error. Debe ejecutar la operación de restauración completa de nuevo después de que el cliente realice la migración tras error al servidor secundario.

Resultados

Si los datos de réplica del servidor secundario no es actual, se le solicita continuar o detener la restauración o la operación de recuperación.

Por ejemplo, para restaurar el directorio de build.sh en la interfaz de línea de mandato, emita el siguiente mandato:

```
dsmc res /build.sh
```

Se visualiza la siguiente salida:

```
IBM Spectrum Protect
Interfaz de línea de mandatos del cliente de copia de seguridad/archivado
Versión de cliente 8, release 1, nivel 0.0
Fecha/hora del cliente: 11/16/2016 12:05:35
(c) Copyright by IBM Corporation y otros 1990, 2016. Reservados todos los derechos.

Nombre de nodo: MY_NODE_NAME
ANS2106I Connection to primary IBM Spectrum Protect server 192.0.2.1 failed

ANS2107I Attempting to connect to secondary server TARGET at
192.0.2.9 : 1501

Nombre de nodo: MY_NODE_NAME
Session established with server TARGET: Windows
Versión de servidor 8, release 1, nivel 0.0
Fecha/hora del servidor: 11/16/2016 12:05:35 Último acceso: 11/15/2016 14:13:32

Session established in failover mode to secondary server
ANS2108I Connected to secondary server TARGET.
Se ha invocado la función de restauración.

ANS2120W The last store operation date reported by the server TARGET of
05/16/2013 22:38:23 does not match the last store operation date of
05/21/2013 21:32:20 stored by the client.
Continue (Yes (Y)/No (N))
```

Si responde con N, se muestra el siguiente mensaje:

```
ANS1074W The operation was stopped by the user.
```

Si responde con Y, el proceso de restauración continúa como normal, pero es posible que los datos que restaure no sean los más actuales.

Conceptos relacionados:

“Configuración y uso de la migración tras error automática del cliente” en la página 94

Tareas relacionadas:

“Determinación del estado los datos replicados del cliente” en la página 100

Restaurar una imagen en archivo

Al realizar una copia de seguridad de una imagen, el cliente de archivado y copia de seguridad realiza una copia de seguridad del primer sector del volumen, pero, al restaurar los datos, omite el primer sector para mantener el bloque de control del volumen lógico original del volumen de destino.

Cuando se realiza una restauración de imagen en archivo, en el archivo se restaura el contenido del volumen completo, incluido el primer sector.

Los volúmenes LVM de AIX de grupos de volúmenes originales contienen el bloque de control de volumen lógico (LVCB) en el primer sector (512 bytes) del volumen. El LVCB contiene metadatos específicos del volumen y que deberían conservar las aplicaciones que utilizan el volumen.

Cuando copie el archivo que contenga la imagen en un volumen LVM desde el grupo de volúmenes original, deberá omitir el LVCB del archivo y del volumen de destino. Para llevar esto a cabo, puede utilizar el mandato **dd** siguiente:

```
dd if=<filename> of=/dev/<vol> bs=512 skip=1 seek=1
```

El mandato **dd** establece el tamaño de bloque en 512 bytes, lo cual hace que la copia se realice muy lentamente. La mejor opción consiste en utilizar **bs=1m** o una especificación similar. Tenemos una forma alternativa de copiar los datos de imagen:

1. Guarde el primer sector original en un archivo:

```
dd if=/dev/<vol> of=firstblk.tmp bs=512 count=1
```

2. Copie la imagen restaurada:

```
dd if=<filename> of=/dev/<vol> bs=1m
```

3. Restaure el primer sector original:

```
dd if=firstblk.tmp of=/dev/<vol> bs=512 count=1
```

Con la introducción de formatos de grupo de volúmenes grandes y escalables en AIX, es posible que el primer sector del volumen lógico no pueda contener LVCB y esté disponible para los datos. Si utiliza grupos de volumen grandes y escalables en su sistema, y tiene que restaurar todo el volumen incluyendo el primer sector, restaure el volumen a un archivo y después, cópielo a un volumen de destino. Para llevar esto a cabo, puede utilizar el mandato **dd** siguiente:

```
dd if=<filename> of=/dev/<vol> bs=1m
```

Conceptos relacionados:

“Restauración de una imagen mediante la línea de mandatos” en la página 240

Tareas relacionadas:

“Restauración de una imagen mediante la GUI” en la página 239

Gestión de datos del sistema de archivos GPFS con agrupaciones de almacenamiento

Con la tecnología Global Parallel File Systems (GPFS), puede gestionar los datos utilizando agrupaciones de almacenamiento. Una agrupación de almacenamiento es una colección de discos o RAID que tienen propiedades similares y que se gestionan conjuntamente como un grupo.

El grupo en el que se gestionan conjuntamente las agrupaciones de almacenamiento es el sistema de archivos. La ubicación y gestión automatizadas de los archivos de la agrupación de almacenamiento la realizan las políticas. Una política es un conjunto de reglas que describe el ciclo útil de los datos de usuario basándose en los atributos del archivo.

Cuando se crea un archivo, la política de ubicación determina la ubicación inicial de los datos del archivo y asigna el archivo a una agrupación de almacenamiento. Todos los datos que se graban en ese archivo se colocan en la agrupación de almacenamiento asignada. La política de gestión determina las operaciones de gestión que han de aplicarse al archivo, como la migración y la supresión. Los archivos contenidos en un sistema de archivos GPFS se distribuyen entre diferentes agrupaciones de almacenamiento, en función de las políticas de ubicación y migración habilitadas.

Durante la restauración, los archivos se colocan en la agrupación de almacenamiento correcta. El servidor de IBM Spectrum Protect no está al tanto de

las migraciones de agrupación a agrupación, por lo tanto los archivos se colocan en la agrupación de almacenamiento desde la que se ha realizado la copia de seguridad. El motor de política sustituye los archivos en función de las políticas de migración.

Si un ID de agrupación de almacenamiento se ha almacenado en los atributos ampliados del archivo, y esa agrupación de almacenamiento está disponible, el archivo siempre se coloca en esa agrupación de almacenamiento. Si la agrupación de almacenamiento no está disponible, la ubicación del archivo la determina la política de ubicación. Si la política de ubicación no coincide con el archivo, el archivo se coloca en la agrupación del sistema.

GPFS maneja la colocación de archivos después de una restauración como se indica a continuación:

- El archivo se coloca en la agrupación que puede seleccionar haciendo coincidir los atributos del archivo guardado con una regla RESTORE
- El archivo se coloca en la agrupación en la que estaba cuando se ha realizado la copia de seguridad.
- La ubicación en la que ha de colocarse el archivo se basa en la política de ubicación actual.
- El archivo se coloca en la agrupación de almacenamiento del sistema.

La regla GPFS RESTORE permite hacer coincidir archivos según los atributos guardados y no según los atributos del archivo actual. Si los atributos del archivo no coinciden, GPFS intenta restaurar el archivo en la secuencia descrita anteriormente.


Para obtener más información acerca de la regla GPFS RESTORE, lea la documentación GPFS acerca de políticas y reglas.

Se aplican las restricciones siguientes:


- La restauración de los archivos apéndice no funciona cuando se utilizan varias agrupaciones de almacenamiento ni con los archivos que tienen ACL.
- La desvinculación de juegos de archivos no está admitida.
- La opción ctime de GPFS debe establecerse en no (valor predeterminado) para evitar que se realicen operaciones de copia de seguridad/archivado no deseadas de los archivos después de la migración de archivos de GPFS de agrupación a agrupación.


Para obtener información sobre la utilización de las agrupaciones de almacenamiento, consulte la documentación del servidor de IBM Spectrum Protect.


Referencia relacionada:

 Almacenamiento de datos en agrupaciones de almacenamiento

Información relacionada:

 Información sobre el producto GPFS

 Mandato mmbackup: Requisitos de IBM Spectrum Protect

 Utilización de las opciones de inclusión y exclusión de IBM Spectrum Protect con el mandato mmbackup de IBM Spectrum Scale

Restauración de datos a un instante específico

Utilice una restauración a un *instante específico* para restaurar archivos al estado que tenían en una fecha y hora específicos.

Acerca de esta tarea

Una restauración a un instante específico puede eliminar el efecto de los datos dañados mediante la restauración de los datos a un momento anterior al problema o puede recuperar una configuración básica a una condición anterior.

Puede llevar a cabo una restauración a un instante específico de un espacio de archivos, directorio o archivo.

También puede llevar a cabo una restauración de punto en el tiempo de las copias de seguridad de imagen.

Lleve a cabo copias de seguridad incrementales para dar soporte a una restauración a un instante específico. Durante una copia de seguridad incremental, el cliente de copia de seguridad y archivado notifica al servidor el momento en que los archivos se suprimen de un espacio de archivos o directorio de cliente. Las copias de seguridad selectivas e incrementales por fecha no informan al servidor de los archivos suprimidos. Ejecute copias de seguridad incrementales con una frecuencia coherente con los requisitos de restauración posibles.

Si solicita una restauración a un instante específico con una fecha y una hora anteriores a la versión más antigua mantenida por el servidor de IBM Spectrum Protect, el objeto no se restaura en el sistema. Los archivos que se hayan borrado de la estación de trabajo antes del instante especificado no se restaurarán.

Nota:

1. El administrador debe definir los valores de grupo de copia que mantengan suficientes versiones inactivas de un archivo para garantizar que se puede restaurar un archivo en una fecha y hora específicas. Si no se mantienen suficientes versiones, es posible que el cliente no pueda restaurar todos los objetos en el instante específico que especifique.
2. Si suprime un archivo o un directorio, la próxima vez que ejecute una copia de seguridad incremental, la versión de copia de seguridad activa pasará a inactiva y las versiones más antiguas que excedan el número especificado por el atributo *Versiones si datos suprimidos* se suprimen de la clase de gestión.

Cuando realice una restauración a un instante específico, tenga en cuenta la siguiente información:

- El cliente restaura las versiones de archivos de la copia de seguridad más reciente anterior a la fecha de instante específico especificada. Asegúrese de que el instante específico que especifique no coincida con la fecha y la hora en que se realizó la copia de seguridad.
- Si la fecha y hora especificadas para el objeto que intenta restaurar son anteriores a las de la versión más antigua que existe en el servidor, el cliente no podrá restaurar dicho objeto.
- Una restauración a un instante específico restaura los archivos que se han suprimido de la estación de trabajo cliente después de la fecha especificada, pero no los archivos suprimidos antes de dicha fecha.

- El cliente no puede restaurar un archivo creado después de la fecha y hora del instante específico. Cuando se ejecute la restauración a un instante específico, no se suprimirán los archivos creados en el cliente en fecha posterior a la especificada como instante específico.

Procedimiento

Para llevar a cabo una restauración a un instante específico utilizando la GUI del cliente, siga los pasos siguientes:

1. Pulse el botón **Restaurar** en la ventana principal. Aparecerá la ventana Restaurar.
2. Pulse el botón **Instante específico** en la ventana Restaurar. Aparecerá la ventana Restauración a un instante específico.
3. Seleccione el recuadro **Utilizar una fecha de instante específico**. Seleccione la fecha y hora y pulse **Aceptar**. El instante especificado aparece en el campo **visualización de instante específico** en la ventana Restaurar.
4. Visualice los objetos que desea restaurar. Puede buscar un objeto por su nombre, filtrar el árbol de directorios o trabajar con los directorios del árbol de directorios.
5. Pulse en las casillas que se encuentran junto a los objetos que desea restaurar.
6. Pulse el botón **Restaurar**. Se abrirá la ventana Destino de restauración. Entre la información pertinente.
7. Pulse el botón **Restaurar** para iniciar la restauración. En la ventana Lista de tareas de restauración se muestra el estado del proceso.

Resultados

Nota: Si no existen versiones de copia de seguridad de un directorio para el instante específico que indique, los archivos que se encuentren en ese directorio no se podrán restaurar desde la GUI . Sin embargo, puede restaurar estos archivos desde la línea de mandatos.

Puede iniciar la restauración a un instante específico desde el cliente de línea de mandatos utilizando las opciones `pitdate` y `pittime` con los mandatos **query backup** y **restore**. Si utiliza las opciones `pitdate` y `pittime` con el mandato **query backup**, se establece el instante específico al que se devuelve la información de archivo. Si utiliza las opciones `pitdate` y `pittime` con el mandato **restore**, los valores de fecha y hora especificados establecen el instante específico al que se devuelven los archivos. Si especifica `pitdate` sin un valor para `pittime`, el valor predeterminado de `pittime` será 23:59:59. Si especifica `pittime` sin un valor para `pitdate`, éste se ignorará.

Conceptos relacionados:

Capítulo 9, “Políticas de gestión de almacenamiento”, en la página 299

Referencia relacionada:

“Backup Image” en la página 674

Restauración de archivos cifrados AIX

Cuando se realiza una copia de seguridad de archivos en formato en bruto a partir de un Sistema de archivos de cifrado (EFS) de JFS2 de AIX, solamente podrá restaurarla en el mismo EFS de JFS2 o en otro. No se pueden restaurar en ningún otro sistema de archivos distinto, ni en ninguna otra plataforma.

Cuando se realiza una copia de seguridad de los archivos EFS en forma de texto legible, podrá restaurarlos en cualquier lugar. Si los restaura en un EFS de JFS2, se volverán a cifrar automáticamente solo si el directorio en el que se restauran tiene establecida la opción "herencia de EFS" de AIX.

Tras restaurar un archivo del que se ha realizado una copia de seguridad en formato bruto, es posible que observe que el archivo ya no se puede descifrar. Es posible que la clave de cifrado original utilizada para el archivo ya no esté disponible en el almacén de claves de usuario. En tal caso, deberá restaurar el almacén de claves utilizado en el momento de realizar la copia de seguridad. Restáurelo en una ubicación distinta de /var/efs y utilice el mandato "efskeymgr -f" de AIX para añadir sus claves al conjunto de claves del kernel.

Para obtener información sobre cómo realizar copias de seguridad de datos EFS, consulte el apartado "Copia de seguridad del sistema de archivos cifrado de JFS2 de AIX" en la página 217.

Restaurar sistemas de archivos con partición de carga de trabajo de AIX

Todos los archivos que se crean mediante la partición de carga de trabajo local (WPAR) y que se copian mediante un cliente de copia de seguridad y archivado que está instalado en la WPAR global se pueden restaurar mediante el cliente instalado en la WPAR global.

Consulte los siguientes ejemplos de partición global y de configuración de WPAR:
Global partition:

```
system name: shimla  
file system: /home /opt
```

WPAR #1 configuration:

```
name: wpar1  
file system: /home; name in global WPAR: /wpars/wpar1/home
```

WPAR #2 configuration:

```
name: wpar2  
file system: /data; name in global WPAR: /wpars/wpar2/data
```

Existen dos formas de restaurar datos WPAR, dependiendo del método utilizado para realizar la copia de seguridad de los archivos de datos WPAR:

- Restaure todos los sistemas de archivos WPAR como espacios de archivo en la partición global. El nombre de espacio de archivos se debe utilizar para identificar el WPAR al cual pertenece. Todos los datos se gestionan en un nodo utilizando una planificación. Aquí encontrará un archivo de ejemplo, `dsm.sys`, que utiliza la configuración de ejemplo mencionada anteriormente, con una sección de servidor para todos los sistemas de archivos, tanto globales como lógicos:

```
SErvername  shimla  
TCPPort    1500  
TCPSeveraddress  servidor.ejemplo.com
```

```

nodename          shimla

PasswordAccess    generate

Domain            /wpars/wpar1/home /wpars/wpar2/data /home /opt

```

Utilice el mandato siguiente para restaurar cada espacio de archivos:

```

dsmc restore /wpars/wpar1/home/*
dsmc restore /wpars/wpar2/data/*
dsmc restore /home/*
dsmc restore /opt/

```

- Restaure cada sistema de archivos WPAR desde un nombre de nodo distinto, si se ha realizado la copia de seguridad bajo un nombre de nodo distinto. Cada WPAR debe tener un nombre de nodo independiente y un planificador en ejecución en la partición global. Además, se han de configurar los tres servicios del planificador, utilizando para cada uno de ellos un archivo dsm.opt distinto correspondiente al nombre de la sección del servidor. Este método permite que cada operación de restauración de WPAR se pueda gestionar de forma independiente de las demás. Aquí encontrará un archivo de ejemplo, dsm.sys, que utiliza la configuración de ejemplo mencionada anteriormente, con tres secciones de servidor: una para wpar1, otra para wpar2 y otra para la partición global shimla:

```

SErvername shimla_wpar1
TCPPort      1500
TCPSErveraddress servidor.ejemplo.com
nodename     wpar1
PasswordAccess generate
Domain       /wpars/wpar1/home

```

```

SErvername shimla_wpar2
TCPPort      1500
TCPSErveraddress servidor.ejemplo.com
nodename     wpar2
PasswordAccess generate
Domain       /wpars/wpar2/data

```

```

SErvername shimla
TCPPort      1500
TCPSErveraddress servidor.ejemplo.com
nodename     shimla
PasswordAccess generate
Domain       /home /opt

```

Tabla 45. mandatos de restauración de WPAR de ejemplo con el archivo dsm.opt

En el archivo dsm.opt file	mandato de restauración de ejemplo
servername shimla_wpar1	dsmc restore /wpars/wpar1/home/*
servername shimla_wpar2	dsmc restore /wpars/wpar2/data/*
servername shimla	dsmc restore /home/* dsmc restore /opt/*

Restaurar sistemas de archivos NAS

Las imágenes del sistema de archivos NAS se restauran mediante el cliente web o la interfaz de línea de mandatos.

Puede restaurar imágenes del sistema de archivos NAS completas o diferenciales de las que se ha hecho una copia de seguridad previamente. Si restaura una

imagen diferencial, IBM Spectrum Protect restaura automáticamente la imagen de copia de seguridad completa, seguida de una imagen diferencial. No es necesario que un nodo cliente monte un sistema de archivos NAS para realizar operaciones de copia de seguridad o de restauración en dicho sistema de archivos.

Conceptos relacionados:

“Descripción general de la configuración del cliente web” en la página 65

Restauración de sistemas de archivos NAS utilizando el cliente web

En esta sección se indican los pasos para restaurar sistemas de archivos NAS mediante la GUI del cliente web.

Procedimiento

1. Pulse el botón **Restaurar** en la ventana principal. Aparecerá la ventana Restaurar.
2. Expanda el árbol de directorios si es preciso. Para expandir un nodo del árbol, pulse en el signo más (+) situado junto al objeto del árbol. Los nodos que se muestran son aquéllos de los que se ha hecho copia de seguridad y para los que el administrador tiene autorización. El nodo raíz denominado **Nodos** no se puede seleccionar. Este nodo sólo aparece si hay un complemento NAS presente en la estación de trabajo cliente. Los nodos NAS se muestran en el mismo nivel que el nodo de la estación de trabajo cliente. Sólo aparecen los nodos para los que tiene autorización el administrador.
3. Expanda el nodo NAS para ver el objeto Imagen.
4. Expanda el objeto Imagen para ver los volúmenes que puede restaurar. No puede expandir los objetos Volumen.
5. Pulse las casillas situadas junto a los volúmenes bajo el objeto Imagen que desea restaurar. Si desea restaurar una imagen NAS de la que se ha efectuado una copia de seguridad en una fecha concreta, pulse el botón **Instante específico**. Al seleccionar una fecha, aparece el último objeto del que se hizo copia de seguridad en dicha fecha o anteriormente, incluidos los objetos que estén inactivos. Si desea ver todas las imágenes (incluidas las activas y las inactivas), antes de seleccionarlás, pulse **Ver → Visualizar archivos activos/inactivos** en la barra de menús.
6. Pulse **Restaurar**. Aparecerá la ventana Destino de restauración. Especifique la información en la ventana Destino de restauración. Si va a realizar la restauración en un destino diferente, sólo podrá restaurar un volumen a la vez. Puede restaurar las imágenes de sistemas de archivos NAS en cualquier volumen del servidor de archivos NAS desde el que se realizó su copia de seguridad. No puede restaurar imágenes en otros servidor de archivos NAS.
7. Pulse **Restaurar**. La ventana **Lista de tareas** de copia de seguridad NAS muestra el estado del proceso y la barra de progreso de la restauración. Si aparece un número junto a la barra de progreso, éste indica el tamaño de la restauración, si se conoce. Una vez finalizada la restauración, la ventana Informe de restauración NAS muestra los detalles del proceso. Si debe cerrar la sesión del navegador web, las operaciones NAS actuales continuarán después de la desconexión. Puede utilizar el botón **Descartar** situado en la ventana **Lista de tareas** de restauración NAS para salir de los procesos de supervisión sin finalizar la operación actual.
8. (Opcional) Para supervisar el procesamiento de una operación, seleccione **Acciones > IBM Spectrum Protect Actividades** en la ventana principal.

Resultados

Consideraciones:

- Las copias de seguridad de estaciones de trabajo y remotas (NAS) se excluyen mutuamente en una ventana Restaurar. Tras haber seleccionado un elemento para restaurar, el siguiente elemento que seleccione deberá ser del mismo tipo (NAS o no NAS).
- No se mostrarán detalles en el marco derecho de la ventana Restaurar correspondientes a los nodos o imágenes NAS. Para ver información sobre una imagen NAS, resalte la imagen NAS y seleccione **Ver > Detalles de archivo** en el menú.
- Para suprimir espacios de archivo NAS, seleccione **Utilities > Delete Filespaces**. Puede suprimir objetos de la estación de trabajo y objetos remotos.

Opciones y mandatos para restaurar sistemas de archivos NAS desde la línea de mandatos.

Este tema enumera algunos ejemplos de las opciones y mandatos que puede utilizar para restaurar las imágenes del sistema de archivos NAS desde la línea de mandatos.

Tabla 46. Opciones y mandatos NAS

Opción o mandato	Definición	Página
query node	Muestra todos los nodos en los que un identificador de usuario de administración determinado dispone de autorización para realizar operaciones. El ID de usuario de administración debe tener como mínimo autorización de propietario de cliente sobre el nodo NAS y sobre el nodo de la estación de trabajo cliente que están utilizando desde la línea de mandatos o desde la web.	" Query Node " en la página 735
query backup	Utilice el mandato query backup con la opción class para mostrar información sobre las imágenes de sistema de archivos de las que se ha realizado una copia de seguridad para un servidor de archivos NAS.	" Query Backup " en la página 720
query filesystem	Utilice el mandato query filesystem con la opción class para visualizar una lista de espacios de archivos pertenecientes a nodo NAS.	" Query Filespace " en la página 727
restore nas	Restaura la imagen de un sistema de archivos que pertenece a un servidor de archivos NAS (Network Attached Storage).	" Restore NAS " en la página 762
monitor process	Muestra los procesos de copia de seguridad y de restauración actuales de todos los nodos NAS en los que el administrador dispone de autorización. El usuario de administración puede seleccionar el proceso que desea supervisar.	" Monitor Process " en la página 714

Tabla 46. Opciones y mandatos NAS (continuación)

Opción o mandato	Definición	Página
cancel process	Muestra los procesos de copia de seguridad y de restauración actuales de todos los nodos NAS en los que el administrador dispone de autorización. Desde la lista, el usuario de administración puede seleccionar el proceso que desea cancelar.	"Cancel Process" en la página 691
delete filesystem	Utilice delete filesystem con la opción class para que se visualice una lista de los espacios de archivos que pertenecen a un nodo NAS y para seleccionar el que desea suprimir.	"Delete Filespace" en la página 698

Independientemente de la plataforma del cliente, las especificaciones del sistema de archivos NAS utilizan como separador la barra inclinada (/), como en el ejemplo siguiente: /vol/vol0.

Nota: Cuando se inicia una operación de restauración NAS utilizando el cliente de línea de mandatos o el cliente web, el servidor empieza un proceso para iniciar, controlar y supervisar la operación. Es posible que tarde unos cuantos minutos en observar el progreso en la interfaz de línea de mandatos porque el servidor debe realizar el montaje y otras tareas necesarias antes de que se produzca el traspaso de datos. Puede que el cliente de línea de mandatos de IBM Spectrum Protect visualice un mensaje Interrumpido... cuando tiene lugar el montaje. Puede pasar por alto este mensaje.

Restaurar copias de seguridad activas o inactivas

El administrador determina cuántas versiones de copia de seguridad mantiene IBM Spectrum Protect para cada archivo de la estación de trabajo.

Tener varias versiones de un archivo le permite restaurar versiones anteriores en el caso de que la copia de seguridad más reciente esté dañada. La versión de copia de seguridad más reciente es la versión *activa*. Cualquier otra versión de copia de seguridad es una versión *inactiva*.

Cada vez que IBM Spectrum Protect hace copias de seguridad de archivos, marca la nueva versión de copia de seguridad como copia de seguridad activa y la copia de seguridad activa anterior pasa a ser inactiva. Cuando se alcanza el número máximo de versiones inactivas, IBM Spectrum Protect suprime la versión inactiva más antigua.

Para restaurar una versión de copia de seguridad inactiva, debe visualizar ambas versiones, la activa y la inactiva, pulsando la opción **Visualizar archivos activos/inactivos** del menú **Ver**. Para ver sólo las versiones activas (opción predeterminada), pulse la opción **Visualizar sólo archivos activos** del menú **Ver**. Si intenta restaurar más de una versión a la vez, sólo se restaurará la versión activa.

En la línea de mandatos de IBM Spectrum Protect, utilice la opción **inactive** para visualizar los objetos activos e inactivos.

Referencia relacionada:

"Inactive" en la página 456

Restauración de datos mediante la GUI

En esta sección figuran los pasos que es necesario seguir para restaurar versiones de copias de seguridad de archivos o subdirectorios individuales.

Procedimiento

1. Pulse **Restaurar** en la ventana principal. Aparecerá la ventana Restaurar.
2. Expanda el árbol de directorios. Seleccione las casillas situadas junto a los archivos o directorios que desea restaurar. Para buscar o filtrar archivos, pulse el icono **Buscar** de la barra de herramientas.
3. Escriba los criterios de búsqueda en la ventana Buscar archivos (Restaurar).
4. Pulse el botón **Buscar**. Aparecerá la ventana Archivos coincidentes (Restaurar).
5. Pulse las casillas que se encuentran junto a los archivos que se desean restaurar y cierre la ventana Archivos coincidentes (Restaurar).
6. Escriba los criterios de filtrado en la ventana Buscar archivos (Restaurar).
7. Pulse el botón **Filtrar**. La ventana Restaurar muestra los archivos filtrados.
8. Pulse en las casillas que se encuentran junto a los archivos o directorios filtrados que desea restaurar.
9. Si desea modificar opciones de restauración específicas, pulse el botón **Opciones**. Las opciones que modifique *sólo* estarán en vigor durante la sesión actual.
10. Pulse **Restaurar**. Aparecerá la ventana Destino de restauración. Especifique la información en la ventana Destino de restauración.
11. Pulse **Restaurar**. La ventana **Lista de tareas** de restauración muestra el estado del proceso de restauración.

Resultados

Nota: En Mac OS X, tenga en cuenta las siguientes consideraciones cuando restaure datos mediante la GUI:

1. Cuando se utiliza **Herramientas de IBM Spectrum Protect para administradores** para iniciar el cliente, este se ejecuta con un ID de usuario de cero. Esto significa que si crea una carpeta en la que restaurar los archivos, dicha carpeta será propiedad del usuario root. Para acceder a los archivos, deberá cambiar los permisos de la carpeta. Podrá cambiar el propietario de la carpeta desde una ventana de terminal con el mandato **sudo chown**. Consulte la documentación relativa al sistema operativo que utilice para obtener más información sobre cómo llevarlo a cabo.
2. Cuando restaure archivos con la opción `replace` establecida en *no*, los archivos existentes no se sobrescribirán, pero sí los directorios. Para dejar intactos los directorios existentes durante una operación de restauración, seleccione el botón **Opciones**,⇒después seleccione el menú desplegable **Todos los archivos y directorios seleccionados** y elija la opción **Solo archivos**.
3. Cuando las carpetas se restauran desde un sistema de archivos UFS o HFSX en un sistema de archivos HFS y sólo difieren en el uso de mayúsculas o minúsculas, el cliente restaura el contenido de ambas carpetas en una sola.

Ejemplos de restauración desde la línea de mandatos

Este tema enumera algunos ejemplos de los mandatos **restore** para su uso en tareas específicas.

En la tabla siguiente se muestran ejemplos de utilización del mandato **restore** para restaurar objetos del almacenamiento del servidor de IBM Spectrum Protect.

Tabla 47. Ejemplos de restauración desde la línea de mandatos

Tarea	Mandato	Consideraciones
Restaurar la versión de copia de seguridad más reciente del archivo /Users/monnett/Documents/h1.doc, aunque la copia de seguridad esté inactiva.	<code>dsmc restore /Users/monnett/Documents/h1.doc -latest</code>	Si el archivo que está restaurando ya no reside en la estación de trabajo y ha realizado una copia de seguridad incremental después de suprimir el archivo, no habrá ninguna copia de seguridad activa del archivo en el servidor. En este caso, utilice la opción <code>latest</code> para restaurar la versión de copia de seguridad más reciente. IBM Spectrum Protect restaura la versión de copia de seguridad más reciente, ya sea activa o inactiva. Consulte el apartado “Latest” en la página 483 para obtener más información.
Visualizar una lista de versiones de copia de seguridad activas e inactivas para seleccionar las versiones que se restaurarán.	<code>dsmc restore "/Users/monnett/Documents/*"-pick -inactive</code>	Si intenta restaurar a la vez las versiones activa e inactiva de un archivo, sólo se restaurará la versión activa. Consulte los apartados “Pick” en la página 512 y “Inactive” en la página 456 para obtener más información.
Restaurar el archivo /Users/monnett/Documents/h1.doc a su directorio original.	<code>dsmc restore /Users/monnett/Documents/h1.doc</code>	Si no especifica ningún destino, los archivos se restaurarán en su ubicación original.
Restaurar el archivo /Users/monnett/Documents/h1.doc bajo un nombre y directorio nuevos.	<code>dsmc restore /Users/monnett/Documents/h1.doc /Users/gordon/Documents/h2.doc</code>	Ninguna
Restaurar los archivos del directorio /Users y todos sus subdirectorios.	<code>dsmc restore /Users/ -subdir=yes</code>	Si restaura una vía de acceso y un archivo específicos, IBM Spectrum Protect restaura de forma recursiva <i>todos</i> los subdirectorios de esa vía de acceso y todas las instancias del archivo especificado que haya en <i>cualquiera</i> de esos subdirectorios. Consulte el apartado “Subdir” en la página 581 para obtener más información sobre la opción <i>subdir</i> .
Restaurar todos los archivos del directorio /Users/gordon/Documents al estado en el que se encontraban a las 13:00 horas del día 17 de agosto de 2003.	<code>dsmc restore -pitd=8/17/2003 -pitt=13:00:00 /Users/gordon/Documents/</code>	Consulte los apartados “Pitdate” en la página 512 y “Pittime” en la página 513 para obtener más información sobre las opciones <i>pitdate</i> y <i>pittime</i> .
Restaurar todos los archivos del directorio /Users/mike/Documents que terminen por .bak al directorio /Users/mike/projectn/.	<code>dsmc restore "/Users/mike/Documents/*.bak" /Users/mike/projectn/</code>	si el destino es un directorio, especifique el delimitador (/) como el último carácter del destino. Si omite el delimitador y el origen especificado es un directorio o una especificación de archivo con un carácter comodín, recibirá un mensaje de error. Si el directorio <i>projectn</i> no existe, se creará.

Tabla 47. Ejemplos de restauración desde la línea de mandatos (continuación)

Tarea	Mandato	Consideraciones
Restaurar los archivos especificados en el archivo restorelist.txt en una ubicación distinta.	dsmc restore -filelist=/Users/user2/Documents/restorelist.txt /Users/NewRestoreLocation/	Consulte el apartado “Filelist” en la página 439 para obtener más información sobre la restauración de una lista de archivos.

Referencia relacionada:

“Restore” en la página 744

Ejemplos: restauraciones mediante la línea de mandatos para grandes cantidades de datos

Si debe restaurar un gran número de archivos, puede obtener un rendimiento más rápido si utiliza el mandato **restore** en lugar de la GUI. Además, puede mejorar el rendimiento especificando varios mandatos **restore** al mismo tiempo.

Por ejemplo, para restaurar todos los archivos del espacio de archivos /home, escriba:

```
dsmc restore /home/ -subdir=yes -replace=all -tapeprompt=no
```

Sin embargo, si especifica varios mandatos para los directorios del espacio de archivos /home, puede restaurar los archivos más rápidamente.

Por ejemplo, puede especificar estos mandatos:

```
dsmc restore /home/monnett/ -subdir=yes -replace=all -tapeprompt=no
dsmc restore /home/gillis/ -subdir=yes -replace=all -tapeprompt=no
dsmc restore /home/stewart/ -subdir=yes -replace=all -tapeprompt=no
```

También puede utilizar la opción **quiet** con el mandato **restore** para ahorrar tiempo de proceso. Sin embargo, no recibirá mensajes informativos para archivos individuales.

Nota: Si ya tiene el conjunto de valores apropiado para las opciones **subdir**, **replace**, **tapeprompt** y **quiet** en el archivo de opciones del usuario cliente, no es necesario que las incluya en los mandatos.

Cuando escriba múltiples mandatos para restaurar los archivos, debe especificar una parte exclusiva del espacio de archivos en cada mandato **restore**. Asegúrese de no utilizar ninguna especificación de archivo que se solape en los mandatos.

Para visualizar una lista de los directorios de un espacio de archivos, utilice el mandato **query backup**. Por ejemplo:

```
dsmc query backup -dirsonly -subdir=no /Users/
```

Como norma general, puede especificar de dos a cuatro mandatos **restore** al mismo tiempo. El número máximo que puede ejecutar a la vez sin disminuir el rendimiento depende de factores tales como la memoria disponible y la carga de trabajo de la red.

La velocidad a la cual puede restaurar los archivos también depende del número de unidades de cintas disponible en el servidor y de si el administrador está utilizando la función de proximidad para mantener los espacios de archivos asignados en tan pocos volúmenes como sea posible.

Por ejemplo, si /Users/user1 y /Users/user2 se encuentran en la misma cinta, la restauración para /Users/user2 deberá esperar hasta que se haya completado la restauración para /Users/user1. Sin embargo, si /Users/user3 se encuentra en una cinta distinta y existen, como mínimo, dos unidades de cinta disponibles, la restauración para /Users/user3 puede iniciarse al mismo tiempo que la restauración para /Users/user1.

Establezca en ilimitados (-1) los valores ulimit del sistema si han de restaurarse archivos muy grandes (2 GB) con HSM o con el cliente de copia de seguridad/archivado. El cliente puede restaurar estos archivos grandes con suficientes recursos del sistema. Si los valores de ulimit se establecen en valores más bajos, puede que se produzcan errores en la restauración.

Restauración estándar de la consulta, sin restauración de la consulta y restauración reinicializable

En este tema se describen los procesos de restauración estándar (o clásica), de restauración sin consulta y de restauración reinicializable.

Proceso de restauración de consulta estándar

El proceso de restauración de consulta estándar también se denomina restauración clásica. En este tema se explica cómo instalar los trabajos de restauración de consulta estándar.

Los trabajos de restauración de consulta estándar funcionan de la siguiente manera:

- El cliente realiza una consulta al servidor para obtener una lista de los archivos de los que se ha hecho copia de seguridad correspondientes al espacio de archivos de cliente que desea restaurar.
- El servidor envía una lista de los archivos de los que se ha hecho copia de seguridad que coinciden con los criterios de la restauración. Si desea restaurar archivos activos e inactivos, el servidor envía información sobre todos los archivos de los que se ha hecho copia de seguridad al cliente.
- La lista de los archivos devuelta desde el servidor se clasifica en la memoria del cliente con el fin de determinar el orden de restauración de los archivos y minimizar el número de montajes de cintas necesarios para ejecutar la restauración.
- El cliente indica al servidor que restaure datos de archivo y objetos de directorio.
- Los directorios y archivos por restaurar se envían del servidor al cliente.

Sin consulta de proceso de restauración

En el proceso de restauración sin consulta, se envía una sola solicitud de restauración al servidor en lugar de consultar al servidor para cada objeto que se debe restaurar.

1. El cliente indica al servidor que va a realizar una restauración sin consulta y le facilita los detalles sobre directorios, archivos y espacios de archivos.
2. El servidor utiliza una tabla independiente para realizar el seguimiento de entradas que guían la restauración.
3. Los datos por restaurar se envían al cliente. Los objetos de archivo y de directorio que se almacenan en el disco se envían inmediatamente, puesto que no es necesario clasificar dichos datos antes de restaurar el objeto.

4. Puede utilizar varias sesiones para restaurar los datos. Si los datos se encuentran en varias cintas, hay diversos puntos de montaje disponibles en el servidor. La combinación de la opción **resourceutilization** y **MAXNUMMP** permite el uso de varias sesiones.

Cuando proporcione una especificación de archivo de origen en el mandato **restore** y no especifique ninguna de las opciones: **inactive**, **latest**, **pick**, **fromdate**, **todate**, el cliente utiliza un método de *restauración sin consulta* para restaurar los archivos y los directorios desde el servidor. Este método se denomina restauración sin consulta ya que en lugar de realizar una consulta al servidor para cada objeto que se debe restaurar, se le envía una única petición de restauración. En este caso, el servidor devuelve los archivos y directorios al cliente sin que el cliente tenga que realizar ninguna acción adicional. Éste simplemente acepta los datos procedentes del servidor y los restaura en el destino especificado en el mandato **restore**.

Utilizando el cliente GUI de IBM Spectrum Protect, un ejemplo de un mandato con carácter comodín sin restricciones sería seleccionar una carpeta de la ventana del árbol de restauración. Un ejemplo de un mandato con carácter comodín con restricciones sería seleccionar archivos individuales de una carpeta.

Utilizando el cliente de línea de mandatos, un ejemplo de un mandato con carácter comodín sin restricciones:

```
"/Users/user1/Documents/2004/*"  
/home/mydocs/2004/*
```

Un ejemplo de una especificación de archivo con carácter comodín con restricciones sería:

```
/Users/user1/Documents/2004/sales.*  
/home/mydocs/2004/sales.*
```

Proceso de restauración reinicialable

Si el proceso de restauración se detiene debido a un corte de la alimentación o a una anomalía de la red, el servidor registra el punto en que se ha interrumpido la restauración.

El cliente conoce este registro como *restauración reinicialable*. Se puede disponer de varias sesiones de restauración reinicialables. Utilice el mandato **query restore** o seleccione **restartable restores** en el menú Acciones para averiguar si su cliente tiene alguna sesión de restauración reinicialable en la base de datos del servidor.

Debe completar una restauración reinicialable antes de intentar llevar a cabo más copias de seguridad del sistema de archivos. Si intenta repetir la restauración interrumpida o realizar una copia de seguridad del espacio de archivos de destino, no lo logrará porque no ha concluido la restauración original. Para reiniciar la restauración en el punto en que se interrumpió, utilice el mandato **restart restore**; para suprimir la restauración reinicialable, utilice el mandato **cancel restore**.

En el cuadro de diálogo **Restauraciones reinicialables** de la GUI de IBM Spectrum Protect, puede seleccionar y suprimir la restauración interrumpida o bien puede reiniciarla. Si reinicia la restauración interrumpida, ésta se reinicia desde la primera transacción, que podría constar de uno o varios archivos, que no se había restaurado por completo en el momento de producirse la interrupción. Por este motivo, puede que reciba algunos mensajes que le preguntarán si han de sustituirse archivos de la transacción interrumpida cuya restauración ya se ha realizado.

Para llevar a cabo restauraciones reiniciables mediante la GUI del cliente Web, siga los pasos siguientes:

1. Seleccione **Acciones**→ **Restauraciones reiniciables** en el panel inicial.
2. Seleccione la sesión de restauración reiniciable que desee llevar a cabo.
3. Pulse el botón **Reiniciar** de la parte superior del panel.

Referencia relacionada:

“Resourceutilization” en la página 539

“Restore” en la página 744

Restauración de sistemas de archivos ZFS de Solaris

Zettabyte File Systems (ZFS) utiliza las agrupaciones de almacenamiento para gestionar el almacenamiento físico.

La forma como se puede restaurar un sistema de archivos ZFS depende de cómo se haya realizado la copia de seguridad.

- Si se ha hecho la copia de seguridad de todos los archivos y carpetas como objetos separados, se pueden restaurar llevando a cabo una restauración a nivel de archivo. Por ejemplo:

```
dsmc restore /tank/myZFS/ -subdir=yes -replace=all
```

No efectúe una restauración a nivel de archivo en un escenario de recuperación tras desastre. Aunque pueda restaurar satisfactoriamente todos los archivos y carpetas de sistema a partir de una copia de seguridad creada con un cliente de archivado y copia de seguridad, es posible que el sistema restaurado sea inestable o genere un error.

- Si ha hecho la copia de seguridad de una instantánea ZFS completa como un solo archivo, tiene que restaurar el archivo de instantánea del servidor en una ubicación temporal. Por ejemplo:

```
dsmc restore /tmpdir/mySnapshotfile
```

A continuación, puede restaurar el sistema de archivos a partir del archivo de instantánea utilizando los mandatos de Oracle Solaris ZFS. Por ejemplo:

```
zfs receive tank/myZFS@mySnapshot < /tmpdir/mySnapshotFile
```

La ventaja de restaurar ZFS a partir de un archivo de instantánea es que se puede restaurar el sistema de archivos completo en un escenario de recuperación tras desastre.

Para obtener información detallada sobre cómo restaurar datos en sistemas de archivos ZFS, consulte la documentación de producto que está disponible en Oracle. Si va a restaurar una agrupación raíz ZFS, consulte los temas donde se describe cómo volver a crear la agrupación raíz y cómo recuperar instantáneas de agrupación raíz.

Tareas relacionadas:

“Realizar la copia de seguridad de sistemas de archivos Solaris Zettabyte” en la página 216

Tareas de restauración adicionales

En este apartado se indican algunas consideraciones avanzadas para la restauración de datos.

Cómo autorizar a otro usuario para que restaure o recupere archivos

Puede autorizar a otro usuario de la misma estación de trabajo o de otra para que restaure versiones de copia de seguridad o recupere copias archivadas de los archivos.

Acerca de esta tarea

Esto permite compartir archivos con otras personas o con otras estaciones de trabajo que utilice con un nombre de nodo distinto. Para autorizar a un usuario de otra estación de trabajo para que restaure o recupere los archivos, la otra estación de trabajo debe ejecutarse en uno de los clientes UNIX y debe estar inscrita en el servidor.

Nota: Mac OS X *sólo* puede restaurar nodos Mac OS X.

Para autorizar a otro usuario para que restaure o recupere los archivos:

Procedimiento

1. Pulse **Herramientas** → **Lista de acceso al nodo** en la ventana principal. Aparece la ventana Lista de acceso al nodo.
2. Pulse el botón **Agregar**. Aparece la ventana Agregar regla de acceso.
3. En la ventana Agregar regla de acceso, seleccione un elemento en el campo Permitir acceso a para especificar el tipo de datos al que el otro usuario puede acceder. Puede seleccionar Objetos en copia de seguridad o bien Objetos archivados.
4. En el campo Otorgar acceso a nodo, escriba el nombre del nodo de la estación de trabajo host del usuario que puede acceder a sus datos.
5. En el campo Usuario, escriba el nombre del usuario de un nodo que puede acceder a sus datos.
6. En el campo Espacio de archivos y directorio, seleccione el espacio de archivos y el directorio al que el usuario puede acceder. No puede seleccionar más de un espacio de archivos y un directorio al mismo tiempo. Si desea dar al usuario acceso a otro espacio de archivos y otro directorio, debe crear otra regla de acceso.
7. Si desea limitar el acceso del usuario a determinados archivos del directorio, escriba en el campo Nombre de archivo el nombre completo o el tipo de los archivos del servidor a los que el otro usuario puede acceder. El campo Nombre de archivo sólo acepta una entrada. Puede ser un único nombre de archivo o un nombre de archivo con caracteres comodín que corresponda a uno o varios archivos. Puede utilizar un carácter comodín como parte del patrón. La entrada debe coincidir con archivos que se hayan almacenado en el servidor.
8. Para la GUI Java: si desea dar acceso a todos los archivos del directorio seleccionado que coinciden con la especificación de nombre de archivo, incluidos los archivos de los subdirectorios, pulse **Incluir subdirectorios**.
9. Pulse el botón **Aceptar** para guardar la regla de acceso y cerrar la ventana Agregar regla de acceso.
10. La regla de acceso que ha creado se muestra en el cuadro de lista de la ventana Lista de acceso al nodo. Cuando ya no necesite la ventana Lista de acceso al nodo, pulse el botón **Aceptar**. Si no desea guardar los cambios, pulse **Cancelar** o cierre la ventana.

Resultados

En la interfaz de línea de mandatos, utilice el mandato **set access** para autorizar otro nodo para restaurar o recuperar los archivos. También puede utilizar el mandato **query access** para ver la lista actual y **delete access** para suprimir nodos de la lista.

Referencia relacionada:

“Delete Access” en la página 692

“Query Access” en la página 717

“Set Access” en la página 778

Restauración o recuperación de archivos de otro nodo cliente

Después de que los usuarios concedan acceso a los archivos del servidor, puede restaurar o recuperar dichos archivos en el sistema local.

Acerca de esta tarea

Puede mostrar espacios de archivos de otro usuario en el servidor, restaurar las versiones de copia de seguridad de otro usuario o recuperar las copias de archivado de otro usuario en el sistema de archivos local:

Procedimiento

1. Pulse **Herramientas** en la ventana principal.
2. Pulse **Acceder a otro nodo**. Aparecerá la ventana Acceder a otro nodo.
3. Escriba el nombre de nodo de la estación de trabajo host en el campo Nombre de nodo. Escriba el nombre del usuario en el campo Nombre usuario.
4. Pulse el botón **Establecer**.

Resultados

Si está utilizando mandatos, utilice las opciones `fromnode` y `fromowner` para indicar el nombre del nodo y el nombre del usuario propietario de los archivos.

Por ejemplo, para restaurar archivos en uno de sus propios sistemas de archivos de los que se hizo copia de seguridad en una estación de trabajo denominada Node1 y propiedad de un usuario cuyo nombre es Ann, escriba:

```
dsmc restore -fromn=node1 -fromo=ann "/home/proj/*" /home/gillis/
```

Utilice el mandato **query filespace** para obtener una lista de los espacios de archivos. Por ejemplo, para obtener una lista de espacios de archivos propiedad de Ann en Node1, escriba:

```
dsmc query filespace -fromn=node1 -fromo=ann
```

Referencia relacionada:

“Fromnode” en la página 447

“Query Filespace” en la página 727

“Restore” en la página 744

“Retrieve” en la página 770

Restaurar o recuperar archivos en otra estación de trabajo

Desde una estación de trabajo distinta, puede restaurar o recuperar archivos de los que ha realizado copia de seguridad anteriormente en su propia estación de trabajo. Debe conocer la contraseña de IBM Spectrum Protect asignada a su nodo.

Para restaurar o recuperar archivos en otra estación de trabajo, utilice la opción `virtualnodename` para especificar el nombre de nodo de la estación de trabajo desde donde se realizó la copia de seguridad de los archivos. La opción `virtualnodename` no puede establecerse en el nombre del host de la estación de trabajo. Puede utilizar la opción `virtualnodename` al iniciar IBM Spectrum Protect o bien puede agregar la opción `virtualnodename` al archivo de opciones del usuario cliente `dsm.opt`. Utilice la opción `virtualnodename` en el mandato **dsmj** si está utilizando la estación de trabajo de otro usuario y no desea actualizar su archivo de opciones del usuario cliente.

IBM Spectrum Protect solicitará la contraseña de su nodo original. Una vez haya escrito la contraseña correcta, todos los sistemas de archivos de su estación de trabajo original aparecerán en la ventana Restaurar o Recuperar. Podrá restaurar o recuperar archivos como si estuviera trabajando en su propia estación de trabajo.

Importante: cuando utilice este método para acceder a archivos, tendrá acceso a todos los archivos con copia de seguridad y copias archivadas de su estación de trabajo. Se le considerará un usuario root virtual.

Puede utilizar la opción `virtualnodename` en un mandato. Por ejemplo, para restaurar los archivos de *projx*, escriba:

```
dsmc restore -virtualnodename=nodeone "/home/monnett/projx/*"
```

Si no desea restaurar o recuperar los archivos en el mismo nombre de directorio de la estación de trabajo alternativa, escriba un destino distinto.

Las consideraciones para la recuperación de archivos son las mismas que las de restauración.

Restauración de un disco en caso de pérdida del mismo

Puede recuperar los archivos si puede ejecutar el cliente. Si el disco que contiene el cliente no se encuentra (porque ha sido robado o por un error en el hardware), debe reinstalar el cliente antes de poder recuperar los archivos. Si pierde el disco que contiene el sistema operativo y el software de comunicación, debe recuperarlos antes de conectarse al servidor IBM Spectrum Protect.

Acerca de esta tarea

Para protegerse ante estas clases de pérdidas, debe agrupar un conjunto de medios de instalación que pueda utilizar para restaurar el sistema en un estado que le permita conectarse al servidor y empezar a recuperar datos. Los medios de instalación deben contener:

Procedimiento

1. Un sistema operativo iniciable que permita realizar funciones básicas.
2. Un programa de comunicaciones configurado correctamente que permita establecer comunicaciones con el servidor.
3. Un cliente con archivos de opciones personalizadas apropiadas. Puede utilizar la interfaz de línea de mandatos del cliente par completar esta tarea.


Resultados

El paquete de comunicación que utilice determina los archivos que necesita. Consulte los manuales del sistema operativo y el software de comunicación para configurar los medios de instalación.

Si también tiene instalado IBM Spectrum Protect for Space Management en la estación de trabajo, el soporte de instalación debe incluir el cliente de línea de mandatos de HSM.

Nota: El administrador puede planificar operaciones de restauración que pueden resultar muy útiles cuando necesita restaurar un número elevado de archivos.

Conceptos relacionados:

 Copia de seguridad y restauración en sistemas de archivos gestionados por espacio

Supresión de espacios de archivos

Si el administrador de IBM Spectrum Protect le concede autorización, puede suprimir espacios de archivos completos del servidor.

Acerca de esta tarea

Cuando se suprime un espacio de archivos, está suprimiendo todos los archivos y las imágenes, tanto las versiones de copia de seguridad como las de copias archivadas que hay en ese espacio de archivos. Por ejemplo, si suprime el espacio de archivos del sistema de archivos `/home/monnet`, está suprimiendo todas las copias de seguridad de todos los archivos de ese sistema de archivos y de cada archivo que archivó en el mismo. **Considere detenidamente si desea suprimir un espacio de archivos.** Debe ser un usuario autorizado para poder realizar esta tarea.

Puede suprimir las versiones individuales de copia de seguridad utilizando el mandato **delete backup**.

Puede suprimir espacios de archivos mediante la GUI de cliente de copia de seguridad y archivado o la interfaz de línea de mandatos del cliente. Para suprimir espacios de fila NAS, utilice el cliente web o la interfaz de línea de mandatos.

Para suprimir un espacio de archivos mediante la GUI, siga estos pasos:

Procedimiento

1. Seleccione **Herramientas** → **Suprimir espacios de archivos** en la ventana principal.
2. Pulse en las casillas que se encuentran junto a los espacios de archivos que desea eliminar.
3. Pulse el botón **Suprimir**. El cliente le pedirá una confirmación antes de eliminarlos.

Resultados

También puede suprimir un espacio de archivos con el mandato **delete filespace**. Utilice la opción **class** con el mandato **delete filespace** para suprimir espacios de archivos NAS.

Referencia relacionada:

“Class” en la página 364

“Delete Backup” en la página 694

“Delete Filespace” en la página 698

Habilite SELinux para restaurar los archivos en el cliente de Red Hat Enterprise Linux 5

Si es un usuario no root y está intentando restaurar archivos en el cliente Red Hat Enterprise Linux 5, en primer lugar debe activar SELinux.

Si no activa SELinux, tendrá problemas si restaura los archivos que se han modificado en los atributos ampliados.

Capítulo 6. Archivar y recuperar datos (UNIX y Linux)

Puede archivar los archivos que se utilizan con poca frecuencia en el servidor de IBM Spectrum Protect y recuperarlos cuando los necesite. Archivar y recuperar archivos es similar a realizar una copia de seguridad y restaurar archivos. Muchas de las ventanas y conceptos son similares.

Todos los procedimientos primarios de archivado y recuperación que aparecen en este tema se aplican también al cliente web, excepto los procedimientos del Editor de preferencias.

Puede completar las siguientes tareas primarias de archivado y recuperación.

- “Archivado de datos con la GUI”
- “Ejemplos de archivado de datos utilizando la línea de mandatos” en la página 270
- “Supresión de datos archivados” en la página 274
- “Recuperación de datos con la GUI” en la página 277
- “Recupere los ejemplos de datos utilizando la línea de mandatos” en la página 277

Conceptos relacionados:

Capítulo 4, “Copia de seguridad de los datos”, en la página 155

Tareas relacionadas:

“Inicio de una sesión de cliente web” en la página 147

Copias de archivado

Para archivar copias, debe seleccionar los archivos específicos que desea archivar. Puede seleccionar los archivos mediante una especificación de archivos o seleccionándolos en el árbol de directorios.

Es posible que el administrador establezca planificaciones para archivar determinados archivos de la estación de trabajo automáticamente. En los apartados siguientes se indica cómo archivar copias sin utilizar una planificación.

Tareas relacionadas:

“Establecimiento del proceso del planificador cliente para que se ejecute como una tarea de fondo y se inicie automáticamente al arrancar” en la página 287

Archivado de datos con la GUI

Puede archivar un archivo a un grupo de archivos utilizando los nombres de archivo. Puede seleccionar los archivos que coinciden con el criterio de búsqueda utilizando un árbol de directorio.

Procedimiento

Archive los archivos mediante el siguiente procedimiento.

1. Pulse **Archivar** en la ventana principal.
2. En la ventana Archive, expanda el árbol del directorio pulsando la señal (+) más o el icono de la carpeta siguiente a un objeto en el árbol. Para buscar o filtrar los archivos, pulse en el icono **Search** desde la barra de herramientas.

3. Escriba el criterio de búsqueda en la ventana Find Files.
4. Pulse **Search**.
5. En la ventana Matching Files, pulse en las casillas de selección que están al lado de los archivos que desea archivar y cerrar la ventana Matching Files.
6. Escriba el criterio de filtrado en la ventana Find Files.
7. Pulse **Filter**. La ventana Archive muestra los archivos filtrados.
8. Pulse las casillas de selección que están al lado de los archivos filtrados o los directorios que desea archivar.
9. Escriba la descripción, acepte la descripción predeterminada o seleccione una descripción existente para el paquete de archivado en la casilla **Description**. La longitud máxima de una descripción es de 254 caracteres. Al utilizar una descripción de archivado existente, los archivos o directorios seleccionados se agregan al paquete archivado. Todos los paquetes archivados con la misma descripción se agrupan para las recuperaciones, consultas y supresiones.
10. Para modificar opciones de archivado específicas, pulse en **Options**. Cualquier opción que se cambie solo es efectiva durante la sesión actual.
11. Pulse en **Archive**. La ventana de archivado Task List muestra los estados de procesamiento de archivado.

Ejemplos de archivado de datos utilizando la línea de mandatos

Puede solicitar servicios de archivado cuando desee conservar copias de archivos en su estado actual, ya sea para utilizarlos más adelante, ya sea para fines históricos o legales. Se muestran ejemplos de archivado de datos mediante la línea de mandatos.

Puede archivar un archivo, un grupo de archivos o todos los archivos en un directorio o subdirectorio. Después de archivar un archivo, puede elegir suprimir el archivo original de la estación de trabajo.

En la tabla siguiente, figuran algunos ejemplos de la utilización del mandato **archive** para archivar objetos.

Tabla 48. Ejemplos de archivado desde la línea de mandatos

Tarea	Mandato	Consideraciones
Realizar el archivado de todos los archivos en el directorio /home/proj1 que tienen la extensión de archivo .txt.	<code>dsmc archive "/home/proj1/*.txt"</code>	Utilice caracteres comodín para archivar más de un archivo a la vez.
Archivar todos los archivos del directorio /home/jones/proj/ y borrarlos de la estación de trabajo.	<code>dsmc archive /home/jones/proj/-deletefiles</code>	Recupere las copias archivadas en la estación de trabajo siempre que las necesite de nuevo. Para obtener más información sobre la opción <code>deletefiles</code> , consulte el apartado "Deletefiles" en la página 383.

Tabla 48. Ejemplos de archivado desde la línea de mandatos (continuación)

Tarea	Mandato	Consideraciones
Archivar los archivos de /home/jones/h1.doc y /home/jones/test.doc.	dsmc archive /home/jones/h1.doc /home/jones/test.doc	Si especifica la opción removeoperandlimit con el mandato archive , el límite de 20 operandos no se aplica y sólo está limitado por los recursos disponibles u otros límites del sistema operativo. Con esta opción, puede especificar más de 20 archivos en un único mandato. Para más información sobre esta opción, consulte "Removeoperandlimit" en la página 528.
Archivar una lista de archivos en el archivo /home/avi/filelist.txt.	dsmc archive -filelist=/home/avi/filelist.txt	Utilice la opción filelist para procesar una lista de archivos. Para obtener más información, consulte "Filelist" en la página 439.
Archivar el archivo /home/jones/ch1.doc y asignarle una descripción.	dsmc archive /home/jones/ch1.doc -description="Capítulo 1, primera versión"	Si no especifica una descripción con el mandato archive , el valor predeterminado es Archive Date:x , donde x es la fecha del sistema actual. Para obtener más información sobre la opción description , consulte el apartado "Descripción" en la página 384.
Archivar todos los archivos en el directorio /home/jones/proj/ y sus subdirectorios.	dsmc archive /home/jones/proj/ -subdir=yes	Para obtener más información sobre la opción subdir , consulte el apartado "Subdir" en la página 581.
Utilice la opción v2archive con el mandato archive para archivar sólo archivos del directorio /home/relx/dir1, pero no los directorios relx o dir1.	dsmc archive "/home/relx/dir1/" -v2archive	El cliente de copia de seguridad y archivado archiva sólo las copias del directorio /home/relx/dir1. Los directorios que haya en la vía de acceso no se procesarán. Para obtener más información sobre la opción v2archive , consulte el apartado "V2archive" en la página 603.
Utilice la opción archmc con el mandato archive para especificar la clase de gestión disponible para el dominio de políticas a la que desea vincular las copias archivadas.	dsmc archive -archmc=ret2yrs /home/plan/proj1/budget.jan	Para obtener más información sobre la opción archmc , consulte el apartado "Archmc" en la página 347. Para obtener más información acerca de las clases de gestión, consulte el apartado Capítulo 9, "Políticas de gestión de almacenamiento", en la página 299.
Suponemos que ha iniciado una instantánea del sistema de archivos /usr y montado la instantánea como /snapshot/day1. Archive el árbol del directorio /usr/dir1/sub1 desde la instantánea local y gestiónela en el servidor de IBM Spectrum Protect en el nombre de espacio de archivos C:\.	dsmc archive /usr/dir1/sub1/ -subdir=yes -snapshotroot=/snapshot/day1	El cliente considera el valor de snapshotroot como el nombre del espacio de archivos. Para obtener más información, consulte "Snapshotroot" en la página 571.

Referencia relacionada:

"**Archive**" en la página 664

Asociación de una instantánea local a un espacio de archivos del servidor

Para asociar los datos de la instantánea local con los datos del espacio de archivos reales que se almacenan en el servidor de IBM Spectrum Protect, utilice la opción `snapshotroot`.

Mediante la opción `snapshotroot` con el mandato **archive** con una aplicación adquirida que proporciona una instantánea de un volumen lógico, puede asociar los datos en la instantánea local con los datos del espacio de archivos reales que se almacenan en el servidor de IBM Spectrum Protect.

No puede utilizar la opción `snapshotroot` para realizar una instantánea de volumen, pero puede utilizar la opción para gestionar los datos que se crean en una instantánea de volumen.

Referencia relacionada:

“Snapshotroot” en la página 571

Archivado de datos mediante el proxy de nodo cliente

El archivado de varios nodos que comparten almacenamiento se puede agrupar en un nombre de nodo de destino común en el servidor de IBM Spectrum Protect.

Antes de empezar

Todos los nodos agente del entorno de varios nodos deberían ser del mismo tipo de plataforma. No utilice los nodos de destino como nodos tradicionales. Utilícelos únicamente para el proceso de varios nodos.

tenga en cuenta las siguientes características de una sesión proxy:

- Una operación de proxy utiliza los valores del nodo de destino (por ejemplo, **maxnummpy deduplication**) y las planificaciones que se definen en el servidor de IBM Spectrum Protect. Los valores del nodo de servidor de IBM Spectrum Protect y las planificaciones del nodo de agente se ignoran.
- No se puede llevar a cabo una restauración o una copia de seguridad de los servicios del sistema o el estado del sistema.
- No puede acceder a otro nodo (ni desde el menú desplegable de la GUI ni utilizando la opción `fromnode`).
- No se puede llevar a cabo una copia de seguridad o una restauración de NAS.

Acerca de esta tarea

Resulta útil consolidar archivos archivados a un nombre de nodo de destino común en el servidor cuando la estación de trabajo responsable de llevar a cabo el archivado puede cambiar con el tiempo, como en el caso de un Xsan o clúster. La opción `asnodename` también permite restaurar datos desde un sistema distinto del que se utilizó para realizar la copia de seguridad. Utilice la opción `asnodename` con el mandato adecuado para hacer una copia de seguridad, archivar restaurar y recuperar datos bajo el nombre del nodo de destino del servidor de IBM Spectrum Protect. Este soporte está sólo disponible con IBM Spectrum Protect V5.3 y posterior.

También se realiza una copia de seguridad de los clientes Tivoli Storage Manager FastBack mediante el proxy de nodo de cliente.

Configurar el entorno para operaciones con el proxy es un procedimiento de varios pasos que implica definir opciones y mandatos en el cliente de archivado y copia de seguridad y en el servidor.

Procedimiento

Siga los pasos del 1 al 5 para instalar y otorgar autoridad de proxy a los nodos que pueden llevar a cabo procedimientos de archivado en nombre de otro nodo.

1. Instale el cliente de copia de seguridad/archivado en todos los nodos de un entorno de datos compartido.
2. Registre cada nodo con el servidor de IBM Spectrum Protect, si éste no existe. Registre el nombre de nodo de destino común que vaya a compartir cada uno de los nodos agente utilizado en el entorno de datos compartido.
3. Registre cada uno de los nodos en el entorno de datos compartido con el servidor de IBM Spectrum Protect. Éste es el nombre de nodo agente que se utiliza con fines de autenticación. Los datos no se almacenan con el nombre de nodo cuando se utiliza la opción `asnodename`.
4. Otorgue la autorización de proxy a todos los nodos del entorno compartido para acceder al nombre de nodo de destino en el servidor de IBM Spectrum Protect, mediante el uso del mandato `GRANT PROXYNODE` (administrador de IBM Spectrum Protect).
5. Utilice el mandato de cliente de administración `QUERY PROXYNODE` para visualizar los nodos de cliente del usuario autorizado, otorgados mediante el mandato `GRANT PROXYNODE`.

Con el paso 6 se garantiza que los archivos archivados se cifran en el servidor.

6. Establezca la opción `encryptkey` en el archivo de opciones.

Especifique `encryptkey=save` en el archivo de opciones para guardar la clave de cifrado en el archivo de contraseñas de IBM Spectrum Protect. Realice la copia de seguridad de un archivo como mínimo con `asnode=ProxyNodeName` para crear una clave de cifrado local en cada nodo agente del entorno de varios nodos.

Especifique `encryptkey=prompt` en el archivo de opciones si desea que los usuarios del nodo gestionen la clave de cifrado. Asegúrese de que los usuarios de los nodos agente del entorno de varios nodos utilicen la misma clave de cifrado.

Si cambia la clave de cifrado, deberá repetir los pasos anteriores. Utilice la misma clave de cifrado para todos los archivos de los que se haya realizado una copia de seguridad en el entorno de nodos compartido.

Lleve a cabo los pasos desde 7 hasta el paso 10 para habilitar el funcionamiento de varios nodos desde la GUI.

7. Compruebe que el nodo de cliente dispone de una autorización de proxy a un nodo de destino (o que está autorizado para actuar como nodo de destino) utilizando el mandato de cliente de administración `QUERY PROXYNODE`.
8. Seleccione **Edit > Preferences** para abrir la ventana de preferencias.
9. Seleccione la ficha **General** y rellene el campo **Como nombre de nodo** con el nombre de nodo de destino con autorización de proxy.
10. Pulse **Aplicar** y, a continuación, **Aceptar** para cerrar la ventana de preferencias.

Lleve a cabo el paso 11 en la página 274 para verificar que el nodo de cliente accede ahora al servidor como nodo de destino.

11. Abra la ventana de árbol y verifique que se visualiza el nodo de destino especificado en el campo **Como nombre de nodo**. También puede verificar que se muestra el nombre del nodo de destino en el campo **Acceso como nodo** en la ventana **Información de conexión**.
12. Opcional: Para volver a la operación de nodo único, suprima **Como nombre de nodo** del campo **Acceso como nodo** en la pestaña **General > Preferencias**.

Referencia relacionada:

“Asnodename” en la página 349

“Valores de sesión y planificaciones de una operación de proxy” en la página 350

Supresión de datos archivados

Puede eliminar los objetos de archivado individuales desde el servidor de IBM Spectrum Protect, sin tener que suprimir el espacio de archivos completos al que pertenecen.

Antes de empezar

El administrador de IBM Spectrum Protect debe concederle los permisos para suprimir los objetos archivados. Para determinar si tiene estos permisos, seleccione **File > Información de conexión** desde la GUI del cliente de copia de seguridad y archivado o desde el menú principal del cliente web. La autoridad del estado de supresión de archivado aparece en el campo Delete Archive Files. Si este campo muestra No, no puede suprimir los objetos archivados de no ser que el administrador le conceda los permisos para hacerlo.

Procedimiento

Para suprimir un objeto archivado desde el servidor, lleve a cabo estos pasos en la GUI o en el cliente web. Como una alternativa a utilizar la GUI o el cliente web, puede suprimir los objetos archivados desde la línea de mandatos mediante el mandato **delete archive**.

1. Seleccione **Suprimir datos archivados** en el menú **Herramientas**.
2. En la ventana Archive Delete, expanda el árbol del directorio pulsando en el signo más (+) o en el icono de la carpeta que está al lado del objeto que desea expandir. Los objetos del árbol están agrupados según la descripción del paquete de archivado.
3. Seleccione los objetos archivados que desea suprimir.
4. Pulse **Suprimir**. El cliente le solicitará que confirme antes de comenzar a suprimir los objetos seleccionados. La ventana Archive Delete Task List muestra el progreso de la operación de supresión.

Referencia relacionada:

“Delete Archive” en la página 693

Tareas de archivado avanzadas

Los permisos de acceso, los enlaces simbólicos y los enlaces fijos son funciones avanzadas que deberá tener en cuenta al archivar datos.

Permisos de acceso

Al archivar un archivo, el cliente guarda los permisos de acceso estándares de UNIX asignados al archivo.

En función del sistema operativo, también guarda permisos ampliados. Por ejemplo, para archivos de una estación de trabajo AIX, el cliente guarda listas de control de accesos.

Si usted es un usuario y archiva un archivo para el que dispone de acceso de lectura, pasa a ser el propietario de la copia del archivo. Usted es el único usuario que puede recuperar el archivo archivado a menos que otorgue acceso a otro usuario.

Archivar y recuperar enlaces simbólicos

El cliente de copia de seguridad y archivado archiva y recupera los vínculos simbólicos de forma distinta a como maneja los directorios y archivos normales.

La manera en la que el cliente archiva y recupera los enlaces simbólicos depende de la configuración de las opciones, de la posibilidad de acceder o no al directorio de destino y de la forma de especificación de los objetos.

Un *enlace simbólico UNIX* es un archivo que contiene un puntero a otro archivo o directorio. El objeto al que señala el vínculo simbólico se denomina *objeto de destino*.

Se puede realizar una copia de seguridad de un enlace simbólico como información de la vía de acceso a un directorio de destino o como un directorio. Si se realiza una copia de seguridad del enlace simbólico como un directorio, también se podrá hacer una copia de seguridad de los archivos y carpetas de ese directorio de destino.

La forma de realizar la copia de seguridad del vínculo determina los elementos y el ámbito de la restauración, la configuración de la opción `followsymbolic` y la posibilidad de acceder al directorio de destino en el momento de la restauración.

Para obtener más información sobre cómo se manejan los vínculos simbólicos durante una operación de archivado, consulte la opción `archsymb linkasfile`.

Nota: el proceso de los enlaces simbólicos que se describe en este apartado no es aplicable a Mac OS X. El archivado de los enlaces simbólicos se hace siempre como archivos y nunca se siguen.

En la tabla siguiente se muestran las funciones de recuperación y archivado de los vínculos simbólicos y la acción que se lleva a cabo:

Tabla 49. Tabla de gestión de vínculos simbólicos para archivado y recuperación

Función	Acción efectuada
Archivado de un vínculo de archivo.	Archiva el archivo al que hace referencia el vínculo simbólico.
Archivado de un vínculo de directorio.	Archiva el directorio y el contenido de éste.
Archivado de un archivo con <code>subdir=yes</code> .	Archiva el archivo, la vía de acceso del directorio y todos los archivos con nombre parecido en el subárbol.
Archivado de un directorio con <code>subdir=yes</code> .	Archiva el directorio y el contenido de éste y de sus subdirectorios.
Archivado de un vínculo simbólico que hace referencia a un archivo o directorio que no existe.	Archiva el vínculo simbólico.

Tabla 49. Tabla de gestión de vínculos simbólicos para archivado y recuperación (continuación)

Función	Acción efectuada
Recuperación de un vínculo simbólico que hace referencia a un archivo; el archivo y el vínculo existen.	Sustituye el archivo si se ha establecido <code>replace=y</code> .
Recuperación de un vínculo simbólico que hace referencia a un archivo; el vínculo simbólico ya no existe.	Recupera el archivo sustituyendo el nombre del archivo por el nombre del vínculo simbólico y lo coloca en el directorio en el que reside el vínculo simbólico.
Recuperación de un vínculo simbólico que hace referencia a un directorio; el vínculo simbólico y el directorio ya no existen.	Se crea un directorio en el directorio en el que reside el vínculo simbólico y se restauran todos los archivos y subdirectorios en ese directorio. El nombre del vínculo simbólico se utiliza como el nuevo nombre de directorio.
Recuperación de un vínculo simbólico que hace referencia a un directorio; el vínculo simbólico y el directorio todavía existen.	El directorio no se recupera mientras exista el vínculo simbólico.

Referencia relacionada:

“Archsymlinkasfile” en la página 348

Enlaces fijos

Cuando archive copias que tienen un enlace fijo, el cliente de copia de seguridad y archivado archivará cada instancia del archivo enlazado.

Por ejemplo, si archiva dos copias que tienen un enlaces fijos, el cliente archiva los datos por duplicado.

Cuando se recuperan archivos con vínculo fijo, el cliente restablece los vínculos. Por ejemplo, si se había establecido un vínculo fijo entre dos archivos y solo se encuentra uno en su estación de trabajo, al recuperar ambos archivos habrá un vínculo fijo entre los dos. La única excepción de este procedimiento se da cuando se archivan dos archivos entre los que hay un vínculo fijo y se interrumpe la conexión entre estos en la estación de trabajo. Si recupera los dos archivos desde el servidor, el cliente respeta el sistema de archivos actual y no recupera el vínculo fijo.

Consejo: Si no archiva y recupera al mismo tiempo todos los archivos que tienen vínculos fijos, pueden producirse problemas. Para garantizar que los archivos con enlaces fijos permanecen sincronizados, archive y recupere todos los enlaces fijos al mismo tiempo.

Recuperar archivos

Recupere un archivo cuando desee devolver una copia archivada del servidor a la estación de trabajo.

Muchas de las consideraciones avanzadas para la recuperación de archivos son las mismas que las de restauración.

Importante: Cuando recupera un archivo sin especificaciones y existe más de una versión de la copia archivada en el servidor, el cliente recupera todas las copias.

Una vez recuperada la primera copia, se recupera la segunda. Si existe una copia en la estación de trabajo cliente, se le solicitará que la sustituya, la omita o cancele.

Conceptos relacionados:

“Restaurar o recuperar archivos en otra estación de trabajo” en la página 266

Tareas relacionadas:

“Cómo autorizar a otro usuario para que restaure o recupere archivos” en la página 264

“Restauración o recuperación de archivos de otro nodo cliente” en la página 265

Recuperación de datos con la GUI

Puede recuperar un archivo archivado con la GUI.

Procedimiento

1. Pulse **Retrieve** desde el cliente de la ventana principal de la GUI de Java. Aparece la ventana Retrieve.
2. Expanda el árbol de directorios pulsando el signo más (+) o el icono de carpeta junto a un objeto que desee expandir. Para buscar o filtrar los archivos, pulse en el icono **Search** desde la barra de herramientas.
3. Escriba el criterio de búsqueda en la ventana Find Files.
4. Pulse **Search**. Aparece la ventana Matching Files.
5. Pulse en las cajas de selección que aparecen al lado de los archivos que desea recuperar y cierre la ventana Matching Files.
6. Escriba el criterio de filtrado en la ventana Find Files.
7. Pulse **Filter**. La ventana Retrieve muestra los archivos filtrados.
8. Pulse las casillas de selección de los archivos filtrados o directorios que desea recuperar.
9. Para modificar o recuperar opciones específicas, pulse **Options**. Cualquier opción que cambie será eficaz solo durante la sesión actual.
10. Pulse **Retrieve**. Aparece la ventana Retrieve Destination. Escriba la información apropiada en la ventana Retrieve Destination.
11. Pulse **Retrieve**. La ventana Task List muestra el estado de recuperación del proceso.

Recupere los ejemplos de datos utilizando la línea de mandatos

Puede recuperar un archivo, un grupo de archivos o todos los archivos de un directorio o subdirectorio.

Cuando recupere un archivo, el servidor IBM Spectrum Protect le enviará una copia del mismo. La copia archivada permanece en el almacenamiento.

Utilice el mandato **retrieve** para recuperar archivos del almacenamiento de la estación de trabajo. En la tabla siguiente, figuran algunos ejemplos de la utilización del mandato **retrieve**.

Tabla 50. Ejemplos de recuperación de archivos desde la línea de mandatos

Tarea	Mandato	Consideraciones
Recuperar el archivo /home/jones/h1.doc en su directorio original.	dsmc retrieve /home/jones/h1.doc	Si no especifica un destino, los archivos se recuperan en su ubicación original.

Tabla 50. Ejemplos de recuperación de archivos desde la línea de mandatos (continuación)

Tarea	Mandato	Consideraciones
Recuperar el archivo /home/jones/h1.doc con un nuevo nombre y en otro directorio.	dsmc retrieve /home/jones/h1.doc /home/smith/h2.doc	Ninguna.
Recuperar todos los archivos del directorio /home/jones que terminen con los caracteres .bak en el directorio /home/smith.	dsmc retrieve "/home/jones/*.bak" /home/smith/	Ninguna.
Recuperar el archivo /home/jones/ch1.doc y asignar una descripción.	dsmc retrieve /home/jones/ch1.doc -description="Capítulo 1, primera versión"	Si no realiza una descripción con el mandato retrieve , el valor predeterminado será Retrieve Date:x, donde x será la fecha actual del sistema.
Utilizar la opción pick para ver una lista de copias archivadas en la que puede seleccionar los archivos que desea recuperar.	dsmc retrieve "/home/jones/*" -pick	Ninguna.
Recuperar una lista de archivos que se han especificados en el archivo retrievelist.txt y colocarlos en su directorio original.	dsmc retrieve -filelist=/home/dir2/retrievelist.txt	Ninguna.

Referencia relacionada:

“Retrieve” en la página 770

“Descripción” en la página 384

“Filelist” en la página 439

“Pick” en la página 512

Archivar clases de gestión

El cliente de copia de seguridad y archivado comprueba las opciones include de la lista de opciones de inclusión/exclusión para determinar la clase de gestión que debe asignar a los archivos archivados.

Si no asigna una clase de gestión a un archivo mediante la opción include, el cliente asigna al archivo la clase de gestión predeterminada. El cliente puede archivar solo un archivo si la clase de gestión seleccionada contiene un grupo de copia de archivado.

Puede sobrescribir la clase de gestión predeterminada utilizando la opción **archmc** o si pulsa en **Options** en la ventana Archive de la GUI, pulsando en **Override include/exclude list**, y después seleccionando las clases de gestión.

También puede añadir sentencias de inclusión/exclusión la GUI Java del cliente de copia de seguridad y archivado o en árbol de directorios del cliente web. Después, puede utilizar la función de **Utilities Preview Include-Exclude** para obtener la vista previa de la lista de inclusión/exclusión antes de enviar los datos al servidor.

Conceptos relacionados:

“Asignar una clase de gestión a los archivos” en la página 306

“Visualizar información sobre clases de gestión y grupos de copia” en la página 301

Referencia relacionada:

"Preview Archive" en la página 715

"Previsualizar copia de seguridad" en la página 716

Capítulo 7. Visión general del planificador de IBM Spectrum Protect

El planificador central de IBM Spectrum Protect permite llevar a cabo automáticamente operaciones en los plazos especificados.

Para entender la planificación con IBM Spectrum Protect, es necesario definir varios términos:

definición de planificación

Una definición de planificación en el servidor de IBM Spectrum Protect especifica las propiedades críticas de una actividad automatizada, incluyendo el tipo de acción, la hora en la que debe llevarse a cabo la acción y la frecuencia de la misma. Se pueden definir otras varias propiedades de una planificación. Para obtener información sobre **DEFINE SCHEDULE**, consulte la documentación del servidor de IBM Spectrum Protect.

asociación de planificación

Una asociación de planificación es una asignación de un nodo cliente a una definición de planificación específica. Varias asociaciones de planificación permiten que muchos nodos clientes puedan utilizar definiciones de planificación individuales. Puesto que las definiciones de planificaciones están incluidas en dominios de políticas concretos, sólo es posible asociar los nodos definidos para cierto dominio de políticas con las planificaciones definidas dentro de ese dominio.

evento planificado

Un evento planificado es un caso específico del momento en que se ejecuta una planificación para un nodo. Para que los eventos planificados automáticos tengan lugar para un cliente, deben satisfacerse las siguientes condiciones:

- Debe existir una definición de planificación para un dominio de políticas específico.
- Debe existir una asociación de planificación para el nodo requerido, que pertenece a dicho dominio de políticas.
- El proceso del planificador cliente debe estar ejecutándose en el sistema cliente.

Al crear una definición de planificación en el servidor de IBM Spectrum Protect, las acciones de planificación que se pueden llevar a cabo son: incremental, selective, archive, restore, retrieve, image backup (no se aplica a Mac OS X), image restore (no se aplica a Mac OS X), command y macro. La acción planificada que se utiliza más frecuentemente es incremental con el parámetro **objects** sin definir. Con este valor, el cliente de archivado y copia de seguridad realiza una copia de seguridad incremental del dominio de todas los sistemas de archivo definidos mediante la opción de dominio del cliente. Una definición de planificación mediante la acción **command** permite que se ejecute un mandato del sistema operativo o un script del shell. Al automatizar tareas para los clientes de IBM Spectrum Protect for Data Protection, se deben utilizar las definiciones de planificación de las acciones de **command**, que invocan a las herramientas de línea de mandatos de esas aplicaciones.

El *intervalo de inicio* de la planificación indica el período de tiempo aceptable para que se inicie un evento planificado. El intervalo de inicio se define mediante estos parámetros de definición de planificación: **startdate**, **starttime**, **durunits** y **duration**. Las opciones **startdate** y **starttime** definen el principio del intervalo de inicio para el primer evento planificado. El principio de los intervalos de inicio para eventos planificados posteriores varía según los valores de **period** y **perunit** de la definición de planificación. Los parámetros **duration** y **durunits** definen la duración de la ventana de inicio. La acción de planificación debe empezar obligatoriamente dentro del intervalo de inicio. Para ilustrarlo, considere los resultados de la siguiente definición de planificación:

```
define schedule standard test1 action=incremental starttime=12:00:00 period=1
perunits=hour dur=30 duru=minutes
```

Evento	Inicio de ventana	Fin de ventana	Inicio real (es sólo un ejemplo, las horas varían)
1	12:00:00	12:30:00	12:05:33
2	13:00:00	13:30:00	13:15:02
3	14:00:00	14:30:00	14:02:00
etcétera			

La variación en las horas de inicio reales es el resultado de la característica de aleatorización que proporciona el planificador central de IBM Spectrum Protect que ayuda a equilibrar la carga de las sesiones planificadas en el servidor de IBM Spectrum Protect.

Ejemplos: manejo de espacios en blanco en nombres de archivos de definiciones de planificación

Al definir o actualizar un parámetro **objects** de planificación o el parámetro **options** de planificación con especificaciones de archivos que contienen espacios en blanco, especifique entre comillas dobles (") cada especificación de archivo que contenga espacios en blanco y entre comillas simples (') todas las especificaciones.

Los siguientes ejemplos muestran como delimitar parámetros **object** de planificación cuando las especificaciones de archivo contienen caracteres de espacio:

```
objects="/home/proj1/Some file.doc"
objects="/home/proj1/Some file.doc" "/home/Another file.txt" /home/noblanks.txt'
objects="/home/My Directory With Blank Spaces/"
objects="/Users/user1/Documents/Some file.doc"
objects="/Users/user1/Documents/Some file.doc"
"/Users/user5/Documents/Another file.txt" /Users/user3/Documents/noblanks.txt'
objects="/Users/user1/My Directory With Blank Spaces/"
```

Esta sintaxis garantiza que las especificaciones de archivo que contengan un espacio, como /home/proj1/Some file.doc, se traten como un solo nombre de archivo, en vez de como dos archivos distintos (/home/proj1/Some y file.doc).

Los siguientes ejemplos muestran como delimitar parámetros **options** de planificación cuando las especificaciones de archivo contienen caracteres de espacio:

```
options='-preschedulecmd="/home/me/my files/bin/myscript"
-postschedulecmd="/home/me/my files/bin/mypostsript" -quiet'
options='-presched="/home/me/my files/bin/precmd" -postsched=finish'
```

También puede consultar la información de los parámetros **objects** y **options** de los mandatos **DEFINE SCHEDULE** y **UPDATE SCHEDULE**. Para obtener descripciones de estos mandatos y sus parámetros, consulte la documentación del servidor de IBM Spectrum Protect.

Conceptos relacionados:

“Especificación de cadenas de entrada que contengan espacios en blanco o comillas” en la página 145

Horas de inicio preferentes para determinados nodos

Puede que, de vez en cuando, desee asegurarse de que un nodo en particular inicia la actividad que se ha planificado para éste a una hora lo más cercana posible a la hora de inicio definida de la planificación. Esta necesidad suele darse cuando se utiliza la planificación en modalidad de petición.

En función del número de nodos cliente asociados a la planificación y en qué lugar de la secuencia de petición se encuentra el nodo, es posible que el nodo reciba la petición considerablemente más tarde que la hora de inicio de la planificación.

En este caso, puede realizar los siguientes pasos:

1. Copie la planificación en una nueva planificación con un nombre distinto (o defina una nueva planificación con los atributos preferidos)
2. Establezca el nuevo atributo de prioridad de planificación de modo que tenga una prioridad más alta que la planificación original.
3. Suprima la asociación entre el nodo y la planificación original y luego asocie el nodo a la nueva planificación.

Ahora el servidor de IBM Spectrum Protect procesa primero la nueva planificación.

Opciones de proceso de planificador

Las opciones de proceso del planificador determinan las operaciones que se llevan a cabo cuando se inicia un trabajo del planificador.

Puede definir la mayoría de estas opciones de proceso del planificador en el archivo de opciones del cliente. No obstante, algunas de estas opciones se pueden definir en el servidor de IBM Spectrum Protect, de forma que afecten a todos los clientes.

En la tabla siguiente se muestran las opciones definidas por el cliente y las del servidor y cuáles sobrescribe el servidor. Una X en una columna indica dónde se puede especificar la opción.

Opción	Cliente definido	Servidor definido	Modificación global de servidor
manageservices	X		
maxcmdretries	X		Mandato SET MAXCMDRETRIES
maxschedsessions		X	
postschedulecmd, postnschedulecmd	X		
preschedulecmd, prenschedulecmd	X		

Opción	Cliente definido	Servidor definido	Modificación global de servidor
querschedperiod	X		Mandato SET QUERSCHEDPERIOD
randomize		X	
retryperiod	X		Mandato SET RETRYPERIOD
schedcmddisabled	X		
schedlogname	X		
schedlogretention	X		
schedmode	X		Mandato SET SCHEDMODES
sessioninitiation	X	X	Mandato UPDATE NODE
tcpclientaddress	X	X (también se define en el servidor cuando sessioninit=serveronly como parte de la definición de nodo)	
tcpclientport	X	X (también se define en el servidor cuando sessioninit=serveronly como parte de la definición de nodo)	

Las definidas por el cliente se definen en el archivo `dsm.sys` o `dsm.opt`. El servidor de IBM Spectrum Protect también puede definir algunas opciones en un archivo de opciones del cliente o como parte del parámetro de opciones de la definición de la planificación. El servidor de IBM Spectrum Protect también puede establecer globalmente algunas opciones para todos los clientes. De forma predeterminada, se respeta el valor del cliente para estas opciones. Si se establece la modificación global en el servidor de IBM Spectrum Protect, se ignora el valor del cliente para la opción. La definición de opciones del cliente como parte de la definición de la planificación es útil si desea utilizar opciones específicas para una acción planificada que difiere de los valores de la opción que el nodo cliente utiliza normalmente o que son distintas para cada planificación que el nodo ejecuta.

La opción `schedmode` controla la interacción de las comunicaciones entre el servidor y cliente de IBM Spectrum Protect. La modalidad de planificación ofrece dos variantes: *sondeo de cliente* y *por solicitud del servidor*. Estas variantes se explican en la documentación del servidor de IBM Spectrum Protect.

Evaluar códigos de retorno de planificación en scripts de planificación

Puede utilizar variables de entorno para determinar el código de retorno de IBM Spectrum Protect actual antes de ejecutar un script utilizando las opciones de cliente `preschedulecmd` o `postschedulecmd`.

IBM Spectrum Protect proporciona el valor actual del código de retorno en la variable de entorno denominada `TSM_PRE_CMD_RC`. La variable `TSM_PRE_CMD_RC` es el valor actual del código de retorno de IBM Spectrum Protect antes de ejecutar un script de planificación. El valor de la variable `TSM_PRE_CMD_RC` no es necesariamente el mismo que el código de retorno emitido por IBM Spectrum Protect tras la ejecución del script de planificación. La variable `TSM_PRE_CMD_RC` se puede utilizar en scripts de planificación para determinar el estado actual de la planificación.

La variable `TSM_PRE_CMD_RC` se establece en cada una de las siguientes opciones de planificación: `preschedule`, `prenschedule`, `postschedule` y `postnschedule`. `TSM_PRE_CMD_RC` afecta a las planificaciones que tienen especificada la opción `ACTION=COMMAND`.

Un ejemplo de la variable `TSM_PRE_CMD_RC` que se está utilizando:

```
if [[ -n ${TSM_PRE_CMD_RC} ]] ; then

    if [[ ${TSM_PRE_CMD_RC} == 0 ]] ; then
        echo "The TSM_PRE_CMD_RC is 0"

    elif [[ ${TSM_PRE_CMD_RC} == 4 ]] ; then
        echo "The TSM_PRE_CMD_RC is 4"

    elif [[ ${TSM_PRE_CMD_RC} == 8 ]] ; then
        echo "The TSM_PRE_CMD_RC is 8"

    elif [[ ${TSM_PRE_CMD_RC} == 12 ]] ; then
        echo "The TSM_PRE_CMD_RC is 12"
    else
        echo "The TSM_PRE_CMD_RC is an unexpected value: ${TSM_PRE_CMD_RC}"
    fi

else
    echo "The TSM_PRE_CMD_RC is not set"
fi
```

Códigos de retorno de los scripts `preschedulecmd` y `postschedulecmd`

Se describen los códigos de retorno que puede ver al utilizar las opciones `preschedulecmd` y `postschedulecmd`.

- Si el mandato especificado por la opción `preschedulecmd` finaliza con un código de retorno distinto de cero, IBM Spectrum Protect supone que el mandato ha fallado. En este caso, no se puede ejecutar el suceso planificado ni ningún mandato `postschedulecmd` o `postnschedulecmd`. El mandato de administración **query event** con la opción `format=detailed` muestra que el evento no se ha realizado satisfactoriamente con el código de retorno 12.
- Si el mandato especificado por la opción `postschedulecmd` finaliza con un código de retorno distinto de cero, IBM Spectrum Protect considera que el mandato ha fallado. El mandato administrativo **query event** con la opción `format=detailed`

muestra que el suceso se ha completado con el código de retorno 8. La excepción es si la operación planificada se ha completado con un código de retorno más alto, en cuyo caso tiene prioridad el código de retorno más alto. Por lo tanto, si la operación planificada finaliza con el código de retorno 0 o 4 y el mandato `postschedulecmd` no se realiza satisfactoriamente, el mandato de administración **query event** muestra que el evento se ha completado con el código de retorno 8. Si la operación planificada finaliza con el código de retorno 12, dicho código de retorno prevalece y **query event** muestra que el evento no se ha realizado satisfactoriamente con el código de retorno 12.

Al interpretar el código de retorno desde un mandato, IBM Spectrum Protect considera que 0 significa éxito y cualquier otro valor significa anomalía. Aunque este comportamiento se acepta ampliamente en el sector, no se garantiza al 100%. Por ejemplo, el desarrollador del mandato del widget puede finalizar con un código de retorno 3, si el widget se ha ejecutado correctamente. Por consiguiente, es posible que el mandato `preschedulecmd` o `postschedulecmd` finalice con un código de retorno distinto de cero y sea a pesar de ello satisfactorio. Para evitar que IBM Spectrum Protect trate dichos mandatos como anómalos, puede incluir estos mandatos en un script y codificar el script de modo que interprete los códigos de retorno de mandato correctamente. El script sale con el código de retorno 0 si el mandato se ha ejecutado satisfactoriamente; de lo contrario, sale con un código de retorno distinto de cero. La lógica para un script que ejecuta el widget puede tener el mismo aspecto que este ejemplo:

```
run 'widget'
  if lastcc == 3
    exit 0
  else
    exit 1
```

Referencia relacionada:

“`Postschedulecmd/Postnschedulecmd`” en la página 514

“`Preschedulecmd/Prenschedulecmd`” en la página 517

Servicios del planificador de aceptación de clientes frente a los servicios del planificador tradicional

Puede configurar el cliente de IBM Spectrum Protect para gestionar el proceso de planificador utilizando el daemon de aceptación de cliente de IBM Spectrum Protect.

El daemon de aceptación de clientes proporciona un temporizador sencillo que inicia y detiene automáticamente el proceso del planificador cuando resulta necesario. Si no, el método tradicional mantiene el proceso del planificador de IBM Spectrum Protect ejecutándose continuamente. En general, el método preferido para gestionar el planificador es utilizar el daemon de aceptación de clientes.

La información a continuación es una comparación de los métodos de servicios gestionados por el daemon de aceptación de clientes y los servicios del planificador tradicional.

Servicios gestionados por el daemon de aceptación de clientes

- Se definen mediante la utilización de la opción `managedservices schedule` y se inician con los servicios del daemon de aceptación de clientes (`dsmcad`).
- El daemon de aceptación de clientes inicia y detiene el proceso del planificador cuando sea necesario para cada acción planificada.

- Requiere menos recursos del sistema cuando está desocupado.
- Las opciones del cliente de IBM Spectrum Protect y las opciones de modificación del servidor de IBM Spectrum Protect se renuevan cada vez que los servicios del daemon de aceptación de clientes inician una copia de seguridad planificada.
- No pueden utilizarse con copias de seguridad
SESSIONINITiation=SERVEROnly.

Servicios del planificador tradicional de IBM Spectrum Protect

- Se inician con el mandato `dsmc sched`.
- Permanecen activos, incluso después de finalizar la copia de seguridad planificada.
- Requieren un mayor uso de los recursos del sistema cuando está desocupado.
- Las opciones del cliente de IBM Spectrum Protect y las opciones de sustitución del servidor de IBM Spectrum Protect sólo se procesan una vez cuando se inicia `dsmc sched`; si elimina una opción de un conjunto de opciones de cliente, debe reiniciar el planificador para que este esté al tanto de la supresión

Recomendación: reinicie el planificador tradicional periódicamente para liberar los recursos del sistema que las llamadas al sistema han utilizado anteriormente.

Establecimiento del proceso del planificador cliente para que se ejecute como una tarea de fondo y se inicie automáticamente al arrancar

Puede configurar el planificador del cliente de IBM Spectrum Protect para que se ejecute como una tarea de fondo del sistema que se inicie automáticamente al arrancar el sistema.

Acerca de esta tarea

Puede completar esta tarea tanto si utiliza el aceptador de clientes para gestionar el planificador como si utiliza el método tradicional para iniciar el planificador del cliente del planificador.

Cuando ejecute una planificación gestionada por el aceptador de clientes, establezca el proceso del aceptador de clientes para que se inicie automáticamente en el momento del arranque; no utilice el proceso del planificador. En el método tradicional, establezca el proceso del planificador para que se inicie automáticamente al arrancar.

Puede configurar el aceptador de clientes para que se ejecute como una tarea de fondo del sistema que se inicie automáticamente al arrancar el sistema. Para configurar el aceptador de clientes para que gestione copias de seguridad planificadas, utilice la opción `managedservices` para especificar si el cliente gestiona únicamente el planificador, únicamente el cliente web o ambos. El método para establecer el aceptador de clientes como una tarea del sistema varía en cada plataforma.

Para que el planificador se inicie de forma desatendida, debe permitir al cliente almacenar su contraseña estableciendo la opción `passwordaccess` en **generate** y almacenar la contraseña ejecutando un mandato simple de cliente como `dsmc query`

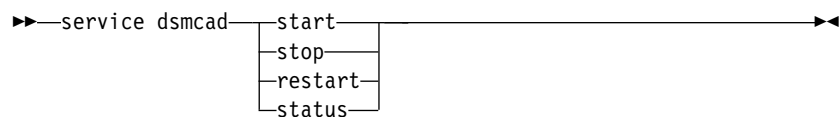
session. Para fines de prueba, siempre puede iniciar el planificador en primer plano ejecutando `dsmc sched` desde un indicador de mandatos (sin definir ninguna sección `managedservices`).

Para iniciar el planificador automáticamente durante el arranque, utilice el método gestionado por el aceptador de clientes o el método tradicional.

Método gestionado por el aceptador de clientes

1. En el archivo `dsm.sys`, establezca la opción `managedservices` en **`schedule`** o **`schedule webclient`**.
2. Inicie el aceptador de clientes.
 - a. En clientes AIX y Solaris, añada la entrada siguiente al archivo de inicio del sistema (`/etc/inittab` en la mayoría de las plataformas):


```
tsm::once:/usr/bin/dsmcad > /dev/null 2>&1 # TSM Client
          Acceptor Daemon
```
 - b. En los clientes Linux, el programa de instalación creará un script de inicio para el aceptador de clientes (`dsmcad`) en `/etc/init.d`. El aceptador de clientes (`dsmcad`) debe iniciarse antes de poder gestionar tareas de planificador o gestionar el cliente web. Como root, utilice el siguiente mandato para iniciar, detener o reiniciar el aceptador de clientes o para comprobar su estado:



Para permitir que el aceptador de clientes se inicie automáticamente tras arrancar el sistema, agregue el servicio como sigue, cuando se lo indique el shell:

```
# chkconfig --add dsmcad
```

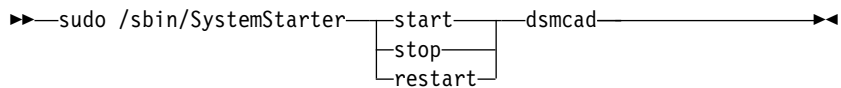
Si el sistema operativo Linux ejecuta el servicio de inicialización `systemd`, siga estos pasos para iniciar `dsmcad` y ejecutarlo durante el inicio del sistema:

- 1) Copie el archivo de unidad de `systemd` `/opt/tivoli/tsm/client/ba/bin/dsmcad.service` en el directorio `/etc/systemd/system/`.
- 2) Ejecute el siguiente mandato para renovar la lista de unidades `systemd`:


```
systemctl daemon-reload
```
- 3) Ejecute el mandato siguiente para iniciar el aceptador de clientes al arrancar el sistema:


```
systemctl enable dsmcad.service
```
- 4) Ejecute el mandato siguiente para iniciar el aceptador de clientes:


```
systemctl start dsmcad.service
```
- c. En Mac OS X, el aceptador de clientes debe instalarse como elemento de inicio. Para instalar e iniciar el aceptador de clientes, un administrador del sistema debe utilizar las Herramientas para administradores de IBM Spectrum Protect. Para iniciar, detener o reiniciar el aceptador de clientes, utilice el siguiente mandato:



3. En el archivo `dsm.sys`, establezca la opción `passwordaccess` en **generate**.
4. Ejecute un mandato como `dsmc query sess` para almacenar la contraseña de nodo.

Método tradicional:

1. Establezca la opción `managedservices`.
 - En clientes AIX, Linux y Solaris, elimine la opción en su totalidad (el valor predeterminado es **webclient**) o establézcala en **webclient**.
 - En clientes Mac OS X, establezca la opción `managedservices` en **webclient** o **none**. No establezca la opción en `schedule`.
2. En AIX, Linux y Solaris, añada la entrada siguiente en el archivo de inicio del sistema, por ejemplo, `/etc/inittab`, si está admitido:
`tsmsched::once:/usr/bin/dsmc sched > /dev/null 2>&1 # TSM scheduler`
3. En el archivo `dsm.sys`, establezca la opción `passwordaccess` en **generate**.
4. Ejecute un mandato como `dsmc query sess` para almacenar la contraseña de nodo.
5. Para iniciar el planificador cliente en el nodo cliente y conectarlo al planificador del servidor, escriba el siguiente mandato:

```
dsmc schedule
```

Si el directorio actual no está en la variable de entorno `PATH`, escriba el siguiente mandato:

```
./dsmc schedule
```

Cuando inicie el planificador de cliente, éste se ejecutará continuamente hasta que cierre la ventana, finalice el proceso o cierre la sesión del sistema.

Para ejecutar el mandato **schedule** en segundo plano y seguir ejecutando el planificador de cliente, incluso si finaliza la sesión del sistema, entre el mandato siguiente:

```
nohup dsmc schedule 2> /dev/null &
```

Referencia relacionada:

“`Cadlistenonport`” en la página 362

Ejemplos: visualización de información sobre trabajo planificado

Las planificaciones pueden ser clásicas o ampliadas, según como se haya definido el intervalo de la siguiente ejecución.

Las planificaciones clásicas permiten que el período de tiempo sea de como máximo una hora. Las planificaciones ampliadas permiten que las acciones se ejecuten en unos determinados días.

Para visualizar las planificaciones definidas para el nodo cliente, entre:

```
dsmc query schedule
```

El cliente de copia de seguridad y archivado muestra información detallada sobre todos los trabajos planificados del nodo cliente. En la Tabla 51 se visualiza un ejemplo de la salida clásica de **query schedule**.

Tabla 51. Ejemplo de la salida clásica de query schedule

Nombre de planificación:	DAILY_INC
Descripción:	Copia de seguridad diaria de todo el sistema
Estilo de planificación:	Clásico
Action:	Incremental
Opciones:	QUIET
Objetos:	
Prioridad:	1
Próxima ejecución:	30 minutos
Duración:	4 horas
Período:	1 día
Día de la semana:	Cualquiera
Mes:	
Día de la semana:	
Semana del mes:	
Caduca:	Nunca
Nombre de planificación:	WEEKLY_INC
Descripción:	Copia de seguridad semanal para archivos proyecto
Estilo de planificación:	Clásico
Action:	Incremental
Opciones:	QUIET
Objetos:	/proj
Prioridad:	1
Próxima ejecución:	60 minutos
Duración:	8 horas
Período:	7 días
Día de la semana:	viernes
Mes:	
Día de la semana:	
Semana del mes:	
Caduca:	Nunca

La planificación denominada **WEEKLY_INC** inicia una copia de seguridad incremental semanal en el sistema de archivos /proj.

La planificación denominada **DAILY_INC** inicia una copia de seguridad incremental diaria. La copia de seguridad incremental siguiente se inicia transcurridos 30 minutos. Como no se listan objetos, el cliente ejecuta la copia de seguridad incremental en el dominio predeterminado. La planificación no tiene fecha de caducidad.

Para determinar de forma más precisa el estado de los sucesos planificados, la salida del mandato **query schedule** de una planificación ampliada, en clientes de IBM Spectrum Protect versión 5.3 y posteriores, incluye campos nuevos. Estos campos aparecen siempre, tanto si se trata de una planificación clásica como de una sesión de cliente de la versión 5.3 con un servidor de una versión anterior a la 5.3, pero los campos nuevos estarán vacíos. Tenga en cuenta que para un cliente de nivel inferior (anterior a la versión 5.3), el servidor informa de los períodos como indefinidos y el día de la semana es como un día no permitido. En la Tabla 52 en la página 291 se muestra un ejemplo de la salida ampliada de **query schedule**.

Tabla 52. Ejemplo de salida ampliada del mandato query schedule

Nombre de planificación:	QUARTERLY_FULL
Descripción:	Copia de seguridad completa trimestral
Estilo de planificación:	Ampliado
Acción:	Selectiva
Opciones:	subdir=yes
Objetos:	/* /Volumes/fs2/*
Prioridad:	5
Próxima ejecución:	1744 horas y 26 minutos
Duración:	1 Día
Período:	
Día de la semana:	viernes
Mes:	marzo, junio, septiembre, diciembre
Día del mes:	Cualquiera
Semana del mes:	Última
Caduca:	Nunca

Visualizar información sobre el trabajo completado

Al ejecutar el mandato **schedule** en primer plano, aparece en pantalla la salida de los mandatos planificados.

La salida también se dirige al archivo dsmsched.log en el directorio de instalación a menos que modifique el nombre de directorio y de archivo mediante la opción schedlogname .

Cuando se ejecuta el mandato **schedule** como proceso de fondo, la salida de los mandatos planificados se dirige al archivo dsmsched.log del directorio actual, o a la vía de acceso y el nombre de archivo que se han especificado. El archivo dsmsched.log no puede ser un vínculo simbólico.

Nota: En Mac OS X, se puede encontrar el registro por defecto en una de estas ubicaciones:

```
~/Library/Logs/tivoli/tsm
/Library/Logs/tivoli/tsm
```

Una vez realizado el trabajo planificado, compruebe las anotaciones de planificación para verificar que todo el trabajo ha acabado correctamente.

Cuando se procesa un mandato planificado, las anotaciones de planificación contienen las entradas siguientes:

El evento planificado *nombreevento* finalizó satisfactoriamente

Si el evento planificado no se ha completado correctamente, recibirá un mensaje similar al siguiente:

ANS1512E El evento planificado *nombre_evento* ha fallado. Código de retorno = *código*.

El cliente indica si IBM Spectrum Protect ha emitido correctamente el mandato planificado que se asocia a *nombre_evento* (action=command). No se intenta determinar el motivo de la ejecución correcta o incorrecta del mandato. Puede averiguar el estado del mandato evaluando el código de retorno del mandato planificado de las anotaciones de planificación. La entrada de las anotaciones de planificación correspondiente al código de retorno del mandato está precedida del texto siguiente:

Mandato finalizado. El código de retorno es:

El tamaño de las anotaciones de planificación sigue aumentando, a menos que puede éstas mediante la utilización de la opción `shedlogretention` o especifique un tamaño máximo mediante la utilización de la opción `shedlogmax`.

Conceptos relacionados:

“Especificar opciones de planificación”

Especificar opciones de planificación

Puede modificar las opciones de planificación en el archivo de opciones del cliente o la interfaz gráfica de usuario (GUI).

Sin embargo, si el administrador especifica un valor para estas opciones, ese valor prevalece sobre el valor en el cliente.

Conceptos relacionados:

“Opciones de planificación” en la página 330

Opciones del planificador para los mandatos

El planificador ejecuta mandatos con un identificador de usuario de 0 (root); sin embargo, es posible que algunos mandatos deban ejecutarse con un identificador de usuario que no sea 0.

En este caso, el administrador de IBM Spectrum Protect puede definir planificaciones para mandatos que se ejecutan con un identificador de usuario diferente al identificador de usuario del planificador mediante la opción de servidor `shedcmduser`.

La opción `shedcmduser` especifica el nombre de un usuario válido del sistema en el que se ejecuta un mandato planificado. Esta opción sólo puede definirla el administrador del servidor de IBM Spectrum Protect. Si se especifica esta opción, el mandato se ejecuta con la autorización del usuario especificado. De lo contrario, se ejecuta con la autorización del planificador.

►►—SCHEDCMDUser—*nombre_usuario*—◄◄

user_name

Especifica el nombre de un usuario válido del sistema en el que se ejecuta un mandato especificado.

Nota: La opción `shedcmduser` *no* afecta al ID de usuario utilizado para los mandatos previos y posteriores a la planificación. Las tareas de planificación previa y posterior siempre se ejecutan como root (ID de usuario 0).

Activar o desactivar mandatos planificados

Puede utilizar la opción `shedcmddisabled` para desactivar la planificación de mandatos del servidor.

Los mandatos se planifican mediante la opción `action=command` en el mandato del servidor DEFINE SCHEDULE.

La opción `schedcmddisabled` no desactiva los mandatos `preschedulecmd` y `postschedulecmd`. No obstante, puede especificar `preschedulecmd` o `postschedulecmd` con un espacio en blanco o una serie nula para desactivar la planificación de estos mandatos.

Puede utilizar la opción `schedrestretrdisabled` para evitar que el administrador del servidor de IBM Spectrum Protect ejecute operaciones de restauración o recuperación.

Puede utilizar la opción `srvprepostscheddisabled` para evitar que el administrador del servidor de IBM Spectrum Protect ejecute mandatos de planificación previa y posterior al realizar operaciones planificadas.

Puede utilizar la opción `srvprepostsnapdisabled` para evitar que el administrador del servidor de IBM Spectrum Protect ejecute mandatos previos y posteriores a la instantánea al realizar operaciones de copia de seguridad de instantánea planificadas.

Referencia relacionada:

“`Schedcmddisabled`” en la página 544

“`Schedrestretrdisabled`” en la página 552

“`Srvprepostscheddisabled`” en la página 574

“`Srvprepostsnapdisabled`” en la página 575

Gestionar varios requisitos de planificador en un sistema

En determinadas situaciones es preferible tener más de una actividad planificada para cada sistema cliente.

Acerca de esta tarea

Normalmente, se puede hacer asociando un nodo con más de una definición de planificación. Es el método estándar de ejecutar varias planificaciones en un sistema.

Debe asegurarse de que los intervalos de planificación para cada planificación no se superponen. Un único proceso de planificador cliente no puede ejecutar simultáneamente varias acciones planificadas; por lo tanto, si se produce una superposición, se ignora la segunda planificación a iniciar si la primera planificación no finaliza antes de la conclusión del intervalo de inicio de la segunda planificación.

Suponga que se debe hacer una copia de seguridad diaria de la mayoría de los sistemas de archivos del sistema cliente y que debe realizarse una copia de seguridad cada hora de un sistema de archivos que contiene datos críticos. En este caso, sería necesario definir dos planificaciones para manejar este requisito. Para evitar que se produzca un conflicto en la planificación de la copia de seguridad diaria y a cada hora, es necesario que la opción `starttime` de cada planificación sea distinta.

En determinados casos, es necesario ejecutar más de un proceso de planificador en un sistema. Varios procesos requieren un archivo de opciones distinto para cada proceso que debe contener la siguiente información:

- Defina un nombre de nodo exclusivo para cada proceso.
- Especifique anotaciones de planificación y de error exclusivas para cada proceso.

- Cuando se ejecuta en modalidad de petición, utilice la opción `tcpclientport` para especificar un puerto exclusivo para cada proceso.

Las ventajas de utilizar varios procesos de planificación son las siguientes:

- Se puede ejecutar más de una copia de seguridad planificada a la vez.
- Se pueden especificar distintos criterios de copia de seguridad para cada planificación iniciada, mediante el archivo de opciones del cliente o las opciones de modificación del servidor de IBM Spectrum Protect.

Los inconvenientes de utilizar varios procesos de planificación son:

- Se crea un espacio de archivos único para cada nombre de nodo en el servidor de IBM Spectrum Protect.
- Al restaurar los datos, se debe utilizar el mismo nombre de nodo asociado a la copia de seguridad.

En las plataformas UNIX y Linux, pueden ejecutarse varios procesos de planificación, con el método gestionado por el daemon de aceptación de clientes o con el método tradicional de ejecución del planificador. En cualquiera de los dos casos hay determinados requisitos de instalación:

- Cada proceso debe ejecutarse utilizando un nombre de nodo distinto.
- Debe crear varias secciones en el archivo `dsm.sys` para cada proceso del planificador. En cada sección, se debe definir un nombre de nodo exclusivo junto con los valores exclusivos para las opciones `errorlogname` y `schedlogname`. También puede optar por definir sentencias `domain`, `include` y `exclude` personalizadas para cada sección.
- En el archivo `dsm.sys`, establezca la opción `passwordaccess` para que se genere en cada sección. Debe generarse una contraseña para cada nombre de nodo que ejecute un proceso de planificador mediante un mandato como `dsmc query sess`.
- Si se ejecuta con la opción `schedmode` establecida en *prompt*, debe establecer un valor `tcpclientport` exclusivo para cada stanza.

Debe empezar cada mandato `dsmc sched` o instancia con la opción `-servername` para hacer referencia al nombre de sección exclusivo en `dsm.sys`. Para `dsmcad`, es necesario definir la variable de entorno `DSM_CONFIG` para cada instancia de `dsmcad` de modo que haga referencia a su archivo de opciones exclusivo.

A continuación se muestra un ejemplo de configuración de los dos procesos de planificación gestionados por el daemon de aceptación de clientes en el archivo `dsm.sys`. Recuerde que debe utilizar vía de accesos completas para los nombres del archivo de anotaciones para evitar que los archivos se graben en el directorio raíz):

```

servername tsm1_sched1
nodename      aixsvt01_sched1
tcperv        firebat
tcpclientport 1507
passwordaccess generate
domain        /svt1
schedmode     prompted
schedlogname  /tsm/dsmsched1.log
errorlogname  /tsm/dsmerror1.log
managedservices schedule

servername tsm1_sched2
nodename      aixsvt01_sched2
tcperv        firebat
tcpclientport 1508
passwordaccess generate
domain        /svt1
schedmode     prompted
schedlogname  /tsm/dsmsched2.log
errorlogname  /tsm/dsmerror2.log
managedservices schedule

```

Contenido de /test/dsm.opt1:

```
servername tsm1_sched1
```

Contenido de /test/dsm.opt2:

```
servername tsm1_sched2
```

Abra dos ventanas de mandatos del shell:

- En la ventana de mandatos del shell 1, escriba:

```
export DSM_CONFIG=/test/dsm.opt1
sudo dsmcad
```
- En la ventana de mandatos del shell 2, escriba:

```
export DSM_CONFIG=/test/dsm.opt2
sudo dsmcad
```

Nota: Debe escribir estos mandatos en un script de shell si desea que los procesos dsmcad se inicien directamente desde /etc/inittab para poder establecer la variable DSM_CONFIG antes de iniciar el proceso dsmcad.

Capítulo 8. Códigos de retorno del cliente

La interfaz de línea de mandatos de copia de seguridad/archivado y el planificador finalizan con códigos de retorno que reflejan de forma precisa si la operación de cliente se ha realizado correctamente o no.

Los scripts, los archivos de proceso por lotes y otros recursos de automatización pueden utilizar el código de retorno de la interfaz de línea de mandatos. En operaciones que utilicen el planificador de IBM Spectrum Protect, los códigos de retorno se muestran en la salida del mandato administrativo **QUERY EVENT**.

En general, el código de retorno hace referencia al mensaje de mayor gravedad durante la operación de cliente.

- Si el mensaje de mayor gravedad es informativo (ANSnnnnI), entonces el código de retorno es 0.
- Si el mensaje de mayor gravedad es un aviso (ANSnnnnW), entonces el código de retorno es 8.
- Si el mensaje de mayor gravedad es un error (ANSnnnnE o ANSnnnnS), entonces el código de retorno es 12.

Se aplica una excepción a estas reglas cuando los mensajes de aviso o de error indican que no se han podido procesar archivos individuales. Para los archivos que no se pueden procesar, el código de retorno es 4. Examine el archivo `dsmerror.log` para determinar la causa de errores producidos durante las operaciones de cliente. Los errores que se producen durante los sucesos planificados se registran en el archivo `dsmsched.log`.

La Tabla 53 describe los códigos de retorno y sus significados.

Tabla 53. Códigos de retorno del cliente y significado de éstos

Código	Explicación
0	Todas las operaciones se han completado correctamente.
4	<p>La operación no se ha completado correctamente, aunque algunos archivos no se han procesado. No ha habido más errores ni avisos. Este código de retorno es común. Los archivos no se procesan por varias razones; las siguientes razones son las más comunes.</p> <ul style="list-style-type: none">• El archivo satisface una entrada de una lista de exclusión. Los archivos excluidos generan entradas de registro sólo durante las copias de seguridad selectivas.• El archivo estaba siendo utilizado por otra aplicación y el cliente no ha podido acceder al mismo.• El archivo ha cambiado durante la operación hasta alcanzar un grado prohibido por el atributo de serialización de copia. Consulte "Atributo Serialización de copia" en la página 303.
8	<p>La operación se ha completado con al menos un mensaje de aviso. Para eventos planificados, el estado es Completed. Revise el archivo <code>dsmerror.log</code> (y <code>dsmsched.log</code> para los eventos planificados) para determinar qué mensajes de aviso se emitieron y valorar su impacto en la operación.</p>

Tabla 53. Códigos de retorno del cliente y significado de éstos (continuación)

Código	Explicación
12	La operación se ha completado con al menos un mensaje de error (excepto los mensajes de error de los archivos omitidos). Para eventos planificados, el estado es Failed. Revise el archivo dsmerror.log (y dsmsched.log para los eventos planificados) para determinar qué mensaje se emitieron y valorar su impacto en la operación. Generalmente, este código de retorno significa que el error era tan grave como para impedir que la operación terminase correctamente. Por ejemplo, un error que evita que un sistema de archivos que esté siendo procesado emita el código de retorno 12.
otros	<p>Para las operaciones planificadas en las que la acción programada es COMMAND, el código de retorno es el código de retorno desde el mandato que se ejecuta. Si el código de retorno es 0, el estado de la operación planificada es Completed. Si el código de retorno es distinto a cero, el estado es Failed.</p> <p>Puede que algunos mandatos emitan un código de retorno distinto de cero para indicar que la operación se ha completado correctamente. Para estos mandatos, puede evitar un estado Failed introduciendo el mandato en un script que inicia el mandato, interpreta los resultados y lleva a cabo la salida. El script debería producir un código de retorno de 0 si el mandato es correcto o un código de retorno distinto de cero si el mandato falla. A continuación, pida al administrador del servidor de IBM Spectrum Protect que modifique la definición de planificación para que se ejecute el script en lugar del mandato.</p>

El código de retorno correspondiente a un macro de cliente es el código de retorno más elevado emitido entre los mandatos individuales que componen el macro. Por ejemplo, suponga que una macro consta de estos mandatos:

```
selective "/home/devel/*" -subdir=yes
incremental "/home/devel/TestDriver/*" -subdir=yes
archive "/home/plan/proj1/*" -subdir=yes
```

Si el primer mandato finaliza con un código de retorno de 0, el segundo mandato se completa con un código de retorno de 8 y el tercer mandato finaliza con un código de retorno de 4, el código de retorno para la macro es 8.

Para obtener más información sobre el mandato **QUERY EVENT**, consulte la documentación del servidor de IBM Spectrum Protect.

Conceptos relacionados:

“Opciones del planificador para los mandatos” en la página 292

Capítulo 9. Políticas de gestión de almacenamiento

Las políticas de gestión de almacenamiento son reglas que el administrador define con el fin de gestionar las copias de seguridad y las copias archivadas en el servidor.

Los datos se asocian (o vinculan) a estas políticas, y cuando se realice una copia de seguridad de los datos o cuando éstos se archiven, se gestionarán de acuerdo con los criterios de la política. Los criterios de la política incluyen un dominio de políticas, un juego de políticas, una clase de gestión y un grupo de copia.

Las políticas determinan lo siguiente:

- Si el archivo es elegible para los servicios de copia de seguridad o archivado.
- Cuántas versiones de copia de seguridad deben conservarse.
- Durante cuánto tiempo deben conservarse las versiones de copia de seguridad y las copias archivadas inactivas.
- Dónde deben colocarse las copias en el almacenamiento.
- Para las copias de seguridad incrementales, las políticas también determinan:
 - La frecuencia con que puede hacerse una copia de seguridad de un archivo.
 - Si se debe modificar un archivo antes de volver a hacer una copia de seguridad del mismo.

Si tiene el cliente de IBM Spectrum Protect for Space Management instalado, el administrador define también reglas que determinan si los archivos son elegibles para la migración desde los sistemas de archivos locales al almacenamiento.

En este tema se explica lo siguiente:

- Criterios de política (dominios de políticas, juegos de políticas, grupos de copia y clases de gestión).
- Cómo visualizar políticas.
- Cómo se asocian los datos a políticas.

Dominios de políticas y juegos de políticas

Un *dominio de políticas* es un grupo de clientes que tienen unas necesidades similares de copia de seguridad/archivado de datos.

Los dominios de políticas contienen uno o varios juegos de políticas. Un administrador utiliza dominios de políticas para gestionar un grupo de nodos cliente de una forma lógica.

Un dominio de políticas puede incluir, por ejemplo:

- Un departamento, como por ejemplo Contabilidad.
- Una ubicación física, como por ejemplo un edificio o un piso concreto.
- Una red de área local, como por ejemplo todos los clientes asociados a un servidor de archivos concreto.

IBM Spectrum Protect incluye un dominio de políticas predeterminado denominado *Standard*. En primer lugar, el nodo cliente puede estar asociado al dominio de políticas predeterminado. Sin embargo, el administrador puede definir dominios de políticas adicionales si hay grupos de usuarios con unas necesidades de copia de seguridad/archivado exclusivas.

Un *juego de políticas* es un grupo de una o varias clases de gestión. Cada dominio de políticas puede contener varios juegos de políticas. El administrador utiliza un juego de políticas para implementar clases de gestión diferentes basándose en las necesidades de la empresa y del usuario. Sólo uno de estos juegos de políticas puede estar activo a la vez. A éste se le conoce como *juego de políticas activo*. Cada juego de políticas contiene una *clase de gestión predeterminada* y un número cualquiera de clases de gestión adicionales.

Clases de gestión y grupos de copia

Una *clase de gestión* es un conjunto de grupos de copia de seguridad y copia archivada que establece y contiene las necesidades de gestión de almacenamiento específicas para la copia de seguridad y el archivado de datos.

Un administrador puede establecer clases de gestión distintas para satisfacer las necesidades de copia de seguridad/archivado de diferentes tipos de datos, como por ejemplo:

- Datos del sistema que son cruciales para la empresa.
- Datos de la aplicación que cambian a menudo.
- Datos de informe que los encargados de la gestión revisan mensualmente.
- Información legal que debe conservarse indefinidamente, con lo cual se necesita una gran cantidad de espacio de disco.

Nota: Si tiene instalado IBM Spectrum Protect for Space Management, también puede contener requisitos específicos para migrar archivos al almacén.

La mayoría del trabajo que se realiza con las políticas de gestión de almacenamiento tiene que ver con las clases de gestión. Cada archivo y directorio del que realice una copia de seguridad y cada archivo del que se realice una copia archivada está asociado a (o *enlazado a*) una clase de gestión de la forma siguiente:

- Si los datos no están asociados con una clase de gestión, IBM Spectrum Protect utiliza la clase de gestión predeterminada del juego de políticas activo.
- Cuando realice una copia de seguridad de los directorios, podrá especificar una clase de gestión con una sentencia *include* o la opción `dirmc`. Si no especifica ninguna clase de gestión, IBM Spectrum Protect utilizará la clase de gestión del juego de políticas activo que especifique el período de retención "Solo retención". Si varias clases de gestión se ajustan a este criterio, IBM Spectrum Protect utiliza el último que haya encontrado, en orden alfabético.
- Para los directorios de copias archivadas, puede especificar una clase de gestión con una sentencia *include.archive* o la opción `archmc`. Si no especifica una clase de gestión, el servidor asigna al directorio archivado la clase de gestión predeterminada. Si la clase de gestión predeterminada no tiene grupo de copia archivada, el servidor asigna la clase de gestión que tiene actualmente el grupo de copia archivada con el período de retención más corto.

Puede utilizar sentencias de *inclusión* en la lista de inclusión/exclusión para asociar los archivos a las clases de gestión. En el archivo de opciones del sistema cliente, puede asociar directorios con una clase de gestión mediante la opción `dirmc`.

Dentro de una clase de gestión, las necesidades específicas de copia de seguridad/archivado se encuentran en *grupos de copia*. Los grupos de copia definen los atributos específicos de gestión de almacenamiento que describen cómo maneja el servidor los datos de los que se ha hecho copia de seguridad o que se han archivado. Los grupos de copia incluyen tanto los *grupos de copia de seguridad* como

los *grupos de copia archivada*. Una clase de gestión puede tener un grupo de copia de seguridad, un grupo de copia archivada, ambos grupos, o ninguno.

Un *grupo de copia de seguridad* contiene atributos que se utilizan durante el proceso de copia de seguridad para determinar lo siguiente:

- Cuántos días deben transcurrir para que se vuelva a hacer una copia de seguridad de un archivo.
- Cómo se procesa un archivo durante una copia de seguridad si éste está en uso.

También contiene atributos para gestionar las versiones de copia de seguridad de los archivos en el servidor. Estos atributos controlan lo siguiente:

- En qué tipo de medio almacena el servidor las versiones de copia de seguridad de los archivos y directorios.
- Cuántas versiones de copia de seguridad debe conservar el servidor de los archivos y los directorios.
- Durante cuánto tiempo debe conservar el servidor las versiones de copia de seguridad de los archivos y los directorios.
- Durante cuánto tiempo almacena el servidor las copias de seguridad inactivas.
- Durante cuánto tiempo se almacena la última versión inactiva de un archivo.

Un *grupo de copia archivada* contiene atributos que controlan lo siguiente:

- Si se archiva un archivo que está en uso.
- En qué tipo de medio el servidor almacena las copias archivadas de los archivos.
- Durante cuánto tiempo almacena el servidor las copias archivadas de los archivos.

Conceptos relacionados:

“Seleccionar una clase de gestión para los archivos” en la página 305

“Período de gracia de retención” en la página 309

Visualizar información sobre clases de gestión y grupos de copia

Puede mostrar información de política con la interfaz de línea de mandatos o con la interfaz gráfica de usuario.

En una interfaz gráfica de usuario, pulse **Ver información de políticas** en el menú Programas de utilidad. La ventana **Información de política** muestra las clases de gestión disponibles. En una línea de mandatos, utilice el mandato **query mgmtclass** para ver las clases de gestión disponibles. La opción **detail** proporciona más información.

En la Tabla 54 se muestran los valores predeterminados para los grupos de copia de seguridad y copia archivada en la clase de gestión estándar.

Tabla 54. Valores de atributo predeterminados de la clase de gestión estándar

Atributo	Valor predeterminado de copia de seguridad	Valor predeterminado de archivado
Nombre de grupo de copia	Standard	Standard
Tipo de copia	Copia seguridad	Archive
Frecuencia de copia	0 días	CMD (mandato)
Versiones si datos existen	2 versiones	No se aplica
Versiones si datos suprimidos	1 versión	No se aplica

Tabla 54. Valores de atributo predeterminados de la clase de gestión estándar (continuación)

Atributo	Valor predeterminado de copia de seguridad	Valor predeterminado de archivado
Retener versiones adicionales	30 días	No se aplica
Retener única versión	60 días	No se aplica
Serialización de copia	Estática compartida	Estática compartida
Modalidad de copia	Modificado	Absoluta
Destino de copia	Backuppool	Archivepool
Retener versión	No se aplica	365 días
Sin LAN	Destino	No
Eliminación de duplicados habilitada	No	No

Atributo Nombre de grupo de copias

El atributo *nombre de grupo de copias* es el nombre del grupo de copias. El valor predeterminado para la copia de seguridad y el archivado es *estándar*.

Atributo Tipo de copia

El atributo *tipo de grupo de copias* es el tipo del grupo de copias. El valor para la copia de seguridad es siempre *copia de seguridad*; el valor para el archivado es siempre *archivado*.

Atributo Frecuencia de copia

El atributo *Frecuencia de copia* es el número mínimo de días que deben transcurrir entre las sucesivas copias de seguridad incrementales. Utilice este atributo durante la realización de una copia de seguridad incremental completa.

Las copias de frecuencia funcionan con el parámetro **mode**. Por ejemplo, si frequency=0 y mode=modified, se hará copia de seguridad de un archivo o directorio únicamente si se ha modificado des de la última copia de seguridad incremental. Si frequency=0 y mode=absolute, se hará copia de seguridad de un objeto cada vez que se haga una copia de seguridad incremental contra el mismo. Si frequency=0 y mode=absolute, las modificaciones y el número de días desde la última copia de seguridad no afectan en la operación de seguridad actual. En las copias de seguridad selectivas no se comprueba el atributo frequency.

Para los grupos de copia archivada, la frecuencia de copia es siempre CMD (mandato). No hay ninguna restricción en cuanto a la frecuencia con que se archiva un objeto.

La frecuencia de copia se pasa por alto durante una copia de seguridad con registro por diario.

Atributo Versiones si datos existen

El atributo *versiones si datos existen* especifica el número máximo de las diferentes versiones de copia de seguridad que se conservan para los archivos y directorios.

Si selecciona una clase de gestión que permite más de una versión de copia de seguridad, la versión más reciente recibe el nombre de versión *activa*. Al resto de

versiones se las denomina versiones *inactivas*. Si el número máximo de versiones permitidas es cinco, y se ejecuta una copia de seguridad que crea una sexta versión, la versión más antigua se suprime del almacenamiento del servidor.

Atributo Versiones si datos suprimidos

El atributo *Versiones si datos suprimidos* especifica el número máximo de las diferentes versiones de copia de seguridad que se conservan para los archivos y directorios que ha borrados.

Este parámetro se ignora hasta que elimina el archivo o directorio.

Si borra el archivo o el directorio, la próxima vez que ejecute una copia de seguridad incremental, la versión de copia de seguridad activa pasará a estar inactiva. El servidor de IBM Spectrum Protect suprime la versión más antigua por encima del número especificado por este parámetro.

La fecha de caducidad para el resto de versiones depende de los parámetros *Retener versiones adicionales* y *Retener única versión*.

Atributo Retener versiones adicionales

El atributo *Retener versiones adicionales* especifica durante cuántos días deben conservarse todas las versiones de copia de seguridad excepto la más reciente.

La versión más reciente es la versión activa, y las versiones activas no pueden borrarse. Si se especifica *Nolimit*, las versiones de copia de seguridad adicionales se suprimen según el valor del parámetro *versiones si datos existen* o *versiones si datos suprimidos*. En este caso, la versión adicional más antigua se suprime de forma inmediata.

Atributo Retener única versión

El atributo *Retener única versión* especifica durante cuántos días debe conservarse la última versión inactiva restante de un archivo o un directorio.

Si se especifica *Sin límite*, la última versión se conserva indefinidamente.

Este parámetro surte efecto durante la siguiente copia de seguridad incremental después de que se haya suprimido un archivo del sistema cliente. Las actualizaciones posteriores de este parámetro no afectarán a los archivos que ya estén inactivos. Por ejemplo: Si este parámetro está establecido en 10 días cuando se desactiva un archivo durante una copia de seguridad incremental, el archivo se suprimirá del servidor a los 10 días.

Atributo Serialización de copia

El atributo Serialización de copia determina si un archivo puede estar en uso durante un proceso de copia de seguridad o archivado y qué se debe hacer en caso afirmativo.

El valor de este atributo puede ser uno de los siguientes:

- **Estática.** Durante una operación de copia de seguridad o archivado, no deben modificarse ni los archivos ni los directorios. Si se modifica un objeto durante un intento de copia de seguridad o archivado, dichos procesos no se realizarán.
- **Estático compartido.** Durante una operación de copia de seguridad o archivado, no deben modificarse ni los archivos ni los directorios. El cliente intenta realizar

una copia de seguridad o un archivado hasta cuatro veces más, según el valor especificado en la opción `changingretries` de su archivo de opciones. Si se modifica un objeto durante cada intento de copia de seguridad o archivado, dichos procesos no se realizarán.

- **Dinámica.** Se realiza una copia de seguridad o una copia archivada de un archivo o un directorio en el primer intento independientemente de si éste cambia durante dichos procesos.
- **Dinámico compartido.** Se realiza una copia de seguridad o una copia archivada de un archivo o un directorio independientemente de si éste cambia durante dichos procesos. El cliente intenta realizar una copia de seguridad o archivado hasta cuatro veces más. El número de intentos depende del valor que se haya especificado en la opción `changingretries` del archivo de opciones, sin que el archivo cambie durante el intento. En el último intento, se hace copia de seguridad o se archiva el archivo aunque éste haya cambiado.

Si selecciona una clase de gestión que permite realizar una copia de seguridad o archivado mientras el archivo objeto de dichas operaciones está en uso, la versión de copia de seguridad o la copia archivada que está almacenada en el servidor puede ser una copia difusa. Una *copia difusa* es una versión de copia de seguridad o copia archivada que no refleja de forma precisa el contenido real del archivo. Puede que contenga los cambios, pero no todos. Si esto no es aceptable, seleccione una clase de gestión que cree una versión de copia de seguridad o copia archivada sólo si el archivo no cambia durante la copia de seguridad o el archivado. Cuando se utiliza la serialización estática, las aplicaciones no pueden abrir un archivo para el acceso de escritura mientras se hace una copia de seguridad del archivo.

Si restaura o recupera un archivo que contiene una copia difusa, puede que el archivo no sea utilizable. No utilice la serialización dinámica ni la serialización dinámica compartida para hacer copias de seguridad de archivos salvo que esté totalmente seguro de que puede utilizarse una copia difusa restaurada.

Importante: Si selecciona una clase de gestión con un grupo de copia que especifique dinámica compartida o copia de seguridad dinámica de serialización, debe ir con cuidado.

Referencia relacionada:

“Snapshotproviderimage” en la página 570

Parámetro de modalidad de copia

El parámetro **mode** de copia determina si un archivo o directorio se considera para la copia de seguridad incremental sin tener en cuenta si ha cambiado o no desde la última copia de seguridad.

El cliente no comprueba el parámetro de modalidad cuando ejecuta copias de seguridad selectivas.

El valor para este parámetro puede ser uno de los siguientes ajustes:

Modificados

El objeto se tiene en cuenta para la copia de seguridad incremental solo si este ha cambiado desde la última copia de seguridad. Se considera que un objeto ha cambiado cuando se cumple una de las condiciones siguientes:

- La fecha u hora de la última modificación es distinta.
- El tamaño es distinto.

- Si sólo han cambiado los metadatos (como por ejemplo los permisos de acceso), es posible que el cliente sólo haga copia de seguridad de los metadatos.
- El propietario es distinto.

absolute

El objeto se tiene en cuenta para la copia de seguridad incremental independientemente de si ha cambiado desde la última copia de seguridad. Para los grupos de copia archivada, la modalidad es siempre **Absoluta**, lo cual indica que un objeto se archiva independientemente de si ha cambiado desde la última solicitud de archivado.

Referencia relacionada:

“Absolute” en la página 345

Atributo Destino de copia

El atributo *destino de copia* designa el destino en el que se almacenan las copias de seguridad o copias archivadas.

El destino puede ser una agrupación de almacenamiento de dispositivos de disco o una agrupación de almacenamiento de dispositivos que admiten medios extraíbles, como por ejemplo una cinta.

Atributo Retener versiones

El atributo *retener versiones* especifica el número de días que una copia archivada permanece en el almacenamiento.

Cuando transcurre el número de días especificado para una copia archivada de un archivo, ésta se suprime del almacenamiento del servidor.

Atributo Eliminar duplicados de datos

El atributo *Eliminar duplicados de datos* especifica si los datos redundantes se transferirán al servidor de IBM Spectrum Protect durante el proceso de archivado y copia de seguridad.

Conceptos relacionados:

“Deduplicación de datos del lado del cliente” en la página 86

Referencia relacionada:

“Eliminación de duplicados” en la página 381

“Enablededupcache” en la página 413

“Opciones exclude” en la página 425

Seleccionar una clase de gestión para los archivos

Si la clase de gestión predeterminada satisface las necesidades de copia de seguridad/archivado para todos los archivos de su estación de trabajo, no es necesario emprender ninguna acción para asociar los archivos a dicha clase de gestión. Esto tiene lugar automáticamente cuando realice copia de seguridad o archive los archivos.

Si selecciona una clase de gestión diferente para los archivos, tenga en cuenta las tres preguntas siguientes:

- ¿La clase de gestión contiene un grupo de copia de seguridad?

Si intenta realizar una copia de seguridad de un archivo asociado a una clase de gestión que no contiene un grupo de copia de seguridad, la copia de seguridad no se realizará.

- ¿La clase de gestión contiene un grupo de copia archivada?
No puede archivar un archivo asociado a una clase de gestión que no contenga un grupo de copia archivada.
- ¿El grupo de copia de seguridad contiene atributos que realizan copias de seguridad de los archivos con la frecuencia suficiente?
La modalidad y la frecuencia funcionan conjuntamente para controlar con qué frecuencia se realiza copia de seguridad de un archivo cuando se utiliza la copia de seguridad incremental. Estos atributos no se comprueban para copias de seguridad selectivas.
- ¿Qué método de serialización utiliza el grupo de copia?
El método de serialización determina cómo funciona IBM Spectrum Protect cuando un archivo cambia mientras se realiza una copia de seguridad de él.
- ¿El grupo de copia de seguridad especifica un número adecuado de versiones de copia de seguridad para conservar y una cantidad adecuada de tiempo de conservación?
- ¿El grupo de copia archivada especifica una cantidad adecuada de tiempo para conservar las copias archivadas de los archivos?

Conceptos relacionados:

“Atributo Serialización de copia” en la página 303

Asignar una clase de gestión a los archivos

Una clase de gestión define cuándo se incluyen los archivos en una copia de seguridad, durante cuánto tiempo se conservan en el servidor y cuántas versiones del archivo debe conservar el servidor.

El administrador del servidor selecciona una clase de gestión predeterminada. Puede especificar su propia clase de gestión para sustituir la clase de gestión predeterminada.

Para asignar una clase de gestión distinta de la predeterminada a los directorios, utilice la opción `dirmc` en el archivo de opciones de cliente.

Puede asignar una clase de gestión a un archivo o grupo de archivos utilizando una sentencia `include` en el archivo de opciones. También puede asignar una clase de gestión utilizando una sentencia `include` en el archivo de inclusión-exclusión especificado por la opción `incl excl`. Los nombres de clase de gestión no son sensibles a mayúsculas y minúsculas.

Mediante el uso del cliente de línea de mandatos, para asociar todos los archivos del directorio `costs` con la clase de gestión denominada `budget`, deberá entrar:

```
include /home/proj2/costs/* budget
```

Para especificar una clase de gestión denominada `managall` que se utilice para todos los archivos a los que no se asigne de forma explícita una clase de gestión, deberá especificar lo siguiente:

```
include /* managall
```

Los ejemplos siguientes muestran cómo asignar una clase de gestión a archivos:

```
exclude /.../*.sno
include /home/winter/.../*.ice      mcweekly
include /home/winter/december/*.ice mcdaily
include /home/winter/january/*.ice  mcmonthly
include /home/winter/february/white.sno
```

El proceso sigue estos pasos:

1. Se hace una copia de seguridad del archivo `white.sno` del directorio `february` del directorio `winter` siguiendo las reglas de proceso ascendente. Puesto que no se ha especificado ninguna clase de gestión en esta sentencia, el archivo se asigna a la clase de gestión predeterminada.
2. Cualquier archivo con una extensión de `ice` en el directorio `january` se asigna a la clase de gestión denominada `mcmonthly`.
3. Cualquier archivo con una extensión de `ice` en el directorio `december` se asigna a la clase de gestión denominada `mcdaily`.
4. Los demás archivos con una extensión de `ice` en cualquier directorio bajo el directorio `winter` se asignan a la clase de gestión denominada `mcweekly`.
5. Los archivos que tengan una extensión `sno` de cualquier directorio quedarán excluidos de la copia de seguridad. La excepción a esta regla es `white.sno` en el directorio `february`, que está en el directorio `winter`.

Para especificar su propia clase de gestión predeterminada `mgmt_class_name` para los archivos que no se incluyen de forma explícita, ponga la siguiente sentencia en la parte superior de la lista de inclusión:

```
include /.../* nombre_clase_gestión
```

Si archiva un archivo mediante la interfaz gráfica de usuario (GUI), puede seleccionar otra clase de gestión para que sustituya la asignada al archivo.

Referencia relacionada:

“Dirmc” en la página 389

“Opciones include” en la página 458

Sustituirla clase de gestión para las copias archivadas

Al archivar un archivo, puede sustituir la clase de gestión asignada mediante la interfaz gráfica de usuario (GUI), o mediante la opción `archmc` del mandato **archive** .

Sustituir la clase de gestión mediante la GUI equivale a utilizar la opción `archmc` en el mandato **archive** . Para utilizar la GUI, pulse el botón **Opciones** en el árbol de archivado para sustituir la clase de gestión y seleccionar una clase de gestión distinta.

En la línea de mandatos, para asociar el archivo `budget.jan` a la clase de gestión **ret2yrs**, debería escribir este mandato:

```
dsmc archive -archmc=ret2yrs /home/jones/budget.jan
```

Seleccionar una clase de gestión para los directorios

Si la clase de gestión del conjunto de políticas activo que contiene el valor del período más largo para "Retener única versión" (RETONLY) satisface los requisitos de copia de seguridad para los directorios, puede que no sea necesario realizar ninguna acción para asociar los directorios a esa clase de gestión. La asociación de clases de gestión se lleva a cabo automáticamente cuando se realiza la copia de seguridad de los directorios.

Si hay más de una clase de gestión con el valor RETONLY más largo, el cliente de IBM Spectrum Protect selecciona la clase de gestión cuyo nombre ocupe, por orden alfabético, la última posición.

Si la clase de gestión predeterminada no satisface los requisitos, seleccione una clase de gestión para la que se especifique un período de retención adecuado en el parámetro Retener única versión. Por ejemplo, si la clase de gestión realiza la copia de seguridad de los datos directamente en cinta, pero desea que las copias de seguridad de directorio se dirijan al disco, debe seleccionar una clase de gestión distinta. Debe conservar los directorios como mínimo durante el mismo tiempo que conserva los archivos asociados a estos directorios.

Para los directorios de copia de seguridad, utilice la opción `dirmc` para especificar la clase de gestión a la que se vinculan los directorios.

Para los directorios de archivado, utilice la opción `archmc` con el mandato **archive**.

A continuación se indican los métodos que puede utilizar para ver las clases de gestión disponibles y los atributos de éstas:

- GUI o cliente web: seleccione **Ver información de políticas** en el menú **Herramientas**.
- Cliente de línea de mandatos: ejecute `dsmc query mgmtclass -detail`.

Nota: En un servidor de IBM Spectrum Protect, durante el proceso de caducidad, si un directorio archivado reúne los requisitos para la aplicación de la caducidad, el servidor comprueba si alguna de las copias archivadas existentes necesita que se conserve el directorio archivado. En caso afirmativo, al directorio archivado no se le aplica la caducidad, y el cliente de copia de seguridad y archivado actualiza la fecha de inserción del directorio archivado para garantizar que la caducidad del directorio no se producirá antes de que caduquen los archivos que éste contiene.

Vincular clases de gestión a archivos

La *vinculación* asocia un archivo a una clase de gestión.

Cuando se realiza una copia de seguridad de un archivo por primera vez, IBM Spectrum Protect lo enlaza a la clase de gestión predeterminada o bien a la clase de gestión especificada en la lista de inclusión/exclusión.

Si el grupo de copia de seguridad de la clase de gestión especifica que deben conservarse varias versiones de copia de seguridad del archivo, y se solicitan varias copias de seguridad, el servidor siempre tiene una versión de copia de seguridad activa (la versión actual) y una o varias versiones de copia de seguridad del archivo inactivas. Todas las versiones de copia de seguridad de un archivo se vinculan a la misma clase de gestión y se gestionan de acuerdo con los atributos especificados en el grupo de copia de seguridad.

Cuando se archiva un archivo por primera vez, IBM Spectrum Protect lo enlaza a la clase de gestión predeterminada, a la clase de gestión especificada en la lista de inclusión/exclusión o a la clase de gestión indicada al modificar las opciones de archivado durante una operación de archivado.

Las copias archivadas nunca se vuelven a vincular a otra clase de gestión. Si cambia la clase de gestión de un archivo con una sentencia `include.archive`, la opción `archmc` o mediante una interfaz gráfica de usuario del cliente de copia de seguridad y archivado, las copias anteriores de dicho archivo seguirán estando vinculadas a la clase de gestión especificada cuando se archivaron.

Si se suprime un archivo en el sistema cliente, los objetos inactivos del archivo no se vuelven a vincular.

Para obtener información sobre cómo asociar archivos y directorios con clases de gestión, consulte la documentación del servidor de IBM Spectrum Protect.

Revincular las versiones de copias de seguridad a los archivos

La *revinculación* asocia un archivo o una imagen de volumen lógico a una nueva clase de gestión.

Las copias de seguridad de los archivos se vuelven a vincular a una clase de gestión diferente en las condiciones siguientes. En todas estas condiciones, los archivos (activos e inactivos) no se vuelven a vincular hasta la próxima operación de copia de seguridad.

- Se especifica una clase de gestión distinta en una sentencia de inclusión para cambiar la clase de gestión del archivo. Las copias de seguridad se gestionan de acuerdo con la clase de gestión antigua hasta que se ejecute otra copia de seguridad.
- El administrador suprime la clase de gestión del juego de políticas activo. Se utiliza la clase de gestión predeterminada para gestionar las versiones de copia de seguridad cuando se vuelva a hacer una copia de seguridad del archivo.
- El administrador asigna el nodo cliente a un dominio de políticas diferente, y el juego de políticas activo del dominio no contiene una clase de gestión con el mismo nombre. Se utiliza la clase de gestión predeterminada del nuevo dominio de políticas para gestionar las versiones de copia de seguridad.

Para obtener información sobre cómo asociar archivos y directorios con clases de gestión, consulte la documentación del servidor de IBM Spectrum Protect.

Período de gracia de retención

IBM Spectrum Protect también proporciona un *período de gracia de retención de copia de seguridad* y un *período de gracia de retención de copias archivadas* como ayuda para proteger los datos de las copias de seguridad y de las copias archivadas cuando no es posible volver a vincular un archivo con la clase de gestión adecuada.

El período de gracia de retención de copia de seguridad se utiliza en los siguientes casos:

- Se cambia la clase de gestión de un archivo, pero ni la clase de gestión predeterminada ni la nueva clase de gestión contienen un grupo de copia de seguridad.
- La clase de gestión a la que se vincula un archivo ya no existe, y la clase de gestión predeterminada no contiene un grupo de copia de seguridad.

El período de gracia de retención de copia de seguridad, definido en el dominio de políticas, se inicia al ejecutarse una copia de seguridad incremental. El valor predeterminado es 30 días. Sin embargo, el administrador puede ampliar o reducir este período.

Cuando el servidor de IBM Spectrum Protect gestiona un archivo mediante el período de gracia de retención de copia de seguridad, no crea versiones de copia de seguridad del archivo nuevas. Todas las versiones de copia de seguridad del archivo existentes caducan a los 30 días (o el número de días especificado en el dominio de políticas) a partir del día en el que se marcan como inactivas.

Las copias archivadas nunca se vuelven a vincular porque cada operación de archivado crea una copia archivada distinta. Las copias archivadas permanecen vinculadas al nombre de clase de gestión especificado cuando el usuario las archivó. Si la clase de gestión a la que está vinculada una copia archivada ya no existe o ya no contiene un grupo de copia archivada, el servidor utiliza la clase de gestión predeterminada. Si más adelante se cambia o restituye la clase de gestión predeterminada, el servidor utiliza la clase de gestión predeterminada actualizada para gestionar la copia archivada. Si la clase de gestión predeterminada no contiene un grupo de copia archivada, el servidor utiliza el período de gracia de retención de copias archivadas especificado para el dominio de políticas.

Protección de retención de políticas basadas en sucesos

Todas las clases de gestión que tienen un grupo de copia archivada deben especificar un período de retención; por ejemplo, el número de días que un objeto archivado se almacena en el servidor antes de suprimirse.

La política basada en eventos ofrece la opción de iniciar el período de retención en el momento de archivar el objeto o bien posteriormente, cuando se envía un evento de activación relacionado con ese objeto al servidor.

Si se establece el valor `RETINIT=CREATE` para el grupo de copias, el período de retención de datos se inicia cuando se archiva el archivo. Si se utiliza el valor de grupo de copias `RETINIT=EVENT` el período de retención de datos se inicia cuando el servidor recibe la notificación de que se ha producido el evento.

Este concepto se demuestra en el ejemplo siguiente:

El usuario tiene dos archivos, `create.file` y `event.file`. El usuario dispone de dos clases de gestión; `CREATE`, con `RETINIT=CREATE`, y `EVENT`, con `RETINIT=EVENT`. Las dos clases de gestión tienen un período de retención de 60 días. El usuario realiza el archivado de ambos archivos el mismo día:

```
dsmc archive create.file -archmc=CREATE
dsmc archive event.file -archmc=EVENT
```

Diez días después, el usuario emite el mandato **set event** `-type=hold` para el archivo `create.file`, por lo que el archivo no puede suprimirse. El mismo día, el usuario emite el mandato **set event** `-type=activate` para el archivo `event.file`. En ese momento, el período de retención restante de `create.file` es de 50 días y el de `event.file` es de 60 días. Si no se realiza ninguna otra acción, `create.file` se conserva en el servidor indefinidamente y `event.file` caduca 70 días después de haberse creado (60 días después de que se haya producido el evento de éste). Sin embargo, si transcurren 20 días desde la realización del archivado inicial, el usuario emite **set event** `-type=release` para el archivo `create.file`. Han transcurrido

treinta días del período de retención de éste y, por lo tanto, el archivo caduca en 30 días (la ejecución de la retención, hold, no amplía el período de retención).

Para obtener información sobre el valor de grupo de copias RETINIT, consulte la documentación del servidor de IBM Spectrum Protect.

Referencia relacionada:

“Set Event” en la página 781

Archivar archivos en un servidor de retención de datos

Hasta ahora, no se ha mostrado que existan diferencias entre el archivado de los archivos en un servidor normal o en un servidor de retención de datos.

En el siguiente ejemplo se muestran las diferencias que existen entre los dos servidores, y qué acción puede realizarse en el día 5:

Si los archivos se han archivado en un servidor sin retención de datos, el usuario puede emitir el mandato **delete archive** *create.file event.file* y, con ello, se suprimen ambos archivos. Si los archivos se han archivado en un servidor de retención de datos, el mismo mandato falla en ambos archivos. En el servidor de retención de datos, el usuario se ve obligado a conservar los archivos hasta que se han satisfecho los criterios de retención establecidos.

Estas son las diferencias que existirán en el día 15 (después de la aplicación de la retención, hold):

Ahora, el mandato **delete archive** *create.file event.file*, en el servidor sin retención de datos, suprime *event.file*, pero devuelve un error de tipo *no puede suprimirse* para *create.file*, pues se encuentra en estado de retención, hold. Ese mismo mandato en un servidor de retención de datos seguirá rechazando la supresión de ambos archivos.

Capítulo 10. Opciones de proceso

Puede utilizar valores predeterminados de las opciones de proceso de cliente o bien puede ajustar las opciones de proceso para adaptarlas a sus necesidades específicas. Consulte la información general sobre opciones de proceso y la guía de referencia de opciones, que contiene información detallada sobre cada una de las opciones.

Conceptos relacionados:

“Utilización de opciones con mandatos” en la página 336

Referencia relacionada:

“Lectura de diagramas de sintaxis” en la página xiv

Visión general de las opciones de proceso

IBM Spectrum Protect utiliza las *opciones de proceso* para controlar las comunicaciones, el proceso de copia de seguridad/archivado y otros tipos de proceso.

Puede especificar opciones de proceso en el archivo de opciones de sistema del cliente (dsm.sys), en el archivo de opciones de usuario del cliente (dsm.opt) o en la línea de mandatos.

Puede definir los siguientes tipos de opciones:

- Opciones de comunicación
- Opciones de servidor y nodo
- Opciones de proceso de copia de seguridad/archivado
- Opciones de proceso de restauración y recuperación
- Opciones de planificación
- Opciones de formato
- Opciones de proceso de mandatos
- Opciones de autorización
- Opciones de proceso de errores
- Opciones de proceso de transacciones
- Opciones de cliente Web
- Opciones de diagnóstico

El cliente de copia de seguridad y archivado también incluye un grupo de opciones de mandatos de cliente que pueden entrarse únicamente en la línea de mandatos con mandatos específicos. Pueden modificarse temporalmente algunas de las opciones del archivo de opciones, entrando dichas modificaciones con mandatos de copia de seguridad/archivado adecuados.

Conceptos relacionados:

“Especificación de opciones con un mandato” en la página 336

Tareas relacionadas:

“Creación y modificación del archivo opciones del sistema del cliente” en la página 56

Opciones de comunicación

Las opciones de comunicación se utilizan para especificar cómo se comunica su nodo cliente con un servidor de IBM Spectrum Protect. Este tema proporciona información sobre los tipos de opciones de comunicación que se pueden utilizar.

Para clientes UNIX y Linux, utilice uno de los protocolos de comunicación siguientes:

- TCP/IP
- Memoria compartida (AIX, Linux)

Utilice la opción `commmethod` para especificar el protocolo de comunicación.

Para establecer sus opciones de comunicación, solicite asistencia al administrador de IBM Spectrum Protect.

Referencia relacionada:

“`Commmethod`” en la página 366

Opciones de TCP/IP

Para utilizar el protocolo de comunicaciones TCP/IP, debe incluir la opción TCP/IP `tcpserveraddress` en el archivo de opciones de cliente.

Las demás opciones de TCP/IP tienen valores predeterminados que pueden modificarse si se desea cambiar el valor predeterminado. Este tema proporciona información sobre los tipos de opciones de comunicación que se pueden utilizar.

Tabla 55. Opciones de TCP/IP

Opción	Descripción
<code>httpport</code> “ <code>Httpport</code> ” en la página 450	Especifica una dirección de puerto TCP/IP para el cliente web.
<code>lanfreetcpport</code> “ <code>Lanfreetcpport</code> ” en la página 481	Especifica el número de puerto TCP/IP en el que el agente de almacenamiento de IBM Spectrum Protect está a la escucha.
<code>lanfreetcpsrveraddress</code> “ <code>Lanfreetcpsrveraddress</code> ” en la página 482	Especifica la dirección TCP/IP para el agente de almacenamiento IBM Spectrum Protect.
<code>tcpbuffsize</code> “ <code>Tcpbuffsize</code> ” en la página 586	Especifica el tamaño en kilobytes del búfer de comunicaciones TCP/IP interno.
<code>tcpnodelay</code> “ <code>Tcpnodelay</code> ” en la página 589	Especifica si el servidor y el cliente desactiva la demora de enviar paquetes pequeños consecutivos en la red. Esta opción es para todos los clientes UNIX..
<code>tcpadminport</code> “ <code>Tcpadminport</code> ” en la página 585	Especifica un número de puerto TCP/IP independiente en el que el servidor espera peticiones de sesiones de cliente de administración, lo que permite sesiones de administración seguras dentro de una red privada.
<code>tcpcadaddress</code> “ <code>Tpcadaddress</code> ” en la página 586	Especifica una dirección TCP/IP para <code>dsmcad</code> .
<code>tcpport</code> “ <code>Tcpport</code> ” en la página 590	Especifica la dirección del puerto TCP/IP para un servidor de IBM Spectrum Protect.
<code>tcpserveraddress</code> “ <code>Tcpserveraddress</code> ” en la página 590	Especifica la dirección TCP/IP para un servidor de IBM Spectrum Protect.

Tabla 55. Opciones de TCP/IP (continuación)

Opción	Descripción
tcpwindowsize "Tcpwindowsize" en la página 591	Especifica el tamaño en kilobytes de la ventana deslizante de TCP/IP para el nodo cliente.
webports "Webports" en la página 650	Permite utilizar el cliente web fuera de un cortafuegos especificando el número de puerto TCP/IP utilizado por el daemon de aceptación de clientes y el servicio de agente de cliente web (el agente de cliente web no se aplica a Mac OS X) para las comunicaciones con la GUI web.

Referencia relacionada:

"Nfstimeout" en la página 500

Opciones de memoria compartida

En este tema se proporciona información sobre las opciones de memoria compartida que se pueden utilizar.

Tabla 56. Opciones de comunicación de memoria compartida

Opción	Descripción
lanfreeshmport "Lanfreeshmport" en la página 480	Especifica el número exclusivo que el cliente y el agente de almacenamiento utilizarán para identificar el área de memoria compartida utilizada para las comunicaciones.
lanfreeshmport "Shmport" en la página 558	Especifica el número exclusivo que el cliente y el servidor utilizarán para identificar el área de memoria compartida utilizada para las comunicaciones.

Opciones de servidor

Utilice la opción servername del archivo dsm.sys para empezar un grupo de opciones (secciones) que se utilizan para conectarse al servidor de IBM Spectrum Protect.

Puede establecer varios grupos de secciones en el archivo dsm.sys para la conexión con distintos servidores. Debajo de cada sección de servername debe aparecer todas las secciones de opciones de clientes necesarias para establecer comunicación con un servidor. La lista de secciones también puede contener otras opciones para las operaciones de copia de seguridad/archivado.

Si el archivo de opciones del sistema cliente contiene sólo una sección: el nodo de cliente contacta con el servidor que se especifique en esa sección para todos los servicios.

Si el archivo de opciones del sistema cliente contiene más de una sección: puede especificar un servidor predeterminado con la opción defaultserver. No especifique un servidor predeterminado, IBM Spectrum Protect establece contacto con el servidor en la primera sección del archivo dsm.sys.

Establezca la opción defaultserver al principio del archivo dsm.sys delante de cualquier sección del servidor. Para obtener más información, consulte el apartado "Defaultserver" en la página 383.

Utilice la opción servername en el archivo de opciones del usuario cliente (dsm.opt) o en la línea de mandatos para especificar un servidor con el que se desea

contactar para los servicios de copia de seguridad/archivado. Esto altera temporalmente el servidor predeterminado especificado en el archivo (dsm.sys).

Nota: No puede sustituir el servidor de migración especificado en el archivo de opciones del sistema cliente.

Tabla 57 muestra un archivo dsm.sys de ejemplo.

Tabla 57. Archivo de opciones del sistema cliente de ejemplo

Archivo dsm.sys de ejemplo	
DEFAULTServer	server2
SErvername	server1
NODename	node1
COMMMethod	TCPip
TCPPort	1500
TCPServeraddress	node.domain.company.com
PASSWORDAccess	generate
GGroups	system adsm
USERS	ashton stewart kaitlin
INCLExcl	/adm/adsm/backup1.excl
SErvername	server2
COMMMethod	SHAREdmem
shmpport	1520
PASSWORDAccess	prompt
GGroups	system adsm
USERS	danielle derek brant
INCLExcl	/adm/adsm/backup2.excl

Opciones de proceso de copia de seguridad/archivado

Puede especificar opciones de cliente para controlar algunos aspectos del proceso de archivado y copia de seguridad.

Tabla 58. Opciones de proceso de copia de seguridad/archivado

Opción	Descripción
afmskipuncachedfiles "Afmskipuncachedfiles" en la página 346	Utilice la opción afmskipuncachedfiles para especificar si los archivos no almacenados en memoria caché y sucios de conjuntos de archivos de Active File Management de General Parallel File System (GPFS™) se procesan para operaciones de copia de seguridad, archivado y migración.
archmc "Archmc" en la página 347	Utilice la opción archmc con el mandato archive para especificar la clase de gestión disponible para el dominio de políticas a la que desea vincular las copias archivadas.
archsymblinkasfile "Archsymblinkasfile" en la página 348	Especifica si desea que el cliente siga un enlace simbólico y archive el archivo o directorio al que éste hace referencia o que sólo archive el enlace simbólico.

Tabla 58. Opciones de proceso de copia de seguridad/archivado (continuación)

Opción	Descripción
asnodename "Asnodename" en la página 349	Utilice la opción asnodename para permitir a nodos agente realizar copias de seguridad o restauración de datos en nombre de otro nodo (el nodo de destino). Esta opción permite realizar operaciones simultáneas desde varios nodos para almacenar datos en el mismo nodo de destino y espacio de archivos en paralelo.
automount "Automount" en la página 358	Utilice esta opción con la opción domain para especificar todos los sistemas de archivos montados automáticamente que el cliente intentará montar en las circunstancias siguientes: <ul style="list-style-type: none"> • Cuando se inicia el cliente de copia de seguridad y archivado • Cuando se inicia la copia de seguridad • Cuando el cliente de copia de seguridad y archivado alcanza a un sistema de archivos montado automáticamente durante la operación de copia de seguridad
autofsrename "Autofsrename" en la página 356	Especifica si debe renombrarse un espacio de archivos existente en un servidor activado para Unicode de modo que pueda crearse un espacio de archivos activado para Unicode para la operación actual.
changingretries "Changingretries" en la página 363	Especifica el número de veces que el cliente intenta realizar una copia de seguridad o archivar un archivo que está en uso.
compressalways "Compressalways" en la página 369	La opción compressalways especifica si se debe continuar la compresión si el objeto aumenta de tamaño durante la compresión. Utilice esta opción con la opción compression.
compression "Compression" en la página 370	La opción compression comprime los archivos antes de enviarlos al servidor. La compresión de archivos reduce el almacenamiento de datos necesario para almacenar versiones de copia de seguridad y copias archivadas de los archivos.
createnewbase "Createnewbase" en la página 373	La opción createnewbase crea una instantánea de base y la utiliza para ejecutar una copia de seguridad incremental completa. Al definir esta opción se garantiza que se hace copia de seguridad de cualquier archivo que se haya omitido durante la copia de seguridad incremental por diferencia de instantánea.

Tabla 58. Opciones de proceso de copia de seguridad/archivado (continuación)

Opción	Descripción
eliminación de duplicados "Eliminación de duplicados" en la página 381	Especifica si deben eliminarse los datos redundantes en el lado del cliente cuando éste transfiere datos al servidor de IBM Spectrum Protect durante el proceso de archivado o copia de seguridad.
dedupcachepath "Dedupcachepath" en la página 380	Especifica la ubicación en la que se creará la base de datos de memoria caché de deduplicación de datos del lado del cliente si se establece la opción <code>enablededupcache=yes</code> durante el proceso de archivado o copia de seguridad.
dedupcachesize "Dedupcachesize" en la página 381	Determina el tamaño máximo del archivo de la memoria caché de eliminación de duplicados de datos.
enablededupcache "Enablededupcache" en la página 413	Especifica si se desea habilitar la memoria caché de eliminación de duplicados de datos del lado del cliente para que el cliente de copia de seguridad y archivado obtenga los datos modificados de la memoria caché.
deletefiles "Deletefiles" en la página 383	<p>Utilice la opción <code>deletefiles</code> con el mandato archive para suprimir archivos de la estación de trabajo después de haber realizado el archivado de éstos.</p> <p>También puede utilizar esta opción con el mandato restore image y la opción <code>incremental</code> para suprimir archivos de la imagen restaurada si éstos se han suprimido después de haber creado la imagen.</p>
description "Descripción" en la página 384	La opción <code>description</code> asigna o especifica una descripción para los archivos cuando el cliente efectúa operaciones de archivado, supresión, recuperación, consulta de archivado, o consulta de juegos de copias de seguridad.
detail "Detail" en la página 385	Utilice la opción <code>detail</code> para listar información sobre la clase de gestión, el espacio de archivos, las copias de seguridad y las copias archivadas, según el mandato con el que se utilice.
diffsnapshot "Diffsnapshot" en la página 387	Utilice la opción <code>diffsnapshot</code> para determinar si el cliente crea una instantánea diferencial.
dirmc "Dirmc" en la página 389	Especifica la clase de gestión que debe utilizarse para los directorios. Si no especifica esta opción, el cliente utiliza la clase de gestión del juego de políticas activo del dominio de políticas cuyo período de retención sea más largo.

Tabla 58. Opciones de proceso de copia de seguridad/archivado (continuación)

Opción	Descripción
dirsonly "Dirsonly" en la página 390	Realiza copias de seguridad, restaura, archiva, recupera o efectúa consultas sólo de directorios.
diskcachelocation "Diskcachelocation" en la página 393	Especifica la ubicación en la que se creará la base de datos de caché en disco si se establece la opción <code>memoryefficient=diskcachemethod</code> durante la realización de una copia de seguridad incremental.
domain "Domain" en la página 394	Especifica los sistemas de archivo que se van a incluir en el dominio de cliente predeterminado en una copia de seguridad incremental.
domain.image "Domain.image" en la página 399	Especifica los sistemas de archivos montados y los volúmenes lógicos RAW que desea incluir en el dominio de cliente para una copia de seguridad de imagen. Esta opción es únicamente para AIX, Linux x86_64, Linux on POWER y Solaris.
domain.nas "Domain.nas" en la página 400	Especifica los volúmenes que deben incluirse en el dominio predeterminado para las copias de seguridad de imagen NAS.
domain.vmfull "Domain.vmfull" en la página 401	Especifica las máquinas virtuales que se van a incluir en copias de seguridad a nivel completo de máquinas virtuales de VMware.
efsdecrypt "Efsdecrypt" en la página 410	Especifica si los archivos cifrados por un sistema de archivos de cifrado (EFS) de AIX se leerán en formato cifrado o descifrado.
enablearchiveretentionprotection "Enablearchiveretentionprotection" en la página 412	Permite al cliente conectar con un proveedor de retención de datos.
enablelanfree "Enablelanfree" en la página 416	Especifica si debe activarse una ruta disponible fuera de la LAN para un dispositivo de almacenamiento conectado a una red de área de almacenamiento (SAN).
"Opciones exclude" en la página 425	Utilice estas opciones para excluir un archivo o un grupo de archivos de los servicios de copia de seguridad y de los servicios de gestión de espacio (si el cliente de HSM está instalado). La opción <code>exclude.backup</code> sólo excluye archivos de la copia de seguridad normal, no de HSM.
exclude exclude.backup exclude.file exclude.file.backup	
encryptiontype "Encryptiontype" en la página 417	Seleccione el cifrado de datos de bits AES-256 o AES-128. El cifrado de datos AES de 256 bits proporciona el nivel más alto de cifrado de datos.

Tabla 58. Opciones de proceso de copia de seguridad/archivado (continuación)

Opción	Descripción
encryptkey "Encryptkey" en la página 418	Especifica si se debe guardar la contraseña de clave de cifrado localmente cuando el cliente hace una operación de archivado y copia de seguridad o si se debe pedir la contraseña de la clave de cifrado.
exclude.archive "Opciones exclude" en la página 425	Excluye sólo de los servicios de archivado el archivo o grupo de archivos que coincidan con el patrón.
exclude.attribute.symlink "Opciones exclude" en la página 425	Excluye un archivo o un grupo de archivos que son vínculos simbólicos o alias (los alias se aplican a Mac OS X) sólo del proceso de copia de seguridad.
exclude.compression "Opciones exclude" en la página 425	Excluye archivos del proceso de compresión si define la opción <code>compression</code> a <i>yes</i> . Esta opción se aplica a copias de seguridad y copias archivadas.
exclude.dir "Opciones exclude" en la página 425	Excluye un directorio, sus archivos y todos sus subdirectorios y sus archivos del proceso de copia de seguridad.
exclude.encrypt "Opciones exclude" en la página 425	Excluye archivos especificados del proceso de cifrado.
exclude.fs "Opciones exclude" en la página 425	Excluye los espacios de archivos que coinciden con un patrón. Esta opción es válida para todos los clientes UNIX.
exclude.fs.nas "Opciones exclude" en la página 425	Excluye sistemas de archivos del servidor de archivos NAS del proceso de copias de seguridad de imágenes cuando se utiliza con el mandato backup nas . Esta opción es únicamente para los clientes AIX y Solaris.
exclude.image "Opciones exclude" en la página 425	Excluye sistemas de archivos montados y volúmenes lógicos RAW que coincidan con el patrón especificado de las operaciones de copia de seguridad de imágenes completas. Esta opción es válida únicamente para clientes AIX, Solaris y todos los de Linux.
fbbranch "Fbbranch" en la página 431	Especifica el ID de ramificación del servidor remoto de FastBack para el cual se va a iniciar un proceso de copia de seguridad o archivado.
fbclientname "Fbclientname" en la página 432	Especifica el nombre de uno o varios clientes de FastBack cuya copia de seguridad se va a realizar desde el proxy de copia de seguridad.
fbpolicyname "Fbpolicyname" en la página 434	Especifica el nombre de una o más políticas de Tivoli Storage Manager FastBack de las que se desea hacer una copia de seguridad desde el proxy de copia de seguridad.

Tabla 58. Opciones de proceso de copia de seguridad/archivado (continuación)

Opción	Descripción
fbreposlocation "Fbreposlocation" en la página 435	Especifica la ubicación del repositorio de Tivoli Storage Manager FastBack para el proxy del cliente de IBM Spectrum Protect para conectarse y emitir los mandatos MOUNT DUMP , MOUNT ADD y MOUNT DEL .
fbserver "Fbserver" en la página 436	Especifica el nombre de host de la estación de trabajo del servidor FastBack o de la estación de trabajo FastBack Disaster Recovery Hub que es propietaria del repositorio especificado por la opción fbreposlocation.
fbvolumename "Fbvolumename" en la página 438	Especifica el nombre de uno o más volúmenes de Tivoli Storage Manager FastBack para hacer una copia de seguridad desde el proxy de copia de seguridad.
filelist "Filelist" en la página 439	Especifica una lista de archivos para que los procese el mandato. El cliente abre la lista de archivos designada y procesa los archivos que contiene la lista de acuerdo con el mandato.
filesonly "Filesonly" en la página 443	Realiza copias de seguridad, restaura, recupera o efectúa consultas sólo de archivos.
groupname "Groupname" en la página 449	Utilice esta opción con el mandato backup group para especificar el nombre completo del líder de un grupo.
ieobjtype "Ieobjtype" en la página 452	Especifica un tipo de objeto para la operación de eliminación de duplicación de datos del lado del cliente. Esta opción se utiliza con las opciones include.dedup y exclude.dedup.
imagegapsize "Imagegapsize" en la página 454	Especifica el tamaño mínimo de las regiones vacías en un volumen que desee omitir durante una copia de seguridad de imagen. Esta opción es válida para clientes AIX JFS2.
inlexcl "Inlexcl" en la página 456	Especifica la ruta y el nombre de archivo de un archivo de opciones de inclusión/exclusión.
"Opciones include" en la página 458	Utilice estas opciones para incluir archivos o asignar clases de gestión para el proceso de copias de seguridad.
include include.backup include.file	
include.archive "Opciones include" en la página 458	Incluye archivos o asigna clases de gestión para los procesos de archivado.

Tabla 58. Opciones de proceso de copia de seguridad/archivado (continuación)

Opción	Descripción
<code>include.attribute.symlink</code> "Opciones include" en la página 458	Incluye un archivo o un grupo de archivos que son vínculos simbólicos o alias (los alias se aplican a Mac OS X) de un grupo amplio de archivos excluidos en el proceso de copia de seguridad.
<code>include.compression</code> "Opciones include" en la página 458	Incluye archivos para el proceso de compresión si establece la opción <code>compression</code> en <i>yes</i> . Esta opción se aplica a copias de seguridad y copias archivadas.
<code>include.encrypt</code> "Opciones include" en la página 458	Incluye los archivos especificados para el proceso de cifrado. De forma predeterminada, el cliente no realiza el proceso de cifrado.
<code>include.fs</code> "Opciones include" en la página 458	Utilice la opción <code>include.fs</code> para controlar cómo el cliente procesa el espacio de archivos en la copia de seguridad incremental.
<code>include.fs.nas</code> "Opciones include" en la página 458	Utilice la opción <code>include.fs.nas</code> para vincular una clase de gestión a sistemas de archivos de almacenamiento conectado a red (NAS). También puede especificar si el cliente ha de guardar la información de la Tabla de contenido (TOC) durante una copia de seguridad de imágenes del sistema de archivos NAS, utilizando la opción <code>toc</code> con la opción <code>include.fs.nas</code> en el archivo <code>dsm.sys</code> . Para obtener más información, consulte el apartado "Toc" en la página 596. Esta opción solo es válida para los clientes AIX y Solaris.
<code>include.image</code> "Opciones include" en la página 458	Especifica el sistema de archivos o el volumen lógico que debe incluirse para el proceso de copia de seguridad de imagen. Esta opción también proporciona un método para especificar una asignación de clase de gestión explícita para un sistema de archivos o un volumen lógico específico. El mandato <code>backup image</code> ignora todas las demás opciones de inclusión. Esta opción es válida para AIX, Solaris y todos los clientes Linux.
<code>incrbydate</code> "Incrbydate" en la página 474	Para solicitar una copia de seguridad incremental por fecha, utilice esta opción con el mandato incremental .

Tabla 58. Opciones de proceso de copia de seguridad/archivado (continuación)

Opción	Descripción
incremental "Incremental" en la página 475	Utilice esta opción con el mandato restore image para asegurarse de que los cambios efectuados en la imagen base también se apliquen a la imagen restaurada. Esta opción es válida para clientes AIX, Solaris y todos los de Linux.
memoryefficientbackup "Memoryefficientbackup" en la página 491	Especifica un algoritmo de copia de seguridad de bajo consumo de memoria para copias de seguridad incrementales cuando se utiliza con el mandato incremental .
mode "Mode" en la página 492	<p>Utilice la opción mode con estos mandatos, como se indica a continuación:</p> <p>backup image Para especificar si ha de realizarse una copia de seguridad de imagen selectiva o incremental de los sistemas de archivos de cliente.</p> <p>backup nas Para especificar si ha de realizarse una copia de seguridad de imagen completa o diferencial de los sistemas de archivos NAS.</p> <p>backup group Para especificar si ha de realizarse una copia de seguridad de grupo completa o diferencial que contenga una lista de archivos de uno o más orígenes de espacio de archivos.</p> <p>backup vm Para especificar si se debe realizar una copia de seguridad selectiva o incremental de sistemas VMware.</p>
monitor "Monitor" en la página 496	Especifica si desea supervisar una copia de seguridad de imagen de los sistemas de archivos pertenecientes a un servidor de archivos de almacenamiento conectado a red (NAS).
noprompt "Noprompt" en la página 503	Suprime la solicitud de confirmación que presentan los mandatos delete group , delete archive , expire y set event .
noprompt "Noprompt" en la página 503	Suprime la solicitud de confirmación que presentan los mandatos delete group , delete archive , expire , restore image y set event .

Tabla 58. Opciones de proceso de copia de seguridad/archivado (continuación)

Opción	Descripción
nojournal "Nojournal" en la página 502	Utilice esta opción con el mandato incremental para especificar que desea realizar la copia de seguridad incremental completa tradicional, en lugar de realizar la copia de seguridad con registro por diario predeterminada.
optfile "Optfile" en la página 506	Especifica el archivo de opciones del cliente que desea utilizar para iniciar una sesión del cliente de copia de seguridad y archivado.
postsnapshotcmd "Postsnapshotcmd" en la página 516	Durante una copia de seguridad basada en instantáneas, esta opción le permite abrir de forma manual una aplicación después de crear la instantánea. Esta opción es válida sólo para las operaciones basadas en instantáneas de JFS2 de AIX o LVM de Linux.
preservelastaccessdate "Preservelastaccessdate" en la página 519	Puede utilizar esta opción durante una operación de copia de seguridad o archivado para especificar si debe restablecer la fecha del último acceso de cualquier archivo especificado a su valor original tras una after operación de copia de seguridad o archivado. De forma predeterminada, el cliente no reinicia la última fecha de acceso de ningún archivo de copia de seguridad o archivado a su valor original antes de realizar la operación de archivado o copia de seguridad.
presnapshotcmd "Presnapshotcmd" en la página 523	Durante una operación de copia de seguridad basada en instantáneas, esta opción permite detener manualmente una aplicación antes de crear la instantánea. Esta opción es válida solo para operaciones basadas en instantánea de AIX JFS2 o Linux LVM.
removeoperandlimit "Removeoperandlimit" en la página 528	Especifica que el cliente ha de eliminar el límite de 20 operandos. Si especifica la opción <code>removeoperandlimit</code> con los mandatos incremental , selective o archive , no se aplicará el límite de 20 operandos, y las únicas restricciones serán los recursos disponibles u otros límites del sistema operativo.
skipacl "Skipacl" en la página 559	Especifica si se debe omitir completamente el proceso de ACL.
skipaclupdatecheck "Skipaclupdatecheck" en la página 560	Especifica si se debe realizar la suma de comprobación y las comparaciones de tamaño antes y después de la copia de seguridad y durante el proceso incremental.

Tabla 58. Opciones de proceso de copia de seguridad/archivado (continuación)

Opción	Descripción
snapdiff “Snapdiff” en la página 561	Especifica una copia de seguridad incremental de los archivos que NetApp ha notificado como cambiados en lugar de explorar el volumen y buscar los archivos que han cambiado. Utilice esta opción con una copia de seguridad incremental de volumen completa de NAS.
snapshotcachesize “Snapshotcachesize” en la página 567	Linux y AIX únicamente: utilice esta opción para especificar un tamaño de instantánea adecuado para que se puedan almacenar todos los bloques de datos anteriores durante la modificación y supresión de archivos. Un tamaño de instantánea del 100% asegurará que la instantánea sea válida. El valor predeterminado es 100 por ciento.
snapshotproviderfs “Snapshotproviderfs” en la página 569	Utilice la opción snapshotproviderfs para habilitar las operaciones de archivado y copia de seguridad de archivo basadas en instantáneas, y para especificar un proveedor de instantáneas. Debe ser un usuario root para poder realizar una operación de archivado o de copia de seguridad de archivos basada en instantáneas. Si no es usuario root, la operación fallará y mostrará un mensaje de error.
snapshotproviderimage “Snapshotproviderimage” en la página 570	Utilice la opción snapshotproviderimage para activar la copia de seguridad de imágenes basada en instantánea y para especificar un proveedor de instantáneas. Debe ser usuario root para realizar una operación de copia de seguridad de imagen basada en instantáneas. Si no es usuario root, la operación fallará y mostrará un mensaje de error.
snapshotroot “Snapshotroot” en la página 571	Utilice la opción snapshotroot con los mandatos incremental , selective o archive con una aplicación de un proveedor de software independiente que proporcione una instantánea de un volumen lógico para asociar los datos de la instantánea local a los datos del espacio de archivos reales que se almacenan en el servidor de IBM Spectrum Protect. Esta opción es válida para todos los clientes UNIX y Linux.
subdir “Subdir” en la página 581	Especifica si deben incluirse los subdirectorios de un directorio especificado.

Tabla 58. Opciones de proceso de copia de seguridad/archivado (continuación)

Opción	Descripción
tapeprompt "Tapeprompt" en la página 583	Especifica si el cliente debe esperar el montaje de la cinta cuando éste sea necesario en un proceso de copia de seguridad, archivado, restauración o recuperación, o si se debe preguntar al usuario.
toc "Toc" en la página 596	Utilice la opción toc con el mandato backup nas o la opción include.fs.nas para especificar si el cliente ha de guardar la información de la Tabla de contenido (TOC) para cada copia de seguridad del sistema de archivos. Si guarda la información de la TOC, podrá utilizar el mandato de servidor QUERY TOC para determinar el contenido de la copia de seguridad de un sistema de archivos con el mandato de servidor RESTORE NODE para restaurar archivos individuales o árboles de directorios. También puede utilizar el cliente web para examinar todo el árbol del sistema de archivos y seleccionar los archivos y directorios que han de restaurarse.
type "Type" en la página 600	Utilice la opción type con el mandato query node para especificar el tipo de nodo que ha de consultarse.
v2archive "V2archive" en la página 603	Utilice la opción v2archive con el mandato archive para realizar el archivado sólo de los archivos en el servidor. El cliente no procesa los directorios que existen en la vía de acceso de la especificación de archivo de origen.
virtualfsname "Virtualfsname" en la página 606 (no se aplica a Mac OS X)	Utilice esta opción con el mandato backup group para especificar el nombre del contenedor del grupo en el que desea realizar la operación.
virtualmountpoint "Virtualmountpoint" en la página 606	Define un punto de montaje virtual para un sistema de archivos si desea realizar una copia de seguridad de los archivos que empiezan en un directorio determinado de dicho sistema de archivos.
vmchost "Vmchost" en la página 612	Utilizado con los mandatos backup VM , restore VM o query VM para especificar el nombre de host del servidor de VMware VirtualCenter o ESX donde se dirigen los mandatos.
vmcpw "Vmcpw" en la página 613	Utilizado con los mandatos backup VM , restore VM o query VM para especificar la contraseña de VirtualCenter o del usuario ESX que se especifica con la opción vmcuser.

Tabla 58. Opciones de proceso de copia de seguridad/archivado (continuación)

Opción	Descripción
vmcuser "Vmcuser" en la página 615	Utilizado con los mandatos backup VM , restore VM o query VM para especificar el nombre de usuario del servidor de VMware VirtualCenter o ESX donde se dirigen los mandatos.
vmmxvirtualdisks "Vmmxvirtualdisks" en la página 629	Se utiliza con el mandato backup VM para especificar el tamaño máximo de los discos de máquina virtual (VMDK) VMware a incluir en una operación de copia de seguridad.
vmskipmaxvirtualdisks "Vmskipmaxvirtualdisks" en la página 638	Se utiliza con el mandato backup VM para especificar cómo la operación de copia de seguridad procesa los discos de máquina virtual (VMDK) VMware que superan el tamaño de disco máximo. En V7.1.3 y anterior, la opción vmskipmaxvirtualdisks se llamaba vmskipmaxvmdks.

Opciones de proceso de restauración y recuperación

Puede utilizar opciones de cliente para controlar algunos aspectos del proceso de restauración y recuperación.

Tabla 59 enumera las opciones de proceso de restauración y recuperación que están disponibles.

Tabla 59. Opciones de proceso de restauración y recuperación

Opción	Descripción
dirsonly "Dirsonly" en la página 390	Califica la operación (copia de seguridad, archivado, restauración, recuperación) para que procese sólo directorios.
disablenqr "Disablenqr" en la página 391	Especifica si el cliente de copia de seguridad y archivado puede utilizar el método de restauración sin consulta para restaurar archivos y directorios desde el servidor.
filelist "Filelist" en la página 439	Especifica un archivo que contiene una lista de archivos que deben procesarse mediante el mandato especificado.
filesonly "Filesonly" en la página 443	Califica la operación (copia de seguridad, archivado, restauración, recuperación) para que procese sólo archivos.
followsymbolic "Followsymbolic" en la página 444	Especifica si desea restaurar archivos en vínculos simbólicos o utilizar un vínculo simbólico como punto de montaje virtual.
fromdate "Fromdate" en la página 446	Utilice la opción fromdate con la opción fromtime para especificar una fecha y una hora a partir de las cuales desea buscar copias de seguridad o copias archivadas durante una operación de restauración, recuperación o consulta.

Tabla 59. Opciones de proceso de restauración y recuperación (continuación)

Opción	Descripción
fromnode "Fromnode" en la página 447	Permite que un nodo realice mandatos para otro nodo. Un usuario de otro nodo debe utilizar el mandato set access para permitirle consultar, restaurar o recuperar archivos o imágenes del otro nodo.
fromowner "Fromowner" en la página 448	Muestra los espacios de archivos de un propietario alternativo. También especifica un propietario alternativo desde el que restaurar o recuperar archivos.
fromtime "Fromtime" en la página 448	Utilice la opción fromtime con la opción fromdate para especificar una fecha a partir de las cuales desea buscar copias de seguridad o copias archivadas durante una operación de restauración, recuperación o consulta.
ifnewer "Ifnewer" en la página 453	Sustituye un archivo existente por la última versión de copia de seguridad si ésta es más reciente que el archivo existente.
imagetofile "Imagetofile" en la página 455	Utilice la opción imagetofile con el mandato restore image para especificar que desea restaurar la imagen de origen en un archivo. Puede que tenga que restaurar la imagen de un archivo en caso de que existan sectores defectuosos en el volumen de destino o si desea manipular los datos de la imagen. Esta opción es válida para clientes AIX, Linux y Solaris.
inactive "Inactive" en la página 456	Muestra una lista de los archivos activos e inactivos cuando se utiliza con la opción pick.
latest "Latest" en la página 483	Restaura la última versión de copia de seguridad de un archivo independientemente de que esté activa o inactiva.
localbackupset "Localbackupset" en la página 484	Especifica si la GUI del cliente de copia de seguridad y archivado pasa por alto la conexión inicial con el servidor para restaurar un juego de copias de seguridad locales en una estación de trabajo independiente.
makesparsefile "Makesparsefile" en la página 484 (no se aplica a Mac OS X)	Utilice la opción makesparsefile con los mandatos restore o retrieve para especificar el modo en que los archivos esparcidos se volverán a crear.
monitor "Monitor" en la página 496	Especifica si desea supervisar una restauración de imagen de uno o más sistemas de archivos pertenecientes a un servidor de archivos de almacenamiento conectado a red (NAS).
noprompt "Noprompt" en la página 503	Suprime la solicitud de confirmación que presentan los mandatos delete group , delete archive , expire y set event .
noprompt "Noprompt" en la página 503	Suprime la solicitud de confirmación que presentan los mandatos delete group , delete archive , expire , restore image y set event .
optfile "Optfile" en la página 506	Especifica el archivo de opciones del cliente que desea utilizar para iniciar una sesión del cliente de copia de seguridad y archivado.

Tabla 59. Opciones de proceso de restauración y recuperación (continuación)

Opción	Descripción
pick "Pick" en la página 512	Crea una lista de versiones de copia de seguridad, imágenes o copias archivadas que coinciden con la especificación de archivo que se entre. En esta lista, puede seleccionar las versiones que se desee procesar. Incluya la opción <code>inactive</code> para ver los objetos activos e inactivos.
pitdate "Pitdate" en la página 512	Utilice la opción <code>pitdate</code> con la opción <code>pittime</code> para establecer un instante específico para el cual desea visualizar o restaurar la última versión de las copias de seguridad.
pittime "Pittime" en la página 513	Utilice la opción <code>pittime</code> con la opción <code>pitdate</code> para establecer un instante específico para el cual desea visualizar o restaurar la última versión de las copias de seguridad.
preservepath "Preservepath" en la página 520	Especifica qué volumen del directorio origen se reproducirá como parte del directorio destino cuando se restauran o recuperan archivos en una ubicación nueva.
replace "Replace" en la página 529	Especifica si debe sustituirse un archivo existente o si debe solicitársele su elección al restaurar o recuperar archivos.
showmembers "Showmembers" en la página 559 (no se aplica a Mac OS X)	Visualiza todos los miembros de un grupo.
subdir "Subdir" en la página 581	Especifica si desea incluir los subdirectorios de un directorio especificado.
tapeprompt "Tapeprompt" en la página 583	Especifica si desea que el cliente de copia de seguridad y archivado espere el montaje de una cinta que es necesaria para una operación de restauración o recuperación, o si debe preguntar al usuario.
todate "Todate" en la página 597	Utilice la opción <code>todate</code> con la opción <code>totime</code> para especificar una fecha y una hora finales hasta las que desea buscar copias de seguridad o copias archivadas durante una operación de restauración, recuperación o consulta.
totime "Totime" en la página 598	Utilice la opción <code>totime</code> con la opción <code>todate</code> para especificar una fecha y una hora finales hasta las que desea buscar copias de seguridad o copias archivadas durante una operación de restauración, recuperación o consulta.
type "Type" en la página 600	Utilice la opción <code>type</code> con el mandato query node para especificar el tipo de nodo que ha de consultarse.
verifyimage "Verifyimage" en la página 605	Utilice la opción <code>verifyimage</code> con el mandato restore image para especificar que desea activar la detección de los sectores defectuosos en el volumen de destino. Si se detectan sectores defectuosos en el volumen de destino, el cliente emite un mensaje de aviso en la consola y en el registro de errores.

Las siguientes opciones son opciones del cliente de copia de seguridad y archivado que se aplican a los archivos migrados de IBM Spectrum Protect HSM for

Windows. Para obtener más información sobre estas opciones, consulte los temas del IBM Knowledge Center en http://www.ibm.com/support/knowledgecenter/SSERFH_8.1.0/hsmwin/welcome.html.

- Checkreparsecontent
- Restorecheckstubaccess
- Restoremigstate
- Skipmigrated

Las siguientes opciones son opciones del cliente de copia de seguridad y archivado que se aplican a los archivos migrados de IBM Spectrum Protect for Space Management. Para obtener más información sobre estas opciones, consulte los temas del IBM Knowledge Center en http://www.ibm.com/support/knowledgecenter/SSERBH_8.1.0/hsmul/welcome.html.

- Restoremigstate
- Skipmigrated

Opciones de planificación

En este tema se explican las opciones que puede utilizar para regular la planificación central. El cliente de copia de seguridad y archivado sólo utiliza las opciones de planificación cuando el planificador está en ejecución.

Tabla 60 enumera las opciones de planificación que están disponibles.

Tabla 60. Opciones de planificación

Opción	Descripción
cadlistenonport “Cadlistenonport” en la página 362	Especifica si se deben abrir puertos de escucha para el aceptador de clientes cuando este se utiliza para gestionar planificaciones en modalidad de sondeo.
managedservices “Managedservices” en la página 486	Especifica si el aceptador de clientes gestiona el cliente web, el planificador o ambos programas.
maxcmdretries “Maxcmdretries” en la página 488	Especifica el número máximo de veces que el planificador cliente intenta procesar un mandato planificado que da error.
postschedulecmd/postnschedulecmd “Postschedulecmd/Postnschedulecmd” en la página 514	Especifica un mandato que debe procesarse después de la ejecución de una planificación.
preschedulecmd/preschedulecmd “Preschedulecmd/Preschedulecmd” en la página 517	Especifica un mandato que debe procesarse antes de la ejecución de una planificación.
querryschedperiod “Querryschedperiod” en la página 524	Especifica el número de horas que el planificador cliente espera entre intentos de establecer contacto con el servidor para realizar trabajos planificados.
retryperiod “Retryperiod” en la página 542	Especifica el número de minutos que el planificador cliente debe esperar entre los intentos de procesar un mandato planificado que da error o entre los intentos fallidos de informar de los resultados al servidor.

Tabla 60. Opciones de planificación (continuación)

Opción	Descripción
<code>schedcmddisabled</code> “Schedcmddisabled” en la página 544	Especifica si debe desactivarse la planificación de mandatos genéricos especificados por el administrador de IBM Spectrum Protect.
<code>schedcmduser</code> (solo servidor definido) “Opciones del planificador para los mandatos” en la página 292	El planificador ejecuta mandatos con el identificador de usuario 0; sin embargo, puede que haya otros usuarios que tengan identificadores de usuario distintos. En ese caso, con esta opción el administrador de IBM Spectrum Protect puede definir planificaciones y permitir que éstas se ejecuten bajo un identificador de usuario diferente de 0. La API de cliente de IBM Spectrum Protect no admite esta opción.
<code>schedlogmax</code> “Schedlogmax” en la página 545	Especifica el tamaño máximo de las anotaciones del planificador y las anotaciones de cliente web, en megabytes.
<code>schedlogname</code> “Schedlogname” en la página 547	Especifica la ruta y el nombre de archivo donde desea almacenar la información de anotaciones de planificación.
<code>schedlogretention</code> “Schedlogretention” en la página 549	Especifica el número de días que se van a mantener las entradas del archivo de anotaciones en las anotaciones de planificación y las anotaciones del cliente web, y si se guardan las entradas eliminadas.
<code>schedmode</code> “Schedmode” en la página 550	Especifica qué modo de planificación se va a utilizar <i>polling</i> o <i>prompted</i> .
<code>schedrestretrdisabled</code> “Schedrestretrdisabled” en la página 552	Especifica si se va a impedir que el administrador del servidor de IBM Spectrum Protect ejecute las operaciones planificadas de restauración o recuperación.
<code>sessioninitiation</code> “Sessioninitiation” en la página 556	Utilice la opción <code>sessioninitiation</code> para controlar si el servidor o el cliente ha de iniciar las sesiones a través de un cortafuegos. El valor predeterminado es que el cliente puede iniciar sesiones.
<code>srvprepostscheddisabled</code> “Srvprepostscheddisabled” en la página 574	Especifica si se va a impedir que el administrador del servidor de IBM Spectrum Protect ejecute los mandatos de preplanificación y postplanificación al realizar operaciones planificadas.
<code>srvprepostsnapdisabled</code> “Srvprepostsnapdisabled” en la página 575	Especifica si se va a impedir que el administrador del servidor de IBM Spectrum Protect ejecute los mandatos previos y posteriores a la instantánea al realizar operaciones planificadas de copia de seguridad de instantáneas de imagen.

Tabla 60. Opciones de planificación (continuación)

Opción	Descripción
tcpclientaddress "Tcpclientaddress" en la página 587	Especifica una dirección TCP/IP si el nodo cliente tiene más de una dirección y desea que el servidor contacte con una dirección distinta de la utilizada para realizar el primer contacto del servidor. El servidor utilizará esta dirección cuando comience la operación planificada por petición de servidor. Consulte schedmode <i>prompted</i> ("Schedmode" en la página 550) para obtener información detallada.
tcpclientport "Tcpclientport" en la página 588	Especifica un número de puerto TCP/IP para que el servidor contacte con el cliente cuando el servidor comience la operación planificada por petición de servidor. Consulte schedmode <i>prompted</i> ("Schedmode" en la página 550) para obtener información detallada.

Opciones de formato e idioma

Las opciones de formato e idioma le permiten seleccionar formatos diferentes para fecha, hora y números para idiomas diferentes.

Las opciones de formato le permiten seleccionar formatos diferentes para fecha, hora y números.

Tabla 61. Opciones de formato e idioma

Opción	Descripción
dateformat "Dateformat" en la página 376	Especifica el formato para visualizar fechas.
numberformat "Numberformat" en la página 504	Especifica el formato para visualizar números.
timeformat "Timeformat" en la página 592	Especifica el formato para visualizar la hora.

Opciones de proceso de mandatos

En este tema se explican las opciones que puede utilizar con los mandatos del cliente de copia de seguridad y archivado.

Opciones de proceso de mandato que permiten controlar parte del formateo de datos en la pantalla terminal.

Tabla 62. Opciones de proceso de mandatos

Opción	Descripción
quiet "Quiet" en la página 526	Limita el número de mensajes que se muestran en la pantalla durante el proceso. Esta opción puede ser modificada temporalmente por el servidor.
scrolllines "Scrolllines" en la página 552	Especifica el número de líneas de información que deben aparecer en pantalla a la vez. Utilice esta opción sólo si scrollprompt está establecida en <i>yes</i> .

Tabla 62. Opciones de proceso de mandatos (continuación)

Opción	Descripción
scrollprompt "Scrollprompt" en la página 553	Especifica si se desea que el cliente de copia de seguridad y archivado se detenga y espere después de visualizar el número de líneas de información que ha especificado con la opción scrolllines o bien si se desea que se desplace hasta el final de la lista de información y se detenga.
verbose "Verbose" en la página 604	Especifica que la información de proceso debe visualizarse en la ventana. La alternativa es quiet. Esta opción puede ser modificada temporalmente por el servidor.

Opciones de autorización

Las opciones de autorización controlan el acceso al servidor de IBM Spectrum Protect.

Tabla 63 enumera las opciones de autorización que están disponibles.

Tabla 63. Opciones de autorización

Opción	Descripción
autodeploy "Autodeploy" en la página 355	Especifica si desea habilitar o inhabilitar un despliegue automático del cliente si es necesario un reinicio.
groups "Grupos (obsoleto)" en la página 450	Especifica los grupos de la estación de trabajo a los que se desea autorizar para que soliciten los servicios de IBM Spectrum Protect al servidor.
password "Contraseña" en la página 507	Especifica la contraseña de IBM Spectrum Protect.
passwordaccess "Passwordaccess" en la página 509	Especifica si se desea utilizar una contraseña generada o si debe aparecer una solicitud para la contraseña cada vez que inicie el cliente.
passworddir "Passworddir" en la página 511	Especifica el directorio en el que desea almacenar la contraseña generada dinámicamente para su nodo cliente. La clave y la contraseña de cifrado se cifran y almacenan en el archivo TSM.PWD.
revokeremoteaccess "Revokeremoteaccess" en la página 543	Impide que un administrador con privilegios de acceso a cliente acceda a una estación de trabajo a través del cliente web.
users "Usuarios (obsoleto)" en la página 603	Autoriza a determinados usuarios de la estación de trabajo a que soliciten servicios de un servidor.

Opciones de proceso de errores

Las opciones de proceso de errores especifican el nombre del archivo de registro de errores y cómo el cliente de copia de seguridad y archivado trata las entradas del archivo de registro.

Tabla 64 en la página 334 enumera las opciones de proceso de errores que están disponibles.

Tabla 64. Opciones de proceso de errores

Opción	Descripción
errorlogmax "Errorlogmax" en la página 420	Especifica el tamaño máximo de las anotaciones de errores, en megabytes.
errorlogname "Errorlogname" en la página 422	Especifica la ruta completa y el nombre de archivo donde desea almacenar información acerca de los errores que se produzcan durante el proceso.
errorlogretention "Errorlogretention" en la página 423	Especifica durante cuántos días van a conservarse las entradas de las anotaciones de errores antes de eliminarlas y si se van a guardar las entradas eliminadas.

Opciones de proceso de transacciones

Las opciones de proceso de transacciones controlan el modo en que se procesan las transacciones entre el servidor y el cliente de IBM Spectrum Protect.

Tabla 65 enumera las opciones de proceso de transacciones que están disponibles.

Tabla 65. Opciones de proceso de transacciones

Opción	Descripción
collocatebyfilespec "Collocatebyfilespec" en la página 365	Especifica que se desea que el cliente de copia de seguridad y archivado utilice solamente una sesión de servidor para enviar objetos generados desde una especificación de archivo. El establecimiento de la opción <code>collocatebyfilespec</code> en <i>yes</i> eliminará la entremezcla de archivos de distintas especificaciones de archivo, limitando al cliente a una única sesión de servidor por especificación de archivo. Por consiguiente, si almacena los datos en una cinta, los archivos para cada especificación de archivo se almacenan conjuntamente en una cinta (a menos que se necesite otra para mayor capacidad).
commrestartduration "Commrestartduration" en la página 367	Especifica el número máximo de minutos durante los que se desea que el cliente intente volver a conectarse al servidor de IBM Spectrum Protect después de producirse un error en la comunicación.
commrestartinterval "Commrestartinterval" en la página 368	Especifica el número de segundos que el cliente debe esperar entre los reintentos de conexión al servidor de IBM Spectrum Protect después de producirse un error de comunicación.
diskbuffsize "Diskbuffsize" en la página 392	Especifica el tamaño máximo de búfer de E/S del disco (en kilobytes) que el cliente puede utilizar al leer archivos.
largecommbuffers "Diskbuffsize" en la página 392	Esta opción se ha sustituido por la opción <code>diskbuffsize</code> . En este momento, el cliente de archivado y copia de seguridad sigue aceptando la opción <code>largecommbuffers</code> para facilitar la transición a la nueva. No obstante, el valor especificado por <code>largecommbuffers</code> se omite en favor del valor de <code>diskbuffsize</code> . Importante: Deje de utilizar <code>largecommbuffers</code> , ya que es posible que releases posteriores del cliente no acepten esta opción.
nfstimeout "Nfstimeout" en la página 500	Especifica el número de segundos que el servidor espera a que se reciba una llamada de estado del sistema en un sistema de archivos NFS antes de que se exceda el tiempo de espera.

Tabla 65. Opciones de proceso de transacciones (continuación)

Opción	Descripción
resourceutilization "Resourceutilization" en la página 539	Utilice la opción resourceutilization en el archivo dsm.sys para regular el nivel de recursos que el servidor y el cliente de IBM Spectrum Protect pueden utilizar durante el proceso.
txnbytelimit "Txnbytelimit" en la página 599	Especifica el número de kilobytes que el programa cliente guarda en el búfer antes de enviar una transacción al servidor.

Opciones de cliente Web

Para configurar el cliente web IBM Spectrum Protect se utilizan varias opciones de cliente de archivado y copia de seguridad.

Tabla 66 enumera las opciones de cliente web que están disponibles.

Tabla 66. Opciones de cliente Web

Opción	Descripción
httpport "Httpport" en la página 450	Especifica una dirección de puerto TCP/IP para el cliente web.
managedservices "Managedservices" en la página 486	Especifica si el daemon de aceptación de clientes gestiona el cliente web, el planificador o ambos programas.
revokeremoteaccess "Revokeremoteaccess" en la página 543	Restringe el acceso de un administrador a una estación de trabajo cliente a través del cliente web.
webports "Webports" en la página 650	Permite utilizar el cliente web fuera de un cortafuegos especificando el número de puerto TCP/IP utilizado por el daemon de aceptación de clientes y el servicio de agente de cliente web para las comunicaciones con el cliente web.

Opciones de diagnóstico

Utilice el mandato **query systeminfo** para recopilar información sobre el sistema de IBM Spectrum Protect y colocar dicha información en un archivo o en la consola.

El mandato **query systeminfo** está concebido principalmente como una ayuda de diagnóstico. Puede enviar la información resultante al personal del servicio técnico para resolver los problemas de diagnóstico.

Tabla 67 enumera las opciones de diagnóstico que están disponibles.

Tabla 67. Opciones de diagnóstico

Opción	Descripción
console "Console" en la página 372	Utilice la opción console con el mandato query systeminfo para que la información del sistema se visualice en la consola.

Tabla 67. Opciones de diagnóstico (continuación)

Opción	Descripción
filename "Filename" en la página 442	Utilice la opción filename con el mandato query systeminfo para especificar un nombre de archivo en el que almacenar la información del sistema.

Referencia relacionada:

"Query Systeminfo" en la página 739

Utilización de opciones con mandatos

Puede modificar temporalmente diversas opciones del archivo de opciones del cliente (dsm.opt) especificándolas con los mandatos adecuados del cliente de copia de seguridad y archivado.

Puede modificar temporalmente diversas opciones del archivo dsm.sys o del archivo de opciones del usuario cliente (dsm.opt) especificándolas con los mandatos adecuados del cliente de copia de seguridad y archivado.

El cliente procesa las opciones siguiendo este orden (precedencia):

1. Opciones definidas en el servidor con opciones del cliente obligadas por el servidor. El servidor modifica los valores del cliente.
2. Opciones escritas localmente en la línea de mandatos.
3. Opciones definidas en el servidor para una planificación utilizando los parámetros de las opciones.
4. Opciones escritas localmente en el archivo de opciones.
5. Opciones recibidas del servidor con opciones del cliente no establecidas como implementadas por el servidor. El servidor *no* modifica los valores del cliente si no se le fuerza a ello.
6. Valores predeterminados de la opción.

El cliente también incluye un grupo de opciones de mandatos de cliente que pueden entrarse *únicamente* en la línea de mandatos con mandatos específicos. Para obtener una lista completa de las opciones de línea de mandatos y una descripción, y para determinar a dónde debe dirigirse para obtener información adicional, consulte el tema Tabla 68 en la página 338.

Especificación de opciones con un mandato

Debe seguir las reglas generales que se aplican a la especificación de opciones con un mandato.

- Escriba un mandato, un guión (-), el nombre de la opción, un signo de igual (=) y un parámetro o valor para la opción. No incluya ningún espacio a ambos lados del signo =.

A continuación, se muestran algunos ejemplos de esta sintaxis en distintos clientes:

```
dsmc archive -description="year end 1999" /home/
```

- Para opciones que no incluyen parámetros, escriba un mandato, un guión (-) y el nombre de la opción. Por ejemplo:

```
dsmc incremental -quiet
```

Nota: utilice un guión (-) para indicar que el texto que sigue es el nombre de una opción. Si un nombre de objeto empieza con un guión, deberá especificar éste entre comillas simples (') o bien entre comillas dobles ("). La mayoría de los

procesadores de línea de mandatos del sistema eliminan las comillas antes de enviar los argumentos de la línea de mandatos a la aplicación cliente de IBM Spectrum Protect. En esos casos, puede utilizar caracteres de escape o indicar el doble de comillas para que el cliente pueda recibir un nombre de objeto entre comillas. En la modalidad de bucle, especifique este tipo de objetos entre comillas simples (') o bien entre comillas dobles (").

- Puede escribirse el nombre de opción o una abreviatura del nombre de opción. Por ejemplo, para la opción `latest`, escriba `-lat` o `-latest`. En la sintaxis de la opción, las letras mayúsculas indican la abreviatura mínima del nombre de dicha opción.

- Entre las opciones antes o después de los parámetros del mandato. Por ejemplo, puede entrar la opción antes o después de una especificación de archivo:

```
dsmc selective -subdir=yes "/home/devel/proj1/*"  
dsmc selective "/home/devel/proj1/*" -subdir=yes
```

- Si especifica varias opciones en un mandato, separe cada una de ellas con un espacio en blanco.

- Si el valor de la opción que entre contiene un espacio en blanco, especifique el valor entre comillas (" "). Por ejemplo:

```
dsmc archive -description="Project A" "/home/devel/proj1/*"
```

- La mayor parte de opciones que se especifican en la línea de mandatos alteran temporalmente el valor establecido en el archivo de preferencias. Sin embargo, cuando utiliza la opción `domain` con el mandato **incremental**, ésta se añade al dominio especificado en el archivo de opciones del cliente en lugar de modificar temporalmente el valor actual.

- En AIX, Solaris, Linux on z y Mac: el número máximo de caracteres de un nombre de archivo es 255. La longitud máxima combinada del nombre del archivo y del nombre de la vía de acceso es de 1024 caracteres. La representación Unicode de un carácter puede ocupar varios bytes, de modo que el número máximo de caracteres que un nombre de archivo contiene puede variar.

- En Linux: la longitud máxima de un nombre de archivo es de 255 bytes. La longitud máxima combinada del nombre del archivo y del nombre de la vía de acceso es de 4096 bytes. Esta longitud coincide con el valor `PATH_MAX` soportado por el sistema operativo. La representación Unicode de un carácter puede ocupar varios bytes, por lo tanto, el número máximo de caracteres de los que consta un nombre de vía de acceso y de archivo puede variar. La limitación real es el número de bytes de los componentes de vía de acceso y archivo, que puede corresponder o no a un número de caracteres igual.

En Linux: para las operaciones de archivado o recuperación, la longitud máxima que se puede especificar para una vía de acceso y un nombre de archivo (combinados) se mantiene en 1024 bytes.

- Para Mac OS X, la longitud máxima de un nombre de archivo se limita a 504 bytes (no caracteres). La representación Unicode de un carácter puede ocupar varios bytes, por lo tanto, el número máximo de caracteres que un nombre de archivo contiene puede variar.

La Tabla 68 en la página 338 muestra las opciones de mandatos de clientes que pueden especificarse únicamente en la línea de mandatos con mandatos específicos.

Tabla 68. Opciones de mandatos de cliente

Opción de mandato	Descripción	Mandatos
archmc "Archmc" en la página 347	Utilice la opción archmc con el mandato archive para especificar la clase de gestión disponible para el dominio de políticas a la que desea vincular las copias archivadas.	archive
class "Class" en la página 364	Especifica si se debe mostrar una lista de objetos NAS u objetos de cliente al utilizar los mandatos siguientes.	query backup delete filespace query filespace
console "Console" en la página 372	Utilice la opción console con el mandato query systeminfo para que la información del sistema se visualice en la consola.	query systeminfo
deletefiles "Deletefiles" en la página 383	Suprime la copia local de los archivos de la estación de trabajo después de que los archivos estén archivados en el servidor.	archive
deletefiles "Deletefiles" en la página 383	Suprime la copia local de los archivos de la estación de trabajo después de que los archivos estén archivados en el servidor. También puede utilizarse con el mandato restore image y la opción incremental para suprimir archivos de la imagen restaurada que se han suprimido del espacio de archivos después de la creación de la imagen.	archive restore image
description "Descripción" en la página 384	Asigna o especifica una descripción para los archivos cuando se efectúan operaciones de archivado, supresión, recuperación o consulta de archivado.	archive delete archive query archive query backupset retrieve
detail "Detail" en la página 385	Muestra información sobre la clase de gestión, el espacio de archivos, las copias de seguridad y las copias archivadas en función del mandato con el que se utilice.	delete filespace query archive query backup query filespace query mgmtclass
dirsonly "Dirsonly" en la página 390	Realiza copias de seguridad, restaura, archiva, recupera o efectúa consultas sólo de directorios.	archive incremental query archive query backup restore restore backupset retrieve selective
dynamicimage "Dynamicimage" en la página 410	Realiza una copia de seguridad de imagen dinámica.	backup image

Tabla 68. Opciones de mandatos de cliente (continuación)

Opción de mandato	Descripción	Mandatos
filelist "Filelist" en la página 439	Especifica una lista de archivos para que los procese el mandato. El cliente de copia de seguridad y archivado abre la lista de archivos designada y procesa los archivos que contiene la lista de acuerdo con el mandato.	archive backup group delete archive delete backup expire incremental query archive query backup restore retrieve selective
filename "Filename" en la página 442	Utilice la opción filename con el mandato query systeminfo para especificar un nombre de archivo en el que almacenar la información del sistema.	query systeminfo
filesonly "Filesonly" en la página 443	Realiza copias de seguridad, restaura, recupera o efectúa consultas sólo de archivos.	archive incremental query archive query backup restore restore backupset retrieve selective
fromdate "Fromdate" en la página 446	Utilice la opción fromdate con la opción fromtime para especificar una fecha y una hora a partir de las cuales desea buscar copias de seguridad o copias archivadas durante una operación de restauración, recuperación o consulta.	delete backup query archive query backup restore restore group retrieve
fromnode "Fromnode" en la página 447	Permite que un nodo realice mandatos para otro nodo. Un usuario de otro nodo debe utilizar el mandato set access para permitir que otro usuario consulte, restaure o recupere archivos o imágenes para el nodo del primer usuario.	query archive query backup query filespace query group query image query mgmtclass restore restore group restore image retrieve
fromowner "Fromowner" en la página 448	Muestra los espacios de archivos para otro propietario. También especifica otro propietario desde el que restaurar o recuperar archivos.	query archive query backup query group query image restore restore group restore image retrieve

Tabla 68. Opciones de mandatos de cliente (continuación)

Opción de mandato	Descripción	Mandatos
fromtime "Fromtime" en la página 448	Especifica una hora de comienzo en la fecha especificada. Se utiliza con la opción fromdate. Esta opción se pasa por alto si la opción fromdate no se ha especificado.	query archive query backup restore restore group retrieve
groupname "Groupname" en la página 449	Especifica el nombre completo de un grupo.	backup group
ifnewer "Ifnewer" en la página 453	Sustituye los archivos existentes con la última versión de copia de seguridad, si ésta es más reciente que la versión existente.	restore restore backupset restore group retrieve
imagnetofile "Imagnetofile" en la página 455	Utilice la opción imagnetofile con el mandato restore image para especificar que desea restaurar la imagen de origen en un archivo. Puede que tenga que restaurar la imagen de un archivo en caso de que existan sectores defectuosos en el volumen de destino o si desea manipular los datos de la imagen. Esta opción es válida para clientes de AIX, Linux y Oracle Solaris.	restore image
inactive "Inactive" en la página 456	Muestra una lista de los archivos activos e inactivos cuando se utiliza con la opción pick.	delete group query backup query group query image query nas restore restore group restore image restore nas
incrbydate "Incrbydate" en la página 474	Solicita una copia de seguridad incremental por fecha.	incremental
incremental "Incremental" en la página 475	Aplica cambios a la imagen base utilizando información de las copias de seguridad incrementales realizadas después de la copia de seguridad de imágenes original. Esta opción solo es válida para clientes de AIX, Linux x86_64, Linux on POWER y Oracle Solaris.	restore image
latest "Latest" en la página 483	Restaura la última versión de copia de seguridad de un archivo independientemente de que esté activa o inactiva.	restore restore group

Tabla 68. Opciones de mandatos de cliente (continuación)

Opción de mandato	Descripción	Mandatos
mode "Mode" en la página 492	<p>Utilice la opción mode con estos mandatos, como se indica a continuación:</p> <p>backup image Para especificar si ha de realizarse una copia de seguridad de imagen selectiva o incremental de los sistemas de archivos de cliente.</p> <p>backup nas Para especificar si ha de realizarse una copia de seguridad de imagen completa o diferencial de los sistemas de archivos NAS.</p> <p>backup group Para especificar si ha de realizarse una copia de seguridad de grupo completa o diferencial que contenga una lista de archivos de uno o más orígenes de espacio de archivos.</p>	<p>backup group backup nas backup image restore nas</p>
monitor "Monitor" en la página 496	<p>Especifica si desea supervisar una copia de seguridad o restauración de imagen de uno o más sistemas de archivos pertenecientes a un servidor de archivos de almacenamiento conectado a red (NAS).</p> <p>Especifica si desea supervisar una restauración de uno o más sistemas de archivos pertenecientes a un servidor de archivos de almacenamiento conectado a red (NAS).</p>	<p>backup nas restore nas</p>
nojournal "Nojournal" en la página 502	Utilice esta opción con el mandato incremental para especificar que desea realizar la copia de seguridad incremental completa tradicional, en lugar de realizar la copia de seguridad con registro por diario predeterminada.	incremental
noprompt "Noprompt" en la página 503	Suprime la solicitud de confirmación que presentan los mandatos delete group , delete archive , expire y set event .	<p>delete archive delete backup delete group expire</p>
noprompt "Noprompt" en la página 503	Suprime la solicitud de confirmación que presentan los mandatos delete group , delete archive , expire , restore image y set event .	<p>delete archive delete backup delete group expire restore image</p>
optfile "Optfile" en la página 506	Especifica el archivo de opciones del cliente que desea utilizar para iniciar una sesión del cliente de copia de seguridad y archivado.	dsmc
pick "Pick" en la página 512	Crea una lista de versiones de copia de seguridad, imágenes o copias archivadas que coinciden con la especificación de archivo que se entre. En esta lista, puede seleccionar las versiones que se desee procesar. Incluya la opción inactive para ver los objetos activos e inactivos.	<p>delete archive delete group expire query nas restore restore group restore image restore nas retrieve</p>

Tabla 68. Opciones de mandatos de cliente (continuación)

Opción de mandato	Descripción	Mandatos
pitdate "Pitdate" en la página 512	Utilice la opción pitdate con la opción pittime para establecer un instante específico para el cual desea visualizar o restaurar la última versión de las copias de seguridad.	query backup query group query image query nas restore restore group restore image restore nas
pittime "Pittime" en la página 513	Utilice la opción pittime con la opción pitdate para establecer un instante específico para el cual desea visualizar o restaurar la última versión de las copias de seguridad.	query backup query image query nas restore restore image restore nas
preservepath "Preservepath" en la página 520	Especifica qué volumen del directorio origen se reproducirá como parte del directorio destino cuando se restauran o recuperan archivos en una ubicación nueva.	restore restore backupset restore group retrieve
removeoperandlimit "Removeoperandlimit" en la página 528	Especifica que IBM Spectrum Protect ha de eliminar el límite de 20 operandos. Si especifica la opción removeoperandlimit con los mandatos incremental , selective o archive , no se aplicará el límite de 20 operandos, y las únicas restricciones serán los recursos disponibles u otros límites del sistema operativo.	incremental selective archive
showmembers "Showmembers" en la página 559	Visualiza todos los miembros de un grupo.	query group restore group
todate "Todate" en la página 597	Utilice la opción todate con la opción totime para especificar una fecha y una hora finales hasta las que desea buscar copias de seguridad o copias archivadas durante una operación de restauración, recuperación o consulta.	query archive query backup restore restore group retrieve
totime "Totime" en la página 598	Utilice la opción totime con la opción todate para especificar una fecha y una hora finales hasta las que desea buscar copias de seguridad o copias archivadas durante una operación de restauración, recuperación o consulta.	query archive query backup restore restore group retrieve
type "Type" en la página 600	Utilice la opción type con el mandato query node para especificar el tipo de nodo que ha de consultarse.	query node
v2archive "V2archive" en la página 603	Utilice la opción v2archive con el mandato archive para realizar el archivado sólo de los archivos en el servidor. El cliente no procesará los directorios que existen en la vía de acceso de la especificación de archivo de origen.	archive

Tabla 68. Opciones de mandatos de cliente (continuación)

Opción de mandato	Descripción	Mandatos
verifyimage “Verifyimage” en la página 605	Utilice la opción verifyimage con el mandato restore image para especificar que desea activar la detección de los sectores defectuosos en el volumen de destino. Si se detectan sectores defectuosos en el volumen de destino, el cliente emite un mensaje de aviso en la consola y en el registro de errores. Esta opción es válida para clientes de AIX, Linux y Oracle Solaris.	restore image
virtualfsname “Virtualfsname” en la página 606	Especifica el nombre del espacio de archivos virtual del grupo en el que desea ejecutar la operación.	backup group

Opciones que sólo son válidas en la línea de mandatos inicial

Un subconjunto de las opciones de cliente que solo es válido en la línea de mandatos inicial. Muchas de estas opciones establecen el entorno de ejecución, como las opciones commmethod u optfile. Las opciones de esta categoría no son válidas en las modalidades interactiva, de macro ni de planificador. Estas opciones generan un error y hacen que el proceso se detenga.

Tabla 69 lista las opciones que sólo son válidas en la línea de mandatos inicial.

Tabla 69. Opciones que sólo son válidas en la línea de mandatos inicial

Opciones válidas en la línea de mandatos inicial

commmethod	preschedulecmd/prenschedulecmd (puede incluirse en la definición de planificación)
eliminación de duplicados	querschedperiod
diskbuffsize	resourceutilization
editor	retryperiod
enablededupcache	schedlogmax
enablelanfree	schedlogname
errorlogmax	schedlogretention
errorlogname	schedmode
errorlogretention	servername
lanfreecommmethod	sessioninitiation
lanfreeshmport	tcpbuffsize
lanfreetcppport	tcpcadaddress
maxcmdretries	tcpclientaddress
nfstimeout	tcpclientport
nodename	tcpwindowsize
optfile	txnbytelimit
password	virtualnodename
postschedulecmd/postnschedulecmd (puede incluirse en la definición de planificación)	

Opciones del cliente que pueden establecerse con el servidor de IBM Spectrum Protect

Algunas opciones del cliente pueden establecerse con el servidor de IBM Spectrum Protect.

Tabla 70 en la página 344 enumera las opciones que pueden establecerse con el servidor.

Tabla 70. Opciones que pueden establecerse con el servidor de IBM Spectrum Protect
Opciones que pueden establecerse con el servidor de IBM Spectrum Protect

- "Afmskipuncachedfiles" en la página 346
- "Archsymlinkasfile" en la página 348
- "Changingretries" en la página 363
- "Collocatebyfilespec" en la página 365
- "Compressalways" en la página 369
- "Compression" en la página 370
- "Eliminación de duplicados" en la página 381
- "Dirmc" en la página 389
- "Disablenqr" en la página 391
- "Diskcachelocation" en la página 393
- "Domain" en la página 394
- "Domain.image" en la página 399
- "Domain.nas" en la página 400
- "Encryptiontype" en la página 417
- "Encryptkey" en la página 418
- "Opciones exclude" en la página 425
- "Incl excl" en la página 456
- "Opciones include" en la página 458
- maxcandprocsmaxcandprocs
- maxmigratorsmaxmigrators
- "Memoryefficientbackup" en la página 491
- "Nfstimeout" en la página 500
- "Postschedulecmd/Postnschedulecmd" en la página 514
- "Postsnapshotcmd" en la página 516
- "Preschedulecmd/Prenschedulecmd" en la página 517
- "Preserveleastaccessdate" en la página 519
- "Presnapshotcmd" en la página 523
- "Querschedperiod" en la página 524
- "Quiet" en la página 526
- "Resourceutilization" en la página 539
- "Retryperiod" en la página 542
- "Schedmode" en la página 550
- "Scrolllines" en la página 552
- "Scrollprompt" en la página 553
- "Snapshotcachesize" en la página 567
- "Snapshotproviderfs" en la página 569
- "Snapshotproviderimage" en la página 570
- "Stagingdirectory" en la página 581
- "Subdir" en la página 581
- "Tapeprompt" en la página 583
- "Txnbytelimit" en la página 599
- "Verbose" en la página 604
- "Vmchost" en la página 612
- "Vmcuser" en la página 615
- "Vmprocessvmwithindependent" en la página 634
- "Vmprocessvmwithprdm" en la página 636

Nota:

1. Consulte la documentación del producto IBM Spectrum Protect for Space Management en el IBM Knowledge Center, en <http://www.ibm.com/support/knowledgecenter/SSERBH/welcome>.
2. Consulte la documentación del producto IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server en el IBM Knowledge Center, en <http://www.ibm.com/support/knowledgecenter/SSERBW/welcome>.

Tareas relacionadas:

-  Control de operaciones de cliente mediante conjuntos de opciones de cliente

Consulta de opciones del cliente

En los apartados siguientes se proporciona información detallada sobre cada una de las opciones de proceso de IBM Spectrum Protect.

La información sobre cada una de las opciones incluye:

- Una descripción
- Un diagrama de sintaxis
- Descripciones detalladas de los parámetros.
- Ejemplos de uso de la opción en el archivo de opciones de cliente (si procede)
- Ejemplos de uso de la opción en la línea de mandatos (si procede)

Las opciones en cuyo ejemplo de línea de mandatos se indica **No se aplica** no pueden utilizarse con la línea de mandatos ni con mandatos planificados.

Nota:

1. No incluir un valor de opción entre comillas simples o dobles, a menos que el valor sea una especificación de archivo que contenga espacios o caracteres comodín. Por ejemplo, la siguiente opción no es válida:
`passwordaccess "generate"`
2. Todas las opciones del archivo `dsm.sys`, excepto para la opción `defaultserver`, se deben colocar dentro de una stanza de servidor. Una stanza de servidor es una colección de sentencias de opciones en `dsm.sys` que comienzan con una opción `SERVERName` y terminan bien con la siguiente opción `SERVERName` bien con el final del archivo.

Absolute

Utilice la opción **absolute** con el mandato **incremental** para imponer una copia de seguridad de todos los archivos y directorios que coincidan con la especificación de archivo o **domain**, aunque los objetos no se hayan modificado desde la última copia de seguridad incremental.

Esta opción modifica el parámetro `mode` del grupo de copia de clase de gestión para grupos de copia de seguridad; no afecta al parámetro `frequency` ni a ninguno de los otros parámetros del grupo de copia de seguridad. Esta opción no modifica las sentencias **exclude**, de modo que los objetos que se excluyen de la copia de seguridad no son aptos para copia de seguridad, aunque se especifique la opción **absolute**.

Importante: Antes de utilizar la opción `absolute`, tenga en cuenta los siguientes efectos que puede tener esta opción sobre copias de seguridad y operaciones del servidor de IBM Spectrum Protect:

- Las copias de seguridad consumen más recursos de base de datos y almacenamiento del servidor.
- Las copias de seguridad consumen más ancho de banda de red.
- Las operaciones del servidor, como por ejemplo caducidad del inventario, copia de seguridad de agrupación de almacenamiento, migración de agrupación de almacenamiento, reclamación y réplica de nodo, requieren más tiempo en completarse. La optimización de datos puede ayudar a mitigar algunos de estos efectos, pero no evita el proceso necesario para reconstituir los datos optimizados a su formato original cuando la agrupación de almacenamiento se migra o se copia en almacenamiento no optimizado.

Esta opción sólo es válida como un parámetro de línea de mandatos para el mandato **incremental** cuando se realizan las siguientes operaciones:

- Copias de seguridad incrementales progresivas completas o parciales de sistemas de archivos o unidades de disco.
- Copias de seguridad de diferencial de instantánea cuando también se especifica `createnewbase=yes`.

Para imponer una copia de seguridad completa de un sistema de archivos que utiliza copia de seguridad basada en registro por diario, especifique las opciones `nojournal` y `absolute` en el mandato **incremental**.

Para utilizar la opción `absolute` en copias de seguridad incrementales planificadas, el administrador del servidor de IBM Spectrum Protect debe crear una planificación de copia de seguridad separada que incluya la opción `absolute` en el parámetro `options` de la planificación.

Clientes soportados

Esta opción es válida para todos los clientes como parámetro de línea de mandatos para el mandato **incremental**. Esta opción no se pueden añadir a un conjunto de opciones de cliente en el servidor de IBM Spectrum Protect.

Sintaxis

►►—ABSolute—◄◄

Parámetros

No hay parámetros para esta opción.

Ejemplos

Línea de mandatos:

```
dsmc incr -absolute "/Users/sparky/source/*.c"
```

Afmskipuncachedfiles

La opción `afmskipuncachedfiles` especifica si los archivos no almacenados en memoria caché y sucios de conjuntos de archivos de Active File Management de General Parallel File System (GPFS) se procesan para operaciones de copia de seguridad, archivado y migración.

Los estados de archivos de GPFS Active File Management, *no almacenado en memoria caché* y *sucio* se explican en Información sobre el producto GPFS.

La ejecución de HSM en sistemas de archivos GPFS que utilizan conjuntos de archivos de Active File Management se explica en Orientación para integrar IBM Spectrum Scale AFM con IBM Spectrum Protect .

Si realiza una copia de seguridad, archiva o migra archivos de un sistema de archivos que contiene conjuntos de archivos de Active File Management, establezca `afmskipuncachedfiles=yes`.

Restricción: Si Active File Management se ejecuta en modalidad de actualización local (LU), la opción **afmskipuncachedfiles** del archivo de caché se debe establecer en **No**.

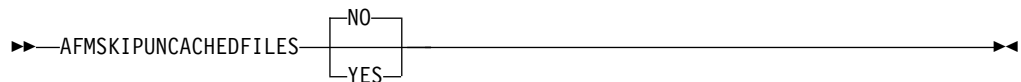
Clientes soportados

Esta opción es válida para clientes de archivado y copia de seguridad que se ejecutan en sistemas AIX y Linux.

Archivo de opciones

Ponga esta opción en el archivo `dsm.sys` antes de cualquier stanza de servidor.

Sintaxis



Parámetros

NO El estado de archivo de Active File Management se ignora durante las operaciones de copia de seguridad, archivado y migración. Las operaciones de migración en archivos no almacenados en memoria caché o sucios fallan y producen el mensaje de error ANS9525E. Las operaciones de copia de seguridad y archivado en archivos no almacenados en memoria caché necesitan operaciones de captación de Active File Management. Las operaciones de captación pueden producir tráfico de red significativo entre el inicio y la memoria caché de Active File Management. Este parámetro es el predeterminado.

YES

Los archivos no almacenados en memoria caché o sucios en conjuntos de archivos de Active File Management se saltan durante el proceso de copia de seguridad, archivado y migración.

Archmc

Utilice la opción **archmc** con el mandato **archive** para especificar la clase de gestión disponible para el dominio de políticas a la que desea vincular los directorios o las copias archivadas.

Cuando realice una copia archivada, podrá modificar temporalmente la clase de gestión asignada mediante la utilización de la opción **archmc** en el mandato **archive** o bien mediante la utilización del cliente web. La modificación temporal de la clase de gestión que se realiza mediante el cliente web equivale a la utilización de la opción **archmc** en el mandato **archive**.

Si no utiliza la opción **archmc**, el servidor vincula los directorios archivados a la clase de gestión. Si la clase de gestión predeterminada no tiene grupo de copias archivadas, el servidor vincula los directorios archivados a la clase de gestión con el período de retención más reducido.

Clientes soportados

Esta opción es válida para todos los clientes UNIX y Linux. La API de IBM Spectrum Protect no admite esta opción.

Sintaxis

►► ARCHMc = *clasegesti3n* ◀◀

Parámetros

clasegesti3n

Especifica una clase de gesti3n disponible en el conjunto de pol3ticas activo del dominio de pol3ticas. Esta clase de gesti3n modifica temporalmente la clase de gesti3n predeterminada y cualquier sentencia incluye que se haya especificado para los archivos y directorios cuya copia archivada est3 realizando.

Ejemplos

L3nea de mandatos:

```
dsmc archive -archmc=ret2yrs /Users/van/Documents/budget.jan
dsmc archive -archmc=ret2yrs /home/plan/proj1/budget.jan
```

Archsymlinkasfile

La opci3n archsymlinkasfile especifica si el cliente de copia de seguridad y archivado sigue un v3nculo simb3lico y archiva el directorio o el archivo al que hace referencia, o bien si archiva 3nicamente el v3nculo simb3lico. Utilice esta opci3n con el mandato **archive**.

Clientes soportados

Esta opci3n es v3lida para todos los clientes UNIX, a excepci3n de Mac OS X. El servidor tambi3n puede definir esta opci3n.

Archivo de opciones

Establezca esta opci3n en el archivo de opciones del usuario cliente (dsm.opt).

Sintaxis

►► ARCHSYMLinkasfile

Yes
No

 ◀◀

Parámetros

Yes

Especifica que el cliente debe seguir un v3nculo simb3lico y archiva el archivo o directorio asociado. 3ste es el valor predeterminado.

No Especifica que el cliente archiva el v3nculo simb3lico y no el archivo o directorio asociado.

Ejemplos

Archivo de opciones:

```
archsymlinkasfile no
```

L3nea de mandatos:

```
-archsym1=no
```


Asnodename

Utilice la opción **asnodename** para permitir a nodos agente realizar copias de seguridad o restauración de datos en nombre de otro nodo (el nodo de destino). Esto permite realizar operaciones simultáneas desde varios nodos para almacenar datos en el mismo nodo de destino y espacio de archivos en paralelo.

El nodo cliente debe tener garantizado el acceso al nodo de destino a través del mandato **grant proxynode** del cliente administrativo del servidor de IBM Spectrum Protect, y debe ser un usuario root para utilizar la opción **asnodename**.

Cuando el administrador de IBM Spectrum Protect ha otorgado autorización a un proxy de nodo y se utiliza la opción **asnodename** para convertirse en ese nodo, pueden consultarse y restaurarse todos los archivos como si se dispusiera de autorización de usuario root.

Un nodo de agente es un nodo cliente al que se ha otorgado autorización para realizar operaciones de cliente en nombre de un nodo de destino.

Un nodo de destino es un nodo cliente que otorga autorización a uno o varios nodos de agente para realizar operaciones en nombre de éste.

Una operación de proxy utiliza los valores del nodo de destino (por ejemplo, **maxnummp** y **deduplication**) y las planificaciones que se definen en el servidor. Los valores del nodo de servidor de IBM Spectrum Protect y las planificaciones del nodo de agente se ignoran.

Por ejemplo, puede utilizar el siguiente mandato para realizar la copia de seguridad de los datos compartidos para el espacio de archivos que se ha almacenado en el nombre de nodo MyCluster:

```
/cluster1/mydata  
dsmc incremental /Users -asnodename=MyCluster
```

También puede utilizar la opción **asnodename** para restaurar los datos bajo otro nombre de nodo en el servidor. Sólo puede restaurar los datos que son de su propiedad.

La opción **asnodename** difiere de la opción **nodename** en lo siguiente:

- Cuando utiliza la opción **nodename**, debe escribir la contraseña del nombre de nodo que especifica.
- Cuando utiliza la opción **asnodename**, debe especificar la contraseña del nodo de agente cliente para poder acceder a los datos que se han almacenado para el nodo de destino cliente.

Restricciones: no puede utilizar la opción **asnodename** con **-fromnode** ni puede realizar una copia de seguridad de NAS mediante la utilización de **asnodename**. La opción **asnodename** puede utilizarse para sistemas de clústeres, aunque no se admite ningún software de clúster específico.

Clientes soportados

Esta opción es válida para todos los clientes UNIX y Linux.

Archivo de opciones

Incluya esta opción en el archivo `dsm.sys` *dentro* de una stanza de servidor. Puede establecer esta opción en la ficha **General** del editor de preferencias.

Sintaxis

►►—ASNODENAME— *—targetnode—*◄◄

Parámetros

targetnode

Especifica el nombre de nodo en el servidor de IBM Spectrum Protect bajo el que se desea realizar la copia de seguridad o restaurar los datos.

Ejemplos

Archivo de opciones:

asnodename mycluster

Línea de mandatos:

-asnodename=mycluster

Esta opción no es válida en modalidad interactiva, pero puede definirse en la parte de opciones de una definición de planificación.

Valores de sesión y planificaciones de una operación de proxy

Una operación de proxy se produce cuando un nodo de agente utiliza la opción `asnodename` *nombre_nodo_destino* para realizar operaciones en nombre del nodo de destino especificado.

Una operación de proxy utiliza los valores del nodo de destino (por ejemplo, **maxnummp**, **cloptset** y **deduplication**) y las planificaciones que se definen en el servidor de IBM Spectrum Protect. Los valores del nodo de servidor y las planificaciones del nodo de agente se pasan por alto.

Se aplican las siguientes consideraciones a las operaciones de proxy.

- Todas las operaciones utilizan las construcciones y los valores de dominio de políticas del nodo de destino, aunque el nodo de agente pertenezca a un dominio diferente. Los valores y construcciones del dominio de la política del agente se pasan por alto.
- El nodo de agente se autentica en el servidor IBM Spectrum Protect utilizando la contraseña del nodo de agente.
- Para ejecutar operaciones de proxy, el nodo de agente y nodo de destino no deben estar bloqueados en el servidor.
- Las relaciones de nodo proxy no son transitivas. Si un nodo de destino se define como nodo proxy para otro nodo, el nodo de agente no puede utilizarse para ejecutar operaciones en ese otro nodo, a menos que el agente también se defina como nodo proxy para ese otro nodo.

Por ejemplo, supongamos las siguientes definiciones de proxy entre los nodos TAURUS, SCORPIO y GEMINI:

- TAURUS es un nodo proxy de SCORPIO.
- TAURUS no es un nodo proxy de GEMINI.
- SCORPIO es un nodo proxy de GEMINI.

Las definiciones de proxy producen los siguientes resultados:

- TAURUS puede ejecutar operaciones en nombre de SCORPIO.
- SCORPIO puede ejecutar operaciones en nombre de GEMINI.
- TAURUS no puede ejecutar operaciones en nombre de GEMINI.

Auditlogging

Use la opción `auditlogging` para generar una anotación de auditoría que contenga una entrada para cada archivo que se procese durante una operación incremental, de selección, de archivado, de restauración o recuperación.

La anotación de auditoría se puede configurar para que capture un nivel básico de información o un nivel de información más inclusivo (completo).

El nivel básico de la función de anotación de auditoría captura la información que se encuentra en la anotación de planificación y registra la información de que se ha hecho una copia de seguridad de un archivo, se ha archivado, actualizado, restaurado, recuperado, caducado, eliminado, omitido o ha fallado durante una operación de copia de seguridad incremental, de copia de seguridad selectiva, de archivado, de restauración o de recuperación. Asimismo, el nivel básico de la anotación de auditoría captura el mandato de entrada de los mandatos que se ejecutan mediante la línea de mandatos de copia de seguridad/archivado o los clientes del planificador.

El nivel completo de anotación de auditoría graba una acción de cada archivo que procesa el cliente de copia de seguridad/archivado. Además de todos los eventos grabados mediante el nivel básico de la anotación de auditoría, el nivel completo de anotación de auditoría graba información de un archivo que se ha excluido o no se ha enviado durante una operación de copia de seguridad incremental progresiva porque el archivo no ha cambiado.

A continuación puede ver un ejemplo de los mensajes que se emiten cuando la anotación de auditoría se configura para que capture el nivel básico de información:

```
04/21/07 15:25:05 ANS1650I Command:
    sel /home/spike/test/*
04/21/07 15:25:05 ANS1651I Backed Up:
    /home/spike/test/file.txt
04/21/07 15:25:05 ANS1652I Archived:
    /home/spike/test/file.txt
04/21/07 15:25:05 ANS1653I Updated:
    /home/spike/test/file.txt
04/21/07 15:25:05 ANS1654E Failed:
    /home/spike/test/file.txt
04/21/07 15:25:05 ANS1655I Restored:
    /home/spike/test/file.txt
04/21/07 15:25:05 ANS1656I Retrieved:
    /home/spike/test/file.txt
04/21/07 15:25:05 ANS1657I Expired:
    /home/spike/test/file.txt
04/21/07 15:25:05 ANS1658I Deleted:
    /home/spike/test/file.txt
04/21/07 15:25:05 ANS1659I Skipped:
    /home/spike/test/file.txt
```

Los siguientes mensajes se pueden emitir cuando el registro de auditoría se ha configurado para capturar el nivel completo de información (además de todos los mensajes emitidos para el nivel básico del registro de auditoría):

```
04/21/07 15:25:05 ANS1660I Excluded:
/home/spike/test/file.txt
04/21/07 15:25:05 ANS1661I Unchanged:
/home/spike/test/file.txt
```

La anotación de auditoría no es un sustituto ni un reemplazo de la anotación de errores estándar (`dsmerror.log`) ni de la anotación de planificación (`dsmsched.log`). Si se produce un error que impide que un archivo pueda procesarse, en el registro de auditoría aparecerá un mensaje que indicará que se ha producido un error, aunque el mensaje no indicará la naturaleza del error. Para diagnósticos de problemas se debe usar todavía la anotación de errores estándar.

Las entradas de la anotación de auditoría sólo contienen una indicación de la hora y un nombre de objeto. No hay información para distinguir entre archivos y directorios ni tampoco ninguna información sobre el tamaño de un objeto.

El cliente de archivado y copia de seguridad de Mac OS X creará el registro de auditoría en formato de archivo Unicode (UTF-16).

De forma predeterminada, el nombre de la anotación de auditoría es `dsmaudit.log` y se incluye en el mismo directorio que la anotación de error, `dsmerror.log`. El nombre y la ubicación de la anotación de auditoría se pueden configurar mediante la opción `auditlogname`. No existe ningún parámetro que permita controlar el tamaño de la anotación de auditoría ni realizar la operación de poda de ésta. La opción `auditlogname` no se puede definir como opción en un conjunto de opciones de cliente del servidor de IBM Spectrum Protect.

El mandato **auditlogging** se admite con mandatos de copia de seguridad que interactúan con objetos de nivel de archivo como **backup groups**.

El mandato **auditlogging** no se admite con los mandatos de copia de seguridad que interactúan con objetos de nivel de imagen como **backup image** o **restore image**. El mandato **auditlogging** se admite con mandatos de copia de seguridad que interactúan con objetos de nivel de archivo como **backup groups**.

Si ha activado el registro de auditoría para una operación y se produce una anomalía al intentar grabar en el registro de auditoría (por ejemplo, el disco en el que reside la anotación de auditoría no dispone de espacio suficiente), el registro de auditoría se desactivará para el resto de la operación y el código de retorno de la operación se establecerá en 12, con independencia del resultado de la operación.

Cientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor.

Sintaxis



Parámetros

off

Especifica que el recurso de anotación de auditoría no está ocupado. Éste es el valor predeterminado.

basic

Especifica que la anotación de auditoría captura un nivel básico de información.

full

Especifica que la anotación de auditoría captura un nivel más amplio de información.

Ejemplos

Ejecutar una copia de seguridad incremental con la anotación de auditoría activada.

Línea de mandatos:

```
dsmc i -auditlogging=basic
```

Realizar la copia de seguridad de una lista de archivos mediante la utilización del nivel máximo de auditoría, que permite que otra aplicación, como un script Perl, verifique los resultados.

Auditlogname

La opción `auditlogname` especifica la vía de acceso y el nombre del archivo donde desea que se almacene la información de las anotaciones de auditoría. Esta opción se aplica cuando se habilita la anotación de auditoría.

Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor.

Sintaxis

►►—AUDITLOGName—*filespec*—————►►

Parámetros

filespec

Especifica la vía de acceso y el nombre de archivo donde quiere que el cliente de copia de seguridad y archivado almacene la información de anotación de auditoría.

Si se especifica únicamente un nombre de archivo, el archivo se almacena en el directorio actual. El valor predeterminado es el directorio de instalación con el nombre de archivo `dsmaudit.log`. El archivo `dsmaudit.log` no puede ser un enlace simbólico.

Ejemplos

Ejecutar una copia de seguridad incremental con la anotación de auditoría activada.

Salida de ejemplo

A continuación puede ver una muestra de ejecución y un archivo de salida:

```
> dsmc inc /SMSVT/mfs1 -auditlogging=full
  -auditlogname=/home/cliv3/audit.log
IBM Spectrum Protect
Interfaz de línea de mandatos del cliente de copia de
seguridad/archivado
Versión de cliente 8, release 1, nivel 0.0
Fecha/hora del cliente: 11/16/2016 12:05:35
(c) Copyright by IBM Corporation y otros 1990, 2016.
Reservados todos los derechos.

Nombre de nodo: NAXOS_CLUSTER
Sesión establecida con servidor
ODINHSMSERV: AIX-RS/6000
Versión de servidor 8, release 1, nivel 0.0
Fecha/hora del cliente: 11/16/2016 12:05:35
Último acceso: 11/15/2016 12:01:57

Copia de seguridad incremental del volumen '/SMSVT/mfs1'
Directory--> 4,096 /SMSVT
/mfs1/ [Sent]
Normal File--> 32,768 /SMSVT
/mfs1/test0 [Sent]
Normal File--> 32,768 /SMSVT
/mfs1/test1 [Sent]
Normal File--> 32,768 /SMSVT
/mfs1/test2 [Sent]
Normal File--> 32,768 /SMSVT
/mfs1/test3 [Sent]
Normal File--> 32,768 /SMSVT
/mfs1/test4 [Sent]
Normal File--> 32,768 /SMSVT
/mfs1/test5 [Sent]
Normal File--> 32,768 /SMSVT
/mfs1/test6 [Sent]
Normal File--> 32,768 /SMSVT
/mfs1/test7 [Sent]
Normal File--> 32,768 /SMSVT
/mfs1/test8 [Sent]
Normal File--> 32,768 /SMSVT
/mfs1/test9 [Sent]
La copia de seguridad incremental de '/SMSVT/mfs1'
se ha realizado correctamente

Número total de objetos inspeccionados: 11
Número total de objetos de copia de seguridad: 11
Número total de objetos actualizados: 0
Número total de objetos revinculados: 0
Número total de objetos suprimidos: 0
Número total de objetos caducados: 0
Número total de objetos con errores: 0
Número total de bytes transferidos: 320,31 KB
Tiempo de transferencia de datos: 0,01 s
Velocidad de transferencia de datos de red: 17.141,84 KB/s
Velocidad de transferencia de datos compuesta: 297,43 KB/s
Objetos comprimidos al: 0%
Tiempo transcurrido en el proceso: 00:00:01
```

A continuación puede ver el contenido de la anotación de auditoría:

```

07/03/07 12:05:14 ANS1650I Command:
inc /SMSVT/mfs1
07/03/07 12:05:15 ANS1651I Backed Up:
/SMSVT/mfs1/
07/03/07 12:05:15 ANS1651I Backed Up:
/SMSVT/mfs1/test0
07/03/07 12:05:15 ANS1651I Backed Up:
/SMSVT/mfs1/test1
07/03/07 12:05:15 ANS1651I Backed Up:
/SMSVT/mfs1/test2
07/03/07 12:05:15 ANS1651I Backed Up:
/SMSVT/mfs1/test3
07/03/07 12:05:15 ANS1651I Backed Up:
/SMSVT/mfs1/test4
07/03/07 12:05:15 ANS1651I Backed Up:
/SMSVT/mfs1/test5
07/03/07 12:05:15 ANS1651I Backed Up:
/SMSVT/mfs1/test6
07/03/07 12:05:15 ANS1651I Backed Up:
/SMSVT/mfs1/test7
07/03/07 12:05:15 ANS1651I Backed Up:
/SMSVT/mfs1/test8
07/03/07 12:05:15 ANS1651I Backed Up:
/SMSVT/mfs1/test9

```

Información relacionada

Para obtener más información acerca del recurso de anotación de auditoría, consulte el tema “Audit logging” en la página 351.

Autodeploy

Utilice la opción autodeploy para habilitar o inhabilitar un despliegue automático del cliente si es necesario un reinicio.

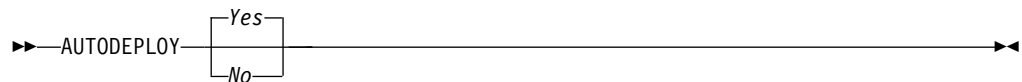
Clientes soportados

Esta opción es válida para clientes AIX, Linux, Mac y Solaris.

Archivo de opciones

También puede establecer esta opción incluyéndola en el archivo de opciones del cliente. También puede establecer la interfaz gráfica de usuario de Java pulsando **Editar > Cliente** y seleccionando la opción apropiado en la ficha **General**.

Sintaxis



Parámetros

Yes

Especifica que el cliente se despliega automáticamente desde el servidor. *Yes* es el valor predeterminado.

No Especifica que el cliente no se despliega automáticamente desde el servidor.

Ejemplos

Archivo de opciones:

autodeploy no

Línea de mandatos:

No se aplica.

Importante: Utilice la opción `schedmode prompted` junto con la opción `autodeploy` para habilitar el planificador a fin de procesar la planificación del despliegue del cliente de forma inmediata.

Conceptos relacionados:

“Despliegue automático del cliente de copia de seguridad y archivado” en la página 2

Autofsrename

La opción `autofsrename` cambia el nombre de un espacio de archivos existente que no está activado para Unicode en el servidor de IBM Spectrum Protect para que pueda crearse un espacio de archivos activado para Unicode con el nombre original para la operación actual.

Cuando especifica `autofsrename yes` en el archivo de opciones del cliente y el valor del servidor `autofsrename` se ha establecido en `client`, el servidor de IBM Spectrum Protect genera un nombre exclusivo añadiendo `_OLD` al nombre del espacio de archivos que especifica en la operación actual. Por ejemplo, el servidor cambiará el nombre del espacio de archivos Jaguar por Jaguar_OLD. Si el nuevo nombre del espacio de archivos es demasiado largo, el sufijo sustituirá los últimos caracteres del nombre del espacio de archivos. Por ejemplo, el nombre del espacio de archivos `nombrelargosistemaarchivos` se cambiará por:

`nombrelargosistemaarchivos_OLD`

Si el nuevo nombre del espacio de archivos ya existe en el servidor, el servidor cambiará el nuevo nombre del espacio de archivos por Jaguar_OLDx, donde la x es un número exclusivo.

El servidor creará nuevos espacios de archivos activados para Unicode que sólo contengan los datos que se especifican en la operación actual. Por ejemplo, imaginemos que Jaguar es el nombre del disco de arranque y que desea realizar el archivado de todos los archivos `.log` en el directorio `/Users/user5/Documents`. Antes de que se produzca la operación de archivado, el servidor cambia el nombre del espacio de archivos por Jaguar_OLD. La operación de archivado coloca los datos especificados en la operación actual en el espacio de archivos activado para Unicode denominado Jaguar. Ahora, el nuevo espacio de archivos activado para Unicode sólo contiene el directorio `/Users/user5/logs` y los archivos `*.log` especificados en la operación. El servidor almacena todas las posteriores copias de seguridad selectivas incrementales completas y parciales y archiva los datos en los nuevos espacios de archivos activados para Unicode.

Por ejemplo, imaginemos que Jaguar es el nombre del disco de arranque y que desea realizar el archivado de todos los archivos `.log` en el directorio `/Users/user5/Documents`. Antes de que se produzca la operación de archivado, el servidor cambia el nombre del espacio de archivos por Jaguar_OLD. La operación de archivado coloca los datos especificados en la operación actual en el espacio de archivos activado para Unicode denominado Jaguar. Ahora, el nuevo espacio de archivos activado para Unicode sólo contiene el directorio `/Users/user5/logs` y los

Parámetros

Yes

Especifica que el servidor de IBM Spectrum Protect cambia automáticamente el nombre de todos los espacios de archivos que no están activados para Unicode en la operación de copia de seguridad o archivado actual.

No Especifica que el servidor no cambia el nombre de los espacios de archivos que no están activados para Unicode en la operación de copia de seguridad o archivado actual.

Prompt

Especifica que se le preguntará si desea cambiar el nombre de los espacios de archivos no activados para Unicode en la operación actual. Éste es el valor predeterminado.

Consideraciones:

- Esta opción solo se aplica cuando el servidor establece la opción `autofsrename` en `client`.
- Cuando el planificador cliente está en ejecución, el procedimiento predeterminado consiste en no presentar ninguna solicitud de información. La siguiente sesión interactiva solicita al usuario que cambie el nombre del espacio de archivos.
- El cliente *sólo* le presentará una única solicitud de información por espacio de archivos. Si especifica *no* en el indicador, más adelante el cliente no puede cambiar el nombre de los espacios de archivos. Sin embargo, el administrador de IBM Spectrum Protect podrá cambiar el nombre de los espacios de archivos en el servidor.
- Cuando la copia de seguridad de los archivos se realiza en un espacio de archivos no activado para Unicode, el cliente activado para Unicode pasa por alto los archivos y directorios que tienen nombres que contienen caracteres de una página de códigos que es distinta de la del entorno regional actual.
- Si las copias de seguridad de archivos y directorios cuyos nombres contenían caracteres de una página de códigos distinta de la del entorno regional actual se habían realizado con un cliente no habilitado para Unicode, es posible que hayan caducado. El cliente activado para Unicode hará caducar estos archivos si no se realiza una migración del espacio de archivos a un espacio de archivos activado para Unicode. Puede hacer una copia de seguridad de estos archivos y archivarlos en un espacio de archivos Unicode.

Ejemplos

Archivo de opciones:

```
autofsrename yes
```

Automount

La opción `automount` añade al dominio un sistema de archivos montado automáticamente montándolo. Utilice esta opción con la opción `domain`.

Utilice esta opción para especificar todos los sistemas de archivos montados automáticamente que el cliente de copia de seguridad y archivado intenta montar en las siguientes situaciones:

- Cuando se inicia el cliente
- Cuando se inicia la copia de seguridad
- Cuando el cliente ha accedido a un sistema de archivos montado automáticamente durante la copia de seguridad

Monte el sistema de archivos antes de que el cliente realice una copia de seguridad de dicho sistema. Si el sistema de archivos siempre se monta antes de realizar la copia de seguridad, no es necesario especificar explícitamente un sistema de archivos montado automáticamente en la opción automount. Sin embargo, añada este sistema de archivos en la opción automount para asegurarse de que dicho sistema se ha montado en todas las circunstancias mencionadas anteriormente. Los sistemas de archivos montados automáticamente se vuelven a montar si se han desactivado mientras se realizaba una operación de copia de seguridad.

Clientes soportados

Esta opción es válida para todas las plataformas UNIX, a excepción de Mac OS X. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Establezca esta opción en el archivo de opciones del usuario cliente (dsm.opt).

Sintaxis



Parámetros

filespacename

Especifica uno o más sistemas de archivos montados automáticamente completamente cualificados que se montan y se añaden al dominio.

Ejemplos

Archivo de opciones:

automount /home/Fred /home/Sam

Línea de mandatos:

No se aplica.

Información relacionada

Consulte el apartado “Domain” en la página 394 para obtener más información sobre el uso de los sistemas de archivos montados automáticamente y la opción domain.

Backmc

La opción backmc especifica la clase de gestión que aplicar al mandato **backup fastback** para fines de retención.

Utilice la opción backmc con el mandato **backup fastback** .

Si realiza una copia de seguridad de un objeto en varias ocasiones y especifica una clase de gestión diferente para cada copia de seguridad, todas las versiones de copia de seguridad del objeto se vuelven a enlazar con la última clase de gestión especificada.

Clientes soportados

Esta opción es válida para clientes de Linux x86_64.

Archivo de opciones

Ninguno. Esta opción sólo puede especificarse en la línea de mandatos o en el planificador.

Sintaxis

►►—BACKMc=*nombre_clase_gestión*—◄◄

Parámetros

nombre_clase_gestión

Especifica el nombre de la clase de gestión.

Ejemplos

Línea de mandatos:

```
dsmc backup fastback -fbpolicyname=policy1 -fbserver=server1  
-backmc=ret2yrs
```

Backupsetname

La opción backupsetname especifica el nombre del juego de copias de seguridad del servidor de IBM Spectrum Protect.

Puede utilizar la opción backupsetname con los mandatos siguientes:

- **query backup**
- **query filespace**
- **query image**
- **restore image**

Nota: Los mandatos siguientes toman backupsetname como parámetro de posición. El parámetro de posición backupsetname tiene un comportamiento distinto que la opción backupsetname. Para ver una descripción de cómo afecta el parámetro de posición backupsetname a cada uno de estos mandatos consulte las explicaciones del mandato:

```
query backupset  
restore  
restore backupset
```

Clientes soportados

Esta opción es válida para todos los clientes UNIX y Linux. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Ninguna. Esta opción sólo puede especificarse en la línea de mandatos.

Sintaxis

►►—BACKUPSETName—*nombre_conjunto_copias*—◀◀

Parámetros

nombre_juegocopias

Especifica el nombre de un juego de copias de seguridad del servidor de IBM Spectrum Protect. No puede utilizar caracteres comodín.

Ejemplos

Línea de mandatos:

```
dsmc query backup /Volumes/bkSets/file.1
-backupsetname=YEAR_END_ACCOUNTING.12345678
dsmc query backup /usr/projects -subdir=yes
-backupsetname=YEAR_END_ACCOUNTING.12345678
dsmc restore image /home/proj
-backupsetname=ACCOUNTING_2007.12345678
dsmc query image -backupsetname=WEEKLY_BSET.21435678
```

Información relacionada

“Restauración de datos desde un conjunto de copias de seguridad” en la página 240

Basesnapshotname

La opción `basesnapshotname` especifica la instantánea a utilizar como instantánea base, cuando se realiza una copia de seguridad diferencial de instantánea (`snappdiff`) de un volumen de archivador NetApp. Si especifica esta opción, también debe utilizar la opción `snappdiff` o se produce un error. Si no se especifica `basesnapshotname`, la opción `useexistingbase` selecciona la instantánea más reciente en el volumen de archivador como la instantánea base.

Si no se puede encontrar la instantánea especificada, se notifica un error y la operación de copia de seguridad falla.

Clientes soportados

Esta opción puede utilizarse con clientes Linux x86_64 soportados.

Archivo de opciones

Esta opción puede especificarse en el archivo de opciones del cliente o bien en la línea de mandatos.

Sintaxis

►►—BASESNAPSHOTName— —*nombre_instantánea*—◀◀

Parámetros

nombre_instantánea

Especifica el nombre de una instantánea existente que utilizar como instantánea base. El nombre especificado puede ser un nombre de instantánea,

por ejemplo `voll_snap`, o puede ser el nombre de una copia de seguridad de NetApp planificada con un nombre como `nocturno.x`, donde *x* es el número de secuencia (donde `nightly.0` es la instantánea más antigua).

También puede utilizar un patrón con caracteres comodín para seleccionar una instantánea. Los caracteres comodín pueden ser los siguientes:

* Un asterisco (*) coincide con cualquier carácter.

? El signo de interrogación (?) coincide con un solo carácter.

Los caracteres comodín son útiles si las instantáneas siguen un patrón, por ejemplo incluir la fecha o la fecha y hora como parte del nombre de instantánea. Por ejemplo, una instantánea creada el 12 de noviembre de 2012 a las 11:10:00 AM puede guardarse como `UserDataVol_121103111000_snapshot`. La instantánea más reciente que coincide con el patrón se selecciona como la base existente. Por ejemplo, si hay dos instantáneas guardadas (`UserDataVol_121103111000_snapshot` y `UserDataVol_121103231000_snapshot`), se selecciona `UserDataVol_121103231100_snapshot` porque es 12 horas posterior a la otra instantánea.

```
-basesnapshotname="UserDataVol_*_snapshot"
```

Los signos de interrogación funcionan bien para las copias de seguridad planificadas que siguen un patrón de nombre coherente. Esta sintaxis selecciona la copia de seguridad "nocturno" más frecuente como la instantánea que debe utilizarse como base existente.

```
-basenameshotname="nightly.?"
```

Ejemplos

Archivo de opciones:

```
basesnapshotname nightly.?
```

```
basesnapshotname volum_base_snap
```

Línea de mandatos:

```
dsmc incr \\DRFiler\UserDataVol_Mirror_Share -snapdiff  
-useexistingbase -basesnapshotname="nightly.?"
```

Información relacionada

Useexistingbase

Cadlistenonport

La opción `cadlistenonport` especifica si se debe abrir un puerto de escucha para el aceptador de clientes.

Cuando un puerto de escucha está abierto, puede aceptar cualquier conexión de entrada. Sin embargo, el puerto no se utiliza si el aceptador de clientes solo gestiona el planificador y este se ejecuta en modalidad de sondeo. Puede utilizar esta opción para evitar que el aceptador abra el puerto no utilizado.

El valor predeterminado de esta opción es `yes`. Utilice `cadlistenonport no` solo si se utilizan `managedservices schedule` y `schedmode polling`.

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Coloque esta opción en el archivo de opciones del cliente (dsm.sys) de una stanza de servidor.

Sintaxis



Parámetros

Yes

Especifica que el aceptador de clientes debe abrir un puerto de escucha. Este parámetro es el predeterminado.

No Especifica que el aceptador de clientes no debe abrir un puerto de escucha. Utilice este valor cuando utilice el aceptador de clientes solo para gestionar el planificador en modalidad de sondeo.

Este valor inhabilita otras características que dependen del aceptador de clientes, como las operaciones de copia de seguridad y restauración de clientes, IBM Spectrum Protect for Virtual Environments: operaciones de la GUI de Data Protection for VMware vSphere y operaciones de copia de seguridad y restauración de IBM Spectrum Protect Snapshot.

Ejemplo

Archivo de opciones:

```
cadlistenonport no
```

Línea de mandatos:

No se aplica.

Referencia relacionada:

“Managedservices” en la página 486

“Schedmode” en la página 550

Changingretries

La opción **changingretries** especifica cuántas veces se desea que el cliente intente efectuar copia de seguridad o archivado de un archivo que se esté utilizando en ese momento. Utilice esta opción con los mandatos **archive**, **incremental** y **selective**.

Esta opción sólo se aplica cuando serialización de copia (atributo de un grupo de copias de clase de gestión) es estática compartida o dinámica compartida.

Con una serialización estática compartida, si un archivo está abierto durante una operación, la operación se repite el número de veces que especifique. Si el archivo está abierto durante cada uno de los intentos, no se realiza la operación.

Con una serialización dinámica compartida, si un archivo está abierto durante una operación, la operación se repite el número de veces que especifique. La operación de copia de seguridad o archivado tiene lugar durante el último intento tanto si el archivo está abierto como si no.

Clientes soportados

Esta opción es válida para todos los clientes UNIX y Linux. El servidor también puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor. Puede establecer esta opción en la ficha **Copia de seguridad**, en el campo **Número de reintentos si el archivo se está utilizando** del Editor de preferencias.

Sintaxis

►►—CHAngingretries— *numberretries* —————►►

Parámetros

númeroreintentos

Especifica el número de veces que se intenta una operación de copia de seguridad o de archivado si se está utilizando el archivo. El rango de valores es de 0 a 4, siendo 4 el valor predeterminado.

Ejemplos

Archivo de opciones:

changingretries 3

Línea de mandatos:

-cha=3

Class

La opción class especifica si ha de visualizarse una lista de objetos NAS o de cliente al utilizar los mandatos **delete filespace**, **query backup** y **query filespace**.

Por ejemplo, para mostrar una lista de los espacios de archivos que pertenezcan a un nodo NAS, especifique el mandato siguiente:

query filespace -class=nas

Clientes soportados

Esta opción solo es válida para clientes AIX, Linux y Oracle Solaris. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Ninguna. Esta opción sólo puede especificarse en la línea de mandatos.

Sintaxis

►►—CLASS = *client*
nas —————►►

Parámetros

client

Especifica que se desea visualizar una lista de espacios de archivos para un nodo cliente. Éste es el valor predeterminado.

nas

Especifica que se desea visualizar una lista de espacios de archivos para un nodo NAS.

Ejemplos

Ninguna. Esta opción sólo puede especificarse en la línea de mandatos.

Línea de mandatos:

```
q backup -nasnodename=nodename -class=nas
```

Collocatebyfilespec

Utilice la opción `collocatebyfilespec` para especificar si el cliente de copia de seguridad y archivado utiliza solamente una sesión de servidor para enviar objetos generados a partir de especificación de archivo.

El establecimiento de la opción `collocatebyfilespec` en `yes` dará lugar a que se intente eliminar la entremezcla de archivos de especificaciones de archivo distintas, limitando al cliente a una única sesión de servidor por especificación de archivo. Por consiguiente, si almacena los datos en una cinta, los archivos para cada especificación de archivo se almacenan conjuntamente en una cinta (a menos que se necesite otra para mayor capacidad).

Consideraciones:

- Utilice la opción `collocatebyfilespec` sólo si la agrupación de almacenamiento va directamente a cinta. Si utiliza esta opción para una agrupación de almacenamiento en disco, ello podría afectar al equilibrado de carga y, por consiguiente, al rendimiento.

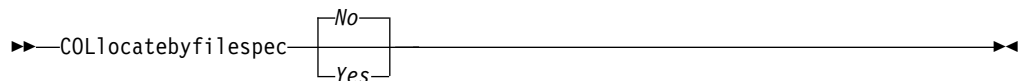
Clientes soportados

Esta opción es válida para todos los clientes UNIX y Linux. El servidor también puede definir esta opción.

Archivo de opciones

Establezca esta opción en el archivo de opciones de usuario del cliente (`dsm.opt`).

Sintaxis



Parámetros

Yes

Especifica que se desea que el cliente utilice solamente una sesión de servidor para enviar objetos generados desde una especificación de archivo. Por lo tanto, si almacena los datos en cinta, los archivos correspondientes a cada

especificación de archivo se almacenan en la misma cinta, a menos que se requiera otra cinta para obtener más capacidad. Como resultado puede aumentar el rendimiento de la restauración.

No Especifica que el cliente (en función de la dinámica de ejecución y de si la opción `resourceutilization` se ha establecido en 3 o en un valor superior) puede utilizar una o varias sesiones de servidor para enviar los archivos desde una única especificación de archivo. Éste es el valor predeterminado.

A consecuencia de ello, el rendimiento de la copia de seguridad puede aumentar. Si la copia de seguridad de los archivos se realiza en una cinta, los archivos se almacenarán en varias cintas. Por lo general, los archivos especificados en la especificación de archivo serán contiguos.

Ejemplos

Archivo de opciones:

```
collocatebyfilespec yes
```

Línea de mandatos:

```
-collocatebyfilespec=yes
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Commethod

La opción `commethod` especifica el método de comunicación que se utiliza para proporcionar conectividad en la comunicación entre cliente y servidor.

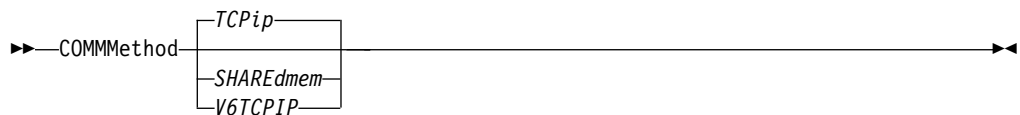
Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. Puede establecer esta opción en la ficha **Comunicación** del editor de preferencias.

Sintaxis



Parámetros

TCPip

Protocolo de control de transmisiones/Protocolo de Internet (TCP/IP) Éste es el valor predeterminado.

V6Tcpi

Indica que se debe usar la versión 4 o 6 de TCP/IP, según la configuración del sistema y los resultados de una búsqueda de servicio de nombre de dominio. Debe haber disponible un entorno DNS válido.

SHAREdmem

Utilice el método de comunicación de memoria compartida cuando el cliente y el servidor estén ejecutándose en el mismo sistema. Esto proporciona un mejor rendimiento sobre el protocolo TCP/IP.

Esta opción es válida para clientes de AIX, Linux y Oracle Solaris.

Cuando este método de comunicación se especifica en AIX, el cliente puede conectarse como usuario root o como usuario no root, en tanto que el servidor se ejecute como root. Si el servidor no se está ejecutando como root, el ID de usuario que ejecuta el cliente debe coincidir con el que ejecuta el servidor.

Importante: Cuando utilice `commmethod sharedmem` en Linux, es posible que reciba un mensaje de error: `ANR8294W Shared Memory Session unable to initialize` en el servidor o en la consola del agente de almacenamiento. De forma predeterminada, Linux no se ha configurado con suficientes recursos del sistema para crear las colas de mensajes. Debe aumentar el parámetro del kernel, `MSGMNI`, a 128 (el valor predeterminado es 16). Puede modificar este parámetro mediante la ejecución del mandato siguiente:

```
echo 128 > /proc/sys/kernel/msgmni
```

Para que este parámetro sea un parámetro permanente después de reiniciar el sistema, puede añadir la siguiente línea al archivo `/etc/sysctl.conf` y, a continuación, reiniciar el sistema:

```
kernel.msgmni=128
```

Para ver el valor de ipc actual, ejecute este mandato:

```
ipcs -l
```

Compruebe ahora el valor de `max queues system wide`. El valor predeterminado es 16.

Ejemplos

Archivo de opciones:

Utilice solo TCP/IP V4.

```
commmethod      tcpip
```

Use tanto TCP/IP V4 como V6, según cómo esté configurado el sistema y los resultados de una búsqueda del servicio de nombres de dominio.

```
commmethod V6Tcpi
```

Nota: El mandato `dsmd schedule` no puede utilizarse cuando se han especificado tanto `SCHEDMODE prompt` como `commmethod V6Tcpi`.

Línea de mandatos:

```
-comm=tcpip
```

```
-comm=V6Tcpi
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Commrestartduration

La opción `commrestartduration` especifica el número máximo de minutos durante los que el cliente intentará conectarse de nuevo al servidor de IBM Spectrum Protect después de producirse un error de comunicación.

Nota: Un evento planificado seguirá ejecutándose si el cliente vuelve a conectarse al servidor antes de que haya transcurrido el valor que se ha especificado en `commrestartduration`, aunque haya transcurrido el plazo de tiempo de arranque del evento.

Puede utilizar la opción `commrestartduration` y `commrestartinterval` en entornos de red con gran actividad o inestables para disminuir los errores de conexión.

Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. Puede establecer esta opción en la ficha **Comunicación**, en la sección **Opciones comunes** del Editor de preferencias.

Sintaxis

►►—`COMMRESTARTDuration— minutos`—►►

Parámetros

minutos

Especifica el número máximo de minutos durante los cuales se desea que el cliente intente restablecer conexión con un servidor después de producirse un error de comunicación. El rango de valores es de 0 a 9999, siendo 60 el valor predeterminado.

Ejemplos

Archivo de opciones:

`commrestartduration 90`

Línea de mandatos:

No se aplica.

Commrestartinterval

La opción `commrestartinterval` especifica el número de segundos que deben transcurrir entre los intentos que realiza el cliente para volver a conectarse al servidor de IBM Spectrum Protect después de producirse un error de comunicación.

Nota: utilice esta opción sólo si el valor de `commrestartduration` es mayor que cero.

Puede utilizar la opción `commrestartduration` y `commrestartinterval` en entornos de red con gran actividad o inestables para disminuir los errores de conexión.

Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor. Puede establecer esta opción en la ficha **Comunicación**, en la sección **Opciones comunes** del Editor de preferencias.

Sintaxis

►►—COMMRESTARTInterval— *segundos* —►►

Parámetros

segundos

Especifica el número de segundos que debe transcurrir entre los intentos que realiza un cliente para restablecer la conexión con un servidor después de producirse un error de comunicación. El rango de valores es de 0 a 65535, siendo 15 el valor predeterminado.

Ejemplos

Archivo de opciones:

commrestartinterval 30

Línea de mandatos:

No se aplica.

Compressalways

La opción compressalways especifica si se debe continuar la compresión si el objeto aumenta de tamaño durante la compresión.

Utilice esta opción con la opción compression y con los mandatos **archive**, **incremental** y **selective**.

La opción compressalways se omite cuando la deduplicación del lado de cliente está habilitada.

Clientes soportados

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción.

Archivo de opciones

Establezca esta opción en el archivo de opciones de usuario del cliente (dsm.opt). Puede establecer esta opción en la ficha **Copia de seguridad**, en el recuadro de selección **Continuar compresión si el objeto crece** del Editor de preferencias.

Sintaxis

►►—COMPRESSAlways—

Yes
No

 —►►

Parámetros

Yes

La compresión de archivos continúa incluso si el archivo crece como resultado de la compresión. Éste es el valor predeterminado.

No Los objetos de cliente de copia de seguridad/archivado se envían de nuevo sin comprimir si su tamaño aumenta durante la operación de compresión. El comportamiento de la API depende de la aplicación. Las copias de seguridad de la aplicación puede que no se realicen correctamente.

Ejemplos

Archivo de opciones:

`compressalways yes`

Línea de mandatos:

`-compressa=no`

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Compression

La opción `compression` comprime los archivos antes de enviarlos al servidor.

La compresión de archivos reduce el almacenamiento de datos necesario para almacenar versiones de copia de seguridad y copias archivadas de los archivos. Sin embargo, puede afectar al rendimiento de IBM Spectrum Protect. Un procesador rápido en una conexión de red lenta se beneficia de la compresión, pero un procesador lento en una conexión de red rápida, no.

Utilice la opción `compression` con los mandatos **archive**, **incremental** y **selective**.

El mandato **backup image** utiliza el valor de la opción `compression` que se especifica en el archivo `dsm.sys`. Esta opción es válida en la línea de mandatos inicial y en modalidad interactiva. El servidor también puede definir esta opción, que modifica temporalmente el valor del cliente.

El cliente de copia de seguridad y archivado hace copia de seguridad de un archivo esparcido si la compresión del cliente está desactivada. Establezca `compression yes` para habilitar la compresión de archivos al realizar copias de seguridad de archivos dispersos con el fin de minimizar el tiempo de transacción de la red y de maximizar el espacio de almacenamiento del servidor.

Si establece `compressalways yes`, la compresión continuará aunque se incremente el tamaño del archivo. Para detener la compresión si el tamaño del archivo crece y reenviar el archivo sin comprimir, establezca `compressalways no`.

Si establece `compression yes`, puede controlar el proceso de compresión de las formas que se indican a continuación:

- Utilice la opción `exclude.compression` en el archivo de opciones del cliente (`dsm.sys`) para excluir archivos o grupos de archivos específicos del proceso de compresión.
- Utilice la opción `include.compression` en el archivo de opciones del cliente (`dsm.sys`) para incluir archivos de un amplio grupo de archivos excluidos en el proceso de compresión.

Esta opción controla la compresión solo si su administrador especifica que el nodo de cliente pueda comprimir archivos antes de enviarlos al servidor.

El tipo de compresión que utiliza el cliente viene determinado por la combinación de compresión y duplicación de datos del cliente que se utiliza durante proceso de copia de seguridad o archivado. Se utilizan los siguiente tipos de compresión:

LZ4 Un método de compresión más rápido y eficiente que el cliente utiliza cuando los datos deduplicados del cliente se envían a una agrupación de almacenamiento de contenedor compatible con LZ4 en el servidor de IBM Spectrum Protect. El servidor debe tener la versión 7.1.5 o posterior y debe utilizar agrupaciones de almacenamiento de contenedor. La compresión LZ4 del cliente solo se utiliza cuando la deduplicación de datos del cliente está habilitada.

LZW Un tipo tradicional de compresión que el cliente utiliza en cualquiera de las situaciones siguientes:

- Los datos deduplicados del cliente se envían a agrupaciones de almacenamiento tradicionales (no de contenedor) del servidor.
- Los datos del cliente no pasan por el proceso de deduplicación de datos. (No se aplica a Data Protection for VMware ni a Data Protection for Microsoft Hyper-V, donde solo se pueden comprimir los datos deduplicados del cliente.)
- Los datos del cliente solo pasan por el proceso de deduplicación de datos tradicional del servidor. (No se aplica a Data Protection for VMware ni a Data Protection for Microsoft Hyper-V, donde solo se pueden comprimir los datos deduplicados del cliente.)

Ninguna

El cliente no comprime el objeto. El objeto no se comprime porque la opción `compression` tiene el valor *no* o no se ha especificado durante el proceso de copia de seguridad o archivado. Aunque el cliente no comprime el objeto, es posible que lo comprima el servidor.

No es necesario definir el tipo de compresión. Viene determinado por el cliente de copia de seguridad y archivado en el momento del proceso de la copia de seguridad o archivado.

Clientes soportados

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción.

Archivo de opciones

Establezca esta opción en el archivo `dsm.sys` dentro de una sección de servidor. Puede establecer esta opción en la ficha **Copia de seguridad**, en la casilla de verificación **Comprimir objetos** del Editor de preferencias.

Sintaxis



Parámetros

No Los archivos no se comprimen antes de enviarlos al servidor. Éste es el valor predeterminado.

Yes

Los archivos se comprimen antes de enviarlos al servidor.

Ejemplos

Archivo de opciones:

compression yes

Línea de mandatos:

-compressi=no

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Referencia relacionada:

“Eliminación de duplicados” en la página 381

“Opciones exclude” en la página 425

“Opciones include” en la página 458

Console

Utilice la opción **console** con el mandato **query systeminfo** para que la información del sistema se visualice en la consola.

- DSMOPTFILE: el contenido del archivo dsm.opt.
- DSMSYSFILE - El contenido del archivo dsm.sys.
- ENV: variables de entorno.
- ERRORLOG - El archivo de anotaciones de errores de IBM Spectrum Protect.
- FILE - Atributos para el nombre de archivo que especifique.
- INCLEXCL - Compila una lista de sentencias de inclusión/exclusión en el orden en el que se procesan durante las operaciones de copia de seguridad y archivado.
- OPTIONS - Opciones compiladas.
- OSINFO - Nombre y versión del sistema operativo cliente (incluye información ULIMIT para UNIX y Linux).
- POLICY - Vuelco del conjunto de políticas.
- SCHEDLOG - Contenido de las anotaciones de planificación de IBM Spectrum Protect (por lo general, dsmsched.log).
- CLUSTER - Información de clústeres de AIX.

Nota: La principal finalidad del mandato **query systeminfo** es ayudar al soporte de IBM en el diagnóstico de problemas, aunque los usuarios que estén familiarizados con los conceptos relacionados con esta información también podrían encontrarlo de utilidad. Si utiliza la opción **console**, no se realiza ningún formato especial de la salida para ajustarla a la altura o anchura de la pantalla. Por consiguiente, es posible que la salida de la consola sea difícil de leer debido a la longitud y a la acomodación de líneas. En este caso, se recomienda utilizar la opción **filename** con el mandato **query systeminfo** para que la salida se grabe en un archivo que, posteriormente, podrá enviarse al soporte de IBM.

Clientes soportados

Esta opción es válida para todos los clientes.

Sintaxis

►—CONSOLE—◄

Parámetros

No hay parámetros para esta opción.

Ejemplos

Línea de mandatos:

```
query systeminfo dsmpoptfile errorlog -console
```

Información relacionada

“Filename” en la página 442

Createnewbase

La opción `createnewbase` crea una instantánea base y la utiliza como fuente para ejecutar una copia de seguridad incremental completa.

Algunos archivos pueden no copiarse cuando se ejecuta el mandato de copia de seguridad incremental por diferencia de instantánea. Si los archivos se pasan por alto, puede ejecutar el mandato con la opción `createnewbase` para copiar esos archivos omitidos. Consulte “`Snapdiff`” en la página 561 para conocer las razones por las que un archivo puede no copiarse al ejecutar el mandato de copia de seguridad por diferencia de instantánea.

Una razón por la que se puede omitir un archivo durante el proceso de copia de seguridad es porque NetApp Data ONTAP no admite el nombre de archivo. Las versiones 8.0 y las versiones anteriores a 7.3.3 de NetApp Data ONTAP permiten utilizar solo nombres de archivo no pertenecientes al juego de caracteres ASCII de 7 bits. NetApp Data ONTAP versión 7.3.3 y versiones posteriores a 8.0.0 admiten nombres de archivo Unicode. Si ha actualizado NetApp Data ONTAP desde una versión que no admite nombres de archivo Unicode a una versión que sí los admite, ejecute una copia de seguridad incremental con la opción `createnewbase=migrate`.

Clientes soportados

Esta opción es válida para los clientes siguientes:

- Clientes Linux x86_64

Escriba la opción `createnewbase` en la línea de mandatos. Especifique esta opción con la opción `snapdiff`.

Sintaxis



Parámetros

No Especifica que se ejecuta una copia de seguridad incremental por diferencia de instantánea. Si el cliente de copia de seguridad y archivado detecta que el servidor de archivos de NetApp Data ONTAP se ha migrado desde una versión que no permite utilizar nombres de archivo Unicode a un servidor de archivos que sí lo permite, se anota un mensaje de aviso en el registro cronológico de errores y en el registro de actividad del servidor de IBM Spectrum Protect. El mensaje de aviso indica que debe ejecutar una copia de seguridad incremental completa y anota un código de retorno 8 aunque la operación se completara satisfactoriamente.

Este parámetro es el valor predeterminado.

Yes

Especifica que se ejecuta una copia de seguridad incremental completa mediante la creación de una nueva instantánea base, la cual se utiliza para ejecutar una copia de seguridad incremental basada en la exploración de diferencias. Utilice esta opción para copiar cambios de archivo que puedan no haber sido detectados por la API de diferencia de instantánea.

Si la operación se completa satisfactoriamente, el mandato finaliza con un código de retorno de 0.

No especifique `createnewbase=yes` para ninguna planificación en la que se ejecute una copia diaria por diferencia de instantánea. En lugar de ello, cree una planificación mensual separada donde se utilice la opción `createnewbase=yes`.

IGNoRe

Especifica que se ejecuta una copia de seguridad incremental por diferencia de instantánea cuando el cliente de copia de seguridad y archivado detecta que el servidor de archivos NetApp Data ONTAP se ha actualizado para permitir la utilización de nombres de archivo Unicode.

La opción `ignore` se diferencia del parámetro `no` en que la opción `ignore` suprime el mensaje de aviso. En lugar de ello, se anota un mensaje informativo en el registro cronológico de errores y en el registro de actividad de IBM Spectrum Protect para indicarle que ejecute una copia de seguridad incremental completa.

Si el mandato finaliza satisfactoriamente, devuelve el código de retorno 0.

Utilice la opción `ignore` si ha actualizado el servidor de archivos NetApp Data ONTAP para que soporte Unicode pero aún no ha ejecutado una copia de seguridad incremental completa. Esta opción se utiliza solamente cuando el cliente de copia de seguridad y archivado detecta que el servidor de archivos se ha migrado y todavía no se ha ejecutado una copia de seguridad incremental completa. Esta opción no se tiene en cuenta en todos los demás casos.

MIGRate

Especifica que si el servidor de archivos NetApp Data ONTAP se ha actualizado a una versión que soporta nombres de archivo Unicode, se crea

una instantánea base y se ejecuta una copia de seguridad incremental basada en la exploración de diferencias. La opción `migrate` es distinta de la opción `yes` porque la opción `migrate` crea una instantánea base solo cuando el cliente detecta que se ha actualizado la versión del servidor de archivos NetApp Data ONTAP. La opción `yes` crea una instantánea base cada vez que se ejecuta el mandato.

Tras completarse la copia de seguridad incremental, no se registran más mensajes relacionados con migración en el registro cronológico de errores ni en el registro de actividad del servidor de IBM Spectrum Protect. Cuando la operación se completa correctamente, el mandato finaliza con un código de retorno de 0.

Utilice la opción `migrate` si ha actualizado el servidor de archivos NetApp Data ONTAP para que soporte Unicode pero aún no ha ejecutado una copia de seguridad incremental completa. La opción `migrate` se ignora si no se ha actualizado el servidor de archivos NetApp Data ONTAP.

Ejemplos

Línea de mandatos:

```
dsmc incremental -snapdiff -createnewbase=yes /net/home1
```

Tareas relacionadas:

“Configuración de NetApp y IBM Spectrum Protect para copias de seguridad incrementales de diferencia de instantánea” en la página 114

Referencia relacionada:

“Snapdiff” en la página 561

Datacenter

Especifica la ubicación de destino del centro de datos que contendrá los datos de la máquina restaurada.

Utilice esta opción en mandatos **restore vm**.

Si las carpetas se utilizan dentro del centro virtual para organizar centros de datos, el nombre de la carpeta debe incluirse en la especificación del centro de datos, separado por una barra inclinada.

Si está restaurando utilizando un servidor de ESX en lugar de un centro virtual, debe utilizarse la opción `-datacenter=ha-datacenter`.

La ubicación de destino predeterminada es el centro de datos donde se ha almacenado la máquina virtual en el momento de la copia de seguridad.



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Ejemplos

Restaurar una máquina virtual en un centro de datos USEast organizado bajo un nombre de carpeta llamada Producción en el centro virtual.

```
dsmc restore vm my_vm -datacenter=Production/USEast
```

Restaurar una copia de seguridad de máquina virtual realizada por un centro virtual, pero utilizando un servidor de ESX en el momento de la restauración.

```
restore vm my_vm -datacenter=ha-datacenter
```

Restaurar una máquina virtual en el centro de datos USWest.

```
restore vm my_vm -datacenter=USWest
```

Datastore

Especifica el destino del almacén de datos que utilizar durante la operación de restauración de VMware.



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Ejemplo

Restaurar la máquina virtual en un centro de datos denominado ds8k_prod1:

```
restore vm my_vm -datacenter=ds8k_prod1
```

Dateformat

La opción `dateformat` especifica el formato que desea utilizar para visualizar o especificar fechas.

De manera predeterminada, los clientes de copia de seguridad/archivado y de administración obtienen la información de formato de la definición del entorno regional que esté en vigor en el momento en que se inicia el cliente. Consulte la documentación del sistema local para obtener más detalles sobre la configuración del entorno regional.

Nota:

1. La opción `dateformat` no afecta al cliente web. El cliente web utiliza el formato de fecha para el entorno regional en el que se está ejecutando el navegador. Si un navegador no se está ejecutando en un entorno regional que admite el entorno local, el cliente web utiliza el formato de fecha para inglés de Estados Unidos.
2. si el formato de fecha se modifica y se utiliza la opción `schedlogretention` para eliminar las anotaciones de planificación, el cliente elimina todas las entradas de las anotaciones de planificación cuyo formato de fecha sea diferente al eliminar las anotaciones. Si el formato de fecha se modifica y se utiliza la opción `errorlogretention` para eliminar el registro de errores, el cliente elimina todas las entradas de el registro de errores cuya fecha sea diferente al eliminar las anotaciones. Cuando modifique el formato de fecha, copie las anotaciones de planificación y de errores si desea conservar las entradas de anotaciones cuyo formato de fecha sea diferente.

Puede utilizar la opción `dateformat` con los mandatos siguientes.

- **delete archive**
- **delete backup**
- **expire**
- **query archive**
- **query backup**
- **query filespace**

- **query image**
- **restore**
- **restore image**
- **restore nas**
- **retrieve**
- **set event**

Si se incluye la opción `dateformat` con un mandato, ésta debe anteponerse a las opciones `fromdate`, `pitdate` y `todate`.

Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Establezca esta opción en el archivo de opciones de usuario del cliente (`dsm.opt`). Puede establecer esta opción en la ficha **Configuración regional**, en la lista desplegable **Formato de fecha** del Editor de preferencias.

Sintaxis

►►—`DATEformat`— *—número_formato—*►►

Parámetros

número_formato

Muestra la fecha en uno de los siguientes formatos. Seleccione el número que se corresponda con el formato de fecha que desee utilizar:

- 0** Utilice el formato de fecha que especifica el entorno regional (no se aplica a Mac OS X).

Para AIX y Solaris: es el valor predeterminado si el formato de fecha que especifica el entorno local consta de dígitos y de caracteres de separación.

- 1** MM/DD/AAAA

Para AIX y Solaris: es el valor predeterminado si el formato de fecha que especifica el entorno local consta de cualquier carácter a excepción de dígitos y caracteres de separación.

Éste es el valor predeterminado para las siguientes traducciones disponibles:

- Inglés de Estados Unidos
- Chino (tradicional)
- Coreano

- 2** DD-MM-AAAA

Éste es el valor predeterminado para las siguientes traducciones disponibles:

- Portugués de Brasil
- Italiano

- 3** AAAA-MM-DD

Éste es el valor predeterminado para las siguientes traducciones disponibles:

- Japonés
- Chino (simplificado)
- Polaco

4 DD.MM.AAAA

Éste es el valor predeterminado para las siguientes traducciones disponibles:

- Alemán
- Francés
- Español
- Checo
- Ruso

5 AAAA.MM.DD

Éste es el valor predeterminado para las siguientes traducciones disponibles:

- Húngaro

6 AAAA/MM/DD

7 DD/MM/AAAA

Ejemplos

Archivo de opciones:

```
dateformat 3
```

Línea de mandatos:

```
-date=3
```

Esta opción es válida en la línea de mandatos inicial y en modalidad interactiva. Si utiliza esta opción en modalidad interactiva, sólo afectará al mandato con el que se especifica. Cuando se complete la ejecución de ese mandato, el valor se revierte al comienzo de la sesión interactiva. Será el valor del archivo dsm.opt, a menos que se haya modificado mediante la línea de mandatos inicial o mediante una opción que el servidor ha forzado.

Consideraciones adicionales para especificar los formatos de fecha y hora

El formato de fecha y hora que especifique con esta opción debe utilizarse en las opciones que acepten una entrada de fecha y hora. Por ejemplo: totime, fromtime, todate, fromdate y pittime.

Por ejemplo, si especifica la opción timeformat como TIMEFORMAT 4, el valor que proporciona en la opción fromtime o totime debe especificarse como una hora, por ejemplo, 12:24:00pm. Si especifica 13:24:00, no será válido porque TIMEFORMAT 4 necesita un entero de hora menor o igual a 12. Si desea especificar valores de hasta 24 horas en una opción y utilizar comas como separadores, debe especificar TIMEFORMAT 2.

Configuración de los formatos de fecha y hora en el archivo de configuración del entorno regional del sistema

Puede especificar formatos de fecha y hora configurándolos en el archivo de entorno regional del sistema. Si especifica formatos de fecha y hora en el archivo del entorno regional, deben definirse utilizando un subconjunto de especificadores de formato de producción de números soportados por la función strftime() del lenguaje C. Puede utilizar los siguientes especificadores para establecer los formatos de fecha y hora en los valores de configuración del entorno regional.

Especificadores de fecha

- %Y - el año, en cuatro dígitos. Por ejemplo, 2011.

- %y - el año, solo con los dos últimos dígitos. Por ejemplo, 11; no 2011.
- %m - el mes, como un número decimal (1-12).
- %d - el día del mes (1-31).

En los especificadores de fecha, sólo puede especificar un especificador de año. No especifique %Y ni %y. El modificador E (un E en mayúsculas) puede preceder los especificadores de fecha para crear la forma alternativa del entorno local para el año, mes o día. Si no existe ningún formato alternativo, el modificador E se ignora. Separe los especificadores con un carácter ASCII de 7 bits. Los separadores más utilizados son los dos puntos (:), las comas (,), los puntos (.), (.), guiones (-) o barras diagonales (/). No utilice caracteres de varios bytes como separadores.

Especificadores de hora

- %H - la hora, en formato de 24 horas (00-23).
- %I - la hora, en formato de 12 horas (00-12).
- %M - minutos después de la hora (00-59).
- %S - segundos después del minuto (00-59)
- %p - añade el indicador AM (antes de mediodía) o PM (después de mediodía).

En los especificadores de hora, sólo puede especificar un especificador de hora. No especifique %I y %H a la vez.

El modificador O (una O mayúscula) puede ir antes que los especificadores de hora para producir el formato alternativo del entorno regional para la hora, los minutos o los segundos. El modificador O no puede ir antes que el especificador %p. Separe los especificadores con un carácter ASCII de 7 bits. Los separadores más utilizados son los dos puntos (:), las comas (,) o los puntos (.). No utilice caracteres de varios bytes como separadores. No especifique un separador entre el especificador %p y el separador que le precede o le sigue.

Ejemplos de formato de hora, configurados en los valores de entorno regional

Para establecer un formato de hora en particular, edite el archivo de configuración del entorno regional que utiliza y modifique la línea `t_fmt` en función de sus necesidades. Sea cual sea el formato de hora seleccionado, se aplica tanto a la salida como a la entrada. Una vez editado el archivo de configuración del entorno regional, debe ejecutarse el mandato **localedef** para crear el archivo del entorno regional final.

Tabla 71. Valores del formato de hora de ejemplo en la configuración del entorno regional (línea `t_fmt`)

Ejemplo	Resultado
"%H:%M:%S"	Muestra la hora en el formato <i>hh:mm:ss</i> , siendo valores válidos para <i>hh</i> el rango de 0 a 23.
"%H,%M,%S"	Muestra la hora en el formato <i>hh,mm,ss</i> , siendo valores válidos para <i>hh</i> el rango de 0 a 23.
"%I,%M,13p"	Muestra la hora en el formato <i>hh,mm,ssA/P</i> , donde <i>hh</i> puede estar entre 1 y 12, y donde <i>A/P</i> es la abreviatura local de antemeridiano (AM en inglés) o postmeridiano (PM en inglés).

Ejemplos de formato de fecha, configurados en los valores de entorno regional

Para establecer un formato de fecha en particular, edite el archivo de configuración y modifique la línea `d_fmt` en función de sus necesidades. Sea cual sea el formato de fecha seleccionado, se aplica tanto a la salida como a la entrada.

Tabla 72. Valores del formato de fecha de ejemplo en la configuración del entorno regional (línea `d_fmt`)

Ejemplo	Resultado
"%m/%d/%y"	Visualiza la fecha con el formato MM/DD/AA.
"%d.%m.%Y"	Visualiza la fecha con el formato DD.MM.AAAA.

Dedupcachepath

Utilice la opción `dedupcachepath` para especificar la ubicación donde se creó la base de datos de la memoria caché de eliminación de duplicados de datos del lado del cliente.

Esta opción se pasa por alto si la opción `enablededupcache=no` se establece durante el proceso de copia de seguridad o archivado.

Clientes soportados

Esta opción es válida para todos los clientes. Esta opción también es válida para la API de IBM Spectrum Protect.

Archivo de opciones

Coloque esta opción en el archivo de opciones del sistema (`dsm.sys`). Puede establecer esta opción en el campo **Deduplication Cache Location** del Editor de preferencias. Esta opción se puede definir en el conjunto de opciones de cliente del servidor de IBM Spectrum Protect.

Sintaxis

►►—DEDUPCACHEPath—*path*—————►►

Parámetros

path

Especifica la ubicación en la que se creará la base de datos de caché en disco si `enablededupcache` se ha establecido en `yes`. La ubicación predeterminada es para crear el archivo de caché de la eliminación de duplicados de datos del directorio de instalación del cliente de copia de seguridad y archivado o de la API.

Ejemplos

Archivo de opciones:

`dedupcachepath /volumes/temp`

Línea de mandatos:

No se aplica.

Referencia relacionada:

"Enablededupcache" en la página 413

Dedupcachesize

Utilice la opción `dedupcachesize` para determinar el tamaño máximo del archivo de la caché de la eliminación de duplicados de datos. Cuando el archivo de la caché alcanza su tamaño máximo, se elimina el contenido de la caché y se añaden las entradas nuevas.

Clientes soportados

Esta opción es válida para todos los clientes. Esta opción también es válida para la API de IBM Spectrum Protect.

Archivo de opciones

Establezca esta opción en el archivo de opciones del sistema (`dsm.sys`). Puede establecer esta opción en el campo **Eliminación de duplicados > Memoria caché de la eliminación de duplicados > Tamaño máximo** en el editor Preferencias. La opción se puede establecer en el conjunto de opciones de cliente del servidor de IBM Spectrum Protect.

Sintaxis

►►—DEDUPCACHESize—*dedupcachesize*————►►

Parámetros

dedupcachesize

Especifica el tamaño máximo, en megabytes, del archivo de la caché de la eliminación de duplicados de datos. El rango de valores es de 1 a 2048, siendo 256 el valor predeterminado.

Ejemplos

Archivo de opciones:

`dedupcachesize 1024`

Línea de mandatos:

No se aplica.

Referencia relacionada:

“Eliminación de duplicados”

Eliminación de duplicados

Utilice la opción `deduplication` para especificar si habilita la eliminación de datos redundantes por parte del cliente cuando se transfieren los datos al servidor IBM Spectrum Protect durante el proceso de copia de seguridad y archivado.

La eliminación de datos duplicados se inhabilita si se define la opción `enablelanfree`. Se excluyen los archivos cifrados del cliente de copia de seguridad y archivado de la eliminación de duplicados de datos por parte del cliente. También se excluyen los archivos de los sistemas de archivos cifrados.

Para dar soporte a la eliminación de duplicados de datos por parte del cliente, se deben cumplir los siguientes criterios:

- La eliminación de duplicados de datos del lado de cliente está habilitada en el servidor.

- El destino de la agrupación de almacenamiento para los datos debe ser una agrupación de almacenamiento habilitada para la eliminación de duplicados de datos. La agrupación de almacenamiento debe tener el tipo de dispositivo "file".
- Los archivos pueden excluir del proceso de eliminación de duplicados de datos del lado del cliente (todos los archivos están incluidos de forma predeterminada).
- El servidor puede limitar el tamaño máximo de transacción para optimización de almacenamiento de datos definiendo la opción CLIENTDEDUPTXNLIMIT en el servidor. Para obtener más información sobre esta opción, consulte la documentación del servidor de IBM Spectrum Protect.
- El archivo debe tener un tamaño superior a 2 KB.

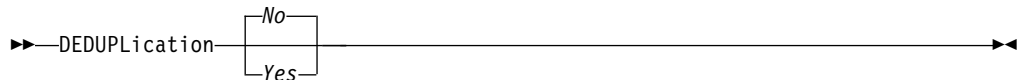
Clientes soportados

Esta opción es válida para todos los clientes; también se puede utilizar en la API de IBM Spectrum Protect.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema (dsm.sys) en una stanza de servidor. Puede establecer esta opción seleccionando la casilla de verificación **Eliminación de duplicados** > **Habilitar eliminación de duplicados** en el editor Preferencias. Esta opción se puede definir en el conjunto de opciones de cliente del servidor de IBM Spectrum Protect.

Sintaxis



Parámetros

No Especifica que no desea habilitar la eliminación de duplicados de datos por parte del cliente para el proceso de copia de seguridad y archivado. No es el valor predeterminado.

Yes

Especifica que desea habilitar la eliminación de duplicados de datos por parte del cliente para el proceso de copia de seguridad y archivado.

Ejemplos

Archivo de opciones:

deduplication yes

Línea de mandatos:

-deduplication=yes

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Referencia relacionada:

"Opciones include" en la página 458

"Opciones exclude" en la página 425

Defaultserver

Utilice la opción `defaultserver` para especificar el nombre del servidor de IBM Spectrum Protect a contactar para los servicios de copia de seguridad/archivado si se ha definido más de un servidor en el archivo `dsm.sys`.

De forma predeterminada, el cliente de copia de seguridad y archivado establecerá contacto con el servidor que se ha definido mediante la primera stanza del archivo `dsm.sys`. Esta opción sólo se utiliza si no se especifica la opción `servername` en el archivo de opciones del usuario cliente (`dsm.opt`).

Si se tiene instalado el cliente de HSM en la estación de trabajo y no se especifica un servidor de migración con la opción `migrateserver`, utilice esta opción para especificar el servidor donde desea migrar los archivos. Para obtener más información, consulte la documentación de producto de IBM Spectrum Protect for Space Management en el IBM Knowledge Center, en <http://www.ibm.com/support/knowledgecenter/SSERBH/welcome>.

Clientes soportados

Esta opción es válida para todos los clientes UNIX.

Archivo de opciones

Establezca esta opción *al principio* del archivo `dsm.sys` *delante* de cualquier sección de servidor.

Sintaxis

►►—DEFAULTServer— —servername—►►

Parámetros

servername

Especifica el nombre del servidor predeterminado en el que desea almacenar las copias de seguridad o las copias archivadas. El servidor donde se migran los archivos de los sistemas de archivos locales también puede especificarse con esta opción.

Ejemplos

Archivo de opciones:

defaults server_a

Línea de mandatos:

No se aplica.

Deletefiles

Utilice la opción `deletefiles` con el mandato **archive** para suprimir archivos de la estación de trabajo después de haber realizado el archivado de éstos.

También puede utilizar esta opción con el mandato **restore image** y la opción **incremental** para suprimir archivos de la imagen restaurada si éstos se han suprimido después de haber creado la imagen. La supresión de archivos se

realizará correctamente si el grupo de copia de seguridad del servidor de IBM Spectrum Protect cuenta con suficientes versiones para los archivos existentes y suprimidos.

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Sintaxis

►—DELetefiles—◄◄

Parámetros

No hay parámetros para esta opción.

Ejemplos

Línea de mandatos:

```
dsmc archive "/Users/dgordon/Documents/*.c" -deletedefiles
dsmc archive "/home/foo/*.c" -deletedefiles
dsmc restore image /local/data -incremental -deletedefiles
```

Descripción

La opción `description` asigna o especifica una descripción para los archivos cuando se efectúan operaciones de archivado, supresión de archivado, recuperación, consulta de archivado o consulta de juego de copias de seguridad.

Por ejemplo, si desea archivar un archivo denominado `budget.jan` y asignarlo a la descripción "Presupuesto de 2002 para proy. 1", especificaría lo siguiente:

```
dsmc archive -des="Presupuesto de 2003 para proy. 1" /home/plan/
proj1/budget.jan
```

Nota:

1. La longitud máxima de una descripción es de 254 caracteres.
2. Si el valor de la opción que contiene un espacio en blanco, especifique el valor entre comillas (" ").

Utilice la opción `description` con los mandatos siguientes:

- **archive**
- **delete archive**
- **query archive**
- **query backupset**
- **retrieve**

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Sintaxis

Parámetros

description

Asigna una descripción al archivo que se está archivando. Si no especifica una descripción con el mandato **archive**, el valor predeterminado es `Archive Date:x`, donde `x` es la fecha del sistema actual. Tenga en cuenta que la fecha siempre consta de 10 caracteres. Si en su formato de fecha el año se indica con dos dígitos, habrá dos espacios en blanco al final de la fecha. Por ejemplo, una descripción predeterminada en la que el año se indique con cuatro dígitos puede ser `"Archive Date: 2002/05/03"`, y la misma descripción predeterminada en la que el año se indique con dos dígitos sería `"Archive Date: 02/05/03 "` (observe que hay dos espacios al final). Al recuperar archivos utilizando la descripción de año con dos dígitos, puede especificar la opción `-description` de cualquiera de estas maneras:

```
-description="ArchiveDate: 02/05/03 "
o bien
-description="ArchiveDate: 02/05/03*"
```

Si se utiliza el mandato **archive** para archivar más de un archivo, la descripción que especifique se aplica a cada archivo. Por ejemplo, para archivar un grupo de archivos y asignar la misma descripción, *Proyecto X*, a cada archivo, escribiría:

```
dsmc archive -description="Proyecto X" "/Users/van/Documents/*.x"
dsmc archive -description="Project X" "/home/allproj/*"
```

Posteriormente podrá utilizarse la descripción para recuperar todos los archivos.

Ejemplos

Línea de mandatos:

```
dsmc archive "/Users/van/Documents/*.prj" -des="Presupuesto de
2003 para proy. 1"
dsmc archive "/home/foo/*.prj" -des="2003 Budget for Proj 1"
dsmc query backupset -loc=server -descr="Mi portátil"
```

Detail

Utilice la opción `detail` para ver información sobre la clase de gestión, el espacio de archivos, las copias de seguridad, las copias archivadas y otra información adicional en función del mandato con el que se utilice.

Utilice la opción `detail` con el mandato **query mgmtclass** para visualizar información detallada acerca de cada clase de gestión del juego de políticas activo. Si no utiliza la opción `detail`, sólo se mostrará el nombre de la clase de gestión y una breve descripción. Si especifica la opción `detail`, se mostrará información sobre los atributos de cada grupo de copia que contiene cada clase de gestión. Una clase de gestión puede contener un grupo de copia de seguridad, un grupo de copia archivada, ambos grupos o ninguno.

Puede que un espacio de archivos activado para Unicode no se visualice correctamente si el servidor no puede visualizar el nombre en Unicode. En este caso, utilice el `fsID` (identificador de espacio de archivos) del espacio de archivos para identificar estos espacios de archivos en el servidor. Utilice la opción `detail`

con los mandatos **delete filespace** y **query filespace** para determinar el ID de espacio de archivos de un espacio de archivos. El ID de espacio de archivos también aparece en el diálogo de información de archivos de las GUI del cliente de copia de seguridad/archivado y del cliente web.

Utilice la opción **detail** con los mandatos **query backup** y **query archive** para que se visualicen los atributos del archivo que ha especificado:

- Fecha de última modificación
- Fecha de último acceso
- Compresión
- Tipo de cifrado
- Deduplicación de datos del lado del cliente
- Indica si el cliente HSM ha migrado o premigrado el archivo

Utilice el mandato **detail** con el mandato **query VM** para visualizar las estadísticas siguientes:

- El número medio de objetos de IBM Spectrum Protect necesarios para describir una megablock único, entre todos los megablocks de una copia de seguridad.
- El número medio de objetos de IBM Spectrum Protect necesarios para describir una megablock único, para todos los megablocks de una copia de seguridad.
- La proporción de la cantidad de datos, de los que informa Change Block Tracking, frente a la cantidad de datos de los que realmente se ha realizado una copia de seguridad, en una copia de seguridad determinada.
- La proporción de la cantidad de datos, de los que informa Change Block Tracking, frente a la cantidad de datos de los que realmente se ha realizado una copia de seguridad, para todas las copias de seguridad de este espacio de archivos.
- El número de copias de seguridad que se han creado desde que se ha realizado la última copia de seguridad completa a partir de los discos de producción.

Los valores devueltos en **query vm** pueden ayudarle a ajustar el heurística (consulte las opciones **Mbobjrefreshthresh** y **Mbpctrefreshthresh**) para ajustar el desencadenante de los valores para renovaciones megablock.

Utilice la opción **detail** con los mandatos siguientes:

- **delete filespace**
- **incremental**
- **query archive**
- **query backup**
- **query filespace**
- **query inclexcl**
- **query mgmtclass**
- **query vm**

Cientes soportados

Esta opción es válida para todos los clientes. Esta opción no está establecida en el archivo de opciones del cliente; se utiliza mediante la adición a la línea de mandatos cuando se especifique alguno de los mandatos que lo admiten. La API de IBM Spectrum Protect no admite esta opción.

Sintaxis

►► DETail ◀◀

Parámetros

No hay parámetros para esta opción.

Ejemplos

Línea de mandatos:

```
dsmc query mgmtclass -detail
dsmc query filespace -detail
dsmc query backup file1 -detail

dsmc query vm -detail
```

Diffsnapshot

La opción `diffsnapshot` controla si cliente de copia de seguridad y archivado debe crear la instantánea diferencial al ejecutar una copia de seguridad incremental por diferencia de instantánea.

Si el cliente no crea la instantánea diferencial, se utilizará la instantánea más reciente que se encuentre en el volumen como la instantánea diferencial y como el origen de la operación de copia de seguridad.

El valor predeterminado es crear la instantánea diferencial. Esta opción se omite la primera vez que se utiliza la opción `snaptiff`. La primera vez que se utiliza la opción `snaptiff` en un volumen, se debe crear una instantánea y utilizarla como origen de una copia de seguridad incremental completa. El cliente suprime las instantáneas creadas por cliente de copia de seguridad y archivado después de finalizar la siguiente copia de seguridad incremental por diferencia de instantánea.

Las instantáneas se pueden crear con la herramienta Network Appliance FilerView. Utilice el parámetro `latest` si desea que el cliente utilice la instantánea más reciente que se haya creado con éste o con otro método. El cliente no suprime nunca las instantáneas que se han creado con métodos que no son de IBM Spectrum Protect.

Clientes soportados

Esta opción es válida para clientes de Linux x86_64.

Sintaxis

►► DIFFSNAPSHOT *create* *latest* ◀◀

Parámetros

create

Especifique que desea crear una nueva instantánea permanente para que se utilice como instantánea origen. Este es el valor predeterminado.

latest

Especifica que se desea utilizar la instantánea más reciente encontrada en el servidor de archivos como instantánea origen.

Ejemplos

Línea de mandatos:

Realice una copia de seguridad incremental por diferencia de instantánea de un sistema de archivos montado en NFS /vol/vol1 que reside en el servidor de archivos homestore.example.com, donde /net/home1 es el punto de montaje de /vol/vol1.

```
incremental -snapdiff -diffsnapshot=latest /net/home1
```

El valor latest de la opción -diffsnapshot significa que la operación utilizará la instantánea más reciente (la instantánea activa).

Conceptos relacionados:

“Copia de seguridad diferencial de la instantánea con una conexión HTTPS” en la página 178

Tareas relacionadas:

“Configuración de NetApp y IBM Spectrum Protect para copias de seguridad incrementales de diferencia de instantánea” en la página 114

Referencia relacionada:

“Snapdiff” en la página 561

“Snapdiffhttps” en la página 566

“Createnewbase” en la página 373

Diffsnapshotname

La opción diffsnapshotname permite especificar qué instantánea diferencial, en el volumen de archivador de destino, debe utilizarse durante una copia de seguridad diferencial de instantáneas. Esta opción sólo se especifica si también se especifica diffsnapshot=latest.

Si no se especifica esta opción, diffsnapshot=latest selecciona la instantánea existente más reciente en el volumen del archivador y la utiliza como instantánea diferencial.

Clientes soportados

Esta opción puede utilizarse con clientes Linux x86_64 soportados.

Archivo de opciones

Esta opción puede especificarse en el archivo de opciones del cliente o bien en la línea de mandatos.

Sintaxis

►►—DIFFSNAPSHOTName— —snapshot_name—◀◀

Parámetros

snapshot_name

Especifica el nombre de una instantánea existente que utilizar como instantánea diferencial.

También puede utilizar un patrón con caracteres comodín para seleccionar una instantánea. Los comodines pueden ser cualquiera de los caracteres siguientes:

* Un asterisco (*) coincide con cualquier carácter.

? El signo de interrogación (?) coincide con un solo carácter.

La instantánea más reciente que coincide con el patrón comodín se selecciona como la instantánea diferencial.

Ejemplos

Archivo de opciones:

```
diffsnapshotname volume_base_snap
diffsnapshotname nightly.?
```

Línea de mandatos:

```
dsmc incr \\DRFiler\UserDataVol_Mirror_Share -snapdiff
-useexistingbase -basenameshotname="nightly.?"
-diffsnapshot=latest -diffsnapshotname="nightly.?"
```

Información relacionada

Basesnapshotname

Useexistingbase

Dirmc

La opción `dirmc` especifica la clase de gestión que desea utilizar para los directorios.

Si no se especifica esta opción para asociar una clase de gestión con directorios, el programa cliente utiliza la clase de gestión del conjunto de políticas activo del dominio de políticas cuyo período de retención sea más largo. Seleccione una clase de gestión para directorios individuales que retenga los directorios durante, como mínimo, el tiempo que retiene los archivos que se asocian a éstos.

Si especifica una clase de gestión mediante esta opción, todos los directorios especificados en la operación de copia de seguridad están vinculados a dicha clase de gestión.

La opción `dirmc` especifica la clase de gestión de los directorios de los que hace copia de seguridad y no afecta a los directorios archivados. Utilice la opción `archmc` con el mandato **archive** para especificar la clase de gestión disponible para el dominio de políticas al que desea vincular los archivos y los directorios archivados. Si no utiliza la opción `archmc`, el servidor vincula los directorios archivados a la clase de gestión. Si la clase de gestión predeterminada no tiene grupo de copias archivadas, el servidor vincula los directorios archivados a la clase de gestión con el período de retención más reducido.

Importante: Sólo se almacenan los atributos ampliados y los ACLs en las agrupaciones de almacenamiento. La información del directorio, distinta a los

atributos ampliados y a los ACLs, permanece en la base de datos. En sistemas Windows , los directorios ocupan espacio de agrupación de almacenamiento.

Cientes soportados

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción.

Archivo de opciones

Establezca esta opción en el archivo dsm.sys dentro de una sección de servidor. Puede establecer esta opción en la ficha **Copia de seguridad**, en la sección **Clase de gestión de directorios** del Editor de preferencias.

Sintaxis

►►—DIRMc— —*mgmtclassname*—►►

Parámetros

mgmtclassname

Especifica el nombre de la clase de gestión que se desea asociar con los directorios. El cliente utiliza el nombre de clase de gestión especificado para todos los directorios de los que realiza copia de seguridad. Si no especifica esta opción, el cliente asocia la clase de gestión al mayor período de retención con directorios.

Ejemplos

Archivo de opciones:

dirm managdir

Línea de mandatos

No se aplica.

Información relacionada

Si desea realizar la copia de seguridad de archivos específicos de una clase de gestión, consulte el tema “Asignar una clase de gestión a los archivos” en la página 306 para obtener más información.

Dirsonly

La opción dirsonly *sólo* procesa directorios. El cliente no procesa archivos.

La opción dirsonly puede utilizarse con los mandatos siguientes:

- **archive**
- **incremental**
- **query archive**
- **query backup**
- **restore**
- **restore backupset**
- **retrieve**
- **selective**

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Sintaxis

►►—Dirsonly—◄◄

Parámetros

No hay parámetros para esta opción.

Ejemplos

Línea de mandatos:

```
dsmc query backup -dirsonly "/Users/*"
```

Línea de mandatos:

```
dsmc query backup -dirsonly "*" 
```

Disablenqr

La opción `disablenqr` especifica si el cliente de archivado y copia de seguridad puede usar el método de restauración sin consulta para restaurar archivos y directorios del servidor.

Si establece la opción `disablenqr` en `no` (el valor predeterminado), el cliente podrá usar el proceso de restauración sin consulta.

Si establece la opción `disablenqr` en `yes`, el cliente sólo puede utilizar el proceso de restauración estándar (también denominada "restauración clásica").

Nota: No existe ninguna opción ni valor para especificar que el cliente sólo puede utilizar el método de restauración sin consulta.

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción. El servidor también puede definir esta opción.

Archivo de opciones

Coloque esta opción en el archivo `dsm.opt`.

Sintaxis

►►—DISABLENQR—

No
Yes

—◄◄

Parámetros

No Especifica que el cliente puede usar el método de restauración sin consulta. Éste es el valor predeterminado.

Yes

Especifica que el cliente sólo utiliza el método de restauración estándar. No se permite el método de restauración sin consulta.

Ejemplos

Archivo de opciones:

disablenqr yes

Línea de mandatos:

-disablenqr=yes

Diskbuffsize

La opción diskbuffsize especifica el tamaño máximo de memoria intermedia de E/S de disco (en kilobytes) que el cliente puede utilizar al leer archivos. La opción diskbuffsize sustituye a la opción largecommbuffers.

Por lo general, puede obtenerse un rendimiento óptimo del cliente de migración de copia de seguridad, archivado o HSM si el valor de esta opción es igual o menor que la cantidad de lectura anticipada del archivo que proporciona el sistema de archivos del cliente. Un almacenamiento intermedio de mayor tamaño precisará más memoria y es posible que no mejore el rendimiento.

Importante: Utilice el valor predeterminado, a menos que el personal de soporte de IBM le indique algo distinto.

Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor.

Sintaxis

►►—DISKBuffsize— —size—————►►

Parámetros

size

Especifica el tamaño máximo de almacenamiento intermedio de E/S del disco (en kilobytes) que el cliente puede utilizar al leer archivos. El rango de valores es de 16 a 1023; el valor predeterminado es 32. Para AIX: si se define la opción enablelanfree no, el valor predeterminado de diskbuffsize es 256.

Ejemplos

Archivo de opciones:

diskbuffsize 64

Línea de mandatos:

No se aplica.

Diskcachelocation

La opción `diskcachelocation` especifica la ubicación en la que se crea la base de datos de memoria caché de disco si la opción `memoryefficientbackup=diskcachemethod` se especifica durante una copia de seguridad incremental.

Puede especificar la opción `diskcachelocation` en el archivo de opciones o con la opción `include.fs`. Si la opción `diskcachelocation` aparece en el archivo de opciones, el valor de ésta se utilizará para todos los espacios de archivos no representados mediante una opción `include.fs` que contenga el parámetro `diskcachelocation`.

La caché de disco es un archivo temporal que se suprime después de ejecutar el mandato **incremental**. Esta opción puede utilizarse para seleccionar:

1. Una ubicación que cuenta con más espacio libre en el disco si, al utilizar `memoryefficientbackup=diskcachemethod`, recibe el mensaje en el que se le indica que el archivo de caché en disco no puede crearse porque no dispone de suficiente espacio de disco.
2. Una ubicación en un volumen físico diferente para reducir la contención para el mecanismo de acceso al disco y mejorar con ello el rendimiento.

Importante: Por razones de rendimiento, no utilice una unidad remota para `diskcachelocation`.

La cantidad real de espacio en el disco necesaria para el archivo de caché del disco creado por las copias de seguridad incrementales de la caché del disco depende del número de archivos y directorios incluidos en la copia de seguridad y de la longitud promedio de los archivos y directorios de los que se hace copia de seguridad. Para UNIX, Linux, calcule 1 byte por carácter en el nombre de vía de acceso. Para Mac OS X, calcule 4 bytes por carácter en el nombre de vía de acceso. Por ejemplo, si se va a realizar una copia de seguridad de 1.000.000 de archivos y directorios y la longitud promedio de la vía de acceso es de 200 caracteres, la base de datos ocupará aproximadamente 200 MB en los clientes UNIX y Linux y 800 MB en los clientes Mac OS X. Otra forma de calcular a fin de realizar cierta planificación es multiplicar el número de archivos y directorios por la longitud de la vía de acceso más larga a fin de establecer el tamaño máximo de base de datos.

Al realizar copia de seguridad de un sistema de archivos gestionados HSM, se crea un segundo archivo de caché de disco para la lista de archivos migrados. Los archivos de caché de disco combinados, creados por copias de seguridad incrementales de caché de disco y copias de seguridad del sistema de archivos gestionados HSM, pueden necesitar más de 400 MB de espacio de disco para cada millón de archivos de los que se realice copia de seguridad. El archivo de la memoria caché de disco puede ser muy grande. El soporte de archivos grandes debe estar habilitado en el sistema de archivos que se está utilizando para el archivo de memoria caché de disco.

Clientes soportados

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción.

Archivo de opciones

Establezca esta opción en el archivo `dsm.sys` dentro de una stanza de servidor.

Sintaxis

►—DISKCACHELocation— *vía de acceso*—►

Parámetros

vía de acceso

Especifica la ubicación en la que se creará la base de datos de caché en disco si `memoryefficientbackup=diskcachemethod`. La ubicación predeterminada es para crear el archivo de caché del disco en la raíz del espacio de archivo que se está procesando.

Ejemplos

Archivo de opciones:

```
diskcachelocation /home
diskcachelocation /Volumes/hfs2
```

Línea de mandatos:

No se aplica.

Consulte el tema “Opciones include” en la página 458 para obtener más información acerca de `include.fs`.

Domain

La opción `domain` especifica lo que desea incluir en la copia de seguridad incremental.

Solo se realiza copia de seguridad de los objetos de dominio si inicia el mandato **incremental** sin una especificación de archivo.

El cliente de copia de seguridad y archivado utiliza el valor `domain` en las situaciones siguientes para determinar qué sistemas de archivos se han de procesar durante una copia de seguridad incremental:

- Cuando se ejecuta una copia de seguridad incremental utilizando el mandato **incremental** y no especifica qué sistemas de archivos se han de procesar.
- Cuando el administrador de IBM Spectrum Protect define una planificación para ejecutar una copia de seguridad incremental para el usuario, pero no especifica los sistemas de archivos que deben procesarse.
- Cuando selecciona la acción **Copia de seguridad de dominio** en la GUI del cliente de copia de seguridad y archivado.
- Cuando se ejecuta una copia de seguridad incremental con el mandato **incremental** y no se especifica qué unidades deben procesarse.
- Cuando el administrador de IBM Spectrum Protect define una planificación para ejecutar una copia de seguridad incremental para el usuario, pero no especifica las unidades que deben procesarse.
- Cuando selecciona la acción **Copia de seguridad de dominio** en la GUI del cliente de copia de seguridad y archivado.

Puede definir la opción `domain` en las ubicaciones siguientes:

- En un archivo de opciones.
- En la línea de mandatos, cuando se ha especificado con un mandato del cliente.

- En un conjunto de opciones de cliente, que se haya definido en el servidor con el mandato **define clientopt**.
- Como una opción en un mandato planificado, que se haya definido en el servidor con el mandato **define schedule**.

Si alguno de estos orígenes contiene una definición de dominio, el cliente realizará copia de seguridad de ese dominio. Si más de un origen especifica un dominio, el cliente realizará copia de seguridad de todos los dominios especificados. Se puede definir el mismo objeto de dominio más de una vez, pero el efecto es el mismo que si lo define sólo una vez. Si no especifica un dominio, el cliente realiza copia de seguridad del dominio predeterminado, como se describe en el parámetro `all-local`.

Puede excluir objetos del dominio mediante la especificación del operador de exclusión (-) delante del objeto. Si alguna definición de dominio excluye un objeto, ese objeto se excluye del dominio, incluso si otra definición incluye el objeto. No puede utilizar el operador de exclusión de dominio (-) delante de ninguna palabra clave de dominio que empiece por `all-`.

Si una sentencia de dominio excluye uno o más objetos y ninguna sentencia de dominio incluye objetos, el resultado es un dominio vacío (no se realiza copia de seguridad de nada). Debe especificar los objetos que se incluirán en el dominio si alguna sentencia de dominio excluye objetos.

Ejemplo 1: Este ejemplo utiliza una sentencia de dominio para realizar copia de seguridad de todos los sistemas de archivos locales excepto para `/fs1`:

```
domain all-local -/fs1
```

Ejemplo 2: Este ejemplo utiliza varias sentencias de dominio para realizar copia de seguridad de todos los sistemas de archivos locales excepto para `/fs1`:

```
domain all-local domain -/fs1
```

Ejemplo 3: Este ejemplo excluye `/fs1` en una operación de copia de seguridad. Si no se utiliza ninguna otra sentencia de dominio, el resultado es un dominio vacío. No se realiza copia de seguridad de nada.

```
domain -/fs1
```

Si inicia el mandato incremental con una especificación de archivo, el cliente pasa por alto las definiciones de dominio y realiza una copia de seguridad de la especificación de archivo.

Puede incluir un punto de montaje virtual en el dominio del cliente.

Importante: Si está ejecutando GPFS para AIX o GPFS para Linux x86_64 en un clúster de varios nodos, y todos los nodos comparten un sistema de archivos GPFS montado, el cliente procesa este sistema de archivos como un sistema de archivos local. El cliente realiza copias de seguridad del sistema de archivos en cada nodo durante una copia de seguridad incremental. Para evitar esta situación, puede realizar una de las siguientes tareas:

- Configure explícitamente la sentencia `domain` en el archivo de opciones de usuario de cliente (`dsm.opt`) para enumerar los sistemas de archivos de los que desea que dicho nodo realice una copia de seguridad.
- Establezca la opción `exclude.fs` en el archivo de opciones del sistema del cliente para excluir el sistema de archivos GPFS de los servicios de copia de seguridad.

Sistemas de archivos montados automáticamente

Al realizar una copia de seguridad con la opción `domain` establecida en `all-local`, no se hace copia de seguridad de los archivos gestionados por el montador automático y los sistemas de archivo de bucle de retorno.

Si realiza copias de seguridad de un sistema de archivos con la opción `domain` establecida en `all-local`, se excluyen los subdirectorios que sean puntos de montaje de un sistema de archivos automontado (AutoFS) en una operación de copia de seguridad. Todos los archivos existentes en el servidor para el subdirectorio de montaje automático han caducado.

Si se realiza una copia de seguridad con la opción `domain` establecida en `all-lofs`, se hace copia de seguridad de todos los sistemas de archivos de bucle de retorno (LOFS) explícitos y se excluyen todos los sistemas de archivos automontados. Para dispositivos de bucle y sistemas de archivos locales gestionados por el montador automático, establezca la opción `domain` en `all-auto-lofs`.

Utilice la opción `automount` con los parámetros del dominio `all-auto-nfs` y `all-auto-lofs` para especificar uno o varios sistemas de archivos de montaje automático que se van a montar y a añadir al dominio. Si especifica la opción `automount`, los sistemas de archivos automontados se vuelven a montar si se han desactivado durante la ejecución del mandato **incremental**.

Los puntos de montaje virtual no pueden utilizarse con sistemas de archivos montados automáticamente.

Importante: En algunas distribuciones Linux, es posible que las asignaciones o puntos de montaje del sistema de archivos automontado de tipo de sistema de archivos (AutoFS) no aparezcan en la tabla de montaje actual. A consecuencia de ello, los sistemas de archivos automontados, que se desmontan durante el proceso de archivado o copia de seguridad, podrían procesarse de manera incorrecta y almacenarse como parte del dominio equivocado (por ejemplo, como parte del dominio `all-local`, `all-nfs` o `all-lofs`, según el tipo de sistema de archivos real). Por lo tanto, en este tipo de entornos de distribución de Linux, tiene que especificar el valor correcto para la opción `automount`, a fin de procesar adecuadamente el valor de opción de dominio en cualquier momento específico.

Para Mac OS X, los sistemas de archivos automontados no se admiten. Si un sistema de archivos automontado forma parte de una sentencia de dominio, la copia de seguridad falla y no se procesan archivos en el sistema de archivos automontado. Haga una copia de seguridad del sistema de archivos automontado del sistema host y restáurela. No haga una copia de seguridad del sistema de archivos automontado ni la restaure sobre una conexión de red.

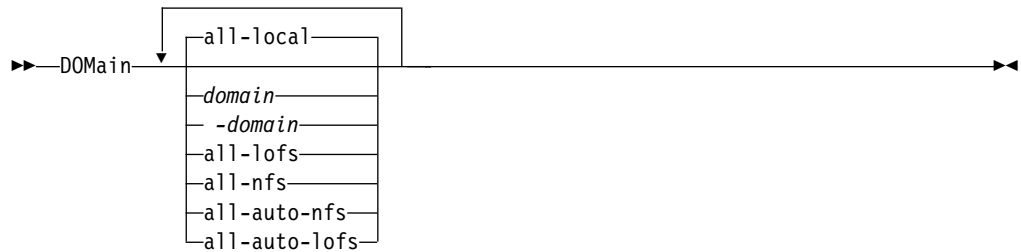
Clientes soportados

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Establezca esta opción en el archivo de opciones, `dsm.opt` o `dsm.sys`. En el archivo `dsm.sys`, debe colocar esta opción dentro de una stanza de servidor. Puede establecer esta opción en la ficha **Copia de seguridad**, en la sección **Dominio para copia de seguridad** del Editor de preferencias.

Sintaxis



Parámetros

all-local

Hace copias de seguridad de todos los sistemas de archivos locales excepto de los sistemas de archivo LOFS y LOFS a través del montador automático. Este parámetro es el predeterminado. El directorio `/tmp` no está incluido.

dominio

Define los sistemas de archivos que deben incluirse en el dominio de cliente predeterminado.

Al utilizar *domain* con el mandato **incremental**, procesa estos sistemas de archivo además de aquellos sistemas de archivos que se especifican en el dominio de cliente predeterminado.

-domain

Define los sistemas de archivos que deben excluirse del dominio de cliente predeterminado.

all-lofs

Realiza una copia de seguridad de todos los sistemas de archivos de bucle de retorno, excepto de los sistemas de archivos gestionados por el montador automático. Este parámetro no recibe soporte en Mac OS X.

all-nfs

Realiza una copia de seguridad de todos los sistemas de archivos de red, excepto de los sistemas de archivos gestionados por el montador automático. Este parámetro no recibe soporte en Mac OS X.

all-auto-nfs

Realiza una copia de seguridad de todos los sistemas de archivos de red (pero no de los sistemas de archivo locales) gestionados por el montador automático. Este parámetro no recibe soporte en Mac OS X.

all-auto-lofs

Realiza una copia de seguridad de todos los dispositivos de bucle y sistemas de archivos locales gestionados por el montador automático. Este parámetro no recibe soporte en Mac OS X.

object

Especifica los objetos del dominio que se han de incluir en el dominio.

Un nombre de objeto debe incluirse entre comillas si el nombre contiene espacios.

-object

Especifica los objetos del dominio que se han de excluir del dominio.

Un nombre de objeto debe incluirse entre comillas si el nombre contiene espacios.

Ejemplos

Archivo de opciones:

Un archivo de opciones puede contener más de una sentencia domain. Sin embargo, todas las sentencias domain son un ejemplo de una sentencia única en un archivo de opciones.

```
domain all-local
domain all-local -/Volumes/volume2
domain all-local '-/Volumes/Macintosh HD'

domain /tst /datasave /joe
"domain all-local"
domain ALL-LOCAL -/home
domain ALL-NFS -/mount/nfs1
```

Una única sentencia de dominio puede listar uno o más objetos para el dominio. Puede utilizar más de una sentencia de dominio. Los dos ejemplos siguientes de dos archivos de opciones proporcionan los mismos resultados de dominio:

Ejemplo 1

```
...
domain fs1
domain all-local
domain -fs3
...
```

Ejemplo 2

```
...
domain all-local fs1 -fs3
...
```

Línea de mandatos:

```
-domain="/ /Volumes/volume2"
-domain="all-local -/Volumes/volume2"
-domain="/fs1 /fs2"
-domain=/tmp
-domain="ALL-LOCAL -/home"
```

Interacción de las definiciones de dominio

El dominio se puede definir en distintos orígenes y el resultado es una suma de todas las definiciones de dominio. Como ejemplo de la interacción de las definiciones de dominio, tenga en cuenta cómo las definiciones de dominio de distintos orígenes proporcionan distintos resultados de copia de seguridad. En la tabla, FS seguido por un número (por ejemplo, FS1) es un sistema de archivos. En esta tabla se muestran solo los mandatos especificados en la línea de mandatos. En el caso de mandatos planificados, la columna "línea de mandatos" no es pertinente y se deben considerar las opciones del mandato planificado.

Tabla 73. Interacción de definiciones de dominio de distintos orígenes

Archivo de opciones	Línea de mandatos	Conjunto de opciones de cliente	Objetos de los que se ha realizado copia de seguridad mediante el mandato incremental
domain FS1	incremental -domain=FS2	domain FS3	FS1 FS2 FS3
domain FS1	incremental	domain FS3	FS1 FS3
	incremental -domain=FS2		FS2
	incremental -domain=FS2	domain FS3	FS2 FS3

Tabla 73. Interacción de definiciones de dominio de distintos orígenes (continuación)

Archivo de opciones	Línea de mandatos	Conjunto de opciones de cliente	Objetos de los que se ha realizado copia de seguridad mediante el mandato incremental
	incremental	domain FS3	FS3
	incremental		all-local
domain all-local	incremental	domain FS3	all-local + FS3
domain all-local domain -FS1	incremental		all-local, pero no FS1
domain -FS1	incremental		ninguno
domain FS1 FS3	incremental	domain -FS3	FS1
domain all-local	incremental	domain -FS3	all-local, pero no FS3
	incremental FS1 -domain=all-local		FS1
	incremental FS1	domain all-local	FS1
domain -FS1	incremental FS1		FS1

Información relacionada

Para obtener información acerca de la definición de un punto de montaje virtual, consulte el tema “Virtualmountpoint” en la página 606.

para obtener información acerca de la especificación de uno o más sistemas de archivos montados automáticamente y añadidos al dominio, consulte “Automount” en la página 358.

Domain.image

La opción `domain.image` especifica lo que desea incluir en el dominio de cliente para una copia de seguridad de imágenes.

Si no especifica un sistema de archivos con el mandato **backup image** se realizará la copia de seguridad de los sistemas de archivos que especifique en la opción `domain.image`.

Cuando especifica un sistema de archivos con el mandato **backup image**, la opción `domain.image` se pasa por alto.

Si no utiliza la opción `domain.image` para especificar sistemas de archivos en el archivo de opciones del cliente y no especifica un sistema de archivos con el mandato **backup image**, se emitirá un mensaje y no se realizará ninguna copia de seguridad.

Clientes soportados

Esta opción es válida para AIX, Linux x86_64, Linux on POWER y Solaris. El servidor también puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

Esta opción es válida para todos los clientes Windows soportados. El servidor también puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor. Puede establecer esta opción en el recuadro **Copia de seguridad > Dominio para copia de seguridad** en el Editor de preferencias.

Sintaxis



Parámetros

domain

Define los sistemas de archivos o volúmenes lógicos RAW que deben incluirse en el dominio de imagen de cliente predeterminado.

Ejemplos

Archivo de opciones:

domain.image /fs1 /fs2

Línea de mandatos:

No se aplica.

Domain.nas

La opción `domain.nas` especifica los volúmenes que deben incluirse en las copias de seguridad de imagen de NAS.

Puede especificar `all-nas` para incluir todos los sistemas de archivos montados en el servidor de archivos NAS a excepción de los sistemas de archivos que excluya con la opción `exclude.fs.nas`.

El cliente de copia de seguridad y archivado utiliza su dominio para copia de seguridad de imágenes NAS cuando ejecuta un mandato **backup nas** y no especifica los volúmenes que deben procesarse.

Cuando utiliza esta opción en el archivo de opciones del sistema cliente (dsm.sys), la opción `domain.nas` define el dominio predeterminado para las copias de seguridad de imágenes NAS. Cuando realiza una copia de seguridad de imágenes del sistema de archivos NAS con el mandato **backup nas**, el cliente añadirá los volúmenes que se especifiquen en la línea de mandatos a los volúmenes definidos en el archivo dsm.sys. Por ejemplo, si especifica `domain.nas nas1/vol/vol0 nas1/vol/vol1` en el archivo dsm.sys y especifica `dsmc backup nas -nasnodename=nas1 /vol/vol2` en la línea de mandatos, el cliente realizará la copia de seguridad de los volúmenes `vol/vol0`, `vol/vol1` y `vol/vol2` en el nodo `nas1`.

Si establece la opción `domain.nas` en `all-nas` en el archivo dsm.opt, el cliente realizará la copia de seguridad de todos los volúmenes montados en el servidor de

archivos NAS. Cuando realiza una copia de seguridad, si utiliza una especificación de archivo y establece la opción `domain.nas` en `all-nas` en el archivo `dsm.sys`, `all-nas` tendrá prioridad.

Clientes soportados

Esta opción solo es válida para los clientes AIX y Solaris. El servidor también puede definir esta opción.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor.

Sintaxis



Parámetros

domain

Define los volúmenes que desea procesar. No es posible excluir volúmenes especificando el operador del guión (-).

all-nas

Procesa todos los volúmenes montados en el servidor de archivos NAS, excepto aquellos que se excluyan con la opción `exclude.fs.nas`. Éste es el valor predeterminado. Si no existe ninguna sentencia `domain.nas` en el archivo `dsm.opt` y no se ha especificado ningún volumen en la línea de mandatos, el cliente realizará la copia de seguridad de todos los volúmenes montados en el servidor NAS.

Ejemplos

Archivo de opciones:

```
domain.nas nas1/vol/vol0 nas1/vol/vol1
domain.nas all-nas
```

Línea de mandatos:

No se aplica.

Domain.vmfull

La opción `domain.vmfull` especifica las máquinas virtuales que se incluirán en sus operaciones de copia de seguridad de imagen de máquina virtual completa.



Las operaciones de máquina virtual solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments.

Para copias de seguridad de máquinas virtuales VMware, la opción `domain.vmfull` funciona con la opción `vmchost`. La opción `vmchost` identifica el servidor vCenter o ESX que contiene las máquinas virtuales que desea proteger. Los parámetros de

`domain.vmfull` se utilizan para centrarse en una operación en un subconjunto de máquinas virtuales que se ejecuten en el sistema identificado por `vmhost`.

Puede especificar qué máquinas virtuales se procesarán con alguna de las técnicas siguientes:

- Utilice la opción `VM=` y especifique el nombre de una máquina virtual.
- Proporcione una lista separada por comas de nombres de máquinas virtuales.
- Utilice la sintaxis de comodín para procesar las máquinas virtuales que coinciden con el patrón de nombre.
- Utilice uno de los siguientes parámetros de dominio-nivel:

```
all-vm
all-windows
schedule-tag
vmhost
vmfolder
vmhostcluster
vmdatastore
vmresourcepool
vmhostfolder
vmdatacenter
```

Al utilizar parámetros de dominio-nivel, las máquinas creadas en el dominio se incluyen automáticamente cuando se produce la siguiente copia de seguridad. Por ejemplo, si utiliza el parámetro `vmfolder` para realizar una copia de seguridad de todas las máquinas virtuales incluidos en una carpeta, las máquinas virtuales nuevas añadidas a dicha carpeta se incluirán en la siguiente copia de seguridad. Esto también se aplica a los nombres de patrón coincidente que se incluyen en una coincidencia comodín.

Las máquinas virtuales especificadas en la opción `domain.vmfull` se procesan sólo cuando el mandato **backup vm** se emite sin especificar una máquina virtual o una lista de máquinas virtuales en la línea de mandatos.

Clientes soportados

Esta opción puede utilizarse con clientes Linux x86_64 soportados.

El servidor también puede definir esta opción.

Archivo de opciones

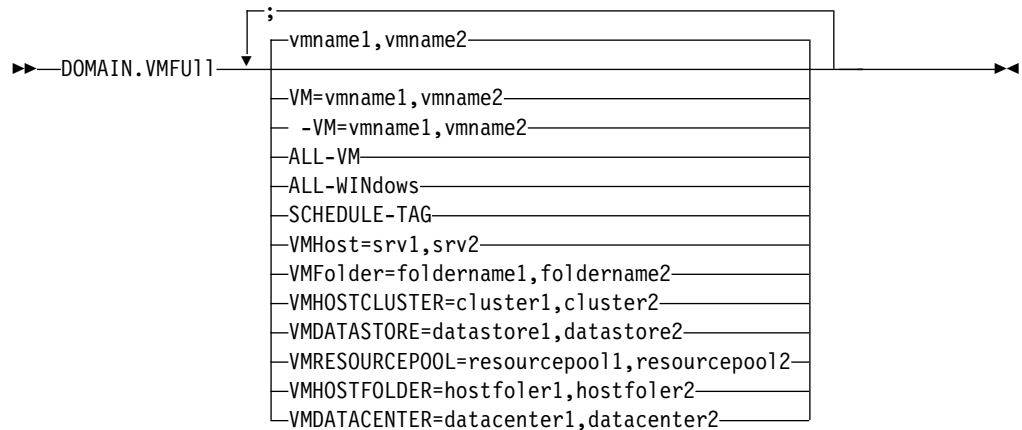
Establezca esta opción en las opciones del cliente, utilizando la línea de mandatos, o mediante el separador **Copia de seguridad de máquina virtual** del editor de preferencias.

Restricción: No se pueden establecer los siguientes parámetros en el Editor de preferencias. Incluya este valor en el archivo de opciones, o en la línea de mandatos al ejecutar un mandato **backup vm**:

```
nombre_máquina_virtual:vmrk=etiqueta_vmrk
schedule-tag
vmresourcepool
```

vmhostfolder
vmdatacenter

Sintaxis para máquinas virtuales VMware



Normas de sintaxis: Varias palabras clave deben estar separadas por punto y coma. No incluya espacios detrás de los signos de punto y coma. Si hay varios nombres de máquina virtual o dominio deben ir separados por comas, sin caracteres de espacio. Por ejemplo, consulte `vm=vmname`. La regla sobre varios nombres de dominio o máquina virtual no se aplica si se utiliza la palabra clave "Schedule-Tag".

Parámetros

vmname

Especifica el nombre de máquina virtual que se quiere procesar. El nombre es el de visualización de la máquina virtual. Puede especificar una lista de nombres de host de máquinas virtuales. Si lo hace, sepárelos con comas (`vm1,vm2,vm5`).

vm=vmname

La palabra clave `vm=` especifica que el siguiente conjunto de valores es una lista de nombres de máquina virtual. La palabra clave `vm=` es el valor predeterminado y no es obligatorio.

En este ejemplo, `vm=` no está especificado y las comas se utilizan para separar los nombres de máquina.

```
domain.vmfull my_vm1,my_vm2
```

Si especifica varias palabras clave, como por ejemplo, `vm=` y `vmfolder=`, los valores a los que hagan referencia deberán separarse por puntos y comas, sin caracteres de espacio:

```
domain.vmfull vm=my_vm1;vm=my_vm2  
domain.vmfull vm=my_vm1;vmfolder=folder1;vmfolder=folder2
```

Se pueden utilizar caracteres comodín para seleccionar nombres de máquina virtual que coincidan con un patrón. Un asterisco (*) coincide con cualquier secuencia de caracteres. El signo de interrogación (?) coincide con cualquier carácter único, por ejemplo:

- Excluir todos los archivos que tengan "test" en el nombre de host:
`-vm=*test*`

- Incluir todas las máquinas virtuales con nombres como: "test20", "test25", "test29", "test2A": vm=test2?

Puede excluir una máquina virtual de una operación de copia de seguridad especificando el operador `excluye (-)` antes de la palabra clave `vm=`. Por ejemplo, `-vm` se utiliza para excluir una máquina o varias máquinas determinadas, desde una copia de seguridad de nivel de dominio como, por ejemplo, `ALL-Windows`, `ALL-VM` y `VMFolder`. Si "vm1" es el nombre de una máquina virtual en una carpeta denominada "accountingDept", podrá realizar copia de seguridad de todas las máquinas virtuales de la carpeta pero impedir que se realice copia de seguridad de la máquina virtual "vm1". Establezca la siguiente opción:

```
domain.vmfull VMFolder=accountingDept;-vm=vm1
```

No podrá usar el operador `excluye (-)` para excluir un dominio como, por ejemplo, `ALL-VM`, `ALL-Windows` o `VMFolder`. El operador `excluye` funciona sólo en el nivel de nombre de máquina virtual.

nombre_máquina_virtual:vmdk=etiqueta_vmdk

La palabra clave `:vmdk=` se aplica únicamente a máquinas virtuales VMware y su uso requiere una licencia de IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Esta opción suele utilizarse para excluir discos (consulte la sintaxis `:-vmdk`) de realizar copia de seguridad. También puede incluir discos de máquina virtual mediante la utilización de la opción `INCLUDE.VMDISK` o excluir discos de máquina virtual mediante la utilización de la opción `EXCLUDE.VMDISK`.

Encontrará las instrucciones detalladas para excluir discos al realizar copias de seguridad de máquinas virtuales de VMware en la documentación de producto de IBM Spectrum Protect for Virtual Environments Data Protection for VMware en el IBM Knowledge Center, en <http://www.ibm.com/support/knowledgecenter/SSERB6>.

Los discos virtuales dentro de una máquina virtual tienen etiquetas de disco que identifican de forma exclusiva cada disco virtual. Utilice la palabra clave `:vmdk=` para especificar las etiquetas de los discos virtuales que desea incluir en la operación **Backup VM**. Si no especifica `:vmdk=` y una etiqueta de disco, se realizará una copia de seguridad de todos los discos virtuales en la máquina virtual.

Supongamos que hay una máquina virtual denominada "mi_ejemplo_de_máquina_virtual". Esta máquina virtual tiene cuatro discos (con la etiqueta `Hard Disk 1`, `Hard Disk 2`, `Hard Disk 3`, `Hard Disk 4`). Para incluir solo el disco duro 2 y el disco duro 3 en una copia de seguridad, añada la palabra clave `:vmdk=` y la etiqueta de disco para esos discos. Las comillas son necesarias alrededor de los parámetros porque las etiquetas de disco contienen caracteres de espacio. Por ejemplo:

```
domain.vmfull "my_vm_example:vmdk=Hard Disk 2:vmdk=Hard Disk 3"
```

El ejemplo siguiente realiza una copia de seguridad del disco duro 1 y el disco duro 2 en VM1, y del disco duro 3 y el disco duro 4 en VM2. Se utiliza una coma para separar la información de la máquina virtual.

```
domain.vmfull "vm1:vmdk=Hard Disk 1:vmdk=Hard Disk 2",
               "vm2:vmdk=Hard Disk 3:vmdk=Hard Disk 4"
```

Al igual que con la palabra clave `-vm=`, también puede usar el operador de exclusión `(-)` con `:vmdk=` para excluir discos de una operación de copia de seguridad.

Para realizar una copia de seguridad de una máquina virtual (vm1) y excluir los discos 3 y 4, utilice la sintaxis siguiente:

```
domain.vmfull "vm1:-vmdk=Hard Disk 3:-vmdk=Hard Disk 4"
```

Para realizar una copia de seguridad dos máquinas virtuales, vm1 y vm2, y excluir a los dos primeros discos en cada máquina, utilice la sintaxis siguiente:

```
domain.vmfull "vm1 :-vmdk=Hard Disk 1:-vmdk=Hard Disk 2",  
"vm2:-vmdk=Hard Disk 1:-vmdk=Hard Disk 2"
```

Puede incluir uno o más discos en una sentencia `domain.vmfull`. Puede excluir uno o más discos en una sentencia `domain.vmfull`. Puede combinar discos de inclusión y exclusión en la misma sentencia. Por ejemplo, la siguiente sentencia es válida:

```
domain.vmfull  
"vm1:vmdk=Hard Disk 1:-vmdk=Hard Disk 2:vmdk=Hard Disk 3:vmdk:Hard Disk 4"
```

Si está presente una sentencia de inclusión, el resto de los discos de la máquina virtual se excluyen de una operación de copia de seguridad, a menos que el resto de los discos también se especifiquen en una sentencia de inclusión. Por ejemplo, la sentencia siguiente excluye todos los discos duros en vm1, excepto para el disco duro 1:

```
domain.vmfull "vm1:vmdk=Hard Disk 1"
```

Los dos siguientes excluyen el disco duro 4 de una copia de seguridad de vm1:

```
domain.vmfull "vm1:vmdk=Hard Disk 1:vmdk=Hard Disk 2:vmdk=Hard Disk 3"  
domain.vmfull "vm1:-vmdk=Hard Disk 4"
```

all-vm

Para máquinas virtuales VMware. Esta opción procesa todas las máquinas virtuales definidas para el Virtual Center o el servidor ESX especificadas en la opción `vmchost`.

all-windows

Para máquinas virtuales VMware. Esta opción procesa todas las máquinas virtuales definidas para el Virtual Center o el servidor ESX especificadas en la opción `vmchost`. Las máquinas virtuales también deben tener un tipo de sistema operativo invitado de Windows.

schedule-tag

Para copias de seguridad planificadas de máquinas virtuales VMware. Esta opción procesa todas las máquinas virtuales definidas para el servidor de Virtual Center especificado en la opción `vmchost`.

El administrador del servidor de IBM Spectrum Protect puede añadir esta opción a una definición de planificación para indicar que la planificación es compatible con el código y la categoría `Schedule` (IBM Spectrum Protect). La copia de seguridad de las máquinas virtuales en objetos de VMware a las que se haya asignado el código `Schedule` se ejecutará siguiendo la planificación.

Requisito: Para posibilitar la compatibilidad con los códigos, la opción `-domain.vmfull` no puede contener ningún parámetro adicional a nivel de dominio, aparte del parámetro `Schedule-Tag` de la definición de planificación. En caso contrario, se omite el código `Schedule` (IBM Spectrum Protect). La opción no distingue entre mayúsculas y minúsculas y no puede contener espacios. El entrecomillado del parámetro `Schedule-Tag` es opcional. No se efectúan copias de seguridad de las máquinas virtuales en contenedores de VMware que se han codificado con planificaciones incompatibles.

Para obtener más información sobre el código `Schedule`, consulte el apartado “Códigos de protección de datos admitidos” en la página 793.

vmhost=hostname

Para máquinas virtuales VMware. Esta opción procesa todas las máquinas virtuales definidas para el Virtual Center o el servidor ESX especificadas en la opción vmhost. El nombre de host que especifique debe coincidir con el nombre completo de host o dirección IP, ya que se especifica en la vista Hosts y clústeres del servidor vCenter.

Todos las máquinas virtuales que se añaden a este host se incluyen automáticamente en el proceso de copia de seguridad y de restauración. Para hacer una inclusión, las máquinas virtuales también deben estar ejecutándose en el servidor ESX especificado por el nombre de host; no se pueden desconectar.

Este parámetro puede incluir varios servidores ESX que están separados por comas. Cuando el Centro virtual contiene varios servidores ESX, esta opción no determina el servidor ESX a partir del que se toma una instantánea. El servidor ESX a partir del cual se toma una instantánea está determinado por el servicio Web de VMware VirtualCenter.

Cuando se conecta directamente a un host ESX o ESXi, la opción vmhost solo se aplica si el **vmhost** es el servidor al que se conecta. De no serlo, se emite un mensaje de advertencia en la consola y este se registra en el archivo dsmerror.log; también se registrará como mensaje de suceso del servidor.

Si la opción vmenabletemplatebackups se establece en yes y las plantillas de VM son parte del dominio, están incluidos en la copia de seguridad.

Restricción: No se puede realizar copia de seguridad de las plantillas de VMware para máquinas virtuales cuando están en un host ESX o ESXi porque los hosts ESX y ESXi no soportan plantillas.

vmfolder=foldername

Para máquinas virtuales VMware. Esta opción procesa todas las máquinas virtuales definidas para el Virtual Center o el servidor ESX especificadas en la opción vmhost. Las máquinas virtuales también deben existir en la carpeta VMware especificada por el nombre de la carpeta. El nombre de carpeta puede incluir varias carpetas de VMware que estén separadas por comas.

vmhostcluster=hostclustername

Para máquinas virtuales VMware. Esta opción procesa todas las máquinas virtuales definidas para el Virtual Center o el servidor ESX especificadas en la opción vmhost. Las máquinas virtuales también deben estar ejecutándose en el servidor ESX especificado por el nombre de clúster del host. Para incluir más de un nombre de clúster de host, separe los nombres de clúster con comas: VMHOSTCLUSTER=cluster1,cluster2.

Si la opción vmenabletemplatebackups se establece en yes y las plantillas de VM son parte del dominio, están incluidos en la copia de seguridad. Un clúster del host de VMware no está disponible si se conecta directamente a un host ESX o ESXi. Si se conecta directamente a un host ESXi/ESX y se procesa un dominio que incluye un clúster de host, se emite un mensaje de nivel de aviso en la consola y dicho mensaje se registra en el archivo dsmerror.log; también se registra como un mensaje de suceso de servidor.

vmdatastore=datastorename

Para máquinas virtuales VMware. Esta opción procesa todas las máquinas virtuales definidas para el Virtual Center o el servidor ESX especificadas en la opción vmhost. La ubicación del almacén de datos configurado de una máquina virtual debe coincidir con el nombre del almacén de datos

especificado por *datastorename*. El nombre de almacén de datos puede incluir varios almacenes de datos separados por comas:
VMDATASTORE=datastore1,datastore2

Las máquinas virtuales pueden tener su disco (archivos vmdk) en más de un almacén de datos; pero sólo existe una ubicación de almacén de datos predeterminada. Esta ubicación de almacén de datos predeterminada está definida en la configuración de máquina virtual y es siempre la ubicación del archivo de configuración de máquina virtual (archivo .vmx). Cuando una máquina se selecciona para la copia de seguridad utilizando una palabra clave de dominio, el archivo de configuración de máquina virtual, y todos los discos de la máquina virtual se incluyen en la copia de seguridad, también los discos que estén en un almacén de datos diferente al especificado como el dominio.

vmresourcepool=resourcepoolname

Para máquinas virtuales VMware. Esta opción procesa todas las máquinas virtuales definidas para el servidor de Virtual Center especificado en la opción vmhost. Las máquinas virtuales también deben existir en la agrupación de recursos de VMware especificada por el nombre de la agrupación de recursos. El nombre de la agrupación de recursos puede incluir varias agrupaciones de recursos separadas por comas, por ejemplo:
VMRESOURCEPOOL=resourcepool1,resourcepool2

vmhostfolder=hostfoldername

Para máquinas virtuales VMware. Esta opción procesa todas las máquinas virtuales definidas para el servidor de Virtual Center especificado en la opción vmhost. Las máquinas virtuales también deben existir en la carpeta de host de VMware que especifica el nombre de la carpeta de host. El nombre de carpeta de host puede incluir varias carpetas de host de VMware separadas con comas, por ejemplo: VMHOSTFOLDER=hostfolder1,hostfolder2

vmdatacenter=datacentername

Para máquinas virtuales VMware. Esta opción procesa todas las máquinas virtuales definidas para el servidor de Virtual Center especificado en la opción vmhost. Las máquinas virtuales también deben existir en el centro de datos de VMware especificado por el nombre del centro de datos. El nombre del centro de datos puede incluir varios centros de datos separados con comas, por ejemplo: VMDATACENTER=datacenter1,datacenter2

Consejo: Si especifica más de un tipo de contenedor, por ejemplo, vmfolder=folder1 y vmhostcluster=cluster2, se protegerán todas las máquinas virtuales que estén contenidas en folder1 y cluster2. Las máquinas virtuales no tienen que estar ubicadas tanto en folder1 como en cluster2.

Puede especificar las máquinas virtuales como se muestra en este ejemplo:
domain.vmfull=vmfolder=folder1;vmhostcluster=cluster2

Ejemplos

Archivo de opciones:

Incluir todas las máquinas virtuales en operaciones de copia de seguridad de máquina virtual completa.

```
domain.vmfull all-vm
```

Incluir todas las máquinas virtuales en operaciones de copia de seguridad de máquina virtual completa, excepto las que tengan el sufijo _test en el nombre.

```
domain.vmfull all-vm;-vm=*_test
```

Incluir todas las máquinas virtuales que tengan Windows como sistema operativo en operaciones de copia de seguridad de máquina virtual completa.

```
domain.vmfull all-windows
```

Incluir todas las máquinas virtuales en servidores de clúster 1, 2 y 3 en operaciones de copia de seguridad de máquina virtual completa.

```
domain.vmfull vmhostcluster=cluster1,cluster2,cluster3
```

Incluir todos los datos de máquina virtual en datastore1 en operaciones de copia de seguridad de máquina virtual completa.

```
domain.vmfull vmdatastore=datastore1
```

Incluir todas las máquinas virtuales en operaciones de copia de seguridad de máquina virtual completa, pero excluir las máquinas virtuales testvm1 y testvm2.

```
domain.vmfull all-vm;-VM=testvm1,testvm2
```

Incluir las máquinas virtuales que se definen en las carpetas de máquina virtual que se denominan lab1 y lab2 en operaciones de copia de seguridad de máquina virtual completa.

```
domain.vmfull vmfolder=lab1,lab2
```

Incluir todas las máquinas virtuales en los hosts ESX denominados “brovar”, “doomzoo”, y “kepler” en operaciones de copia de seguridad de máquina virtual completa.

```
domain.vmfull vmhost=brovar.example.com,  
doomzoo.example.com,kepler.example.com
```

Incluir las máquinas virtuales de las agrupaciones de recursos de VMware resourcepool_A y resourcepool_B en operaciones de copia de seguridad de máquina virtual completa.

```
domain.vmfull vmresourcepool=resourcepool_A,resourcepool_B
```

Incluir las máquinas virtuales que están definidas en las carpetas de host de VMware denominadas hostfolder1 y hostfolder2 en operaciones de copia de seguridad de máquina virtual completa.

```
domain.vmfull vmhostfolder=hostfolder1,hostfolder2
```

Incluir todas las máquinas virtuales del centro de datos de VMware dc1 en operaciones de copias de seguridad de máquina virtual completa.

```
domain.vmfull vmdatacenter=dc1
```

Referencia relacionada:

“Exclude.vmdisk” en la página 430

“Include.vmdisk” en la página 467

“Códigos de protección de datos admitidos” en la página 793

Dontload

Los clientes Linux x86_64 pueden utilizar la opción dontload para evitar que se carguen las bibliotecas de plug-in específicas cuando se inicia el cliente de copia de seguridad-archivado.

El paquete TIVsm_BAhdw.x86_64 incluido en distribuciones Linux x86_64 contiene software necesario para dar soporte a las copias de seguridad incrementales de instantáneas para servidores de archivos NetAPP y N-Series. Si este paquete está instalado en un sistema Linux x86_64 que se utiliza para ejecutar operaciones de transportador de datos para una máquina virtual, los archivos de este paquete

hacen que fallen todas las operaciones de seguridad de VMware. Cuando se producen estos errores, aparece el siguiente mensaje:

ANS8811E

No pueden ejecutarse operaciones VMware cuando el producto de plug-in de hardware TIVsm-BAhbw está instalado y cargado. Desinstale el producto de hardware TIVsm-BAhbw o establezca la opción DONTLOAD PIHDW en el archivo de opciones para evitar que se cargue el plug-in de hardware.

Utilice esta opción para evitar que la biblioteca de plugins se cargue en la RAM cuando se inicie el cliente. Como alternativa, puede desinstalar el paquete TIVsm_BAhbw si no es necesario para operaciones de instantánea.

Clientes soportados

Esta opción sólo es válida para clientes de Linux x86_64.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor.

Sintaxis

►►—DONTLoad—PIHDW—◄◄

Parámetros

PIHDW

Especifica que el plug-in de hardware (TIVsm-BAhbw) no está cargado en la RAM cuando se inicia el cliente. Utilice esta opción en clientes de copia de seguridad-archivado que tengan el plug-in de hardware instalado para evitar que el plug-in provoque anomalías al realizar operaciones de copia de seguridad-archivado en máquinas virtuales de VMware. No existe un valor predeterminado para la opción dontload.

Para determinar si está instalado el plug-in, escriba el siguiente mandato y examine el resultado.

```
rpm -q -a | grep TIV
```

Si el resultado contiene un paquete que empieza por “TIVsm-BAhbw” (seguido por una serie de versión), el paquete de plug-in de hardware está instalado.

Ejemplos

Archivo de opciones:

DONTLoad PIHDW

Línea de mandatos:

No se aplica. No utilice esta opción en la línea de mandatos.

Referencia relacionada:

“Backup VM” en la página 683

“Restore VM” en la página 764

Dynamicimage

Utilice la opción `dynamicimage` con el mandato **backup image** o la opción `include.image` para especificar que desea realizar una copia de seguridad de imagen dinámica.

Clientes soportados

Esta opción es válida para los clientes AIX, Solaris y todos los de Linux. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Establezca la sentencia `include.image` que contiene el valor `dynamicimage` en la sección del servidor en el archivo de opciones del sistema, `dsm.sys`. También puede establecer esta opción mediante el editor de preferencias.

Sintaxis

►►—DYNAMICImage— *value* —————►►

Parámetros

value

Especifique uno de los valores siguientes:

- si** Utilice esta opción sólo si el volumen no puede desmontarse y volverse a montar en modo de sólo lectura. El cliente realiza una copia de seguridad del volumen tal cual, sin volver a montarlo en modalidad de sólo lectura. La copia de seguridad se puede dañar si las aplicaciones escriben datos en el volumen mientras se está realizando la copia de seguridad. En tal caso, ejecute `fsck` después de una restauración y monte manualmente el sistema de archivos para volver a obtener acceso al volumen. Esta opción es válida para los clientes AIX, Solaris y todos los de Linux.

Nota: Esta opción es válida para los sistemas de archivos JFS2 de AIX.

- no** Utilice esta opción si no desea realizar una copia de seguridad de imagen dinámica. Éste es el valor predeterminado. El comportamiento predeterminado depende del tipo del sistema de archivos y la plataforma. En el caso de plataformas y sistemas de archivos que admitan instantáneas, es decir los sistemas de archivos JFS2 de AIX y los sistemas de archivos LVM de LINUX, el valor predeterminado es la copia de seguridad basada en instantánea. Para las demás plataformas y los demás sistemas de archivos UNIX, el valor predeterminado es la copia de seguridad de imágenes estática.

Ejemplos

Archivo de opciones:

```
include.image /kalafs1 dynamicimage=yes
```

Línea de mandatos en la imagen de copia de seguridad:

```
dynamicimage=yes
```

Efsdecrypt

La opción `efsdecrypt` permite controlar si los archivos cifrados mediante un sistema de archivos cifrados (EFS) de AIX se leen con formato cifrado o descifrado.

El valor predeterminado de la opción `efsdecrypt` es `no`, lo cual significa que se ha de hacer la copia de seguridad de los datos cifrados o RAW. Si especifica `yes`, se hace copia de seguridad de los archivos como texto legible, lo que significa que se hace la copia de seguridad como archivos normales, como si los archivos existieran en formato no cifrado en el sistema de archivos.

Importante: siempre que ejecute una copia de seguridad que incluya archivos cifrados en un EFS, debe asegurarse de que utiliza la especificación correcta de la opción `efsdecrypt`. Si el valor de la opción `efsdecrypt` cambia entre las dos copias de seguridad incrementales, se volverá a realizar una copia de seguridad de todos los archivos cifrados de los sistemas de archivos EFS, incluso si no se han modificado desde la última copia de seguridad. Por ejemplo, si ejecuta una copia de seguridad incremental de archivos cifrados de los que anteriormente había hecho una copia de seguridad como "raw", debe asegurarse de que `efsdecrypt` se ha especificado como `no`. Si cambia el valor de `efsdecrypt` a `yes`, se volverá a realizar una copia de seguridad de todos los archivos en texto legible incluso si no se han modificado, así que asegúrese de utilizar esta opción cuidadosamente.

Nota: Ésta es una opción global que se aplica a toda la copia de seguridad. Se exigen dos invocaciones independientes del cliente para hacer copia de seguridad de los archivos cifrados como datos raw y de los otros como texto legible.

Clientes soportados

Esta opción es válida para los clientes AIX.

Archivo de opciones

Establezca esta opción en el archivo `dsm.sys` o el archivo de opciones del usuario cliente (`dsm.opt`). En el archivo `dsm.sys`, debe colocar esta opción dentro de una stanza de servidor.

Sintaxis



Parámetros

No Los archivos cifrados se leen con formato de datos cifrado o raw y se desactiva la compresión y el cifrado de IBM Spectrum Protect. Éste es el valor predeterminado.

Yes

Los archivos cifrados se leen con formato descifrado o texto legible.

Ejemplos

Archivo de opciones:

`EFSDecrypt yes`

Línea de mandatos:

`-EFSDecrypt=no`

Enablearchiveretentionprotection

La opción `enablearchiveretentionprotection` permite al cliente conectarse al servidor de IBM Spectrum Protect for Data Retention. Esto garantiza que los objetos de archivado no se eliminarán del servidor mientras no se cumplan los requisitos de retención basados en políticas de dicho objeto.

Esta opción se ignora si el cliente conecta con un servidor que no está activado para protección de retención. Si la opción es `no` (valor predeterminado) y se realiza un intento de conexión con un servidor de retención de datos, la conexión se rechazará.

El servidor de retención de datos está especialmente configurado para esta tarea, por lo tanto el servidor rechaza el proceso de copia de seguridad o restauración normal. Cuando el cliente conecta con un servidor de retención de datos, los mandatos siguientes no estarán disponibles. Si intenta utilizar estos mandatos, se mostrará un mensaje que indicará que no son válidos con este servidor.

- **incremental**
- **backup** (todos los submandatos)
- **selective**
- **restore** (todos los submandatos excepto **restore backupset -location=file** o **-location=tape**)

Nota: **restore backupset -location=file** o **-location=tape** no conecta con ningún servidor (excepto el virtual) y, por lo tanto, no se bloqueará en ninguna circunstancia.

- **restart restore**
- **delete backup**
- **delete group**
- **expire**
- Todos los mandatos *query*, *excepto*:
 - **query access**
 - **query archive**
 - **query filespace**
 - **query inclexcl**
 - **query managementclass**
 - **query node**
 - **query options**
 - **query schedule**
 - **query session**
 - **query systeminfo**
 - **query tracestatus**

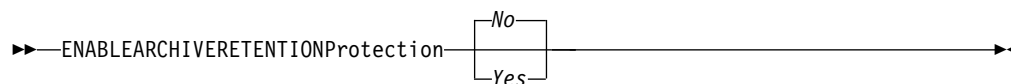
Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Esta opción sólo es válida en el archivo `dsm.sys`, *dentro* de una sección de servidor, y no es válida en un conjunto de opciones del cliente del servidor. No es válida en ninguna línea de mandatos.

Sintaxis



Parámetros

No Se rechaza el servidor de retención de datos. Éste es el valor predeterminado.

Yes

El cliente conecta con un servidor de retención de datos.

Enablededupcache

Utilice la opción `enablededupcache` para especificar si desea utilizar una memoria caché durante la eliminación de duplicados de datos por parte del cliente. El uso de una memoria caché local puede reducir el tráfico de red entre el servidor y el cliente de IBM Spectrum Protect.

Si realiza una copia de seguridad o archivado con la memoria caché de eliminación de duplicados de datos habilitada, la especificación de las extensiones de datos de las que se ha realizado una copia de seguridad o archivado se guarda en la base de datos de la memoria caché. La próxima vez que ejecute una copia de seguridad o archivado, el cliente consultará la memoria caché de la eliminación de duplicados de datos e identificará las extensiones de datos que se han guardado previamente en el servidor. Las extensiones de datos que sean idénticas a las extensiones de datos del servidor no se vuelven a enviar al servidor.

Si el servidor y la memoria caché no están sincronizados, la memoria caché se elimina y se crea una nueva.

Sólo un proceso puede acceder a la memoria caché de la eliminación de duplicados de datos distribuida a la vez. Instancias de copia de seguridad simultáneas en una estación de trabajo, que utiliza el mismo servidor y la misma agrupación de almacenamiento, deben utilizar nombres de nodo únicos o especificaciones de caché únicas. De esta forma, se puede utilizar todas las instancias en una caché local y optimizar la eliminación de duplicados de datos por parte del cliente.

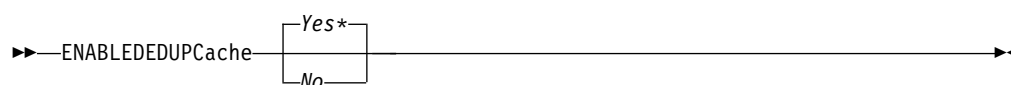
Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect también soporta esta opción.

Archivo de opciones

Especifique esta opción en el archivo de opciones del cliente (`dsm.sys`) de una stanza de servidor. Puede establecer esta opción en la casilla de verificación **Eliminación de duplicados > Habilitar memoria caché para eliminación de duplicados** del editor Preferencias. La opción se puede establecer en el conjunto de opciones de cliente del servidor de IBM Spectrum Protect.

Sintaxis



Parámetros

Yes

Especifica que desea habilitar la memoria caché de eliminación de duplicados de datos. Si no está habilitada la eliminación de duplicados de datos, este valor no es válido. Yes es el valor predeterminado para el cliente de copia de seguridad y archivado. No es el valor predeterminado para la API de IBM Spectrum Protect.

No Especifica que no desea habilitar la memoria caché de eliminación de duplicados de datos.

Ejemplos

Archivo de opciones:

enablededupcache no

Línea de mandatos:

-enablededupcache=no

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Referencia relacionada:

“Eliminación de duplicados” en la página 381

“Dedupcachepath” en la página 380

“Dedupcachesize” en la página 381

Enableinstrumentation

De forma predeterminada, el cliente de copia de seguridad y archivado y la API de IBM Spectrum Protect recopilan automáticamente datos de instrumentación para identificar los cuellos de botella de rendimiento durante el proceso de copia de seguridad y restauración. Para inhabilitar o habilitar más tarde la instrumentación, utilice la opción `enableinstrumentation`.

Con esta opción habilitada, no tiene que esperar que representante de atención al cliente se dirija a usted para que recopile datos de rendimiento cuando se produzca un problema. En su lugar, se pueden recopilar datos cada vez que se ejecute una operación de copia de seguridad o restauración. Esta característica pueden ser útil porque no tiene que reproducir el problema para recopilar datos de rendimiento. El cliente ya recopila dicha información.

Esta opción sustituye las opciones `-TESTFLAG=instrument:detail`, `-TESTFLAG=instrument:API` y `-TESTFLAG=instrument:detail/API` utilizadas en las versiones anteriores del cliente y de la API.

Para cada proceso, se recopilan los siguientes tipos de datos de instrumentación de rendimiento:

- Los nombres de actividad de cada hebra (por ejemplo, File I/O, Data Verb, Compression y Transaction), el tiempo medio transcurrido por actividad y la frecuencia de la actividad.
- El tiempo total de actividad correspondiente a cada hebra.
- El mandato que se ha emitido y las opciones que se han utilizado.
- El resumen del mandato de copia de seguridad, restauración o consulta.

De forma predeterminada, los datos de rendimiento se almacenan en el archivo de registro de instrumentación (`dsminstr.log`) en el directorio que se especifica mediante la variable de entorno `DSM_LOG` (o la variable de entorno `DSMI_LOG` para los productos que dependen de la API como IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server y IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server). Si no ha establecido la variable de entorno `DSM_LOG`, el archivo de registro de instrumentación se almacena en el directorio actual (el directorio en el que se ha emitido el mandato **dsmc**).

Si lo desea, puede cambiar el nombre y la ubicación del archivo de registro de instrumentación mediante la opción `instrlogname`. También puede controlar el tamaño del archivo de registro especificando la opción `instrlogmax`.

No se recopilan datos de rendimiento para la GUI de cliente de copia de seguridad y archivado ni para la GUI de cliente web.

Se recopilan datos de rendimiento para cada uno de los siguientes productos cuando se especifica la opción `enableinstrumentation` en el archivo de opciones del cliente:

- Operaciones de copia de seguridad planificadas a nivel de archivo con el cliente de archivado y copia de seguridad
- Copias de seguridad de IBM Spectrum Protect for Virtual Environments: Data Protection for VMware
- Copias de seguridad de IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V
- Copias de seguridad de IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server
- Copias de seguridad de IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server

También se recopilan datos de rendimiento durante el proceso de archivado y recuperación.

Clientes soportados

Esta opción es válida para todos los clientes y la API de IBM Spectrum Protect.

Archivo de opciones

Coloque esta opción en el archivo de opciones del cliente (`dsm.sys`) de una stanza de servidor. La opción se puede establecer en el conjunto de opciones de cliente del servidor de IBM Spectrum Protect.

Consejo: Esta opción está habilitada de forma predeterminada, de forma que, generalmente, no es necesario que coloque esta opción en el archivo de opciones del cliente, a no ser que tenga que inhabilitar la opción.

Sintaxis



Parámetros

Yes

Especifica que desea recopilar datos de rendimiento durante las operaciones de copia de seguridad y restauración. El valor predeterminado es Yes, lo que significa que se recopilan datos de rendimiento incluso si no especifica esta opción.

De forma predeterminada, los datos de rendimiento se almacenan en el archivo de registro de instrumentación (`dsminstr.log`) en el directorio que se especifica mediante la variable de entorno `DSM_LOG`. Si no ha establecido la variable de entorno `DSM_LOG`, el archivo de registro de instrumentación se almacena en el directorio actual (el directorio en el que se ha emitido el mandato **dsmc**). Si el archivo no existe, el cliente lo crea y agrega al mismo datos de rendimiento.

No Especifica que no desea recopilar datos de rendimiento durante las operaciones de copia de seguridad y restauración. Si el registro de instrumentación ya existe, no se agregan más datos al archivo.

Ejemplos

Archivo de opciones:

```
enableinstrumentation yes
```

Línea de mandatos:

```
dsmc sel /home/mydir/* -subdir=yes -enableinstrumentation=yes
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Tareas relacionadas:

➡ Recopilación de datos de instrumentación del cliente

➡ Recopilación de datos de instrumentación de la API

Referencia relacionada:

“Instrlogmax” en la página 476

“Instrlogname” en la página 477

Enablelanfree

La opción `enablelanfree` especifica si debe activarse una vía de acceso disponible sin LAN a un dispositivo de almacenamiento conectado a una red de área de almacenamiento (SAN).

Una vía de acceso sin LAN permite realizar copias de seguridad, restaurar, archivar y recuperar procesos entre el cliente de copia de seguridad y archivado y el dispositivo de almacenamiento conectado a la SAN.

Para admitir el movimiento de datos sin LAN, debe instalar y configurar el IBM Spectrum Protect para el agente de almacenamiento SAN en la estación de trabajo de cliente.

Nota:

1. Si especifica la opción `enablelanfree` en el archivo de opciones del cliente (`dsm.opt`), pero se transfirieron cero (0) bytes a través de la SAN durante la operación, no olvide vincular los datos a una clase de gestión que sea sin LAN.
2. Para restaurar los conjuntos de copias de seguridad en un entorno SAN, consulte “**Restore Backupset**” en la página 749 para obtener información.

3. Cuando una ruta fuera de la LAN está habilitada, los valores SAN Storage Agent sustituyen las opciones del cliente `tcpserveraddress`, `tcpport` y `ssl`. Esta acción de sustitución se produce para garantizar que tanto el cliente como el agente de almacenamiento utilizan las opciones de comunicación del mismo servidor.

Clientes soportados

Esta opción solo es válida para clientes de AIX, Linux x86_64, Linux on POWER y Oracle Solaris.

Archivo de opciones

Establezca esta opción en el archivo `dsm.sys` dentro de una sección de servidor. También puede establecer esta opción seleccionando el recuadro de selección **Habilitar fuera de la LAN** en el separador **General** del Editor de preferencias.

Sintaxis



Parámetros

Yes

Especifica que se desea activar una vía de acceso disponible fuera de la LAN a un dispositivo de almacenamiento conectado a una SAN.

No

Especifica que no se desea activar una vía de acceso disponible fuera de la LAN a un dispositivo de almacenamiento conectado a una SAN. Éste es el valor predeterminado.

Ejemplos

Archivo de opciones:

`enablelanfree yes`

Línea de mandatos:

`-enablelanfree=yes`

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Información relacionada

Para especificar un protocolo de comunicaciones entre el cliente de copia de seguridad y archivado y el agente de almacenamiento, consulte “`Lanfreecommmethod`” en la página 478.

Encryptiontype

Utilice la opción `encryptiontype` para especificar el algoritmo para el cifrado de datos.

La opción `encryptiontype` sólo afecta las operaciones de archivado y copia de seguridad. Los datos que incluya se almacenarán en formato cifrado, y el cifrado no afectará a la cantidad de datos enviados o recibidos. Durante las operaciones de

restauración y recuperación, los datos cifrados se descifrarán utilizando el algoritmo de cifrado correcto independientemente del valor de esta opción.

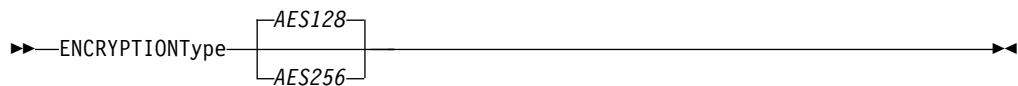
Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor. También puede establecer esta opción en la ficha **Authorization** del editor de preferencias.. El servidor puede modificar esto.

Sintaxis



Parámetros

AES128

Cifrado de datos AES de 128 bits. El valor predeterminado es AES de 128 bits.

AES256

Cifrado de datos AES de 256 bits. El cifrado de datos AES de 256 bits proporciona el nivel más alto de cifrado de datos disponible en operaciones de copia de seguridad y archivado.

Ejemplos

Archivo de opciones:

```
encryptiontype aes128
```

Línea de mandatos:

No se aplica.

Encryptkey

El cliente de copia de seguridad y archivado admite la opción que permite cifrar los archivos cuya copia de seguridad o archivado se realiza en el servidor de IBM Spectrum Protect. Esta opción se activa con la opción `include.encrypt`.

Todos los archivos que coinciden con el patrón de la especificación `include.encrypt` se cifrarán antes de que los datos se envíen al servidor. Hay tres opciones para gestionar la clave utilizada para cifrar los archivos (solicitar, guardar y generar). Las tres opciones pueden utilizarse con el cliente de copia de seguridad/archivado o con la API de IBM Spectrum Protect.

La contraseña de clave de cifrado distingue entre mayúsculas y minúsculas y puede tener un máximo de 64 caracteres de longitud e incluir los caracteres siguientes:

- A-Z** Cualquier letra, de A hasta Z, mayúsculas o minúsculas. No puede especificarlos caracteres de idioma nacional.
- 0-9** Cualquier número, del 0 al 9
- +** Signo más
- .** Punto
- Subrayado

- Guión
- & Símbolo &

Nota:

1. La API dispone de un modo alternativo de especificar `encryptkey=generate`; la opción `enableclientencryptkey=yes` anterior también puede especificarse para solicitar el proceso de generación de cifrado.
2. La opción de la API `enableclientencryptkey=yes` sigue recibiendo soporte, por lo tanto, es una opción posible cuando la API se utiliza para especificar dos opciones en conflicto. Por ejemplo, `enableclientencryptkey=yes` y `encryptkey=prompt` o `encryptkey=save`.
3. Cuando se especifican los valores en conflicto, la API devolverá un mensaje de error.

Atención: Si se utiliza la opción `prompt`, la clave de cifrado no se guarda en el archivo de contraseñas de IBM Spectrum Protect en UNIX. Si olvida la clave, no se podrán recuperar los datos.

Clientes soportados

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. Puede establecer esta opción en la ficha **Autorización**, en la sección **Contraseña de clave de cifrado** del Editor de preferencias.

Sintaxis



Parámetros

save

La contraseña de clave de cifrado se guarda en el archivo de contraseña del cliente de copia de seguridad y archivado. Se emite una solicitud para una contraseña de clave de cifrado inicial y después de la solicitud inicial, la contraseña de clave de cifrado guardada en el archivo de contraseña se usa para las copias de seguridad y el archivado de los archivos que coinciden con la especificación de `include.encrypt`. La clave se recupera desde el archivo de contraseña en las operaciones de restauración y recuperación.

La contraseña puede tener una longitud máxima de 64 bytes.

Cuando se especifica la opción `save` para una aplicación de la API, la contraseña de clave inicial debe proporcionarla la aplicación mediante la utilización de la API en la llamada de función `dsmInitEx`. La API no emite una solicitud para el usuario sino que se basa en la aplicación para solicitar al usuario cuando sea necesario.

Este parámetro es el predeterminado.

Nota: Deben tenerse en cuenta las restricciones siguientes:

- Esta opción sólo se puede usar si también se especifica `passwordaccess generate`.
- El usuario `root` o un usuario autorizado debe especificar la contraseña de clave de cifrado inicial.

prompt

La gestión de la contraseña de clave de cifrado la proporciona el usuario. Al usuario se le solicita la contraseña de clave de cifrado cuando el cliente inicia una operación de copia de seguridad o de archivado. Se emite una solicitud para la misma contraseña cuando se restaura o se recupera el archivo cifrado.

Esta contraseña puede tener una longitud máxima de 64 bytes.

Cuando se especifica la opción `prompt` para una aplicación de la API, la contraseña de clave debe proporcionarla la aplicación mediante la utilización de la API en la llamada de función `dsmInitEx`. La API no emite una solicitud para el usuario sino que se basa en la aplicación para solicitar al usuario cuando sea necesario.

generate

Una contraseña de clave de cifrado se genera dinámicamente cuando el cliente inicia una operación de copia de seguridad o de archivado. Esta clave generada se utiliza para las copias de seguridad de archivos que coinciden con la especificación `include.encrypt`. La contraseña de clave generada, en formato cifrado, se conserva en el servidor de IBM Spectrum Protect. La contraseña de clave se devuelve al cliente para que el archivo pueda descifrarse en las operaciones de restauración y de recuperación.

Ejemplos

Archivo de opciones:

`encryptkey prompt`

Línea de mandatos:

No se aplica.

Errorlogmax

La opción `errorlogmax` especifica el tamaño máximo del registro de errores, en megabytes. El nombre predeterminado para el registro de errores es `dsmerror.log`.

El ajuste de registro se controla con la opción `errorlogmax`. Si `errorlogmax` se establece en cero (0), el tamaño del registro es ilimitado; las entradas registradas no se "ajustan" y comienzan a sobrescribirse las entradas registradas anteriores. Si `errorlogmax` no está establecida en cero, las entradas de registro más recientes sobrescriben las entradas más antiguas del registro cuando el registro alcanza su tamaño máximo.

La eliminación de registros se controla con la opción `errorlogretention`. Los registros eliminados no se ajustan. En su lugar, las entradas de registro más antiguas que el número de días especificado por la opción `errorlogretention` se eliminan del archivo de registro.

Si cambia de ajuste de anotación (opción `errorlogmax`) a eliminación de anotación (opción `errorlogretention`), todas las entradas de las anotaciones existentes se guardan y la anotación se depura mediante el nuevo criterio `errorlogretention`. Las entradas de anotaciones eliminadas se guardan en un archivo llamado `dsmerlog.pru`.

Si cambia de eliminación de registros (opción `errorlogretention`) a ajuste de registros (opción `errorlogmax`), todos los registros del registro existente se copian en el archivo de registro `dsmerlog.pru`, se vacía el registro existente y el registro comienza a utilizar el nuevo criterio de ajuste de registro.

Si simplemente cambia el valor de la opción `errorlogmax`, los registros existentes se amplían o reducen para ajustarse al nuevo tamaño. Si el valor se reduce, las entradas más antiguas se suprimen para reducir el tamaño del nuevo archivo.

Si no se especifica `errorlogmax` ni `errorlogretention`, la anotación de registro cronológico de errores puede crecer sin límite de tamaño. Debe gestionar el contenido de los registros manualmente para evitar que el registro agote los recursos del disco. Cuando la anotación se ha creado sin ninguna opción especificada, si posteriormente emite un mandato y especifica la opción `errorlogretention`, la anotación se elimina mediante el valor de retención especificado. Cuando la anotación se ha creado sin ninguna opción especificada, si posteriormente emite un mandato y especifica la opción `errorlogmax`, la anotación existente se trata como si fuera una anotación eliminada. Es decir, el contenido del archivo `dsmerror.log` se copia en un archivo denominado `dsmerlog.pru`, se crean nuevas entradas de registro en `dsmerror.log` y el registro se ajusta cuando alcanza su tamaño máximo.

Nota: Si especifica un valor distinto de cero para `errorlogmax` (que permite la acomodación de anotaciones), no puede utilizar la opción `errorlogretention` para crear registros eliminados. Los registros se pueden eliminar o ajustar, pero no ambas cosas.

Los registros creados con la opción `errorlogmax` contienen un registro de cabecera de registro que contiene información similar a este registro de ejemplo:

```
LOGHEADERREC 661 104857600 IBM Spectrum Protect 8.1.0 Fri Dec 9 06:46:53 2011
```

Tenga en cuenta que las fechas y las indicaciones de la hora del texto `LOGHEADERREC` no se convierten o formatean utilizando los valores especificados en las opciones `dateformat` o `timeformat`.

Cientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor.

También puede establecer esta opción en la ficha **Preferencias de cliente** en la GUI, seleccionando **Habilitar ajuste de archivo de registro de errores** y especificando un valor distinto de cero para el **tamaño máximo** para el archivo de anotaciones cronológicas. Para impedir el ajuste del archivo de anotaciones, establezca el valor de **tamaño máximo** a cero. Cuando el ajuste máximo se establece en cero, borrar o establecer la opción **Habilitar ajuste de archivo de registro de errores** no tiene ningún efecto; el ajuste de anotaciones no se produce si el **tamaño máximo** se establece en cero.

Sintaxis

►►—ERRORLOGMAX— —*size*—►►

Parámetros

size

Especifica el tamaño máximo, en megabytes, del archivo de anotaciones. El rango de valores es de 0 a 2047; el valor predeterminado es 0, que desactiva la acomodación del archivo de registro y deja que el archivo crezca indefinidamente.

Ejemplos

Archivo de opciones:

errorlogmax 2000

Línea de mandatos:

-errorlogmax=2000

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Errorlogname

Esta opción especifica la vía de acceso totalmente calificada y el nombre de archivo en el que se deben guardar los mensajes de error.

El valor de esta opción modifica temporalmente la variable de entorno DSM_LOG. Los archivos dsmwebcl.log y dsmsched.log se crean en el mismo directorio que el archivo de registro de errores que especifica con la opción errorlogname.

Para Mac OS X, la ubicación predeterminada es una de las siguientes:

~/Library/Logs/tivoli/tsm/
/Library/Logs/tivoli/tsm/

El dsmerror.log no puede ser un enlace simbólico.

Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor. Puede establecer esta opción en la ficha **General**, en el botón **Seleccionar anotaciones de errores** del Editor de preferencias.

Sintaxis

►►—ERRORLOGName— —*filespec*—►►

Parámetros

filespec

La vía de acceso completamente calificada y el nombre del archivo donde se

debe almacenar la información de anotaciones de errores. Si no existe ninguna parte de la ruta que especifica, el cliente intenta crearla.

El archivo `dsmerror.log` no puede ser un enlace simbólico.

Ejemplos

Archivo de opciones:

`errorlogname /tmp/tsmerror.log`

Línea de mandatos:

`-errorlogname=/tmp/tsmerror.log`

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Errorlogretention

La opción `errorlogretention` especifica durante cuántos días van a conservarse las entradas de las anotaciones de errores antes de eliminarlas y si se van a guardar las entradas eliminadas en otros archivos.

El registro de errores se elimina cuando se graba el primer error en el registro después de iniciar una sesión de cliente. Si la única sesión ejecutada es el planificador cliente y está en ejecución las veinticuatro horas del día, puede que las anotaciones de errores no se eliminen según las expectativas. Detenga la sesión y vuelva a iniciarla para que el planificador pueda eliminar las anotaciones de error.

Si cambia de eliminación de anotación (opción `errorlogretention`) a ajuste de anotación (opción `errorlogmax`), todos los registros de las anotaciones existentes se copian en el archivo de anotación `dsmerlog.pru`, la anotación existente se vacía y el registro empieza según los nuevos criterios de ajuste de anotaciones.

Si cambia de ajuste de anotación (opción `errorlogmax`) a eliminación de anotación (opción `errorlogretention`), todas las entradas de las anotaciones existentes se guardan y la anotación se depura mediante el nuevo criterio `errorlogretention`. Las entradas de anotaciones eliminadas se guardan en un archivo llamado `dsmerlog.pru`.

Si no se especifica `errorlogmax` ni `errorlogretention`, la anotación de registro cronológico de errores puede crecer sin límite de tamaño. Debe gestionar el contenido de los registros manualmente para evitar que el registro agote los recursos del disco. Cuando la anotación se ha creado sin ninguna opción especificada, si posteriormente emite un mandato y especifica la opción `errorlogretention`, la anotación se elimina mediante el valor de retención especificado. Cuando la anotación se ha creado sin ninguna opción especificada, si posteriormente emite un mandato y especifica la opción `errorlogmax`, la anotación existente se trata como si fuera una anotación eliminada. Es decir, el contenido del archivo `dsmerror.log` se copia en un archivo llamado `dsmerlog.pru`, se crean nuevas entradas de registro en `dsmerror.log` y la anotación se ajusta cuando llega a su tamaño máximo.

Nota: Si especifica la opción `errorlogretention` para crear anotaciones eliminadas, no podrá especificar la opción `errorlogmax`. Los registros pueden ser eliminados o ajustados, pero no las dos cosas.

Clientes soportados

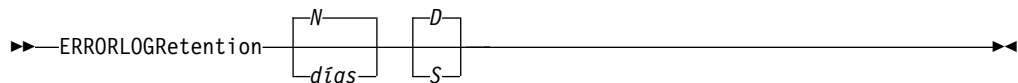
Esta opción es válida para todos los clientes.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor.

También puede establecer esta opción en la ficha **Preferencias de cliente** en la GUI seleccionando **Depurar entradas antiguas** y especificando un valor para **Depurar entradas más antiguas que**. Al seleccionar la opción **Guardar entradas depuradas** se guardan las entradas de anotaciones depuradas en el archivo de registro dsmerlog.pru.

Sintaxis



Parámetros

N o *days*

Especifica cuánto tiempo se debe esperar antes de eliminar las anotaciones de errores.

N No se eliminan el registro de errores. Esto hace que las anotaciones de errores crezcan indefinidamente. Éste es el valor predeterminado.

days

El número de días que se deben conservar las entradas del archivo de anotaciones antes de eliminar las anotaciones. El rango de valores oscila entre 0 y 9999.

D o *S*

Especifica si se deben guardar las entradas eliminadas. Utilice un espacio o una coma para separar este parámetro del anterior.

D Elimina las entradas del registro de errores al eliminarlas. Éste es el valor predeterminado.

S Guarda las entradas de las anotaciones de errores al eliminarlas.

Las entradas depuradas se copian desde el registro de errores al archivo dsmerlog.pru que está situado en el mismo directorio que el archivo dsmerror.log.

Ejemplos

Archivo de opciones:

Eliminar entradas de anotaciones desde el archivo dsmerror.log que tengan más de 365 días y guardar las entradas eliminadas en dsmerlog.pru.errorlogretention 365 S

Línea de mandatos:

-errorlogr=365,S

Archivo de opciones:

Eliminar entradas de anotaciones desde el archivo `dsmerror.log` que tengan más de 365 días y no guardar las entradas eliminadas.
`errorlogretention 365 D`

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Opciones **exclude**

Utilice las opciones **exclude** para excluir objetos de la imagen de copia de seguridad o de los servicios de archivado.

Por ejemplo, puede que desee excluir este tipo de información:

- Todos los archivos temporales
- Todas las memorias caché locales de archivos de red
- Todos los archivos que contienen código objeto compilado que se pueda reproducir fácilmente utilizando otros métodos
- Los archivos del sistema operativo

Puede excluir archivos específicos del proceso de cifrado durante una copia de seguridad.

Nota:

1. A excepción de `exclude.fs`, cuando excluya un archivo que anteriormente se había incluido, las versiones de copia de seguridad existentes se desactivarán durante la siguiente copia de seguridad incremental.
2. El servidor puede definir opciones de exclusión con la opción `incl excl`.

Excluya cualquier archivo de sistemas o imagen que pueda dañar el sistema operativo al recuperarse. También debe excluir el directorio que contiene los archivos de cliente de IBM Spectrum Protect.

Utilice caracteres comodín para excluir un rango amplio de archivos.

Para excluir un directorio completo denominado `/any/test`, especifique lo siguiente:

```
exclude.dir /any/test
```

Para excluir los subdirectorios que empiezan por `test` y que se encuentran en el directorio `/any`, especifique lo siguiente:

```
exclude.dir /any/test*
```

Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. Puede establecer estas opciones en la ficha **Incluir/excluir**, en la sección **Definir opciones de inclusión/exclusión** del Editor de preferencias.

Sintaxis

► *opciones* — *patrón* —►

exclude, exclude.backup, exclude.file, exclude.file.backup

Utilice estas opciones para excluir un archivo o un grupo de archivos de los servicios de copia de seguridad y de los servicios de gestión de espacio (si el cliente de HSM está instalado). La opción `exclude.backup` sólo excluye archivos de la copia de seguridad normal, no de HSM.

exclude.archive

Excluye *sólo* de los servicios de archivado el archivo o grupo de archivos que coincidan con el patrón.

exclude.attribute.symlink

Excluye un archivo o un grupo de archivos que son enlaces simbólicos o alias (los alias se aplican a Mac OS X) sólo del proceso de copia de seguridad.

Nota: Para Mac OS X, se excluyen los alias.

exclude.compression

Excluye archivos del proceso de compresión si la opción `compression` se ha establecido en `yes`. Esta opción se aplica a copias de seguridad y copias archivadas.

exclude.dedup

Excluye archivos para la eliminación de duplicados de datos por parte del cliente. Para controlar una operación de eliminación de duplicados de datos por parte del cliente, especifique `ieobdtype` como valor de la opción `exclude.dedup`.

Los parámetros `ieobdtype` válidos son:

Archivo
Imagen

El valor predeterminado es `File`.

exclude.dir

Excluye un directorio, sus archivos y todos sus subdirectorios y sus archivos del proceso de copia de seguridad. Por ejemplo, la sentencia `exclude.dir /test/dan/data1` excluye el directorio `/test/dan/data1`, sus archivos y todos sus subdirectorios y sus archivos.

Si excluye un directorio que anteriormente se había incluido, el servidor dará caducidad a las versiones de copia de seguridad existentes de los archivos y directorios que se encuentran debajo de éste durante la siguiente copia incremental. Utilice esta opción para excluir una parte de los datos que no tenga archivos subyacentes de los que deba realizarse una copia de seguridad.

Nota: Evite realizar una copia de seguridad selectiva, o una copia de seguridad parcial incremental, de un archivo individual de un directorio excluido. La próxima vez que realice una copia de seguridad incremental, se dará caducidad a los archivos cuya copia de seguridad se ha realizado de esta forma.

exclude.encrypt

Excluye los archivos especificados del proceso de cifrado. Esta opción no afecta a la exclusión de los archivos del proceso de copia de seguridad o archivado, sólo afecta a la exclusión de los archivos del proceso de cifrado.

exclude.fs

Excluye los sistemas de archivos que coinciden con el patrón especificado de las operaciones de copia de seguridad, copia de seguridad de imágenes incremental y operaciones de archivado. Si en algún momento se realizó una copia de seguridad de los archivos de los sistemas de archivos excluidos, no se llevará a cabo la operación de volver a vincular con clase de gestión ni caducarán los archivos suprimidos. No obstante, las versiones de copia de seguridad existentes permanecerán en el servidor según los valores de clases de gestión asociadas. Los archivos previamente archivados del sistema de archivos excluido permanecen en el servidor como copias de archivo.

La opción `exclude.fs` NO impide la copia de seguridad o archivado de ningún punto de montaje virtual que son los subdirectorios del sistema de archivos excluido.

Utilice `exclude.image` para excluir sistemas de archivos de operaciones de copia de seguridad de imágenes.

exclude.fs.nas

Excluye sistemas de archivos del servidor de archivos NAS del proceso de copias de seguridad de imágenes cuando se utiliza con el mandato **backup nas**. El nombre de nodo NAS debe estar prefijado al nombre del sistema de archivos, por ejemplo: `netappsj1/vol/vol1`. Para aplicar esta exclusión a todos los nodos NAS sustituya el nombre de nodo NAS con un comodín, por ejemplo: `*/vol/vol1`. El mandato **backup nas** pasa por alto todas las demás sentencias de exclusión, incluidas las sentencias `exclude.fs` y `exclude.dir`. Esta opción *sólo* es válida para los clientes AIX y Solaris.

exclude.image

Excluye sistemas de archivos montados y volúmenes lógicos RAW que coincidan con el patrón especificado de las operaciones de copia de seguridad de imágenes completas. Esta opción es válida únicamente para AIX, todos los clientes Linux y Solaris. Utilice `exclude.fs` para excluir sistemas de archivos de operaciones de copia de seguridad de imágenes incremental.

Restricción: Esta opción no se aplica a Mac OS X.

Parámetros

patrón

Especifica el archivo o grupo de archivos que se desean excluir.

Nota: En sistemas de archivos NAS, debe añadir un prefijo de nombre de nodo NAS a la especificación de archivo para indicar el servidor de archivos al que se aplica la sentencia de exclusión. Si no especifica un nombre de nodo NAS, el sistema de archivos identificado hará referencia al nombre de nodo NAS que se ha especificado en el archivo de opciones del cliente (`dsm.sys`) o en la línea de mandatos.

Si el patrón comienza con comillas dobles o simples, contiene espacios en blanco intercalados o signos de igual, debe incluir el valor entre comillas simples (') o comillas dobles ("). Los signos que se utilicen para la apertura y el cierre deben ser del mismo tipo.

En la opción `exclude.image`, el patrón es el nombre de un sistema de archivos montado o de un volumen lógico RAW.

Ejemplos

Archivo de opciones:

```

exclude /unix/
exclude ../../core
exclude /home/jones/proj1/*
exclude.archive ../../core
exclude.backup /home/jones/proj1/devplan/
exclude.dir /home/jones/tmp
exclude.backup /users/home1/file1
exclude.image /usr/*/*
exclude.encrypt /users/home2/file1
exclude.compression /home/gordon/proj1/*
exclude.fs.nas netappsj/vol/vol0
exclude.attribute.symlink ../../*
exclude.dedup /Users/Administrator/Documents/Important/../../*

```

Línea de mandatos:

No se aplica.

Información relacionada

consulte el apartado “Archivos del sistema a excluir” en la página 129 para obtener una lista de aquellos archivos que siempre deberían excluirse.

“Incl excl” en la página 456

Consulte el tema “Inclusión y exclusión de grupos de archivos con caracteres comodín” en la página 131 para obtener una lista de los caracteres comodín que puede utilizar. Después, si es necesario, utilice la opción `include` para realizar excepciones.

Control del proceso de enlaces simbólicos y alias

El cliente de copia de seguridad y archivado trata los vínculos simbólicos y los alias (los alias se aplican sólo a Mac OS X) como archivos reales y realiza una copia de seguridad de los mismos. Sin embargo, no se realiza la copia de seguridad del archivo al que hace referencia el enlace simbólico. En algunos casos, los enlaces simbólicos pueden volver a crearse fácilmente y no es necesario realizar una copia de seguridad de los mismos.

Además, realizar una copia de seguridad de estos enlaces simbólicos puede incrementar el tiempo de proceso de la copia de seguridad y puede ocupar un volumen de espacio notable en el servidor de IBM Spectrum Protect. Para excluir un archivo o un grupo de archivos que sean enlaces simbólicos del proceso de copia de seguridad puede utilizar la opción `exclude.attribute.symlink`. Si es necesario, puede utilizar la opción `include.attribute.symlink` para incluir enlaces simbólicos en un grupo amplio de archivos excluidos para el proceso de copia de seguridad.

Por ejemplo, para excluir todos los enlaces simbólicos del proceso de copia de seguridad, excepto los que existen en el directorio `/home/spike`, especifique estas sentencias en el archivo `dsm.sys`:

```

exclude.attribute.symlink ../../*
include.attribute.symlink /home/spike/../../*

```

Referencia relacionada:

“Opciones include” en la página 458

Control del proceso de compresión

En este tema se indican diversos aspectos que han de tenerse en cuenta si desea excluir archivos o grupos de archivos específicos del proceso de compresión durante una operación de copia de seguridad o archivado.

- Recuerde que el cliente de copia de seguridad y archivado compara los archivos que procesa con los patrones especificados en las sentencias de inclusión y exclusión leyéndolas de abajo arriba en el archivo de opciones.
- Debe establecer la opción `compression` en `yes` para activar el proceso de compresión. Si no especifica la opción `compression` o si establece la opción `compression` en `no`, el cliente no realizará el proceso de compresión.
Si establece la opción `compression` en `yes` y no existe ninguna sentencia `exclude.compression`, el cliente considerará todos los archivos para el proceso de compresión.
- El cliente procesará `exclude.fs`, `exclude.dir`, y otras sentencias de inclusión/exclusión en primer lugar. A continuación, el cliente considerará las sentencias `exclude.compression`. Por ejemplo, considerando la siguiente lista de inclusión/exclusión:

```
exclude /home/jones/proj1/*.*
exclude.compression /home/jones/proj1/file.txt
include /home/jones/proj1/file.txt
```

El cliente examina las sentencias (realiza una lectura desde el final hasta el principio) y determina que el archivo `/home/jones/proj1/file.txt` es candidato para la copia de seguridad, pero no es candidato para el proceso de compresión.
- El proceso de compresión de inclusión-exclusión es válido únicamente para procesos de copias de seguridad y archivado. La opción `exclude.compression` no afecta a la exclusión de los archivos del proceso de copia de seguridad o archivado, sólo afecta a la exclusión del proceso de compresión.

Referencia relacionada:

“Compression” en la página 370

Proceso de sistemas de archivos NAS

Utilice la opción `exclude.fs.nas` para excluir sistemas de archivos del proceso de copia de seguridad de imágenes NAS.

Nota: La opción `exclude.fs.nas` no es válida para una copia de seguridad incremental por diferencia de instantánea.

Una especificación del sistema de archivos NAS utiliza los convenios siguientes:

- Los nodos NAS representan un tipo de nodo exclusivo. El nombre de nodo NAS identifica de forma exclusiva un servidor de archivos NAS y sus datos en el cliente de copia de seguridad y archivado. Puede añadir un prefijo de nombre de nodo NAS en la especificación de archivo para indicar el servidor de archivos al que se aplica la sentencia de exclusión. Si no especifica un nombre de nodo NAS, el sistema de archivos identificado se aplica a todos los servidores de archivos NAS.
- Con independencia de la plataforma del cliente utilizada, las especificaciones de sistema de archivos NAS utilizan la barra inclinada (/) como separador, tal como se muestra en el siguiente ejemplo: `/vol/vol0`.

Por ejemplo, para excluir `/vol/vol1` de los servicios de copia de seguridad en todos los nodos NAS, especifique la sentencia de exclusión siguiente:

```
exclude.fs.nas */vol/vol1
```

Opciones `exclude` de la máquina virtual

Las opciones de inclusión y exclusión de la máquina virtual influyen en el comportamiento de las operaciones de copia de seguridad y restauración de máquinas virtuales. Estas opciones se procesan antes de procesar cualquier opción de línea de mandatos, por lo que las opciones en la línea de mandatos pueden

alterar temporalmente las opciones especificadas en cualquiera de las opciones de inclusión o de exclusión de la máquina virtual. Consulte las descripciones de opciones individuales para obtener información sobre las opciones.



Las operaciones de máquina virtual solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments.

Referencia relacionada:

"Exclude.vmdisk"

Exclude.vmdisk:

La opción EXCLUDE.VMDISK excluye un disco de máquina virtual de VMware de las operaciones de copia de seguridad.

La opción EXCLUDE.VMDISK especifica la etiqueta del disco de una máquina virtual que debe incluirse en una operación **Backup VM**. Si excluye un disco en el mandato **Backup VM**, los parámetros de línea de mandatos alteran temporalmente cualquier sentencia EXCLUDE.VMDISK en el archivo de opciones.

Esta opción solo está disponible si se utiliza el producto bajo licencia IBM Spectrum Protect for Virtual Environments. Para obtener información adicional sobre esta opción, consulte la documentación del producto IBM Spectrum Protect for Virtual Environments en el IBM Knowledge Center en <http://www.ibm.com/support/knowledgecenter/SSERB6/welcome>.

Clientes soportados

Esta opción puede utilizarse con clientes Linux x86_64 soportados.

Archivo de opciones

Establezca esta opción en el archivo de opciones del cliente. Los parámetros de línea de mandatos alteran temporalmente las sentencias en el archivo de opciones.

Sintaxis

►►—EXCLUDE.VMDISK—*vmname*—*vmdk_label*—————►►

Parámetros

vmname

Especifica el nombre de la máquina virtual que contiene un disco que desea excluir en una operación **Backup VM**. El nombre es el de visualización de la máquina virtual. Solo puede especificar un nombre de máquina virtual en cada sentencia EXCLUDE.VMDISK. Especifique sentencias EXCLUDE.VMDISK adicionales para cada disco de la máquina virtual que desee excluir.

El nombre de la máquina virtual puede contener un asterisco (*) para que coincida con cualquier serie de caracteres y el signo de interrogación (?) para que coincida con cualquier carácter. Entrecomille el nombre de máquina (" ") si el nombre de máquina contiene caracteres de espacio.

Consejo: Si el nombre de la máquina virtual contiene caracteres especiales, como por ejemplo corchetes ([o]), puede ser que el nombre de la máquina

virtual no coincida correctamente. Si un nombre de máquina virtual utiliza caracteres especiales en el nombre, puede que necesite utilizar el carácter de interrogación (?) para que coincida con los caracteres especiales en el nombre de la máquina virtual.

Por ejemplo, para excluir Hard Disk 1 en la copia de seguridad de una máquina virtual denominada "Windows VM3 [2012R2]", utilice esta sintaxis en el archivo de opciones: EXCLUDE.VMDISK "Windows VM3 ?2012R2?" "Hard Disk 1"

vmdk_label

Especifica la etiqueta de disco del disco que desea excluir. Los caracteres comodín no están permitidos. Utilice el mandato **Backup VM** con la opción -preview para determinar las etiquetas de disco de discos en una máquina virtual determinada. Consulte "**Backup VM**" en la página 683 para conocer la sintaxis.

No excluya los discos en máquinas virtuales que está protegiendo con la opción INCLUDE.VMTSMVSS, si los discos contienen datos de aplicación.

Ejemplos

Archivo de opciones

Supongamos que una máquina virtual llamada vm1 contiene cuatro discos, etiquetados como disco duro 1, disco duro 2, disco duro 3 y disco duro 4. Para excluir solo el disco duro 2 en una operación **Backup VM**, especifique lo siguiente en el archivo de opciones:

```
EXCLUDE.VMDISK "vm1" "Hard Disk 2"
```

Excluir los discos 2 y 3 en operaciones **Backup VM**:

```
EXCLUDE.VMDISK "vm1" "Hard Disk 2"  
EXCLUDE.VMDISK "vm1" "Hard Disk 3"
```

Línea de mandatos

Los ejemplos de línea de mandatos muestran el uso del operador de exclusión (-) delante de la palabra clave vmdk= para indicar que el disco deben excluirse.

Excluir un único disco:

```
dsmc backup vm "vm1:-vmdk=Hard Disk 1"
```

Excluir disco duro 2 y el disco duro 3:

```
dsmc backup vm "vm1:-vmdk=Hard Disk 2:-vmdk=Hard Disk 3"
```

Incluir el disco duro 1 y el disco duro 2 en vm1:

```
dsmc backup vm "vm1:-vmdk=Hard Disk 1:-vmdk=Hard Disk 2"
```

Referencia relacionada:

"**Backup VM**" en la página 683

"**Restore VM**" en la página 764

"Domain.vmfull" en la página 401

"Include.vmdisk" en la página 467

"INCLUDE.VMTSMVSS" en la página 472

Fbbranch

Utilice la opción fbbranch con los mandatos **backup fastback** o **archive fastback**.

La opción `fbbranch` especifica el ID de la ramificación del servidor de FastBack remoto cuya copia de seguridad o archivado se va a ejecutar. La opción `fbbranch` solo es necesaria si el cliente de archivado y copia de seguridad está instalado en el FastBack Disaster Recovery Hub o si hay un proxy dedicado conectado a un repositorio de FastBack Disaster Recovery Hub replicado. No especifique la opción `fbbranch` si el cliente de archivado y copia de seguridad está instalado en el servidor de FastBack.

Clientes soportados

Esta opción es válida para clientes de Linux x86_64.

Archivo de opciones

Ninguna. Esta opción sólo puede especificarse en la línea de mandatos. El servidor también puede definir o sustituir esta opción.

Sintaxis

►►—FBBBranch=*ID_ramificación*—►►

Parámetros

ID_ramificación

Especifica el ID de ramificación del servidor de FastBack. El valor forma parte de la configuración de recuperación tras desastre del servidor de FastBack.

Ejemplos

Línea de mandatos:

```
-FBBBranch=oracle
```

En un cliente de archivado y copia de seguridad instalado en el FastBack Disaster Recovery Hub:

```
dsmc backup fastback -fbpolicyname=policy1 -fbserver=myFbServer  
-fbbranch=oracle
```

Línea de mandatos:

En un cliente de archivado y copia de seguridad conectado a un repositorio en un FastBack Disaster Recovery Hub remoto:

```
dsmc backup fastback -fbpolicyname=policy1 -fbserver=server1  
-fbreposlocation=\\myDrHub.company.com\\REP  
-fbbranch=oracle
```

Si se ha especificado la opción `fbbranch` en una estación de trabajo del cliente de archivado y copia de seguridad que está instalado en el servidor de FastBack, se omite la opción `fbbranch`.

Fbclientname

Utilice la opción `fbclientname` con los mandatos **backup fastback** o **archive fastback** .

La opción `fbclientname` es el nombre de uno o varios clientes de FastBack separados por comas de los que se va a efectuar una copia de seguridad o

archivado desde el proxy de copia de seguridad. Los valores para la opción `fbclientname` no son válidos si se especifica más de una política en la opción `fbpolicyname`.

No puede incluir espacios en los valores de opción `fbclientname`.

Si no especifica los valores de la opción `fbvolumename`, se realizará una copia de seguridad de todos los volúmenes de los clientes de FastBack de la política especificada. Si especifica varios clientes de FastBack en la opción `fbclientname`, no podrá especificar valores para la opción `fbvolumename`.

Clientes soportados

Esta opción es válida para clientes de Linux x86_64.

Archivo de opciones

Ninguna. Esta opción sólo puede especificarse en la línea de mandatos.

Sintaxis



Parámetros

nombre_cliente

Especifica el nombre de uno o varios clientes de FastBack. Puede especificar hasta 10 nombres de cliente de FastBack.

Importante:

Al especificar el mandato **archive fastback** o **backup fastback**:

1. Como mínimo es necesario siempre un `FBpolicyName`.
2. Podrá especificar hasta 10 valores para `FBPolicyName`, si no se ha especificado ningún valor ni para `FBClientName` ni para `FBVolumeName`.
3. Si se especifica un valor de `FBClientName`, debe haber solo un valor para `FBPolicyName`.
4. Podrá especificar hasta 10 valores para `FBClientName` si se ha especificado solo un valor para `PolicyName` y ninguno para `FBVolumeName`.
5. Cuando se especifica la opción `FBVolumeName`, se puede tener solo un `FBPolicy` y un `FBClientName` especificados.
6. Podrá especificar varios `FBVolumeNames` si se cumple la condición 5.
7. Debe especificar siempre la opción `FBReposLocation` para Linux.

Ejemplos

Línea de mandatos:

```
dsmc backup fastback -fbpolicyname=Policy1  
-fbclientname=fbclient1,fbclient2  
-fbserver=myFbServer  
-fbreposlocation=/mnt/FBLocation
```

Realiza copias de seguridad de todos los volúmenes para los clientes fbclient1 y fbclient2 de FastBack que se encuentran en la política Policy1.

Fbpolicyname

Utilice la opción fbpolicyname con los mandatos **backup fastback** o **archive fastback**.

La opción fbpolicyname es el nombre de una o varias políticas de FastBack separadas por comas de las que se va a efectuar una copia de seguridad o archivado desde el proxy de copia de seguridad. Debe especificar, como mínimo, un nombre de política. Especifique varios nombres de políticas utilizando una lista de políticas delimitadas por comas. No hay ningún valor predeterminado.

Si uno o más nombres de políticas FB contiene espacios, debe especificarlos dentro de las comillas. A continuación se muestra un ejemplo: "FB Policy NAME1, FBPolicy Name 2".

Si no se especifica ningún valor para las opciones fbclientname y fbvolumename, se realiza copia de seguridad de todos los volúmenes de todos los clientes de FastBack de la política que se especifiquen. Si especifica varias políticas en la opción fbpolicyname, no puede especificar valores para las opciones fbclientname y fbvolumename.

Si una especificación de política contiene clientes FastBack de Windows y Linux, solo se hará una copia de seguridad de los volúmenes Linux, o bien se archivarán, en el servidor de IBM Spectrum Protect mediante el cliente de copia de seguridad y archivado de Linux.

Debe existir al menos una instantánea en el repositorio de FastBack para las políticas de FastBack que se han archivado, o de las cuales se han realizado copias de seguridad, antes de emitir el mandato **dsmc**

Clientes soportados

Esta opción es válida para clientes de Linux x86_64.

Archivo de opciones

Ninguna. Esta opción sólo puede especificarse en la línea de mandatos.

Sintaxis



Parámetros

nombre_política

Especifica el nombre de las políticas de FastBack. Puede especificar hasta 10 nombres de política de FastBack.

Importante:

Al especificar el mandato **archive fastback** o **backup fastback**:

1. Como mínimo es necesario siempre un FBpolicyName.
2. Podrá especificar hasta 10 valores para FBPolicyName, si no se ha especificado ningún valor ni para FBClientName ni para FBVolumeName.
3. Si se especifica un valor de FBClientName, debe haber solo un valor para FBPolicyName.
4. Podrá especificar hasta 10 valores para FBClientName si se ha especificado solo un valor para PolicyName y ninguno para FBVolumeName.
5. Cuando se especifica la opción FBVolumeName. se puede tener especificado un único FBPolicy y un único FBClientName. Debe especificar exactamente un FBClientName. No se puede omitir.
6. Podrá especificar varios FBVolumeNames si se cumple la condición 5.
7. Debe especificar siempre la opción FBReposLocation para Linux.

Ejemplos

Línea de mandatos:

```
dsmc backup fastback -fbpolicyname=Policy1,Policy2,Policy3
-fbserver=myFbServer
-fbreposlocation=\\myFbServer.company.com\REP
```

Realiza una copia de seguridad de todos los volúmenes de los clientes de FastBack que se encuentran en las políticas Policy1, Policy2 y Policy3.

Para explicar políticas con espacios, inclúyalas entre comillas dobles, por ejemplo:

```
-fbpolicyname="Policy 1,Policy2,Policy3"
```

Fbreposlocation

Utilice la opción fbreposlocation con los mandatos **backup fastback** o **archive fastback**.

La opción fbreposlocation especifica la ubicación del repositorio de Tivoli Storage Manager FastBack para que el proxy del cliente de archivado y copia de seguridad se conecte para emitir los mandatos de shell de Tivoli Storage Manager FastBack necesarios para montar las instantáneas apropiadas.

Esta opción es necesaria para sistemas Linux. No existe una ubicación predeterminada.

Si especifica la opción fbreposlocation para una instantánea en el servidor de FastBack, utilice el formato nombre_servidor@GRUPO_TRABAJO.

Existen dos maneras de especificar la ubicación de repositorio de FastBack en el FastBack Disaster Recovery Hub:

- Especifique la ubicación completa del repositorio mediante la opción -fbreposlocation=\\DR_Hub\rep_server. Cuando se utiliza este formato, DR_Hub es el nombre de máquina de FastBack Disaster Recovery Hub y rep_server es el nombre del repositorio de servidor de FastBack replicado en el DR Hub.
- Especifique la ubicación del repositorio utilizando una combinación de las opciones -fbreposlocation= y -fbbranch. Al utilizar este formato, especifique la ubicación del repositorio del DR Hub mediante la opción -fbreposlocation=DR_Hub@WORKGROUP, y especifique el nombre del repositorio del servidor de FastBack replicado en el DR Hub utilizando la opción -fbbranch.

Si utiliza el formato `-fbr=\\<fbserver>\REP`, especifique dos barras inclinadas invertidas antes de `<fbserver>` y una barra inclinada invertida antes de `REP` al utilizar el cliente de archivado y copia de seguridad en modalidad interactiva. Si utiliza este formato como un mandato de Linux `dsmc backup fastback -fbr=\\\\<servidor_fb>\REP`, debe especificar cuatro barras inclinadas invertidas antes de `<servidor_fb>` y dos barras inclinadas invertidas antes de `REP`. Esto se debe a que el shell de Linux interpreta una barra inclinada invertida como un carácter de escape; la primera barra inclinada se trata como un carácter de escape para la siguiente barra inclinada invertida.

Clientes soportados

Esta opción es válida para clientes de Linux x86_64.

Archivo de opciones

Ninguna. Esta opción sólo puede especificarse en la línea de mandatos. El servidor también puede definir o sustituir esta opción.

Sintaxis

►—FBReposlocation—*ubicación_repositorio*—►

Parámetros

ubicación_repositorio

Especifica la ubicación de repositorio de Tivoli Storage Manager FastBack.

Ejemplos

Línea de mandatos:

```
dsmc backup fastback -fbpolicyname=Policy1  
-fbclientname=fbclient1,fbclient2 -fbserver=myFbDrHub  
-fbreposlocation=\\myFbDrHub\rep_myFbServer
```

Nota: Dado que Linux solo se admite como una configuración de proxy dedicado, siempre es necesaria una ubicación de repositorio en proxy Linux.

Línea de mandatos:

```
dsmc backup fastback -fbpolicyname=Policy1  
-fbclientname=fbclient1,fbclient2 -fbserver=myFbDrHub  
-fbreposlocation=myFbDrHub -fbbranch=rep_myFbServer
```

Nota: Dado que Linux solo se admite como una configuración de proxy dedicado, siempre es necesaria una ubicación de repositorio en proxy Linux.

Fbserver

Utilice la opción `fbserver` con los mandatos **backup fastback** o **archive fastback**.

La opción `fbserver` especifica el nombre de host abreviado de la estación de trabajo de servidor de Tivoli Storage Manager FastBack propietaria del repositorio especificado por la opción `fbreposlocation`. Para un DR Hub, la opción `fbserver` especifica el nombre corto de la estación de trabajo del servidor FastBack a cuyo repositorio de ramificaciones está conectado el cliente de copia de seguridad y archivado.

La opción `fbserver` es la clave para recuperar las credenciales de usuario necesarias para conectarse al repositorio del servidor de FastBack o el repositorio del servidor del concentrador DR para el proceso de montaje.

Clientes soportados

Esta opción es válida para clientes de Linux x86_64.

Archivo de opciones

Ninguna. Esta opción sólo puede especificarse en la línea de mandatos.

Sintaxis

► — `-FBServer` — `—server_name` —►

Parámetros

nombre_servidor

Especifica el nombre de host abreviado de la máquina en la que está instalado el servidor de FastBack.

Ejemplos

Línea de mandatos:

El cliente de archivado y copia de seguridad está instalado en una máquina de cliente proxy de Linux. Utilice este mandato para archivar todos los volúmenes de FastBack para todos los clientes FastBack de Linux definidos para `policy1` de FastBack:

```
dsmc archive fastback -fbpolicyname=Policy1
-fbserver=myfbserver
-fbreposlocation=myfbserver@WORKGROUP
```

La ubicación del repositorio es necesaria. Si no proporciona la ubicación del repositorio, se producirá un error en el mandato.

El nombre del servidor de FastBack, `-myfbserver`, es el nombre de host abreviado del servidor de FastBack donde se encuentra el repositorio.

Línea de mandatos:

El repositorio, `rep_server1`, se encuentra en el FastBack Disaster Recovery Hub, `myFbDrHub`.

```
dsmc archive fastback -fbpolicyname="Policy 1"
-fbserver=myFbDrHub
-fbreposlocation=\\myFbDrHub\rep_server1
```

El nombre del servidor de FastBack, `-myFbDrHub` es el nombre de host abreviado del servidor de FastBack Disaster Recovery Hub donde se encuentra el repositorio

El parámetro `-fbreposlocation` especifica la ubicación del repositorio. La ubicación del repositorio es necesaria. Si no se proporciona la ubicación del repositorio, el mandato falla.

`-fbserver` debería apuntar al nombre de host abreviado del FastBack DR Hub en este caso.

Línea de mandatos:

Archivar todos los volúmenes protegidos por la política de FastBack denominada policy1 del servidor de FastBack denominado basil:

```
dsmc archive fastback -Fbpolicyname=policy1  
-FBServer=basil -ARCHMC="my_tsm_mgmt_class"  
-fbreposlocation=basil@WORKGROUP
```

Fbvolumename

Utilice la opción fbvolumename con los mandatos **backup fastback** o **archive fastback**.

La opción fbvolumename es el nombre de uno o varios volúmenes de Tivoli Storage Manager FastBack separados por comas de los que se va a efectuar una copia de seguridad o archivado desde el proxy de copia de seguridad. Los valores de la opción fbvolumename no son válidos si se especifica más de un cliente de FastBack en la opción fbclientname.

Si especifica varios clientes de FastBack en la opción fbclientname, no podrá especificar valores para la opción fbvolumename.

Clientes soportados

Esta opción es válida para clientes de Linux x86_64.

Archivo de opciones

Ninguna. Esta opción sólo puede especificarse en la línea de mandatos.

Sintaxis



Parámetros

nombre_volumen

Especifica el nombre de los volúmenes de Tivoli Storage Manager FastBack. Puede especificar hasta 10 nombres de volumen de FastBack.

Importante:

Al especificar el mandato **archive fastback** o **backup fastback**:

1. Como mínimo es necesario siempre un FBpolicyName.
2. Podrá especificar hasta 10 valores para FBPolicyName, si no se ha especificado ningún valor ni para FBClientName ni para FBVolumeName.
3. Si se especifica un valor de FBClientName, debe haber solo un valor para FBPolicyName.
4. Podrá especificar hasta 10 valores para FBClientName si se ha especificado solo un valor para PolicyName y ninguno para FBVolumeName.
5. Cuando se especifica la opción FBVolumeName, se puede tener especificado un único FBPolicy y un único FBClientName. Debe especificar exactamente un FBClientName. No se puede omitir.
6. Podrá especificar varios FBVolumeNames si se cumple la condición 5.

7. Debe especificar la opción FBReposLocation.

Ejemplos

Línea de mandatos:

```
dsmc backup fastback -fbpolicyname=Policy1 -fbclientname=client1  
-fbvolumename=data1,data2 -fbserver=myFbDrHub  
-fbreposlocation=\\myFbDrHub\\rep_server1
```

Realiza una copia de seguridad de los volúmenes data1 y data2 desde el cliente client1 de FastBack que se encuentra en la política Policy1.

Filelist

Utilice la opción filelist para procesar una lista de archivos.

Puede utilizar la opción filelist con los mandatos siguientes:

- **archive**
- **backup group**
- **delete archive**
- **delete backup**
- **expire**
- **incremental**
- **query archive**
- **query backup**
- **restore**
- **retrieve**
- **selective**

El cliente de copia de seguridad y archivado abre el archivo que especifique con esta opción y procesa la lista de archivos que contiene de acuerdo con el mandato específico. A excepción de los mandatos **restore** y **retrieve**, cuando utiliza la opción filelist, el cliente pasa por alto todas las demás especificaciones de archivo de la línea de mandatos.

Los archivos (entradas) que contenga filelist deben seguir las siguientes reglas:

- Cada entrada debe ser una vía de acceso completa o relativa de un archivo o directorio. Tenga en cuenta que si incluye un directorio en una entrada de lista de archivo, se realizará una copia de seguridad del directorio, pero no de sus contenidos.
- Cada vía de acceso debe especificarse en una única línea. Cada línea sólo puede contener una única vía de acceso.
- Las vías de acceso no deben contener caracteres de control, como 0x18 (CTRL-X), 0x19 (CTRL-Y) o 0x0A (nueva línea).
- De forma predeterminada, las vías de acceso no debe contener caracteres comodín. No incluya asterisco (*) o interrogaciones (?). en una vía de acceso. Esta restricción se puede alterar temporalmente si habilita la opción denominada wildcardsareliteral. Para obtener más información sobre esta opción, consulte "Wildcardsareliteral" en la página 651.
- Filelist puede ser un archivo MBCS o un archivo Unicode con todas las entradas Unicode. En Mac OS X, la lista de archivos se puede codificar en el lenguaje del sistema operativo actual o UTF-16.
- Si se ha establecido, la opción del cliente denominada quotessareliteral permite que se interpreten literalmente comillas en una especificación de archivo, como comillas y no como delimitadores. Para obtener más información sobre esta opción, consulte "Quotesareliteral" en la página 527. Si no se

establecen `quotesareliteral` ni `wildcardsareliteral`, las comillas dobles y el proceso de comodín funciona tal como se describe en la lista siguiente:

- Si una vía de acceso o un nombre de archivo contiene un espacio, encierre la vía de acceso completamente entre comillas (") o apóstrofes ('). Por ejemplo `"C:\Mis Documentos\spreadsheet.xls"` o `'C:\Mis documentos\spreadsheet.xls'`.
- Si una vía de acceso contiene uno o más apóstrofes ('), encierre la entrada completamente entre comillas ("). Si una vía de acceso contiene una o más comillas dobles, encierre la vía de acceso completamente entre apóstrofes. El proceso de lista de archivos no da soporte a vías de acceso con una mezcla de comillas y apóstrofes.

Los ejemplos siguientes ilustran el uso correcto e incorrecto de comillas dobles y de apóstrofes en las vías de acceso.

Esta vía de acceso de ejemplo contiene un apóstrofo, por lo que debe estar encerrada entre comillas:

```
"/home/gatzby/mydir/gatzby's_report.out"
```

Esta vía de acceso de ejemplo contiene un apóstrofo, por lo que debe estar encerrada entre apóstrofes:

```
'/home/gatzby/mydir/"top10".out'
```

Este ejemplo de vía de acceso contiene un carácter de espacio, por lo que debe encerrarse entre apóstrofes o comillas:

```
"/home/gatzby/mydir/top 10.out"
```

o bien

```
'/home/gatzby/mydir/top 10.out'
```

Esta vía de acceso de ejemplo no está soportada para ser procesada como lista de archivos porque contiene delimitadores no equilibrados (" y '):

```
/home/gatzby/mydir/andy's_"top 10" report.out
```

Estas vías de acceso no están soportadas para el proceso de lista de archivos porque contiene caracteres comodín:

```
/home/gatzby*  
/home/*/20??.txt
```

- Cualquier entrada de lista de archivos de IBM Spectrum Protect que no cumpla con estas reglas será ignorada.

Los siguientes son ejemplos de vías de acceso válidas en una lista de archivos:

```
/home/dir/file1  
/usr/tivoli/file2  
/usr/avi/dir1  
/fs1/dir2/file3  
"/fs2/Ha Ha Ha/file.txt"  
"/fs3/file.txt"
```

Para alterar temporalmente el proceso estándar de caracteres de comillas y comodín, consulte `"Quotesareliteral"` en la página 527 y `"Wildcardsareliteral"` en la página 651.

Puede utilizar la opción `filelist` durante una operación de soporte de archivos abiertos. En tal caso, el cliente procesa las entradas en la lista de archivos del volumen virtual en lugar de en el volumen real.

Si una entrada de filelist se refiere a un directorio, sólo se procesará dicho directorio, y no los archivos que contenga ese directorio.

Si el nombre de archivo (la *filelistspec*) que especifica con la opción *filelist* no existe, el mandato no se ejecuta correctamente. El cliente pasa por alto todas las entradas en *filelist* que no sean archivos o directorios válidos. El cliente registra los errores y el proceso pasa a la siguiente entrada.

Utilice especificaciones de archivo con los mandatos **restore** y **retrieve** para indicar el destino de las entradas restauradas de *filelist*. Por ejemplo, en el siguiente mandato **restore**, la especificación de archivo */usr/record/* representa el destino de la restauración de todas las entradas de *filelist*.

```
restore -filelist=/home/dir/file3 /usr/record/
```

Sin embargo, en el siguiente mandato **selective**, la especificación de archivo */usr/record/* se pasa por alto.

```
selective -filelist=/home/dir/file3 /usr/record/
```

Si especifica un directorio en una lista de archivos para el mandato **delete archive** o **delete backup**, el directorio no se suprime. Las listas de archivos que utilice con el mandato **delete archive** o **delete backup** no deben incluir directorios.

Las entradas de la lista se procesan en el orden en que aparecen en *filelist*. Para obtener un rendimiento óptimo del proceso, clasifique previamente *filelist* por nombre de espacio de archivos y por vía de acceso.

Nota: El cliente puede hacer una copia de seguridad de un directorio dos veces si se producen las condiciones siguientes:

- *Filelist* contiene una entrada para el directorio
- *Filelist* contiene una o varias entradas para los archivos de dicho directorio
- No existe ninguna copia de seguridad del directorio

Por ejemplo, la lista de archivos incluye las entradas */home/dir/file1* y */home/dir*. Si el directorio */dir* no existe en el servidor, el directorio */home/dir* se envían al servidor por segunda vez.

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Sintaxis

►►—FILEList =— —*filelistspec*—————►►

Parámetros

especificaciónlistaarchivos

Especifica la ubicación y el nombre del archivo que contiene la lista de archivos que deben procesarse con el mandato.

Nota: cuando especifique la opción *filelist* en la línea de mandatos, la opción *subdir* se pasa por alto.

Ejemplos

Línea de mandatos:

```
sel -filelist=/home/avi/filelist.txt
```

Información relacionada

“Quotesareliteral” en la página 527

“Wildcardsareliteral” en la página 651

Filename

Utilice la opción **filename** con el mandato **query systeminfo** para especificar un nombre de archivo en el que almacenar la información.

Puede almacenar la información recopilada de uno o varios de los elementos siguientes:

- DSMOPTFILE: el contenido del archivo dsm.opt.
- DSMSYSFILE - El contenido del archivo dsm.sys.
- ENV - Variables de entorno.
- ERRORLOG - El archivo de anotaciones de errores de IBM Spectrum Protect.
- FILE - Atributos para el nombre de archivo que especifique.
- INCLEXCL - Compila una lista de sentencias de inclusión/exclusión en el orden en el que se procesan durante las operaciones de copia de seguridad y archivado.
- OPTIONS - Opciones compiladas.
- OSINFO - Nombre y versión del sistema operativo cliente (incluye información ULIMIT para UNIX y Linux).
- POLICY - Vuelco del conjunto de políticas.
- SCHEDLOG - Contenido del registro de planificación (por lo general, dsmsched.log).
- CLUSTER - Información de clústeres de AIX.

Nota: La principal finalidad del mandato **query systeminfo** es ayudar al soporte de IBM en el diagnóstico de problemas, aunque los usuarios que estén familiarizados con los conceptos relacionados con esta información también podrían encontrarlo de utilidad. Si utiliza la opción **console**, no se realiza ningún formato especial de la salida para ajustarla a la altura o anchura de la pantalla. Por consiguiente, es posible que la salida de la consola sea difícil de leer debido a la longitud y a la acomodación de líneas. En este caso, se recomienda utilizar la opción **filename** con el mandato **query systeminfo** para que la salida se grabe en un archivo que, posteriormente, podrá enviarse al soporte de IBM.

Clientes soportados

Esta opción es válida para todos los clientes.

Sintaxis

►►—FILENAME =— —outputfilename—◄◄

Parámetros

nombrearchivosalida

Especifica un nombre de archivo en el que ha de almacenarse la información.

Si no especifica un nombre de archivo, la información se almacenará, de forma predeterminada, en el archivo dsminfo.txt.

Ejemplos

Línea de mandatos:

```
query systeminfo dsmsoptfile errorlog -filename=tsminfo.txt
```

Información relacionada

“Console” en la página 372

Filesonly

La opción `filesonly` restringe los procesos de copia de seguridad, restauración, recuperación o consulta a *sólo* los archivos.

No puede restaurar o recuperar directorios del servidor de IBM Spectrum Protect cuando utiliza la opción `filesonly` con los mandatos **restore** o **retrieve**. Sin embargo, se crean directorios con atributos predeterminados, si es necesario, como marcadores de posición para los archivos que restaure o recupere.

También puede utilizar la opción `filesonly` con los mandatos siguientes:

- **archive**
- **incremental**
- **query archive**
- **query backup**
- **restore**
- **restore backupset**
- **restore group**
- **retrieve**
- **selective**

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Sintaxis

►►—FILESOnly—◄◄

Parámetros

No hay parámetros para esta opción.

Ejemplos

Línea de mandatos:

```
dsmc incremental -filesonly
```

Followsymbolic

Durante una operación de copia de seguridad, la opción `followsymbolic` especifica si desea utilizar un enlace simbólico como punto de montaje virtual. Durante una operación de restauración o recuperación, la opción `followsymbolic` especifica cómo el cliente de copia de seguridad y archivado restaura un directorio cuyo nombre coincide con un enlace simbólico en el sistema de archivos de destino de restauración.

Para operaciones de copia de seguridad, la opción `followsymbolic` puede influenciar el valor de la opción `virtualmountpoint`. Si utiliza la opción `virtualmountpoint` para especificar un enlace simbólico como punto de montaje virtual, debe establecer también la opción `followsymbolic`.

Durante las operaciones de restauración y recuperación, `followsymbolic` puede influenciar cómo el cliente maneja un enlace simbólico en el sistema de archivos. Establezca la opción `followsymbolic` sólo cuando el cliente intente restaurar un directorio cuyo nombre coincida con un enlace simbólico en el sistema de archivos de destino de la restauración.

Si especifica `followsymbolic=no` (valor predeterminado), el cliente no restaurará el contenido del directorio, sino que devolverá el siguiente mensaje de error:

```
ANS4029E Error al procesar 'nombre de espacio de archivos nombre de vía de acceso
nombre de archivo':
no se pudo crear una vía de acceso de directorio; ya existe
un archivo con el mismo nombre
que un directorio.
```

Si especifica `followsymbolic=yes`, el cliente restaura el contenido del directorio en el destino del enlace simbólico.

Por ejemplo, imaginemos que el cliente ha realizado copia de seguridad de un archivo con esta vía de acceso: `/fs1/dir1/subdir1/file1`. Imaginemos también que existe en el sistema de archivos de destino de la restauración un enlace simbólico `/fs1/dir1`, que está vinculado con `/fs88/dir88/subdir88`. Restaure el archivo con el mandato:

```
restore /fs1/dir1/subdir1/file1
```

Si especifica `followsymbolic=no`, el cliente no restaura el archivo, sino que devuelve el mensaje de error precedente. Si especifica `followsymbolic=yes`, el cliente restaura `file1` en `/fs88/dir88/subdir88/subdir1/file1`.

Si restaura un enlace simbólico (no un directorio) cuyo nombre coincide con un enlace simbólico en el sistema de archivos de destino de la restauración, el cliente restaura el enlace simbólico.

Si se utiliza un enlace simbólico como punto de montaje virtual, la vía de acceso al destino del enlace deberá especificarse utilizando una vía de acceso de archivo absoluta.

Utilice esta opción con los mandatos **restore** y **retrieve**, o en el archivo de opciones de usuario del cliente (`dsm.opt`).

Clientes soportados

Esta opción es válida para todos los clientes UNIX, a excepción de Mac OS X.

Archivo de opciones

Establezca esta opción en el archivo de opciones de cliente (dsm.opt).

Sintaxis



Parámetros

No No realiza copia de seguridad de un punto de montaje que es un enlace simbólico. No restaura un directorio si el sistema de archivos de destino de la restauración contiene un enlace simbólico con un nombre coincidente. Éste es el valor predeterminado.

Yes

Restaura el contenido de un directorio en el destino de un enlace simbólico.

Ejemplos

Archivo de opciones:

`followsymbolic Yes`

Línea de mandatos:

`-fol=Yes`

Información relacionada

Durante el archivado, la opción “Archsymlinksfile” en la página 348 determina cómo el cliente maneja los enlaces simbólicos.

Para sistemas operativos que no sean Mac OS X, consulte “Copias de seguridad de enlaces simbólicos” en la página 229 para obtener más información acerca de cómo maneja el cliente de copia de seguridad y archivado los enlaces simbólicos.

Forcefailover

La opción `forcefailover` permite al cliente migrar tras error inmediatamente al servidor secundario.

Puede utilizar la opción `forcefailover` para conectar inmediatamente con el servidor secundario, aunque el servidor primario continúe en línea. Por ejemplo, puede utilizar esta opción para verificar que el cliente de archivado de copia de seguridad está migrando tras error en el servidor secundario esperado.

No edite esta opción durante las operaciones normales.

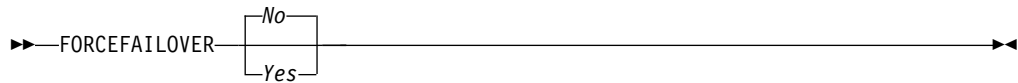
Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Coloque esta opción en el archivo de opciones del sistema cliente (dsm.sys).

Sintaxis



Parámetros

Yes

Especifica que el cliente se conecta inmediatamente al servidor secundario.

No Especifica que el cliente migra tras error al servidor secundario durante el siguiente inicio de sesión si el servidor primario no está disponible. Este es el valor predeterminado.

Ejemplos

Archivo de opciones:

```
FORCEFAILOVER yes
```

Línea de mandatos:

```
-FORCEFAILOVER=yes
```

Conceptos relacionados:

“Configuración y uso de la migración tras error automática del cliente” en la
página 94

Tareas relacionadas:

“Configuración del cliente de migración automática tras error” en la página 98

Fromdate

Utilice la opción `fromdate` con la opción `fromtime` para especificar una fecha y una hora a partir de las cuales desea buscar copias de seguridad o copias archivadas durante una operación de restauración, recuperación o consulta.

Los archivos que fueron objeto de una copia de seguridad o archivado antes de dicha fecha y hora no se incluyen, aunque podrían incluirse directorios más antiguos, si es necesario, para restaurar o recuperar los archivos.

La opción `fromdate` puede utilizarse con los mandatos siguientes:

- delete backup
- query archive
- query backup
- restore
- restore group
- retrieve

Cientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Sintaxis



Parámetros

date

Especifica la fecha a partir de la cual se desea buscar las copias de seguridad o las copias archivadas. Escriba la fecha en el formato seleccionado con la opción `dateformat`.

Si se incluye la opción `dateformat` con un mandato, ésta debe anteponerse a las opciones `fromdate`, `pitdate` y `todate`.

Ejemplos

Línea de mandatos:

```
dsmc query backup -fromdate=12/11/2003 "/Users/van/Documents/*"
```

Línea de mandatos:

```
dsmc query backup -fromdate=12/11/2003 /home/dilbert/*
```

Fromnode

La opción `fromnode` permite que un nodo realice mandatos para otro nodo. Un usuario de otro nodo debe utilizar el mandato **set access** para permitirle consultar, restaurar o recuperar archivos para el otro nodo.

La opción `fromnode` puede utilizarse con los mandatos siguientes:

- **query archive**
- **query backup**
- **query filespace**
- **query image**
- **query mgmtclass**
- **restore**
- **restore group**
- **restore image**
- **retrieve**

Clientes soportados

Esta opción es válida para todos los clientes.

Sintaxis

►► FROMNode = — — *nodo* —————►►

Parámetros

nodo

Especifica el nombre de nodo en una estación de trabajo o un servidor de archivos a cuyas copias de seguridad o copias archivadas se quiere acceder.

Ejemplos

Línea de mandatos:

```
dsmc query archive -fromnode=bob -subdir=yes "/Users/van/Documents/*"
```

Línea de mandatos:

```
dsmc query archive -fromnode=bob -subdir=yes "/home/jones/*"
```

Fromowner

La opción `fromowner` especifica un propietario alternativo del que restaurar versiones de copia de seguridad o copias archivadas o imágenes. El propietario debe otorgar acceso a otro usuario para que éste utilice los archivos o imágenes.

Por ejemplo, para restaurar archivos del directorio `/home/devel/proja` que pertenece al usuario `usermike` del sistema *puma*, y colocar los archivos restaurados en un directorio de su propiedad denominado `/home/id/proja`, introduzca el mandato siguiente:

```
dsmc restore -fromowner=usermike -fromnode=puma /home/devel/proja/  
/home/id/proja/
```

Nota: El archivado de las restauraciones de imágenes no se aplica a los sistemas operativos Mac OS X.

Los usuarios que no sean `root` pueden especificar `-fromowner=root` para acceder a los archivos propiedad del usuario `root`, si éste les ha otorgado acceso a los archivos.

Nota: si se especifica la opción `fromowner` sin la opción `fromnode`, el usuario activo debe estar en el mismo nodo que el usuario `fromowner`.

La opción `fromowner` puede utilizarse con los mandatos siguientes:

- **query archive**
- **query backup**
- **query group**
- **query image**
- **restore**
- **restore image**
- **restore group**
- **retrieve**

Clientes soportados

Esta opción es válida para todos los clientes UNIX y Linux.

Sintaxis

►► `FROMOwner =` `—propietario—` ◀◀

Parámetros

propietario

Nombre de un propietario alternativo.

Ejemplos

Línea de mandatos:

```
dsmc query archive "/home/id/proja/*" -fromowner=mark
```

Fromtime

Utilice la opción `fromtime` con la opción `fromdate` para especificar una fecha a partir de las cuales desea buscar copias de seguridad o copias archivadas durante una operación de restauración, recuperación o consulta.

El cliente de copia de seguridad y archivado pasa por alto esta opción si no especifica la opción `fromdate`.

La opción `fromtime` puede utilizarse con los mandatos siguientes:

- **delete backup**
- **query archive**
- **query backup**
- **restore**
- **restore group**
- **retrieve**

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Sintaxis

►► `FROMTime =` `— hora —` ►►

Parámetros

hora

Especifica una hora de inicio en una fecha específica a partir de la cual desea buscar copias de seguridad o copias archivadas. Si no especifica una hora, se utiliza el valor predeterminado 00:00:00. Especifique la hora en el formato seleccionado con la opción `timeformat`.

Si incluye la opción `timeformat` en un mandato, ésta deberá preceder a las opciones `fromtime`, `pittime` y `totime`.

Ejemplos

Línea de mandatos:

```
dsmc q b -timeformat=4 -fromt=11:59AM -fromd=06/30/2003 -tot=11:59PM  
-tod=06/30/2003 /home/*
```

Groupname

Utilice la opción `groupname` con el mandato **backup group** para especificar el nombre de un grupo. Sólo podrá realizar operaciones en grupos nuevos o en la versión actualmente activa del grupo.

Clientes soportados

Esta opción es válida para todos los clientes UNIX y Linux, a excepción de Mac OS X.

Sintaxis

►► `GROUPName =` `— nombre —` ►►

Parámetros

nombre

Especifica el nombre del grupo que contendrá los archivos de los que se ha

realizado una copia de seguridad utilizando la opción `filelist`. No se permite el uso de delimitadores de directorio en el nombre de grupo, ya que no se trata de una especificación de archivo sino de un campo de nombre.

Ejemplos

Línea de mandatos:

```
backup group -filelist=/home/dir1/filelist1 -groupname=group1  
-virtualfsname=/virtfs -mode=full
```

Grupos (obsoleto)

Esta opción está obsoleta.

Para obtener información sobre cómo restringir el acceso de los usuarios que no son administradores al cliente de copia de seguridad y archivado mediante un grupo de usuarios, consulte el apartado “Restricción del acceso a IBM Spectrum Protect a un grupo de usuarios” en la página 52.

Host

El host especifica la ubicación del servidor ESX de destino donde se crea la máquina virtual durante una operación de restauración de VMware.

Utilice esta opción en mandatos **restore vm** para especificar el servidor de host ESX en el que se deben restaurar los datos.



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Ejemplo

Restaura la máquina virtual en el servidor de ESX denominado `vmesxbld1`.

```
restore vm -host=vmesxbld1.us.acme.com
```

Httpport

La opción `httpport` especifica una dirección de puerto TCP/IP para el cliente web.

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. Puede establecer esta opción en el separador **Cliente web**, en el campo **Puerto HTTP** del editor de preferencias.

Sintaxis

►►—HTTPport— —port_address—►►

Parámetros

port_address

Especifica la dirección de puerto TCP/IP que se utiliza para la comunicación con el cliente web. El rango de valores es de 1000 a 32767, siendo 1581 el valor predeterminado.

Ejemplos

Archivo de opciones:

httpport 1502

Línea de mandatos:

No se aplica.

Hsmreparsetag

La opción hsmreparsetag especifica un código de reanálisis exclusivo que crea un producto HSM instalado en el sistema.

Muchos productos HSM utilizan puntos de reanálisis para recuperar archivos migrados. Tras migrar un archivo, en el sistema de archivos se deja un pequeño archivo de resguardo con el mismo nombre que el archivo original. El archivo de resguardo es un punto de reanálisis que desencadena una recuperación del archivo original cuando un usuario o una aplicación accede al archivo de resguardo. El punto de reanálisis incluye un identificador exclusivo llamado *código de reanálisis* para identificar el producto HSM que migró el archivo.

Si el cliente de archivado y copia de seguridad de IBM Spectrum Protect no reconoce el código de reanálisis en un archivo de resguardo, dicho cliente de archivado y copia de seguridad hace que el producto HSM recupere el archivo original. Puede impedir que los archivos se recuperen si especifica el código de reanálisis con la opción hsmreparsetag.

El cliente de archivado y copia de seguridad reconoce el código de reanálisis de los productos HSM de las siguientes empresas:

- International Business Machines Corp.
- Wisdata System Co. Ltd.
- BridgeHead Software Ltd.
- CommVault Systems, Inc.
- Data Storage Group, Inc.
- Enigma Data Solutions, Ltd.
- Enterprise Data Solutions, Inc.
- Global 360
- GRAU DATA AG
- Hermes Software GmbH
- Hewlett Packard Company
- International Communication Products Engineering GmbH
- KOM Networks
- Memory-Tech Corporation
- Moonwalk Universal
- Pointsoft Australia Pty. Ltd.
- Symantec Corporation

Si el producto HSM que utiliza no está en la lista anterior, utilice la opción `hsmreparsetag` para especificar el código de reanálisis. Pregunte al proveedor de su producto HSM por el código de reanálisis que utiliza el producto.

Clientes soportados

Esta opción es válida para todos los clientes Windows.

Archivo de opciones

Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`).

Sintaxis

►►—HSMREPARSETAG—*valor_código_reanálisis*————►►

Parámetros

valor_código_reanálisis

Un valor en base decimal (base 10) o hexadecimal (base 16) que especifica el código de reanálisis.

Ejemplos

Archivo de opciones:

Especifique un código de reanálisis de HSM en formato decimal:

```
hsmreparsetag 22
```

Especifique un código de reanálisis de HSM en formato hexadecimal:

```
hsmreparsetag 0x16
```

Línea de mandatos:

No se aplica.

Ieobjtype

Utilice la opción `ieobjtype` para especificar un tipo de objeto para la operación de eliminación de duplicación de datos por parte del cliente dentro de las sentencias de inclusión/exclusión.

La opción `ieobjtype` es un parámetro adicional a las opciones `include.dedup` o `exclude.dedup`.

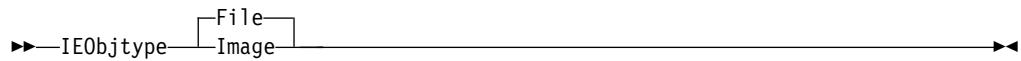
Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect también soporta esta opción.

Archivo de opciones

Establezca esta opción en el archivo de opciones del sistema (`dsm.sys`). Puede establecer esta opción en la ficha **Incluir/excluir** del editor de preferencias. La opción se puede establecer en el conjunto de opciones de cliente del servidor de IBM Spectrum Protect.

Sintaxis



Parámetros

File

Especifica que desea incluir archivos para, o excluir archivos desde, el proceso de eliminación de duplicación de datos por parte del cliente. *File* es el valor predeterminado.

Image

Especifica que desea incluir imágenes para, o excluir imágenes desde, el proceso de eliminación de duplicación de datos por parte del cliente.

Ejemplos

Archivo de opciones:

```
exclude.dedup /home/*/* ieobjtype=image
```

Línea de mandatos:

No se aplica.

Referencia relacionada:

“Opciones exclude” en la página 425

“Opciones include” en la página 458

Ifnewer

La opción *ifnewer* sustituye un archivo existente por la última versión de copia de seguridad si ésta es más reciente que el archivo existente.

Únicamente se tienen en cuenta las copias de seguridad activas, a menos que se utilicen además las opciones *inactive* o *latest*.

Nota: las entradas de directorio se sustituyen por la última versión de copia de seguridad, independientemente de si la versión de copia de seguridad es más antigua o más nueva que la versión existente.

La opción *ifnewer* puede utilizarse con los mandatos siguientes:

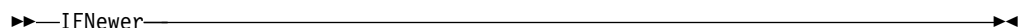
- **restore**
- **restore backupset**
- **restore group**
- **retrieve**

Nota: esta opción se pasa por alto si la opción *replace* está establecida en *No*.

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Sintaxis



Parámetros

No hay parámetros para esta opción.

Ejemplos

Línea de mandatos:

```
dsmc restore "/Users/grover/Documents/*" -sub=y -rep=y -ifnewer
```

```
dsmc restore "/home/grover/*" -sub=y -rep=y -ifnewer
```

Imagegapsize

Utilice la opción **imagegapsize** con el mandato **backup image**, en el archivo de opciones, o con la opción **include.image** para especificar el tamaño mínimo de las regiones vacías de un volumen que desea pasar por alto durante la realización de la copia de seguridad de imágenes.

Utilice esta opción para la copia de seguridad de imagen basada en LAN y sin LAN.

Por ejemplo, si especifica un tamaño de intervalo de 10, significa que no se hará copia de seguridad de una región vacía del disco que tenga más de 10 KB. Se hará copia de seguridad de los intervalos que tengan un tamaño exacto de 10 KB. Se hará una copia de seguridad de las regiones vacías que tienen exactamente 10 KB y menos de 10 KB, aunque no contengan datos. Sin embargo, se hará copia de seguridad de una región vacía que tenga menos de 10 KB, aunque no contenga datos. Un tamaño de intervalo de imagen más pequeño significa que es necesario transferir menos datos, aunque puede reducirse el rendimiento. Un tamaño de intervalo de imagen más grande implica que se transfieren más datos, aunque puede obtenerse un mayor rendimiento.

Clientes soportados

Esta opción sólo es válida para clientes AIX, Linux y JFS2. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Especifique esta opción en la stanza de servidor del archivo de opciones del sistema cliente (**dsm.sys**) o en la sentencia **include.image** del archivo **dsm.sys**.

Sintaxis

►►—IMAGEGapsize— —size—►►

Parámetros

size

Especifica el tamaño mínimo de las regiones vacías de un sistema de archivos JFS2 de AIX que debe pasarse por alto durante una copia de seguridad de imágenes. Puede especificar los calificadores **k** (kilobytes) **m** (megabytes) o **g** (gigabytes) con el valor. Si no se especifica ningún calificador, el valor se interpreta en kilobytes. Los valores válidos van de 0 a 4294967295 KB. Si especifica 0, se realizará copia de seguridad de todos los bloques, incluidos los bloques no utilizados del final del volumen. Si especifica un valor distinto de 0, no se realizará copia de seguridad de los bloques no utilizados del final del

volumen. Para la copia de seguridad de imágenes basada en red de área local y fuera de la red de área local, el valor predeterminado es 32 KB. Esta opción se aplica tanto a la copia de seguridad estática como a la basada en instantánea.

Nota: Esta opción es válida para los sistemas de archivos JFS2 de AIX. Si especifica un valor de `imagegapsize` mayor que 0 para un sistema de archivos que no sea AIX JFS2, recibirá un mensaje de aviso.

Ejemplos

Archivo de opciones:

Añada lo siguiente a la stanza de servidor del archivo `dsm.sys`:
`imagegapsize 1m`

Ejemplo de lista de inclusión/exclusión: `include.image /kalafs1`
`imagegapsize=-128k`

Línea de mandatos:

`-imagegapsize=64k`

Imagetofile

Utilice la opción `imagetofile` con el mandato **restore image** para especificar que desea restaurar la imagen de origen en un archivo.

Puede que tenga que restaurar la imagen de un archivo si existen sectores defectuosos en el volumen de destino o si desea manipular los datos de la imagen. Más tarde, puede utilizar el programa de utilidad de copia de datos que elija para transferir la imagen del archivo a un volumen de disco.

Linux admite el montaje de un archivo de imagen como volumen lógico, por lo tanto, puede obtener acceso a los datos del archivo dentro de la imagen. A continuación se muestran algunos ejemplos:

- El cliente de archivado y copia de seguridad ha realizado una copia de seguridad del sistema de archivos `/usr`. El siguiente mandato restaurará la imagen del sistema de archivos en el archivo `/home/usr.img`:

```
# dsmc restore image /usr /home/usr.img -imagetofile
```
- Para montar el archivo de imagen en el directorio `/mnt/usr`, puede ejecutarse el mandato de montaje siguiente:

```
# mount /home/usr.img /mnt/usr -o loop=/dev/loop0
```

Ahora, el contenido de la imagen está disponible desde `/mnt/usr`, como si en ese directorio se hubiera montado un sistema de archivos normal.

Clientes soportados

Esta opción solo es válida para clientes de AIX, Oracle Solaris y todos los de Linux. La API de IBM Spectrum Protect no admite esta opción.

Sintaxis

►►—IMAGETOfile—◄◄

Parámetros

No hay parámetros para esta opción.

Ejemplos

Línea de mandatos:

```
dsmc restore image /usr /home/usr.img -imagnetofile
```

Inactive

Utilice la opción `inactive` para que se visualicen los objetos activos e inactivos.

Puede utilizar la opción `inactive` con los mandatos siguientes:

- **delete group**
- **query backup**
- **query group**
- **query image**
- **query nas**
- **restore**
- **restore group**
- **restore image**
- **restore nas**

Importante: Cuando utilice la opción `inactive` durante una operación de restauración, utilice también la opción `pick` u otra opción de filtro porque, a diferencia de la opción `latest`, todas las versiones se restaurarán en un orden indeterminado. Esta opción es implícita cuando se utiliza `pitdate`.

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Sintaxis

►►—INActive—►►

Parámetros

No hay parámetros para esta opción.

Ejemplos

Línea de mandatos:

```
dsmc restore "/Users/zoe/Documents/*" -inactive -pick
```

Línea de mandatos:

```
dsmc restore "/home/zoe/*" -inactive -pick
```

Incl excl

La opción `incl excl` especifica la vía de acceso y el nombre de archivo de un archivo de opciones de inclusión/exclusión.

Se permiten varias sentencias `incl excl`. Sin embargo, debe especificar esta opción para cada archivo de inclusión/exclusión.

Asegúrese de almacenar el archivo de opciones de inclusión/exclusión en un directorio para el que todos los usuarios dispongan de acceso de lectura, como /etc.

Durante el proceso, las sentencias de inclusión/exclusión del archivo de inclusión/exclusión se colocan en la posición de lista ocupada por la opción `incl excl`, en el mismo orden, y se procesan en consecuencia.

Si se tiene el cliente de HSM instalado en la estación de trabajo, puede utilizarse un archivo de opciones de inclusión/exclusión para excluir archivos de la copia de seguridad y de la gestión de espacio o para excluir sólo de una de ambas operaciones.

Cientes soportados

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción.

Archivo de opciones

Incluya esta opción en el archivo `dsm.sys` dentro de una stanza de servidor. Puede establecer esta opción en la ficha **Incluir/excluir** del editor de preferencias.

Sintaxis

►►—INCLExcl— *—filespec—*—————►►

Parámetros

filespec

Especifica la vía de acceso y el nombre de archivo de *un* archivo de opciones de inclusión/exclusión.

Ejemplos

Archivo de opciones:

```
INCLExcl /Users/user1/Documents/backup.excl
incl excl /usr/dsm/backup.excl
incl excl /etc/incl excl.def
```

Línea de mandatos:

No se aplica.

Información relacionada

Para obtener más información acerca de la creación de un archivo de opciones de inclusión/exclusión, consulte el tema “Creación de una lista de inclusión/exclusión” en la página 124.

Consideraciones sobre los clientes habilitados para Unicode

Un archivo de inclusión/exclusión puede tener formato Unicode o que no sea Unicode.

Si el juego de códigos utilizado para crear un archivo de lista de inclusión/exclusión no coincide con el juego de códigos utilizado en el sistema

cliente, los caracteres del archivo no correlacionados mediante el juego de códigos del cliente con un carácter visualizable no se podrán procesar cuando se realicen las copias de seguridad.

El uso de codificación Unicode para los archivos que contienen listas de inclusión/exclusión elimina el problema de caracteres sin correlacionar, por lo que ya no tendrá que utilizar caracteres comodín como sustitutos de los caracteres no reconocidos.

Usuarios de Mac: deben crear un archivo de inclusión/exclusión en formato Unicode mediante estos pasos:

1. Abra TextEdit. Pulse **Format > Make PlainText**.
2. Especifique las sentencias `include` y `exclude`.
3. Pulse **Archivo** y después en **Guardar como**.
4. En **PlainText Encoding**, seleccione **Unicode (UTF-8)** o **Unicode (UTF-16)**, especifique el archivo y directorio de destino y, a continuación, guarde el archivo. No añada la extensión `.txt`.
5. Incluya una opción `incl excl` que especifique el archivo de inclusión/exclusión que acaba de crear en el archivo `dsm.sys`.
6. Reinicie el cliente de archivado y copia de seguridad.

Opciones include

Las opciones `include` especifican los objetos que desea incluir para los servicios de copia de seguridad y archivado.

Las opciones de inclusión especifican cualquiera de los elementos siguientes:

- Objetos de un amplio grupo de objetos excluidos que desea incluir para los servicios de copia de seguridad y archivado.
- Objetos de un amplio grupo de objetos excluidos que desea incluir para los servicios de copia de seguridad, archivado, imagen y gestión de espacio.
- Archivos que se incluyen para el proceso de copia de seguridad o archivado que también desea incluir para el proceso de cifrado.
- Archivos que se incluyen para el proceso de copia de seguridad o archivado que desea incluir en el proceso de compresión.
- Objetos a los que se desea asignar una clase de gestión específica.
- Una clase de gestión para asignar a todos los objetos a los que no se asigna una clase de gestión de forma explícita.
- Espacios de archivos a que se desea asignar un proceso de copia de seguridad de memoria eficiente
- Espacios de archivo para los que desea utilizar la opción `diskcachelocation` con el fin de que sistemas de archivos específicos utilicen ubicaciones específicas distintas para la caché en disco de éstos.

Si no se asigna una clase de gestión específica a los objetos, se utiliza la clase de gestión predeterminada del conjunto de políticas activo del dominio de políticas. Utilice el mandato **query mgmtclass** para visualizar información sobre las clases de gestión disponibles en el conjunto de políticas activo.

Recuerde: El cliente de copia de seguridad y archivado compara los archivos que procesa con los patrones especificados en las sentencias de inclusión y exclusión leyéndolas de abajo arriba en el archivo de opciones.

Nota:

1. Las sentencias `exclude.fs` y `exclude.dir` modifican temporalmente todas las sentencias de inclusión que coinciden con el patrón.
2. El servidor también puede definir estas opciones con la opción `incl excl`.

Clientes soportados

Esta opción es válida para todos los clientes. El servidor también puede definir la opción `include.fs.nas`.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. Puede establecer estas opciones en el separador **Incluir/excluir** del editor de preferencias.

Sintaxis

►► `—opciones— —patrón—` —parámetro opcional— ►►

include, include.backup, include.file

Utilice estas opciones para incluir archivos o asignar clases de gestión para el proceso de copias de seguridad.

La opción `include` afecta al proceso de archivado y copia de seguridad. Si desea asignar distintas clases de gestión para proceso de archivado y copia de seguridad, especifique siempre `include.archive` y `include.backup` con sus propias clases de gestión. En el ejemplo siguiente, la clase de gestión `archmc` se asigna cuando se realiza una operación de archivado. La clase de gestión se asigna cuando se realiza una operación de archivado, puesto que `include.backup` utiliza solo para el proceso de copias de seguridad; no se utiliza para el proceso de archivado.

```
include.archive /home/test/* archmc
include.backup /home/test/*
```

include.archive

Incluye archivos o asigna clases de gestión para los procesos de archivado.

include.attribute.symlink

Incluye un archivo o un grupo de archivos que son enlaces simbólicos o alias en un grupo amplio de archivos excluidos del proceso de copia de seguridad únicamente.

Nota: Para Mac OS X, se incluyen los alias.

include.compression

Incluye archivos para el proceso de compresión si establece la opción `compression` en `yes`. Esta opción se aplica a copias de seguridad y copias archivadas.

include.dedup

Incluye archivos para la eliminación de duplicados de datos por parte del cliente. Para controlar una operación de eliminación de duplicados de datos por parte del cliente, especifique `ieobjtype` como valor de la opción `include.dedup`. De forma predeterminada, todos objetos elegibles por

eliminación de duplicación de datos se incluyen en la eliminación de duplicación de datos por parte del cliente.

Los parámetros ieobjtype válidos son:

Archivo
Imagen

El valor predeterminado es File.

include.encrypt

Incluye los archivos especificados para el proceso de cifrado. De forma predeterminada, el cliente no realiza el proceso de cifrado.

Notas:

1. El cifrado solo puede habilitarse en el cliente de copia de seguridad/archivado mediante la opción `include.encrypt`. Si no se utiliza ninguna sentencia `include.encrypt`, no se realizará el cifrado.
2. El cifrado no es compatible con la deduplicación del lado del cliente. Los archivos que se incluyen para el cifrado no se deduplican mediante la deduplicación del lado del cliente.
3. El cifrado no es compatible con las copias de seguridad de máquina virtual VMware que utilizan las modalidades de copia de seguridad siempre incremental (`MODE=IFIncremental` y `MODE=IFFull`). Si el cliente se configura para el cifrado, no se puede utilizar la copia de seguridad siempre incremental.
4. El cifrado no es compatible con IBM Spectrum Protect for Virtual Environments Data Protection for VMware Recovery Agent. Si el cliente se configura para cifrado, puede utilizar el cliente para restaurar las copias de seguridad que se hayan creado con las modalidades de copia de seguridad completa o incremental (`MODE=Full` y `MODE=Incremental`). Sin embargo, no puede utilizar Recovery Agent para restaurar las copias de seguridad cifradas. Las copias de seguridad creadas con la modalidad completa o incremental se han creado con el cliente de la versión 7.1 o anterior.

include.fs

Para los sistemas de archivos JFS2 de AIX: utilice la opción `snapshotcachesize` en el archivo `dsm.sys` o con la opción `include.fs` para especificar un tamaño de instantánea adecuado que permita que todos los bloques de datos antiguos puedan almacenarse mientras tiene lugar la operación de archivado o de copia de seguridad de archivos basada en instantánea.

Para controlar la forma en que el cliente ha de procesar el espacio de archivos para la copia de seguridad incremental, puede especificar estas opciones adicionales en el archivo `dsm.sys`, como valores de la opción `include.fs`: `diskcachelocation` y `memoryefficientbackup`.

Cada una de las opciones `include.fs`, `memoryefficientbackup` y `diskcachelocation` debe estar en la misma línea en el archivo de opciones.

```
include.fs /home
memoryefficientbackup=diskcachemethod
diskcachelocation=/usr
include.fs /usr
memoryefficientbackup=diskcachemethod
diskcachelocation=/home
include.fs /Volumes/hfs3
memoryefficientbackup=diskcachemethod
diskcachelocation=/Volumes/hfs2
AIX JFS2 filesystems only: include.fs
/kalafs1 snapshotproviderfs=JFS2
```


Si estas opciones aparecen en el archivo de opciones y una opción `include.fs`, los valores de `include.fs` se utilizarán para el espacio del archivo especificado en lugar de los valores de un archivo de opciones o de la línea de mandatos.

include.fs.nas

Utilice la opción `include.fs.nas` para vincular una clase de gestión a sistemas de archivos de almacenamiento conectado a red (NAS). También puede especificar si el cliente ha de guardar la información de la Tabla de contenido (TOC) durante una copia de seguridad de imágenes del sistema de archivos NAS, mediante la utilización de la opción `toc` con la opción `include.fs.nas` en el archivo `dsm.sys`. Esta opción solo es válida para los clientes AIX y Solaris.

include.image

Incluye un espacio de archivos o un volumen lógico o asigna una clase de gestión si se utiliza con el mandato **backup image**. El mandato **backup image** ignora todas las demás opciones de inclusión.

Para los clientes Linux x86_64: Utilice la opción `snapshotcachesize` en las siguientes situaciones:

- Con el mandato **backup image**
- En el archivo `dsm.sys`
- Con la opción `include.image`

Utilizar la opción `snapshotcachesize` en estas situaciones le permite especificar un tamaño de instantánea adecuado para que todos los bloques de datos antiguos se puedan almacenar mientras se realiza la copia de seguridad de imagen.

Un tamaño de instantánea del 100% asegurará que la instantánea sea válida.

Para los clientes AIX JFS2_systems: Utilice la opción `snapshotcachesize` en las siguientes situaciones:

- Con el mandato **backup image**
- En el archivo `dsm.sys`
- Con la opción `include.image`

Utilizar la opción `snapshotcachesize` en estas situaciones le permite especificar un tamaño de instantánea adecuado para que todos los bloques de datos antiguos se puedan almacenar mientras se realiza la copia de seguridad de imagen.

Esta opción es válida para clientes de AIX, Linux y Oracle Solaris.

Parámetros

pattern

Especifica los objetos para incluir en el proceso de copia de seguridad o archivado o para asignar una clase de gestión específica.

Nota: en sistemas de archivos NAS, debe añadir un prefijo de nombre de nodo NAS a la especificación de archivo para indicar el servidor de archivos al que se aplica la sentencia de inclusión. Si no especifica un nombre de nodo NAS, el sistema de archivos identificado hará referencia al nombre de nodo NAS que se ha especificado en el archivo de opciones del cliente (`dsm.sys`) o en la línea de mandatos.

Si el patrón comienza con comillas dobles o simples, contiene espacios en blanco intercalados o signos de igual, debe incluir el valor entre comillas simples (') o comillas dobles ("). Los signos que se utilicen para la apertura y el cierre deben ser del mismo tipo.

Para la opción `include.image`, el patrón es el nombre de un sistema de archivos montado o de un volumen lógico RAW.

parámetro_opcional

mgmtclassname

Especifica el nombre de la clase de gestión que se desea asignar a los objetos. Si no especifica ninguna clase de gestión, se utiliza la clase de gestión predeterminada. Para asociar una clase de gestión con un grupo de copia de seguridad en una sentencia de inclusión, utilice la sintaxis siguiente:

```
include virtual_filespace_name\group_name management_class_name
```

donde:

virtual_filespace_name

Especifica el nombre del espacio de archivos virtual del servidor de IBM Spectrum Protect que ha asociado con el grupo, en el mandato **Backup Group**.

group_name

Es el nombre del grupo que ha creado al ejecutar el mandato **Backup Group**.

management_class_name

Es el nombre de la clase de gestión a asociar con los archivos del grupo.

Por ejemplo, un grupo denominado MyGroup se almacena en un espacio de archivos virtual denominado MyVirtualFileSpace. Para asociar una clase de gestión, denominada TEST, con el grupo, utilice la sintaxis siguiente:

```
include MyVirtualFileSpace/MyGroup TEST
```

Tabla 74. Otros parámetros opcionales

parámetro_opcional	Utilizar con la opción
ieobjtype "Ieobjtype" en la página 452	include.dedup
memoryefficientbackup "Memoryefficientbackup" en la página 491	include.fs
diskcachelocation "Diskcachelocation" en la página 393	include.fs
dynamicimage "Dynamicimage" en la página 410	include.image
postsnapshotcmd "Postsnapshotcmd" en la página 516	include.image
presnapshotcmd "Presnapshotcmd" en la página 523	include.image
snapshotcachesize "Snapshotcachesize" en la página 567	include.image
snapshotproviderfs "Snapshotproviderfs" en la página 569	include.image

Tabla 74. Otros parámetros opcionales (continuación)

parámetro_opcional	Utilizar con la opción
snapshotproviderimage "Snapshotproviderimage" en la página 570	include.image

Ejemplos

Archivo de opciones:

```
include /home/proj/text/devel.*
include /home/proj/text/* textfiles
include * managall
include /WAS_ND_NDNODE mgmtclass
include /WAS_APPNODE mgmtclass
include.image /home
include.archive /home/proj/text/
    * myarchiveclass
include.backup /home/proj/text/
    * mybackupclass
include.compression /home/proj/text/
    devel.*
include.encrypt /home/proj/gordon/*
include.fs.nas netappsj/vol/vol0
    homemgmtclass

include.dedup /Users/Administrator/Documents/Important/.../*
AIX only:
```

```
include.image /home
    MGMTCLASSNAME
    snapshotproviderimage=JFS2
    snapshotcachesize=40
include.image /home
    snapshotproviderimage=NONE
include.fs /kalafsl
    snapshotproviderfs=JFS2
```

LINUX only:

```
include.image /home
    snapshotproviderimage=LINUX_LVM
include.image /myfs1 dynamicimage=yes
include.image /home MGMTCLASSNAME
    snapshotproviderimage=NONE
include.image /myfs1 dynamicimage=yes
include.attribute.symlink /home/spike/.../*
include.fs /usr
    memoryefficientbackup=diskcachemethod
```

Línea de mandatos:

No se aplica.

Referencia relacionada:

"Snapshotcachesize" en la página 567

"Toc" en la página 596

Información relacionada:

➞ Mandato mmbackup: Requisitos de IBM Spectrum Protect

➞ Orientación para integrar IBM Spectrum Scale AFM con IBM Spectrum Protect

➞ Utilización de las opciones de inclusión y exclusión de IBM Spectrum Protect con el mandato mmbackup de IBM Spectrum Scale

Control del proceso de enlaces simbólicos y alias

IBM Spectrum Protect trata los enlaces simbólicos y los alias (los alias se aplican sólo a Mac OS X) como archivos reales y realiza una copia de seguridad de los mismos. No obstante, no se realiza una copia de seguridad del archivo al que hace referencia el vínculo simbólico.

En algunos casos, los enlaces simbólicos y los alias pueden volver a crearse fácilmente y no es necesario realizar una copia de seguridad de los mismos. Además, realizar una copia de seguridad de estos enlaces simbólicos o alias puede incrementar el tiempo de proceso de la copia de seguridad y puede ocupar un volumen de espacio notable en el servidor de IBM Spectrum Protect.

Para excluir un archivo o un grupo de archivos que sean enlaces simbólicos o alias del proceso de copia de seguridad puede utilizar la opción `exclude.attribute.symlink`. Si es necesario, puede utilizar la opción `include.attribute.symlink` para incluir enlaces simbólicos o alias en un grupo amplio de archivos excluidos para el proceso de copia de seguridad. Por ejemplo, para excluir todos los enlaces simbólicos o alias del proceso de copia de seguridad, excepto los que existen en el directorio `/home/spike`, especifique estas sentencias en el archivo `dsm.sys`:

```
exclude.attribute.symlink  /.../*
include.attribute.symlink  /home/spike/.../*
```

Referencia relacionada:

“Opciones exclude” en la página 425

Proceso de compresión y cifrado de copia de seguridad

En este tema se indican diversos aspectos que han de tenerse en cuenta si desea incluir archivos o grupos de archivos específicos para el proceso de compresión y cifrado durante una operación de copia de seguridad o archivado.

- Debe establecer la opción `compression` en *yes* para activar el proceso de compresión. Si no especifica la opción `compression` o si establece la opción `compression` en *no*, el cliente de copia de seguridad y archivado no realizará el proceso de compresión.
- El cliente procesará `exclude.fs`, `exclude.dir`, y otras sentencias de inclusión/exclusión en primer lugar. A continuación, el cliente considerará las sentencias `include.compression` e `include.encrypt`. Por ejemplo, considerando la siguiente lista de inclusión/exclusión:

```
exclude /home/jones/proj1/file.txt
include.compression /home/jones/proj1/file.txt
include.encrypt /home/jones/proj1/file.txt
```

El cliente examinará en primer lugar la sentencia `exclude /home/jones/proj1/file.txt` y determinará que `/home/jones/proj1/file.txt` ha de excluirse del proceso de copia de seguridad y que, por lo tanto, no es candidato para el proceso de compresión y cifrado.

- El proceso de compresión de inclusión/exclusión y de cifrado es válido *sólo* para procesos de copias de seguridad/archivado.

Referencia relacionada:

“Compression” en la página 370

Proceso de sistemas de archivos NAS

Utilice la opción `include.fs.nas` para asociar una clase de gestión a sistemas de archivos NAS y para controlar si la información de la tabla de contenido se guarda para la copia de seguridad del sistema de archivos.

Nota: La opción `include.fs.nas` no es válida para una copia de seguridad incremental por diferencia de instantánea.

Una especificación del sistema de archivos NAS utiliza los convenios siguientes:

- Los nodos NAS representan un nuevo tipo de nodo. El nombre de nodo NAS identifica de forma exclusiva un servidor de archivos NAS y sus datos en el cliente de copia de seguridad y archivado. Puede añadir un prefijo de nombre de nodo NAS en la especificación de archivo para indicar el servidor de archivos al que se aplica la sentencia de inclusión. Si no especifica un nombre de nodo NAS, el sistema de archivos que especifique se aplica a todos los servidores de archivos NAS.
- Con independencia del sistema operativo de cliente utilizado, las especificaciones de sistema de archivos NAS utilizan la barra inclinada (/) como separador, tal como se muestra en el siguiente ejemplo: `/vol/vol0`.

Utilice esta sintaxis:

►► *patrón* — *mgmtclassname* — *toc=valor* —◄◄

Donde:

patrón

Especifica los objetos para incluir en los servicios de copia de seguridad, para asignar una clase de gestión específica o para controlar la creación de TOC. Puede utilizar caracteres comodín en el patrón.

mgmtclassname

Especifica el nombre de la clase de gestión que se desea asignar a los objetos. Si no especifica ninguna clase de gestión, se utiliza la clase de gestión predeterminada.

toc=valor

Para obtener más información, consulte “Toc” en la página 596.

Ejemplo 1: para asignar una clase de gestión al sistema de archivos `/vol/vol1` de un nodo NAS denominado `netappsj`, especifique la sentencia de inclusión siguiente:

```
include.fs.nas netappsj/vol/vol1 nasMgmtClass toc=yes
```

Ejemplo 2: para asignar la misma clase de gestión a todas las vías de acceso que están subordinadas al sistema de archivos `/vol/` en un nodo NAS denominado `netappsj` (por ejemplo, `/vol/vol1`, `/vol/vol2`, y `/vol/vol3`), especifique la siguiente sentencia de inclusión:

```
include.fs.nas netappsj/vol/* nasMgmtClass toc=yes
```

Opciones `include` de la máquina virtual

Las opciones de inclusión y exclusión de la máquina virtual influyen en el comportamiento de las operaciones de copia de seguridad y restauración de máquinas virtuales. Estas opciones se procesan antes de procesar cualquier opción de línea de mandatos, por lo que las opciones en la línea de mandatos pueden alterar temporalmente las opciones especificadas en cualquiera de las opciones de inclusión o de exclusión de la máquina virtual. Consulte las descripciones de opciones individuales para obtener información sobre las opciones.



Las operaciones de máquina virtual solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments.

Referencia relacionada:

“Include.vmdisk” en la página 467

“INCLUDE.VMTSMVSS” en la página 472

“INCLUDE.VMSNAPSHOTATTEMPTS” en la página 469

Include.vm:

En operaciones de Hyper-V o VMware, esta opción altera temporalmente la clase de gestión que se especifica en la opción vmc.



Las operaciones de máquina virtual solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments.

La clase de gestión especificado en la opción vmc se aplica a todas las copias de seguridad Hyper-V y VMware. Puede utilizar la opción include.vm para alterar temporalmente dicha clase de gestión, para una o varias máquinas virtuales. La opción include.vm > no modifica ni afecta a la clase de gestión que especifica la opción vmc. La opción vmc vincula los archivos de control de la máquina virtual con máquina virtual a una clase de gestión específica.

Clientes soportados

Esta opción se puede utilizar con clientes Linux soportados configurados para hacer copias de seguridad de máquinas virtuales VMware.

Archivo de opciones

Establezca esta opción en el archivo de opciones del cliente.

Sintaxis

```

>> INCLUDE.VM —vmname— —mgmtclassname—

```

Parámetros

vmname

Parámetro obligatorio. Especifica el nombre de una máquina virtual que desea vincular a la clase de gestión especificada. El nombre es el de visualización de la máquina virtual. Solo se puede especificar una máquina virtual en cada sentencia include.vm. Sin embargo, pueden especificarse tantas sentencias include.vm como desee para vincular cada máquina virtual a una clase de gestión específica.

Puede incluir caracteres comodín en el nombre de la máquina virtual. Un asterisco (*) coincide con cualquier serie de caracteres. El signo de interrogación (?) coincide con un solo carácter. Si el nombre de la máquina virtual contiene un carácter de espacio, escriba el nombre entre comillas dobles (").

Consejo: Si el nombre de la máquina virtual contiene caracteres especiales, escriba el carácter comodín signo de interrogación en lugar de los caracteres especiales cuando especifique el nombre de la máquina virtual.

mgmtclassname

Parámetro opcional. Especifica la clase de gestión que se debe utilizar cuando se realice la copia de seguridad de la máquina virtual. Si este parámetro no se especifica, la clase de gestión predeterminada para la clase de gestión de la máquina virtual se especifica mediante la opción *vmmc*.

Ejemplos

Supongamos que las siguientes clases de gestión existen y están activas en el servidor de IBM Spectrum Protect:

- MCFORTESTVMS
- MCFORPRODVMS
- MCUNIQUEVM

Ejemplo 1

La siguiente sentencia *include.vm* en el archivo de opciones del cliente vincula todas las máquinas virtuales con nombres que comienzan por VMTEST a la clase de gestión denominada MCFORTESTVMS:

```
include.vm vmtest* MCFORTESTVMS
```

Ejemplo 2

La siguiente sentencia *include.vm* del archivo de opciones del cliente vincula una máquina virtual denominada WHOPPER VM1 [PRODUCTION] con la clase de gestión denominada MCFORPRODVMS:

```
include.vm "WHOPPER VM1 ?PRODUCTION?" MCFORPRODVMS
```

El nombre de la máquina virtual debe especificarse entre comillas porque contiene caracteres de espacio. Además, se utiliza el carácter comodín signo de interrogación para que coincida con los caracteres especiales en el nombre de la máquina virtual.

Ejemplo 3

La siguiente sentencia *include.vm* del archivo de opciones del cliente vincula una máquina virtual denominada VM1 a la clase de gestión MCUNIQUEVM:

```
include.vm VM1 MCUNIQUEVM
```

Información relacionada

“Vmmc” en la página 631

Include.vmdisk:

La opción *INCLUDE.VMDISK* incluye un disco de la máquina virtual de VMware en la operación de copia de seguridad. Si no especifica una o más etiquetas de disco, se realiza una copia de seguridad de todos los discos en la máquina virtual.

Esta opción solo está disponible si se utiliza el producto bajo licencia IBM Spectrum Protect for Virtual Environments. Para obtener información adicional sobre esta opción, consulte la documentación del producto IBM Spectrum Protect for Virtual Environments en el IBM Knowledge Center en <http://www.ibm.com/support/knowledgecenter/SSERB6/welcome>.

La opción `INCLUDE.VMDISK` especifica la etiqueta del disco de una máquina virtual que debe incluirse en una operación **Backup VM**. Si incluye un disco en el mandato **Backup VM**, los parámetros de línea de mandatos alteran temporalmente cualquier sentencia `INCLUDE.VMDISK` en el archivo de opciones.

Clientes soportados

Esta opción puede utilizarse con clientes Linux x86_64 soportados.

Archivo de opciones

Establezca esta opción en el archivo de opciones del cliente. Los parámetros de línea de mandatos alteran temporalmente las sentencias en el archivo de opciones.

Sintaxis

►► `INCLUDE.VMDISK—vmname—vmdk_label` ◀◀

Parámetros

vmname

Especifica el nombre de la máquina virtual que contiene un disco que desea incluir en una operación **Backup VM**. El nombre es el de visualización de la máquina virtual. Solo puede especificar un nombre de máquina virtual en cada sentencia `INCLUDE.VMDISK`. Especifique sentencias `INCLUDE.VMDISK` adicionales para cada disco de máquina virtual a incluir.

El nombre de la máquina virtual puede contener un asterisco (*) para que coincida con cualquier serie de caracteres y el signo de interrogación (?) para que coincida con cualquier carácter. Entrecomille el nombre de máquina (" ") si el nombre de máquina contiene caracteres de espacio.

Consejo: Si el nombre de la máquina virtual contiene caracteres especiales, como por ejemplo corchetes ([o]), puede ser que el nombre de la máquina virtual no coincida correctamente. Si un nombre de máquina virtual utiliza caracteres especiales en el nombre, puede que necesite utilizar el carácter de interrogación (?) para que coincida con los caracteres especiales en el nombre de la máquina virtual.

Por ejemplo, para incluir Hard Disk 1 en la copia de seguridad de una máquina virtual denominada "Windows VM3 [2012R2]", utilice esta sintaxis en el archivo de opciones: `INCLUDE.VMDISK "Windows VM3 ?2012R2?" "Hard Disk 1"`

vmdk_label

Especifica la etiqueta de disco del disco que desea incluir. Los caracteres comodín no están permitidos. Utilice el mandato **Backup VM** con la opción `-preview` para determinar las etiquetas de disco de discos en una máquina virtual determinada. Consulte "**Backup VM**" en la página 683 para conocer la sintaxis.

Ejemplos

Archivo de opciones

Suponga que una máquina virtual denominada `vm1` contiene cuatro discos,

etiquetados como Disco duro 1, Disco duro 2, Disco duro 3 y Disco duro 4. Para incluir solo el Disco 2 en una operación **Backup VM**, especifique lo siguiente en el archivo de opciones:

```
INCLUDE.VMDISK "vm1" "Hard Disk 2"
```

Incluir los discos 2 y 3 en operaciones **Backup VM**:

```
INCLUDE.VMDISK "vm1" "Hard Disk 2"  
INCLUDE.VMDISK "vm1" "Hard Disk 3"
```

Línea de mandatos

Incluir un único disco cuando se realiza una copia de seguridad de vm1:

```
dsmc backup vm "vm1:vmdk=Hard Disk 1"
```

Incluir el disco duro 2 y el disco duro 3 en vm1:

```
dsmc backup vm "vm1:vmdk=Disco duro 2:vmdk=Disco duro 3"
```

Referencia relacionada:

“**Backup VM**” en la página 683

“**Restore VM**” en la página 764

“Domain.vmfull” en la página 401

“Exclude.vmdisk” en la página 430

INCLUDE.VMSNAPSHOTATTEMPTS:

Para operaciones de copia de seguridad de VMware, esta opción determina el número total de intentos de instantánea para probar una máquina virtual VMware que falla durante el procesamiento de copia de seguridad debido a un error de instantánea.

Clientes soportados



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Esta opción se puede utilizar con clientes Linux soportados configurados para hacer copias de seguridad de máquinas virtuales VMware.

Archivo de opciones

Establezca esta opción en el archivo de opciones del cliente.

Sintaxis

```
►►—INCLUDE.VMSNAPSHOTATTEMPTS—nombremv—núm_con_detención—núm_sin_detención—◄◄
```

Parámetros

vmname

Esto es un parámetro posicional obligatorio. Especifica el nombre de la máquina virtual para intentar el número total de instantáneas, si un intento de copia de seguridad falla debido a un error de instantánea. El nombre es el de visualización de la máquina virtual.

Sólo se puede especificar una máquina virtual en cada sentencia INCLUDE.VMSNAPSHOTATTEMPTS. Sin embargo, para configurar los intentos de instantáneas totales para otras máquinas virtuales, puede utilizar los métodos siguientes:

- Especifique tantas sentencias INCLUDE.VMSNAPSHOTATTEMPTS como sea necesario para que se reintenten las instantáneas fallidas, para cada máquina virtual en la que desee que se aplique esta opción.
- Utilice caracteres comodín en **vmname** para seleccionar nombres de máquina virtual que coincidan con el patrón de comodín. Un asterisco (*) coincide con cualquier serie de caracteres. El signo de interrogación (?) coincide con un solo carácter. Si el nombre de la máquina virtual contiene un carácter de espacio, escriba el nombre entre comillas dobles ("").

Consejo: Si el nombre de la máquina virtual contiene caracteres especiales, escriba el carácter de comodín de signo de interrogación (?) en lugar de los caracteres especiales cuando especifique el nombre de la máquina virtual.

núm_con_detención

Esto es un parámetro posicional que especifica la siguiente acción:

- Para máquinas virtuales de Windows con la protección de aplicaciones de IBM Spectrum Protect habilitada, *núm_con_detención* especifica el número de veces que se intentará la instantánea con detención de VSS de IBM Spectrum Protect y detención de VSS del proveedor de sistema Microsoft Windows. La detención de VSS solo se aplica a máquinas virtuales Windows.

Según el número especificado, el primer intento de instantánea se realiza siempre con detención de VSS de IBM Spectrum Protect. Los siguientes intentos de instantánea se realizan con detención de VSS del proveedor de sistema Windows.

- En el caso de máquinas virtuales de Windows sin protección de aplicación de IBM Spectrum Protect habilitada y en el caso de las máquinas virtuales de Linux, *núm_con_detención* especifica el número de veces que es necesario intentar realizar la instantánea con detención del sistema de archivos de herramientas de VMware.

El valor máximo que puede especificar es diez (10). El valor predeterminado es dos (2). El valor mínimo que puede especificar es cero (0).

núm_sin_detención

Éste es un parámetro posicional que especifica el número de veces que se intentará la instantánea con la detención del sistema de archivos de herramientas de VMware Tools y la detención de aplicaciones (VSS) inhabilitadas, una vez completado el número especificado de intentos con detención de VSS (*núm_sin_detención*). Por ejemplo, puede especificar este parámetro para una máquina virtual que ya está protegida por un agente IBM Data Protection instalado en una máquina virtual huésped.

El valor máximo que puede especificar es diez (10). El valor mínimo que puede especificar es cero (0), que es el valor predeterminado.

Importante: Cuando este parámetro se aplica a una copia de seguridad de máquina virtual, la copia de seguridad no resulta afectada si se detiene el sistema.. Como resultado, no se garantiza la consistencia de las aplicaciones, el sistema de archivos o el sistema operativo. Un entrada `include.vmsnapshotattempts 0 0` no es válida. Las operaciones de copia de seguridad requieren como mínimo una instantánea.

Ejemplos

Ejemplo 1

La siguiente sentencia INCLUDE.VMSNAPSHOTATTEMPTS del archivo de opciones de cliente realiza dos intentos de instantánea total (con detención de VSS) para la máquina virtual VM_a:

```
INCLUDE.VMSNAPSHOTATTEMPTS VM_a 2 0
```

Ejemplo 2

La siguiente sentencia INCLUDE.VMSNAPSHOTATTEMPTS del archivo de opciones de cliente realiza tres intentos de instantánea total para las máquinas virtuales de Windows que coinciden con la serie vmServer_Dept*:

- El primer intento se realiza con la detención de VSS de IBM Spectrum Protect.
- El segundo intento se realiza con la detención de VSS del proveedor de sistema de Windows.
- El tercer intento de instantánea se realiza sin detención de VSS.

```
INCLUDE.VMSNAPSHOTATTEMPTS vmServer_Dept* 2 1
```

Ejemplo 3

La siguiente sentencia INCLUDE.VMSNAPSHOTATTEMPTS del archivo de opciones de cliente realiza un intento de instantánea total (con detención de VSS) para las máquinas virtuales que coincidan con la serie vmDB_Dept*:

```
INCLUDE.VMSNAPSHOTATTEMPTS vmDB_Dept* 1 0
```

Ejemplo 4

La siguiente sentencia INCLUDE.VMSNAPSHOTATTEMPTS del archivo de opciones de cliente realiza dos intentos de instantánea total (con detención de VSS) para todas las máquinas virtuales.

- El primer intento se realiza con la detención de VSS de IBM Spectrum Protect.
- El segundo intento se realiza con la detención de VSS del proveedor de sistema de Windows.

```
INCLUDE.VMSNAPSHOTATTEMPTS * 2 0
```

Ejemplo 5

En este ejemplo, la máquina virtual DB15 tiene un agente IBM Data Protection instalado en la máquina virtual huésped y no necesita una instantánea coherente con la aplicación. La siguiente sentencia INCLUDE.VMSNAPSHOTATTEMPTS del archivo de opciones de cliente realiza un intento de instantánea total (con detención de VSS) para la máquina virtual DB15:

```
INCLUDE.VMSNAPSHOTATTEMPTS DB15 0 1
```

Importante: Para máquinas virtuales de Windows: Si intenta ejecutar una restauración de máquina virtual completa de una copia de seguridad de protección de aplicaciones creada con 2 o más intentos de instantánea, la instantánea del proveedor de sistema estará presente en la máquina virtual restaurada. A medida que la aplicación escriba en el disco, el espacio de almacenamiento de instantáneas crecerá hasta que se quede sin espacio en disco.

En general, si se ha utilizado la protección de aplicaciones durante una copia de seguridad, utilice solo la restauración de la protección de aplicaciones. Al restaurar

la aplicación, el volumen se revierte automáticamente. Sin embargo, si tiene que restaurar la máquina virtual completa, debe revertir o suprimir la instantánea.

Una vez restaurada la máquina virtual completa, asegúrese de que la restauración se haya realizado correctamente y de que los datos no estén dañados. Si los datos no están dañados, suprima la instantánea. Si los datos están dañados, revierta la instantánea para restaurar la integridad de los datos.

Puede determinar qué instantánea suprimir o revertir buscando el archivo `dsmShadowCopyID.txt` en el directorio raíz de cada volumen restaurado. Este archivo contiene los ID de las instantáneas creadas durante los intentos de instantánea. Puede utilizar el mandato de **diskshadow delete shadows** para suprimir estos ID, o bien el mandato **revert** para revertir la instantánea. Una vez completadas la supresión o la reversión, también puede suprimir el archivo `dsmShadowCopyID.txt`.

Referencia relacionada:

`"INCLUDE.VMTSMVSS"`

INCLUDE.VMTSMVSS:

La opción `INCLUDE.VMTSMVSS` notifica a las aplicaciones de máquina virtual que está a punto de producirse una copia de seguridad. Esta opción permite a la aplicación truncar registros de transacciones y confirmar transacciones, de forma que la aplicación se pueda reanudar de un estado coherente cuando haya finalizado la copia de seguridad. Se puede especificar un parámetro opcional para suprimir el recorte de los registros de transacciones. Para utilizar esta opción, tiene que tener un acuerdo de licencia para utilizar IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Cuando esta opción incluye una máquina virtual, IBM Spectrum Protect proporciona protección de aplicaciones. Es decir, el cliente se congela y desbloquea los grabadores VSS y, opcionalmente, trunca los registros de la aplicación. Si una máquina virtual no está protegida por esta opción, VMware proporciona protección de aplicaciones y bloquea y desbloquea los grabadores VSS, pero los registros de aplicación no se truncan.

Clientes soportados

Esta opción puede utilizarse con clientes Linux x86_64 soportados.

Archivo de opciones

Establezca esta opción en el archivo de opciones del cliente. Esta opción no se puede establecer mediante el editor de preferencias o en la línea de mandatos.

Sintaxis

►► `INCLUDE.VMTSMVSS` *nombre_máquina_virtual* `— —OPTions=KEEPSqllog` ◀◀

Parámetros

vmname

Especifica el nombre de la máquina virtual que contiene las aplicaciones que desea proteger. El nombre es el de visualización de la máquina virtual.

Especifique una máquina virtual por cada sentencia `INCLUDE.VMTSMVSS`. Por

ejemplo, para incluir una máquina virtual denominada Windows VM3 [2012R2], utilice esta sintaxis en el archivo de opciones: INCLUDE.VMTSMVSS "Windows VM3 [2012R2]".

Para proteger todas las máquinas virtuales con esta opción, utilice un asterisco como un comodín (INCLUDE.VMTSMVSS *). También puede utilizar signos de interrogación para hacer coincidir cualquier carácter único. Por ejemplo, INCLUDE.VMTSMVSS vm?? protege todas las máquinas virtuales que tienen nombres que empiezan por vm y que están seguidas por dos caracteres cualquiera (vm10, vm11, vm17, etc.).

Consejo: Si el nombre de la máquina virtual contiene caracteres especiales, como por ejemplo corchetes ([o]), puede ser que el nombre de la máquina virtual no coincida correctamente. Si un nombre de máquina virtual utiliza caracteres especiales en el nombre, puede utilizar el carácter de interrogación (?) para que coincida con los caracteres especiales en el nombre de la máquina virtual.

No existe ningún valor predeterminado para este parámetro. Para habilitar la protección de aplicaciones, debe incluir máquinas virtuales para protegerlas en una o más sentencias INCLUDE.VMTSMVSS. Asegúrese de que no excluye un disco en una máquina virtual (utilizando la opción EXCLUDE.VMDISK) si el disco contiene datos de aplicación que quiera proteger.

OPTions=KEEPSqllog

Si se ha especificado el parámetro OPTions KEEPSqllog en una sentencia INCLUDE.VMTSMVSS, dicho parámetro impide que se trunquen los registros del servidor de SQL cuando un cliente de archivado de copia de seguridad que se instala en un nodo de transportador de datos realiza una copia de seguridad de una máquina virtual que está ejecutando un servidor SQL. La especificación de este parámetro permite al administrador del servidor de SQL gestionar de forma manual (realizar copia de seguridad y, posiblemente, truncar) los registros del servidor de SQL, para que se puedan conservar y se puedan utilizar para restaurar las transacciones de SQL a un determinado punto de comprobación, una vez que se restaure la máquina virtual.

Cuando se especifica esta opción, no se truncará el registro SQL y se visualiza el siguiente mensaje y se registra en el servidor:

La protección de aplicaciones ANS4179I IBM Spectrum Protect
no ha truncado los registros de Microsoft SQL Server en la máquina virtual 'VM'.

Elimine la opción OPTIONS=KEEPSQLLOG para habilitar el truncamiento de los registros SQL al completarse una copia de seguridad.

Nota: El cliente no realiza la copia de seguridad de los archivos de registro de SQL. El administrador de SQL debe realizar una copia de seguridad de los archivos de registro para que se puedan aplicar una vez que se restaure la base de datos.

Ejemplos

Archivo de opciones

Configurar la protección de aplicaciones para una máquina virtual que se denomina vm_example:

```
INCLUDE.VMTSMVSS vm_example
```

Configurar la protección de aplicaciones para vm11, vm12 y vm15:

```
INCLUDE.VMTSMVSS vm11
INCLUDE.VMTSMVSS vm12
INCLUDE.VMTSMVSS vm15 options=keepsqlllog
```

Línea de mandatos

No aplicable; esta opción no puede especificarse en la línea de mandatos.

Referencia relacionada:

“Vmtimeout” en la página 649

“Exclude.vmdisk” en la página 430

“Include.vmdisk” en la página 467

“INCLUDE.VMSNAPSHOTATTEMPTS” en la página 469

Incrbydate

Utilice la opción **incrbydate** con el mandato **incremental** para realizar la copia de seguridad de los archivos nuevos y cambiados que tienen una fecha de modificación posterior a la fecha de la última copia de seguridad incremental almacenada en el servidor, a menos que excluya el archivo de la copia de seguridad.

Importante: Archivos que se han modificado o creado después de que el cliente de copia de seguridad y archivado procesara sus respectivos directorios, pero antes de que se completara la copia de seguridad incremental por fecha, y tampoco se realizará la copia de seguridad en futuras copias de seguridad incrementales por fecha, a menos que los archivos hayan vuelto a modificarse. Por este motivo se debe ejecutar periódicamente una copia de seguridad incremental, sin especificar la opción **incrbydate**.

La copia incremental por fecha actualiza la fecha y la hora de la última copia incremental en el servidor. Si se ejecuta una copia incremental por fecha sólo en parte de un sistema de archivos, no se actualizará la fecha de la última copia incremental completa, y la próxima copia incremental por fecha volverá a efectuar copia de seguridad de estos archivos.

Importante:

la hora de la última copia de seguridad incremental hace referencia a la hora del servidor y la hora de modificación de archivo hace referencia a la hora del cliente. Si las horas del servidor y del cliente no están sincronizadas, o el cliente y el servidor están en distintos husos horarios, esto afectará a la copia de seguridad incremental por fecha y a la copia de seguridad de imágenes con `mode=incremental`.

la hora de la última copia de seguridad incremental hace referencia a la hora del servidor y la hora de modificación de archivo hace referencia a la hora del cliente. Si las horas del servidor y del cliente no están sincronizadas, o el cliente y el servidor están en distintos husos horarios, esto afectará a la copia de seguridad incremental por fecha y a la copia de seguridad de imágenes con `mode=incremental`.

Tanto las copias de seguridad incrementales como las copias de seguridad incrementales por fecha hacen copia de seguridad de los archivos nuevos y modificados. Una copia incremental por fecha tarda menos tiempo en procesarse que una copia incremental completa y requiere menos memoria. Sin embargo, a diferencia de una copia de seguridad incremental completa, una copia de

seguridad incremental por fecha no conserva el almacenamiento del servidor actual de todos los archivos de la estación de trabajo por los motivos siguientes:

- No da caducidad a las versiones de copia de seguridad de los archivos que se han suprimido de la estación de trabajo.
- No revincula versiones de copia de seguridad con una nueva clase de gestión si ésta ha cambiado.
- No realiza la copia de seguridad de los archivos cuyos atributos han cambiado, como los datos de la lista de control de acceso (ACL), a menos que las fechas y las horas de modificación también hayan cambiado.
- No tiene en cuenta el atributo de frecuencia de grupo de copia de las clases de gestión.

Consejo: Si se dispone de un tiempo limitado durante la semana para efectuar copias de seguridad pero se dispone de tiempo extra durante los fines de semana, puede mantener el almacenamiento de servidor actual de los archivos de la estación de trabajo si realiza una copia de seguridad incremental con la opción `incrbydate` durante la semana y una copia de seguridad incremental completa los fines de semana.

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Sintaxis

►►—INCRbydate—◄◄

Parámetros

No hay parámetros para esta opción.

Ejemplos

Línea de mandatos:

```
dsmc incremental -incrbydate
```

Incremental

Utilice la opción `incremental` con el mandato **restore image** para asegurarse de que los cambios que se han realizado en la imagen base también se aplicarán a la imagen restaurada.

Si también utiliza la opción `deletfiles`, los cambios incluyen la supresión de los archivos y directorios que se encontraban en la imagen original pero que posteriormente se han suprimido de la estación de trabajo.

Nota: La utilización de la opción `incremental` con el mandato **restore image** para realizar una copia de seguridad de imágenes dinámica no recibe soporte.

Clientes soportados

Esta opción solo es válida para AIX, Linux x86_64, Linux on POWER y Solaris. La API de IBM Spectrum Protect no admite esta opción.

Sintaxis

►—INCREmental—►

Ejemplos

Línea de mandatos:

```
res i "/home/devel/proyecta/*" -incremental
```

Instrlogmax

La opción `instrlogmax` especifica el tamaño máximo del registro de instrumentación (`dsminstr.log`) en MB. Los datos de rendimiento del cliente se recopilan en el archivo `dsminstr.log` durante el proceso de copia de seguridad o restauración cuando la opción `enableinstrumentation` tiene el valor *yes*.

Si cambia el valor de la opción `instrlogmax`, las anotaciones existentes se amplían o reducen para ajustarse al nuevo tamaño. Si el valor se reduce, las entradas más antiguas se suprimen para reducir el tamaño del nuevo archivo.

Clientes soportados

Esta opción es válida para todos los clientes y la API de IBM Spectrum Protect.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. Esta opción se puede definir en el conjunto de opciones de cliente del servidor de IBM Spectrum Protect.

Sintaxis

►—INSTRLOGMAX— *tamaño*—►

Parámetros

tamaño

Especifica el tamaño máximo, en MB, del archivo de registro de instrumentación. El rango de valores es el comprendido entre 0 y 2047. El valor predeterminado es 25.

Cuando el tamaño del archivo `dsminstr.log` supera el tamaño máximo, se cambia el nombre del archivo de registro por `dsminstr.log.bak`. Los siguientes datos de instrumentación se siguen guardando en el archivo `dsminstr.log`.

Si especifica 0, el archivo de registro crece indefinidamente.

Ejemplos

Archivo de opciones:

```
instrlogmax 100
```

Línea de mandatos:

```
dsmc sel /home/mydir/* -subdir=yes -enableinstrumentation=yes  
-instrlogmax=100
```


Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Referencia relacionada:

“Enableinstrumentation” en la página 414

“Instrlogname”

Instrlogname

La opción `instrlogname` especifica la ruta y el nombre del archivo donde desea que se almacene la información que recopila el cliente de copia de seguridad y archivado.

Cuando se utiliza la opción `enableinstrumentation` yes para recopilar datos de rendimiento durante operaciones de copia de seguridad y restauración, el cliente almacena automáticamente la información en un archivo de registro.

De forma predeterminada, los datos de rendimiento se almacenan en el archivo de registro de instrumentación (`dsminstr.log`) en el directorio que se especifica mediante la variable de entorno `DSM_LOG` (o la variable de entorno `DSMI_LOG` para los productos que dependen de la API IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server y IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server). Si no ha establecido la variable de entorno `DSM_LOG`, el archivo de registro de instrumentación se almacena en el directorio actual (el directorio en el que se ha emitido el mandato **dsmc**).

Utilice esta opción sólo cuando desee cambiar el nombre del archivo y la ubicación del registro de instrumentación.

Si desea controlar el tamaño del archivo de registro, utilice la opción `instrlogmax`.

Clientes soportados

Esta opción es válida para todos los clientes y la API de IBM Spectrum Protect.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. Esta opción se puede definir en el conjunto de opciones de cliente del servidor de IBM Spectrum Protect.

Importante: Establezca la variable de entorno `DSM_LOG` en el nombre de un directorio en el que se deben colocar las anotaciones. El directorio especificado debe tener permisos que permitan el acceso de grabación desde la cuenta en la que se está ejecutando el cliente. El directorio raíz no es un valor válido para `DSM_LOG`.

Sintaxis

►►—INSTRLOGNAME— *filespec*—————►►

Parámetros

filespec

Especifica la ruta y el nombre de archivo donde desea almacenar la

información de rendimiento durante el proceso de copia de seguridad o restauración. Si no existe ninguna parte de la ruta que especifica, el cliente intenta crearla.

Si se especifica únicamente un nombre de archivo, el archivo se almacena en el directorio especificado por la variable de entorno DSM_LOG. Si no ha establecido la variable de entorno DSM_LOG, el archivo de registro de instrumentación se almacena en el directorio actual (el directorio en el que se ha emitido el mandato **dsmc**). El archivo de registro de instrumentación no puede ser un enlace simbólico.

En Mac OS X, si sólo especifica un nombre de archivo, el archivo se almacenará en la carpeta predeterminada. Los directorios predeterminados son:

```
~/Library/Logs/tivoli/tsm  
/Library/Logs/tivoli/tsm
```

Este nombre de archivo de registro de instrumentación sustituye el nombre de archivo de registro de instrumentación anterior `dsminstr.report.pXXX` que se ha creado con la opción `TESTFLAG=instrument:detail` o `instrument:API`.

Ejemplos

Archivo de opciones:

Para clientes AIX, Linux y Oracle Solaris:

```
instrlogname /home/user1/mydir/mydsminstr.log
```

Para clientes Mac OS X:

```
instrlogname /Users/user1/Library/Logs/mydsminstr.log
```

Línea de mandatos:

Para clientes AIX, Linux y Oracle Solaris:

```
dsmc sel /home/user1/mydir/* -subdir=yes -instrlogname=/usr/log/mydsminstr.log
```

Para clientes Mac OS X:

```
dsmc sel /Users/user1/mydir/* -subdir=yes -instrlogname=/Users/user1/Library/Logs/mydsminstr.log
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Referencia relacionada:

“Enableinstrumentation” en la página 414

“Instrlogmax” en la página 476

Lanfreecommmethod

La opción `lanfreecommmethod` especifica el protocolo de comunicaciones entre el cliente y el agente de almacenamiento de IBM Spectrum Protect. Esta opción activa el proceso entre el cliente y el dispositivo de almacenamiento conectado a la SAN.

Si utiliza la recuperación de errores de LAN, debe tener `lanfreecommmethod` en el archivo `dsm.sys` dentro de una stanza de servidor.

Para AIX, Linux y Solaris, utilice la opción `lanfreeshmport` para especificar el número de puerto de la memoria compartida en el que el agente de almacenamiento está a la escucha.

Clientes soportados

Esta opción es válida para clientes de AIX, Linux y Oracle Solaris.

Archivo de opciones

Establezca esta opción en el archivo `dsm.sys` dentro de una stanza de servidor.

Sintaxis

►—LANFREECommmethod— *commethod* —►

Parámetros

métodocomunicación

Especifica el protocolo admitido para el cliente de copia de seguridad y archivado:

TCPip

Protocolo de control de transmisiones/Protocolo de Internet (TCP/IP)

Utilice la opción `lanfreectcpport` para especificar el número de puerto TCP/IP en el que está conectado el agente de almacenamiento. El método de comunicación TCP/IP es el valor predeterminado para los usuarios no root en todas las plataformas admitidas.

V6Tcpip

Indica que se debe usar la versión 4 o 6 de TCP/IP, según la configuración del sistema y el resultado de una búsqueda de servicio de nombre de dominio. La única situación en la que esto no se aplica es cuando se utiliza **dsmc schedule** y se solicita `schedmode`. Debe haber disponible un entorno DNS válido.

SHAREdmem

Utilice el método de comunicación de memoria compartida cuando el cliente y el agente de almacenamiento estén ejecutándose en el mismo sistema. La memoria compartida proporciona mejor rendimiento que el protocolo TCP/IP. Este es el método de comunicación predeterminado para los usuarios root de AIX, Linux y Solaris. Cuando este método de comunicación se especifica en AIX, el usuario del cliente de copia de seguridad/archivado puede haber iniciado la sesión como usuario root o como usuario no root, siempre que el agente de almacenamiento se ejecute como root. Si el Agente de almacenamiento no se está ejecutando como root, el ID de usuario que ejecuta el cliente de copia de seguridad/archivado debe coincidir con el que ejecuta el Agente de almacenamiento.

Ejemplos

Archivo de opciones:

```
lanfreecommmethod tcp
```

Utilice únicamente TCP/IP v4

```
lanfreecommmethod V6Tcpip
```

Use TCP/IP v4 o v6, en función de cómo esté configurado el sistema y del resultado de una búsqueda del servicio de nombres de dominio.

Línea de mandatos:

```
-lanfreec=tcp
```

```
-lanfreec=V6Tcpip
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Información relacionada

“Lanfreeshmport”

“Lanfreetcppport” en la página 481

Lanfreeshmport

Utilice la opción `lanfreeshmport` cuando se haya especificado `lanfreecommmethod=SHAREdmem` para la comunicación entre el cliente de copia de seguridad y archivado y el agente de almacenamiento. Esta opción activa el proceso entre el cliente y el dispositivo de almacenamiento conectado a la SAN.

Clientes soportados

Esta opción es válida para clientes de AIX, Linux y Oracle Solaris.

Archivo de opciones

Coloque esta opción en el archivo de opciones del cliente (`dsm.sys`) de una stanza de servidor.

Sintaxis

►►—LANFREEShmport— —*port_address*—————►►

Parámetros

port_address

Especifica el número que se utiliza para conectar con el agente de almacenamiento. El rango de valores oscila entre 1 y 32767.

Para los clientes de Windows, el valor predeterminado es 1.

Para el resto de los clientes, excepto los clientes Windows, el valor predeterminado es 1510.

Ejemplos

Archivo de opciones:

```
lanfrees 1520
```

Línea de mandatos:

```
-lanfrees=1520
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Información relacionada

“Lanfreecommmethod” en la página 478

Lanfreetcppport

La opción `lanfreetcppport` especifica el número de puerto TCP/IP en el que está escuchando el agente de almacenamiento de IBM Spectrum Protect.

Utilice esta opción cuando haya especificado `lanfreecommmethod=TCPIP` para la comunicación entre el cliente de copia de seguridad y archivado y el agente de almacenamiento. No especifique la opción `lanfreetcppport` si desea utilizar el método de comunicación `NAMedpipes` para la comunicación sin LAN.

Clientes soportados

Esta opción solo es válida para clientes de AIX, Linux x86_64, Linux on POWER y Oracle Solaris.

Archivo de opciones

Establezca esta opción en el archivo `dsm.sys` en una stanza de servidor.

Sintaxis

►►—LANFREETCPPort— *port_address*—◄◄

Parámetros

port_address

Especifica el número de puerto TCP/IP en el que está conectado el agente de almacenamiento. El rango de valores es de 1 a 32767; siendo 1500 el valor predeterminado.

Nota: el valor `lanfreetcppport` del cliente debe coincidir con el valor `tcpport` del agente de almacenamiento para las comunicaciones con el agente de almacenamiento (servidor virtual). El valor `tcpport` del cliente debe coincidir con el valor `tcpport` del servidor para las comunicaciones con el servidor real.

Ejemplos

Archivo de opciones:

`lanfreetcpp 1520`

Línea de mandatos:

`-lanfreetcpp=1520`

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Información relacionada

“`Lanfreecommmethod`” en la página 478

Lanfreessl

Utilice la opción `lanfreessl` para habilitar SSL (Secure Sockets Layer) para proporcionar comunicaciones seguras de cliente y de agente de almacenamiento.

Clientes soportados

Esta opción se soporta en todos los clientes, a excepción de los clientes Mac OS X.

Establezca esta opción en el archivo de opciones del cliente. No puede establecer esta opción en la GUI ni en la línea de mandatos.

$\text{LANFREESSL} \left[\begin{array}{l} No \\ Yes \end{array} \right]$

No Especifica que el cliente de copia de seguridad y archivado no utiliza SSL al comunicarse con el agente de almacenamiento. No es el valor predeterminado.

Especifica que el cliente de copia de seguridad y archivado habilita SSL al comunicarse con el agente de almacenamiento. Para habilitar SSL, especifique `lanfreessl=yes` y cambie el valor de la opción `lanfreetcppport`. Cambie el valor de la opción `lanfreetcppport` si fuera necesario porque el agente de almacenamiento de IBM Spectrum Protect normalmente está configurado para estar a la escucha de las conexiones SSL en un puerto por separado.

```
lanfreessl yes
lanfreessl no
```

No aplicable. No puede establecer esta opción en la línea de mandatos.

La opción `lanfreetcpserveraddress` especifica la dirección TCP/IP del agente de almacenamiento de IBM Spectrum Protect.

Utilice esta opción cuando haya especificado `lanfreemethod=TCPIP` o `V6TCPIP` para la comunicación entre el cliente de copia de seguridad y archivado y el agente de almacenamiento.

La alteración temporal del valor predeterminado para esta opción es útil cuando se configuran datos sin LAN en un entorno en el que el cliente y el agente de almacenamiento se ejecutan en sistemas distintos. Puede obtener esta dirección de agente de almacenamiento del administrador.

Esta opción solo es válida para clientes de AIX, Linux x86_64, Linux on POWER y Oracle Solaris.

Establezca esta opción en el archivo de opciones del sistema del cliente.

Sintaxis

►►—LANFREETCPServeraddress— —stagent_address—►►

Parámetros

dirección_agentealmacenamiento

Especifica una dirección TCP/IP de 1 a 64 caracteres para un servidor.

Especifique un nombre de dominio TCP/IP o una dirección IP numérica. La dirección IP numérica puede ser una dirección TCP/IP v4 o TCP/IP v6. El valor predeterminado es 127.0.0.1 (localhost).

Ejemplos

Archivo de opciones:

```
LANFREETCPServeraddress stagent.example.com
```

```
LANFREETCPServeraddress 192.0.2.1
```

Línea de mandatos:

No se aplica.

Latest

Utilice la opción latest para restaurar la versión de copia de seguridad más reciente de un archivo, aunque la copia de seguridad no esté activa.

Puede utilizar la opción latest con los mandatos siguientes:

- **restore**
- **restore group**

Si va a efectuar una restauración de un instante específico (con la opción pitdate), no es necesario especificar latest porque esta opción es implícita cuando se utiliza pitdate.

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Sintaxis

►►—LATest—►►

Parámetros

No hay parámetros para esta opción.

Ejemplos

Línea de mandatos:

```
dsmc restore "/Users/devel/proyecto/*" -latest
```

Línea de mandatos:

```
dsmc restore "/home/devel/proyecto/*" -latest
```

Localbackupset

La opción `localbackupset` especifica si la GUI del cliente de copia de seguridad y archivado pasa por alto la conexión inicial con el servidor de IBM Spectrum Protect, para restaurar un juego de copias de seguridad locales en una estación de trabajo independiente.

Si establece la opción `localbackupset` en `yes`, la GUI no intentará establecer la conexión inicial con el servidor. En este caso, la GUI sólo activará la función de restauración.

Si establece la opción `localbackupset` en `no` (el valor predeterminado), la GUI intentará establecer la conexión inicial con el servidor y activará todas las funciones de la GUI.

Nota: El mandato `restore backupset` admite la restauración de conjuntos de copias de seguridad locales en una estación de trabajo autónoma sin que se utilice la opción `localbackupset`.

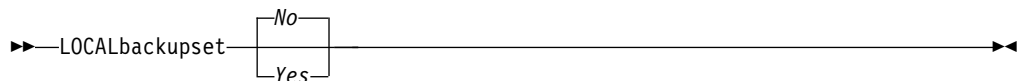
Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor.

Sintaxis



Parámetros

No Especifica que la GUI intenta la conexión inicial con el servidor y activa todas las funciones. Éste es el valor predeterminado.

Yes

Especifica que la GUI no intenta la conexión inicial con el servidor y activa sólo la función de restauración.

Ejemplos

Archivo de opciones:

```
localbackupset yes
```

Esta opción no es válida con el cliente de línea de mandatos **dsmc**.

Información relacionada

“Restore Backupset” en la página 749

Makesparsefile

Utilice la opción `makesparsefile` con los mandatos **restore** o **retrieve** para especificar el modo en que los archivos esparcidos se volverán a crear.

Los archivos esparcidos no tienen espacio de disco asignado para cada bloque en todo el espacio de direcciones, lo que provoca la aparición de espacios vacíos en los archivos. El cliente de copia de seguridad y archivado detecta los archivos esparcidos durante una operación de copia de seguridad y los marca como esparcidos en el servidor de IBM Spectrum Protect. Los espacios vacíos se detectan por su contenido, que siempre son ceros.

Si establece la opción `makesparsefile` en `yes` (que es el valor predeterminado), los espacios vacíos del archivo no se graban en disco, por lo que no se asigna espacio de disco adicional durante una restauración.

Si establece la opción `makesparsefile` en `no`, los espacios vacíos no se vuelven a crear, lo que hace que se asignen bloques de disco para todo el espacio de direcciones. Esto puede provocar que se utilice más espacio de disco. Asegúrese de que tiene espacio de disco suficiente para restaurar todos los datos.

En algunos sistemas UNIX y Linux, puede ser necesario hacer una copia de seguridad de archivos específicos del sistema como archivos no esparcidos. Utilice la opción `makesparsefile` para los archivos que precisen la existencia de bloques de disco físicos, como `ufsboot` en Solaris, que se ejecuta en el momento de arrancar el sistema. El cargador de archivos de arranque del sistema operativo accede a los bloques de disco físicos directamente y no admite los archivos esparcidos.

Cientes soportados

Esta opción es válida para todos los clientes UNIX y Linux, a excepción de Mac OS X.

Archivo de opciones

Establezca esta opción en el archivo de opciones del usuario cliente (`dsm.opt`).

Sintaxis



Parámetros

Yes

Especifica que los espacios vacíos del archivo no se graban para que no se asigne espacio de disco adicional durante una restauración. Éste es el valor predeterminado.

No Especifica que los espacios vacíos no se vuelven a crear, lo que hace que se asignen bloques de disco para todo el espacio de direcciones.

Ejemplos

Archivo de opciones:

```
makesparsefile no
```

Línea de mandatos:

```
-makesparsefile=no
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Managedservices

La opción `managedservices` especifica si el servicio de aceptación de clientes de IBM Spectrum Protect ha de gestionar el planificador, el cliente web o ambos.

Restricción: no puede utilizar `dsmcad` para la planificación cuando establece la opción `sessioninitiation` en `serveronly`.

El daemon de aceptación de clientes sirve de temporizador externo para el planificador. Al iniciar el planificador, éste realiza una consulta al servidor para saber si hay otro evento planificado. El evento se ejecuta de forma inmediata o el planificador se cierra. El daemon de aceptación de clientes reinicia el planificador cuando es el momento de ejecutar el evento planificado.

Nota:

1. Si establece la opción `schedmode` en `prompt`, el servidor solicitará información al daemon de aceptación de clientes cuando sea el momento de ejecutar la planificación. El planificador se conectará y desconectará del servidor cuando el daemon de aceptación de clientes se inicie por primera vez.
El mandato `dsmc schedule` no puede utilizarse cuando se han especificado `schedmode prompt` y `commmethod V6Tcpi`.
2. Para Mac OS X, si no especifica la opción `managedservices`, el daemon de aceptación de clientes gestionará el programa del planificador y el cliente Web de forma predeterminada.
3. Establezca la opción `passwordaccess` en `generate` en el archivo `dsm.sys` y genere una contraseña para que IBM Spectrum Protect queda gestionar la contraseña automáticamente.

La utilización del daemon de aceptación de clientes para gestionar el servicio del planificador puede proporcionar las ventajas siguientes:

- Se resuelven los problemas de retención de memoria que pueden ocurrir con los métodos tradicionales para ejecutar el planificador. La utilización del daemon de aceptación de clientes para gestionar el planificador necesita muy poca memoria entre las operaciones planificadas.
- El daemon de aceptación de clientes puede gestionar el programa del planificador y el cliente web, ambos, con lo que se reduce el número de procesos de fondo de la estación de trabajo.
- Para utilizar el cliente web, debe especificar esta opción en el archivo de opciones del sistema cliente.

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. Puede establecer esta opción en la ficha **Cliente Web** del Editor de preferencias.

Sintaxis

►—MANAGEDServices—mode—◄

Parámetros

mode

Especifica si el daemon de aceptación de clientes ha de gestionar el planificador, el cliente web o ambos.

webclient

Especifica que el daemon de aceptación de clientes ha de gestionar el cliente web. Es el valor predeterminado para UNIX y Linux. *webclient* y *schedule* son los valores predeterminados para Mac OS X.

schedule

Especifica que el daemon de aceptación de clientes ha de gestionar el planificador. *webclient* y *schedule* son los valores predeterminados para Mac OS X.

none

Sólo para Mac OS X, especifica que el daemon de aceptación de clientes no ha de gestionar el cliente web ni planificadores. Establezca *managedservices* en *none* para permitir que el mandato **dsmc schedule**.

Ejemplos

Archivo de opciones:

A continuación se muestran ejemplos de cómo podría especificar la opción *managedservices* en el archivo de opciones del cliente (*dsm.sys*).

Tarea Especificar que el daemon de aceptación de clientes gestiona únicamente el cliente web.

```
managedservices webclient
```

Tarea Especificar que el daemon de aceptación de clientes gestiona únicamente el planificador.

```
managedservices schedule
```

Tarea Especificar que el daemon de aceptación de clientes ha de gestionar el cliente web y el planificador, ambos.

```
managedservices schedule webclient
```

Nota: el orden en que se especifiquen estos valores carece de importancia.

Tarea En Mac OS X, para utilizar el mandato **dsmc schedule**, especifique:

```
managedservices none
```

Línea de mandatos:

No se aplica.

Información relacionada

“Passwordaccess” en la página 509

Consulte el tema “Configuración del planificador” en la página 66 para obtener instrucciones acerca de la configuración del daemon de aceptación de clientes para gestionar el planificador.

“Sessioninitiation” en la página 556

“Cadlistenonport” en la página 362

Maxcmdretries

La opción `maxcmdretries` especifica el número máximo de veces que el planificador cliente (en la estación de trabajo del usuario) intenta procesar un mandato planificado que da error.

El reintento de mandato sólo se inicia si el planificador cliente todavía no ha hecho una copia de seguridad de un archivo, nunca ha conectado con el servidor o ha fallado antes de realizar la copia de seguridad de un archivo. Esta opción sólo se utiliza cuando el planificador se está ejecutando.

El administrador de IBM Spectrum Protect también puede utilizar esta opción. Si el administrador especifica un valor para esta opción, ese valor alterará temporalmente la información que se ha especificado en el archivo de opciones de cliente después de que el nodo de cliente haya establecido contacto con el servidor correctamente.

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción. El servidor también puede definir esta opción.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. Puede establecer esta opción en el separador **Planificador**, en el campo **Número máximo de reintentos de mandatos** del Editor de preferencias.

Sintaxis

►►—MAXCMDRetries— —*maxcmdretries*—►►

Parámetros

maxcmdretries

Especifica el número de veces que el planificador cliente puede intentar procesar un mandato planificado que no se ha conseguido realizar. El rango de valores es de 0 a 9999, siendo 2 el valor predeterminado.

Ejemplos

Archivo de opciones:

`maxcmdr 4`

Línea de mandatos:

`-maxcmdretries=4`

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Mbobjrefreshthresh

La opción `mbobjrefreshthresh` (umbral de renovación de objeto megablock) es un número que define un umbral. Cuando el número de objetos IBM Spectrum Protect necesarios para describir cualquier megablock 128 MB excede este valor, se renueva el megablock completo y los objetos utilizados para representar esta área, en las copias anteriores, caducan.

Cuando realiza la copia de seguridad de una máquina virtual, los datos se almacenan en el servidor IBM Spectrum Protect en 128 MB unidades, denominado *megablocks*. Si un área del disco de producción cambia y se realiza una nueva copia de seguridad incremental, se crea un megablock nuevo para representar los cambios realizados en los datos de la copia de seguridad anterior. Debido a que un megablock nuevo puede crearse con cada copia de seguridad incremental, al final los megablocks pueden afectar negativamente al rendimiento de la base de datos de IBM Spectrum Protect, y, por lo tanto, afectar negativamente al rendimiento de la mayor parte de operaciones de IBM Spectrum Protect.

Utilice esta opción cuando calcule los objetos de IBM Spectrum Protect que representan datos de producción para las copias de seguridad de la máquina virtual. Por ejemplo, cuando el número de objetos de IBM Spectrum Protect exceda este valor, se renovará el megablock. Esta acción significa que el bloque de 128 MB completo se copia en el servidor y se representa como un objeto de IBM Spectrum Protect único. El valor mínimo es 2 y el valor máximo es 8192. El valor predeterminado es 50.

Clientes soportados

Esta opción es válida para los clientes que son nodos de movimiento de datos que protegen las máquinas virtuales de VMware. Para utilizar esta opción, tiene que tener un acuerdo de licencia para utilizar IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Archivo de opciones

Especifique esta opción en el archivo de opciones del cliente.

Sintaxis



Parámetros

El valor mínimo que puede especificar son 2 megablocks, el mayor valor es 8192 megablocks; el valor predeterminado es de 50 megablocks.

Ejemplos

Seleccione esta opción para desencadenar una renovación de megablock cuando el número de objetos necesarios para representar un megablock actualizado supere los 20 objetos:

```
MBOBJREFRESHTHRESH 20
```

Mbpctrefreshthresh

La opción `mbpctrefreshthresh` (umbral de renovación de porcentaje de megablock) es un número que define un umbral. Cuando el porcentaje de objetos IBM Spectrum Protect necesarios para describir cualquier megablock 128 MB excede este valor, se renueva el megablock completo y los objetos utilizados para representar esta área, en las copias anteriores, caducan.

Cuando realiza la copia de seguridad de una máquina virtual, los datos se almacenan en el servidor IBM Spectrum Protect en 128 MB unidades, denominado *megablocks*. Si un área del disco de producción cambia y se realiza una nueva copia de seguridad incremental, se crea un megablock nuevo para representar los cambios realizados en los datos de la copia de seguridad anterior. Dado que se puede crear un megablock nuevo con cada copia de seguridad incremental, finalmente los megablocks pueden afectar negativamente al rendimiento de la base de datos de IBM Spectrum Protect, y, por lo tanto, afectar negativamente al rendimiento de la mayor parte de operaciones de IBM Spectrum Protect.

Utilice esta opción cuando calcule la cantidad de datos adicionales de la que se realiza copia de seguridad para cada máquina virtual. Por ejemplo, cuando un bloque de 128-MB de un disco de producción cambia más del porcentaje especificado, todo el bloque 128-MB se copia en el servidor. El bloque se representa como un único objeto de IBM Spectrum Protect.

Clientes soportados

Esta opción es válida para los clientes que son nodos de movimiento de datos que protegen las máquinas virtuales de VMware. Para utilizar esta opción, tiene que tener un acuerdo de licencia para utilizar IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Archivo de opciones

Especifique esta opción en el archivo de opciones del cliente.

Sintaxis



Parámetros

El valor mínimo que puede especificar son 1 por ciento, el mayor valor es 99 por ciento; el valor predeterminado es 50 por ciento.

Ejemplos

Seleccione esta opción para desencadenar una renovación megablock el 50 por ciento (o más) de los objetos de una megablock en un disco de producción han cambiado:

```
MBPCTREFRESHTHRESHOLD 50
```

Memoryefficientbackup

La opción `memoryefficientbackup` especifica el algoritmo de reserva de memoria que ha de utilizarse para procesar las copias de seguridad de espacio de archivos completas.

Un método hace una copia de seguridad de un directorio a la vez, usando menos memoria. El otro método utiliza mucha menos memoria, pero necesita más espacio de disco.

Utilice la opción `memoryefficientbackup` con el mandato **incremental** cuando la estación de memoria tenga restricciones de memoria. También puede utilizar esta opción como parámetro para la opción `include.fs` para seleccionar el algoritmo que el cliente de copia de seguridad y archivado ha de utilizar en función de cada espacio de archivos.

Utilice `memoryefficientbackup=diskcachemethod` para cualquier espacio de archivos que tenga demasiados archivos como para que el cliente complete la copia de seguridad incremental con el valor predeterminado, `memoryefficientbackup=no`, o con `memoryefficientbackup=yes`.

La cantidad real de espacio en el disco necesaria para el archivo de caché del disco creado por las siguientes copias de seguridad incrementales de la caché del disco depende del número de archivos y directorios incluidos en la copia de seguridad y de la longitud promedio de vía de acceso de los archivos y directorios de los que se hace copia de seguridad. Para UNIX y Linux, calcule 1 byte por carácter en el nombre de la vía de acceso. Para Mac OS X, calcule 4 bytes por carácter en el nombre de vía de acceso. Por ejemplo, si se va a realizar una copia de seguridad de 1.000.000 de archivos y directorios y la longitud promedio de la vía de acceso es de 200 caracteres, la base de datos ocupará aproximadamente 200 MB en los clientes UNIX y Linux y 800 MB en los clientes Mac OS X. Otra forma de calcular a fin de realizar cierta planificación es multiplicar el número de archivos y directorios por la longitud de la vía de acceso más larga a fin de establecer el tamaño máximo de base de datos.

Al realizar copia de seguridad de un sistema de archivos gestionados HSM, se crea un segundo archivo de caché de disco para la lista de archivos migrados. Los archivos de caché de disco combinados, creados por copias de seguridad incrementales de caché de disco y copias de seguridad del sistema de archivos gestionados HSM, pueden necesitar más de 400 MB de espacio de disco para cada millón de archivos de los que se realice copia de seguridad. El archivo de la memoria caché de disco puede ser muy grande. La admisión de archivos grandes se puede habilitar en el sistema de archivos que se está utilizando para el archivo de memoria caché de disco.

Clientes soportados

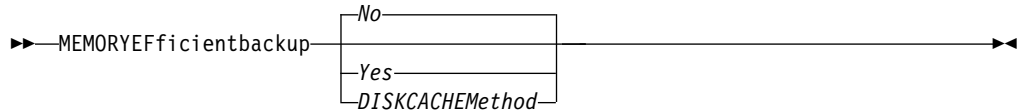
Esta opción es válida para todos los clientes. El servidor también puede definir esta opción.

Archivo de opciones

Esta opción se admite tanto en `dsm.opt` como dentro de una stanza de servidor en `dsm.sys`, pero el valor de `dsm.opt` se pasa por alto si también aparece en `dsm.sys`. También puede incluir esta opción en la línea de mandatos inicial. En la modalidad interactiva, esta opción puede utilizarse con el mandato **incremental**: También

puede definir esta opción en el separador **Ajuste del rendimiento** del Editor de preferencias y seleccionar el recuadro de selección **Utilizar algoritmo de bajo consumo de memoria**.

Sintaxis



Parámetros

No El nodo cliente utiliza el método más rápido y que hace un uso más intensivo de la memoria al procesar copias de seguridad incrementales. Éste es el valor predeterminado.

Yes

El nodo cliente utiliza el método que requiere menos memoria al procesar copias de seguridad incrementales.

Diskcachemethod

El nodo cliente utiliza el método que requiere mucha menos memoria pero más espacio en el disco al procesar copias de seguridad incrementales para sistemas de archivos completos.

Ejemplos

Archivo de opciones:

```
memoryefficientbackup yes
memoryefficientbackup diskcachem
```

Línea de mandatos:

```
-memoryef=no
```

Información relacionada

“Opciones include” en la página 458

Mode

Utilice la opción mode para especificar la modalidad de copia de seguridad que desea utilizar al realizar operaciones de copia de seguridad específicas.

La opción mode no tiene ningún efecto al realizar copias de seguridad de un dispositivo lógico RAW.

Puede utilizar la opción mode con los siguientes mandatos de copia de seguridad:

backup image

Para especificar si ha de realizarse una copia de seguridad de imagen selectiva o incremental de los sistemas de archivos de cliente.

backup nas

Para especificar si ha de realizarse una copia de seguridad de imagen completa o diferencial de los sistemas de archivos NAS.

backup group

Para especificar si ha de realizarse una copia de seguridad de grupo completa o diferencial que contenga una lista de archivos de uno o más orígenes de espacio de archivos.

backup vm

Para máquinas virtuales VMware, este parámetro especifica si debe realizarse una copia de seguridad completa-constante-incremental o incremental-constante-incremental de las máquinas virtuales VMware.



Las operaciones de máquina virtual solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments.

Clientes soportados

Esta opción es válida en todos los clientes soportados excepto Mac OS. La API de IBM Spectrum Protect no admite esta opción.

Sintaxis

Para copias de seguridad de imagen de los sistemas de archivos de cliente



Para copias de seguridad de imagen de los sistemas de archivos NAS



Para copias de seguridad de grupo



Para copias de seguridad de máquinas virtuales VMware



Parámetros

Parámetros de copia de seguridad de imagen

selective

Especifica que desea realizar una copia de seguridad de imagen completa (selectiva). Esta es la modalidad predeterminada para copias de seguridad de imagen de sistemas de archivos de cliente.

incremental

Especifica que se desea realizar una copia de seguridad sólo de los

datos han cambiado desde la última copia de seguridad. Si todavía no se ha creado una copia de seguridad de imagen, entonces la primera copia de seguridad es una copia de seguridad de imagen completa (mode=selective), independientemente de qué opción de modalidad se especifique.

Parámetros de copia de seguridad NAS

differential

Es el valor predeterminado para los objetos NAS. Especifica que desea realizar una copia de seguridad de NAS de los archivos que han cambiado desde la última copia de seguridad completa. Si no existe ninguna una copia de una imagen completa almacenada en el servidor de IBM Spectrum Protect, se realiza una copia de seguridad completa. Si existe una imagen completa, tanto si es restaurable como si está caducada y está siendo mantenida debido a las imágenes diferenciales dependientes, especificar `MODE =differential` envía una copia de seguridad de imagen diferencial. Si se envía una imagen completa durante una copia de seguridad diferencial, queda reflejada como una imagen completa mediante el mandato de servidor `QUERY NASBACKUP`.

Una imagen completa puede ser elegible para caducidad en función del control de versiones o la retención (`verexists retextra`), pero se seguirá manteniendo en el servidor para permitir la restauración de imágenes diferenciales dependientes. Una imagen completa que sea elegible para caducidad no se puede seleccionar para restauración, por lo que no se visualiza mediante el mandato de servidor `QUERY NASBACKUP`. Las copias de seguridad de imágenes diferencias que dependen de una imagen completa "caducada" pueden ser restauradas.

full

Especifica que desea realizar una copia de seguridad completa de sistemas de archivos NAS.

Parámetros de copia de seguridad de grupos

full

Especifica que desea realizar una copia de seguridad completa de sistemas de objetos de grupos. Este es el valor predeterminado para copias de seguridad de grupos.

differential

Especifica que desea realizar una copia de seguridad de grupo de los archivos que han cambiado desde la última copia de seguridad completa. Si no existe ninguna una copia de una imagen completa almacenada en el servidor de IBM Spectrum Protect, se realiza una copia de seguridad completa. Si existe una imagen completa, tanto si es restaurable como si está caducada y está siendo mantenida debido a las imágenes diferenciales dependientes, especificar `MODE =differential` envía una copia de seguridad de imagen diferencial. Si se envía una imagen completa durante una copia de seguridad diferencial, queda reflejada como una imagen completa mediante el mandato de servidor `QUERY GROUP`.

Una imagen completa puede ser elegible para caducidad en función del control de versiones o la retención (`verexists retextra`), pero se seguirá manteniendo en el servidor para permitir la restauración de imágenes diferenciales dependientes. Una imagen completa que sea elegible para caducidad no se puede seleccionar para restauración, por

lo que no se visualiza mediante el mandato de servidor QUERY GROUP. Las copias de seguridad de imágenes diferencias que dependen de una imagen completa "caducada" pueden ser restauradas.

Parámetros de copias de seguridad de máquina virtual VMware

IFFull

Especifica que desea realizar una copia de seguridad completa-constante-incremental de una máquina virtual. Una copia de seguridad completa-constante-incremental realiza una copia de seguridad de todos los bloques utilizados en discos de máquinas virtuales de VMware.

De forma predeterminada, la primera copia de seguridad de una máquina virtual VMware es una copia de seguridad completa-constante-incremental (`mode=iffull`), aunque se especifique `mode=ifincremental` (o se deje el valor predeterminado de la opción `mode`). Las copias de seguridad posteriores tienen el valor predeterminado en `mode=ifincremental`.

No puede utilizar esta modalidad de copia de seguridad para realizar una copia de seguridad de una máquina virtual, si el cliente está configurado para cifrar los datos de copia de seguridad.

Para obtener una descripción de la estrategia de copia de seguridad incremental-constante para máquinas virtuales VMware, consulte Tipos de copia de seguridad y de restauración.

IFIncremental

Especifica que desea realizar una copia de seguridad incremental siempre incremental de una máquina virtual. Una copia de seguridad incremental-constante-incremental realiza una copia de seguridad sólo de los bloques de disco que han cambiado desde la última copia de seguridad.

Esta modalidad es la modalidad de copia de seguridad predeterminada de las copias de seguridad de máquina virtual VMware.

No puede utilizar esta modalidad de copia de seguridad para realizar una copia de seguridad de una máquina virtual, si el cliente está configurado para cifrar los datos de copia de seguridad.

Ejemplos

Tarea Realizar una copia de seguridad de una máquina virtual VMware denominada `vm1` utilizando la modalidad incremental siempre incremental para copiar sólo los datos que han cambiado desde la última copia de seguridad.

```
dsmc backup vm vm1 -mode=ifincremental
-vmbackuptype=full
```

Tarea Realizar la copia de seguridad de imágenes NAS de todo el sistema de archivos.

```
dsmc backup nas -mode=full -nasnodename=nas1
/vol/vol0 /vol/vol1
```

Tarea Realizar la copia de seguridad del espacio de archivos `/home/test` utilizando una copia de seguridad de imágenes incremental que realice la copia de seguridad sólo de los archivos nuevos y de los archivos que han cambiado desde la última copia de seguridad de imágenes completa.

```
dsmc backup image /home/test -mode=incremental -snapshotproviderimage=none
```

Tarea Realizar una copia de seguridad completa de todos los archivos de la lista de archivos /home/dir1/filelist1 en el nombre de espacio de archivos virtual /virtfs que contiene el archivo /home/group1 de líder de grupo.

```
dscm backup group -filelist=/home/dir1/filelist1  
-groupname=group1 -virtualfsname=/virtfs -mode=full
```

Referencia relacionada:

- “Backup VM” en la página 683
- “Backup Group” en la página 672
- “Backup Image” en la página 674
- “Backup NAS” en la página 680

Monitor

La opción monitor especifica si se supervisará una copia de seguridad o una restauración de imagen de sistemas de archivos pertenecientes a un servidor de archivos de almacenamiento conectado a red (NAS).

Si especifica `monitor=yes`, el cliente de copia de seguridad y archivado supervisará la operación actual de copia de seguridad o de restauración de imagen NAS y visualizará la información del proceso en la pantalla. Éste es el valor predeterminado.

Si especifica `monitor=no`, el cliente no supervisará la operación actual de copia de seguridad o de restauración de imagen NAS y estará disponible para procesar el siguiente mandato.

Utilice esta opción con los mandatos **backup nas** o **restore nas**.

Clientes soportados

Esta opción *sólo* es válida para los clientes AIX, HP-UX, Linux y Solaris.

Sintaxis



Parámetros

Yes

Especifica que se desea supervisar la operación actual de copia de seguridad o de restauración de imagen NAS y ver en pantalla la información de proceso. Éste es el valor predeterminado.

No Especifica que no se desea supervisar la operación actual de copia de seguridad o de restauración de imagen NAS.

Ejemplos

Línea de mandatos:

```
backup nas -mode=full -nasnodename=nas1 -monitor=yes  
/vol/vol0 /vol/vol1
```

Myreplicationserver

La opción `myreplicationserver` especifica qué stanza de servidor secundario utiliza el cliente durante una migración tras error.

La stanza de servidor secundario se identifica mediante la opción `replservername` y contiene información de conexión sobre el servidor secundario.

Esta opción se establece mediante el administrador del servidor de IBM Spectrum Protect para el nodo cliente. Durante el proceso de inicio de sesión normal (no migración tras error), la opción se envía al cliente y se guarda en el archivo de opciones del cliente.

No edite esta opción durante las operaciones normales.

Edite esta opción sólo durante situaciones como las siguientes:

- El servidor primario está fuera de línea y la información para el servidor secundario no se encuentra en el archivo de opciones.
- La información del servidor secundario está caducada o es incorrecta.

Todos los valores que edite se eliminarán o se actualizarán la próxima vez que inicie sesión en el servidor primario.

Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Esta opción se coloca dentro de una stanza del servidor en el archivo `dsm.sys`.

Sintaxis

►►—MYREPLICATIONServer—*repl_servername*—————►►

Parámetros

repl_servername

Especifica el nombre de la stanza para el servidor secundario que se utilizará durante una migración tras error. Este valor es normalmente el nombre del servidor secundario, no el nombre de host del servidor. Además, el valor del parámetro `repl_servername` no distingue entre mayúsculas y minúsculas, pero el debe coincidir con el valor especificado para la opción `REPLSERVERName`.

Ejemplos

Archivo de opciones:

```
MYREPLICATIONServer TargetReplicationServer1
```

Línea de mandatos:

No se aplica.

Archivo de opciones:

En el ejemplo siguiente se muestra cómo especificar opciones para tres servidores distintos en el archivo `dsm.sys`, y cómo hacer referencia al servidor secundario. La información de conexión para varios servidor secundario se presenta en stanzas. Cada stanza se identifica mediante la

opción **replservername** y el nombre del servidor secundario. La stanza **servername** debe contener la opción **myreplicationserver**, que apunta al servidor secundario que se especifica mediante la stanza **replservername**. Sólo se puede especificar un servidor secundario por stanza **servername**.

```
REPLSERVERNAME      TargetReplicationServer1
REPLTCPSERVERADDRESS TargetReplicationServer1
REPLTCPPOrt         1505
REPLSSLPORT         1506
REPLSERVERGUID      91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00
```

```
REPLSERVERNAME      TargetReplicationServer2
REPLTCPSERVERADDRESS TargetReplicationServer2
REPLTCPPOrt         1505
REPLSSLPORT         1506
REPLSERVERGUID      91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.02
```

```
SErvername          server_a
COMMMethod           TCPip
TCPPOrt              1500
TCPServeraddress     server_hostname1.example.com
PASSWORDAccess       prompt
MYREPLICATIONServer TargetReplicationServer1
```

```
SErvername          server_b
COMMMethod           TCPip
TCPPOrt              1500
TCPServeraddress     server_hostname2.example.com
PASSWORDAccess       generate
INCLExc1             /adm/tsm/archive.exc1
MYREPLICATIONServer TargetReplicationServer2
```

```
SErvername          server_c
COMMMethod           TCPip
TCPPOrt              1500
TCPServeraddress     server_hostname3.example.com
PASSWORDAccess       generate
MYREPLICATIONServer TargetReplicationServer1
```

Conceptos relacionados:

“Configuración y uso de la migración tras error automática del cliente” en la página 94

Tareas relacionadas:

“Configuración del cliente de migración automática tras error” en la página 98

Nasnodename

La opción **nasnodename** especifica el nombre de nodo del servidor de archivos NAS cuando se procesan sistemas de archivos NAS. El cliente le solicita un ID de administrador.

El nombre de nodo identifica el servidor de archivos NAS en el servidor de IBM Spectrum Protect. El servidor debe inscribir el servidor de archivos NAS.

Puede especificar esta opción en la línea de mandatos o en el archivo de opciones del cliente (dsm.sys).

Puede modificar temporalmente el valor predeterminado en el archivo dsm.sys especificando un valor distinto en la línea de mandatos. Si no especifica la opción **nasnodename** en el archivo dsm.sys, debe especificar esta opción en la línea de mandatos cuando se procesen sistemas de archivos NAS.

Puede utilizar la opción **nasnodename** con los mandatos siguientes:

- **backup nas**
- **delete filespace**
- **query backup**
- **query filespace**
- **restore nas**

El mandato **delete filespace** se puede utilizar para suprimir interactivamente espacios de archivos NAS del almacenamiento del servidor.

Utilice la opción **nasnodename** para identificar el nodo del servidor de archivos NAS. Especifique la opción **nasnodename** en el archivo de opciones del sistema cliente (**dsm.sys**). El valor del archivo de opciones del sistema del cliente es el valor predeterminado, pero este valor puede modificarse temporalmente en la línea de mandatos. Si no especifica la opción **nasnodename** en el archivo de opciones del cliente, deberá especificar esta opción en la línea de mandatos cuando procese sistemas de archivos NAS.

Utilice la opción **class** para especificar la clase del espacio de archivos que se ha de suprimir. Para que se muestre una lista de los espacios de archivos que pertenecen a un nodo NAS y así poder elegir cuál suprimir, utilice la opción **-class=nas**.

Para suprimir espacios de archivos NAS mediante la utilización del cliente web, consulte el tema en el que se explica la realización de la copia de seguridad de los datos.

Cientes soportados

Esta opción solo es válida para los clientes de AIX, Linux y Solaris. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (**dsm.sys**) en una stanza de servidor. Puede establecer esta opción en la ficha **General** del editor de preferencias.

Sintaxis

►►—NASNodename— —*nodename*—►►

Parámetros

nodename

Especifica el nombre de nodo del servidor de archivos NAS.

Ejemplos

Archivo de opciones:

nasnodename nas2

Línea de mandatos:

-nasnodename=nas2

Nfstimeout

La opción `nfstimeout` especifica el número de segundos que el cliente espera a que se reciba una llamada de sistema de estado en un sistema de archivos NFS antes de que exceda el tiempo de espera.

Puede utilizar esta opción para mitigar el funcionamiento predeterminado de las llamadas de estado en los sistemas de archivos. Por ejemplo, si un sistema de archivos NFS es obsoleto, NFS excederá el tiempo de espera de una llamada de sistema de estado (montaje por software) o colgará el proceso (montaje por hardware).

Si el valor de esta opción se cambia por un valor distinto de cero, un thread llamador crea un thread nuevo para emitir la llamada de estado del sistema. El thread llamador excede el tiempo de espera del thread nuevo y la operación puede continuar.

Nota: En Solaris, la opción `nfstimeout` puede fallar si el montaje de NFS es por hardware. Si se cuelga el proceso, desactive la opción `nfstimeout` y monte el sistema de archivos NFS montado por software de este modo:

```
mount -o soft,timeo=5,retry=5 machine:/sistemaarchivos /puntomontaje
```

Los parámetros son los siguientes:

soft Genera un montaje por software del sistema de archivos NFS. Si se produce un error, la función `stat()` devuelve un error. Si se ha utilizado la opción `hard`; `stat()` nunca vuelve hasta que el sistema de archivos está disponible.

timeo=*n*
Establece el tiempo de espera para un error de montaje de tipo `soft` en *n* décimas de segundo.

retry=*n*
Establece los reintentos internos y los reintentos de montaje en *n*; el valor predeterminado es 10000.

Clientes soportados

Esta opción es válida para todos los clientes UNIX y Linux. El servidor también puede definir esta opción.

Archivo de opciones

Establezca esta opción en el archivo `dsf.sys` dentro de una sección del servidor o el archivo de opciones de cliente (`dsf.opt`).

Sintaxis

►—NFSTIMEout— *número* —►

Parámetros

number
Especifica el número de segundos que el cliente espera a que se reciba una

llamada de estado del sistema en un sistema de archivos antes de que exceda el tiempo de espera. El rango de valores es de 0 a 120, siendo 0 segundos el valor predeterminado.

Ejemplos

Archivo de opciones:

```
nfstimeout 10
```

Línea de mandatos:

```
-nfstimeout=10
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Información relacionada

Consulte “Montajes de hard y soft de NFS” en la página 232 para obtener más información sobre cómo manejar montajes de hard y soft.

Nodename

Utilice la opción `nodename` en el archivo de opciones de cliente para identificar la estación de trabajo en el servidor. Puede utilizar nombres de nodo diferentes para identificar varios sistemas operativos en la estación de trabajo.

Cuando se utiliza la opción `nodename`, se le solicita la contraseña asignada al nodo que especifique, en caso de que se requiera.

Si desea restaurar o recuperar archivos del servidor mientras trabaja en una estación de trabajo diferente, utilice la opción `virtualnodename`. También puede utilizar la opción `asnodename`, si el administrador la ha configurado.

Al conectarse a un servidor, el cliente debe identificarse ante el servidor. Esta identificación de conexión se determina del modo siguiente:

- Si no existe una entrada `nodename` en el archivo `dsm.sys` o una entrada `virtualnodename` en el archivo de opciones del cliente (`dsm.opt`) o no se ha especificado un nombre de nodo virtual en una línea de mandatos, el identificador de conexión predeterminado es el nombre que devuelve el mandato **hostname**.
- Si existe una entrada `nodename` en el archivo `dsm.sys`, la entrada `nodename` modificará temporalmente el nombre que devuelve el mandato **hostname**.
- Si existe una entrada `virtualnodename` en el archivo de opciones del cliente (`dsm.sys`) o se ha especificado un nombre de nodo virtual en una línea de mandatos, éste no podrá ser igual al nombre que devuelve el mandato **hostname**. Cuando el servidor acepte el valor de `virtualnodename`, se solicitará una contraseña (si la autenticación está activada), aunque la opción `passwordaccess` se haya establecido en `generate`. Una vez se ha establecido la conexión con el servidor, se permite el acceso a cualquier archivo del que se efectúa copia de seguridad utilizando este identificador de inicio de sesión.

Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Establezca esta opción en el archivo `dsm.sys` dentro de una sección de servidor. Puede establecer esta opción en el separador **General**, en el campo **Nombre de nodo** del editor de preferencias.

Sintaxis

►►—NODename— —*nodename*—►►

Parámetros

nodename

Especifica un nombre de nodo de 1 a 64 caracteres para el que se solicitan servicios de IBM Spectrum Protect. El valor predeterminado es el valor que se devuelve con el mandato **hostname**.

Si no se especifica un nombre de nodo, el nombre de nodo se establecerá de forma predeterminada en el nombre de sistema principal de la estación de trabajo.

Ejemplos

Archivo de opciones:

`nodename pilar`

“Virtualnodename” en la página 608

Nojournal

Utilice la opción `nojournal` con el mandato **incremental** para especificar que desea realizar una copia de seguridad incremental completa tradicional, en lugar de la copia de seguridad basada en registro por diario predeterminada.

La copia de seguridad incremental con diario se diferencia de la copia de seguridad incremental completa tradicional en los siguientes aspectos:

- Las frecuencias de copia no predeterminadas (distintas de 0) no se imponen en el servidor de IBM Spectrum Protect.
- El daemon de registro por diario no detecta los cambios realizados en archivos especiales UNIX y, por lo tanto, no se incluyen en la copia de seguridad.

Por estos motivos, es recomendable utilizar la opción `nojournal` de forma periódica para realizar una copia de seguridad incremental completa tradicional.

Clientes soportados

Esta opción es válida para el cliente de copia de seguridad-archivado de AIX y Linux.

Sintaxis

►►—NOJournal—►►

Parámetros

No hay parámetros para esta opción.

Ejemplos

Línea de mandatos:

```
dsmc incr /home -nojournal
```

Conceptos relacionados:

“Copia de seguridad con registro por diario” en la página 709

Noprompt

La opción **noprompt** suprime la solicitud de confirmación que presentan los mandatos **delete group**, **delete archive**, **expire**, **restore image** y **set event**.

- **delete archive**
- **delete backup**
- **delete group**
- **expire**
- **restore image**

Nota: El mandato **restore image** no se aplica a los sistemas operativos Mac OS X.

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Sintaxis

►►—NOPrompt—◄◄

Parámetros

No hay parámetros para esta opción.

Ejemplos

Línea de mandatos:

```
dsmc delete archive -noprompt "/Users/van/Documents/*"
```

Línea de mandatos:

```
dsmc delete archive -noprompt "/home/project/*"
```

Nrtablepath

La opción **nrtablepath** especifica la ubicación de la tabla de réplica de nodo en el cliente. El cliente de copia de seguridad y archivado utiliza esta tabla para almacenar la información acerca de cada operación de copia de seguridad o archivado en el servidor de IBM Spectrum Protect.

El servidor en el que hace una copia de seguridad de los datos debe ser de la Versión 7.1 o posterior y debe poder replicar datos del nodo del cliente en el servidor secundario.

Cuando se produce una migración tras error, la información que se encuentra en el servidor secundario es posible que no sea la versión más reciente si la réplica no se

ha realizado antes de la migración tras error. El cliente puede comparar la información en la tabla de réplica de nodo en la información que se encuentra en el servidor secundario para determinar si la copia de seguridad del servidor es la versión de copia de seguridad más reciente.

Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Coloque esta opción en el archivo de opciones del sistema cliente (dsm.sys).

Esta opción también se puede configurar en el conjunto de opciones de cliente en el servidor de IBM Spectrum Protect.

Sintaxis

►►—NRTABLEPath—*vía de acceso*—►►

Parámetros

vía de acceso

Especifica la ubicación en que se crea la base de datos de tabla de réplica de nodo. La ubicación predeterminada es el directorio de instalación del cliente de copia de seguridad y archivado.

Para usuarios que no sean root, debe especificar una vía de acceso sobre la que el ID de usuario tenga acceso de grabación, por ejemplo un directorio temporal. La mayoría de los usuarios que no son root no tienen acceso al directorio de instalación del cliente.

Restricción: La tabla de réplica de nodo no se puede crear en el directorio raíz (/). Si decide especificar una ubicación para la tabla de réplica de nodo, no especifique el directorio raíz.

Ejemplo

Archivo de opciones:

```
nrtablepath /Volumes/nrtbl
```

Línea de mandatos:

No se aplica.

Tareas relacionadas:

“Determinación del estado los datos replicados del cliente” en la página 100

“Configuración del cliente de migración automática tras error” en la página 98

Numberformat

La opción numberformat especifica el formato que desea utilizar para visualizar los números.

Los clientes AIX y Solaris admiten entornos regionales distintos del inglés que describen cada interfaz de usuario que varía en función de la ubicación o el idioma.

De manera predeterminada, los clientes de copia de seguridad/archivado y de administración obtienen la información de formato de la definición del entorno local que esté en funcionamiento en el momento en que se llama al cliente. Consulte la documentación del sistema local para obtener más detalles sobre la configuración del entorno local.

Nota: la opción `numberformat` no afecta al cliente web. El cliente web utiliza el formato de número de la configuración regional con la que se ejecuta el navegador. Si el navegador no se está ejecutando en un entorno local compatible, el cliente web utiliza un formato de números para el inglés estadounidense.

Puede utilizar la opción `numberformat` con los mandatos siguientes:

- **delete archive**
- **delete backup**
- **expire**
- **query archive**
- **query backup**
- **query image**
- **query nas**
- **restore**
- **restore image**
- **restore nas**
- **retrieve**
- **set event**

Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Establezca esta opción en el archivo de opciones de usuario del cliente (`dsm.opt`). Puede establecer esta opción en la ficha **Configuración regional**, en el campo **Formato numérico** del Editor de preferencias.

Sintaxis

►►—`Numberformat`— *—number—*—————►►

Parámetros

number

Muestra los números utilizando uno de los siguientes formatos. Especifique el número (0–6) que corresponda al formato de número que desee utilizar.

0 Utiliza el formato de fecha especificado por el entorno local. Es el valor predeterminado (no se aplica a Mac OS X).

1 1,000.00

Éste es el valor predeterminado para las siguientes traducciones disponibles:

- Inglés de Estados Unidos
- Japonés
- Chino (tradicional)
- Chino (simplificado)
- Coreano

2 1,000,00

3 1 000,00

Éste es el valor predeterminado para las siguientes traducciones disponibles:

- Francés
- Checo
- Húngaro
- Polaco
- Ruso

4 1 000.00

5 1.000,00

Éste es el valor predeterminado para las siguientes traducciones disponibles:

- Portugués de Brasil
- Alemán
- Italiano
- Español

6 1'000,00

En AIX and Solaris: para definir formatos de número, modifique las líneas siguientes en el archivo de origen del entorno local. Sea cual sea el formato seleccionado se aplica tanto a la salida como a la entrada.

punto_decimal

El carácter que separa el número entero de la parte decimal.

separador_miles

El carácter que separa las centenas, los millares y los millones.

grouping

El número de dígitos que se incluye en cada grupo se separa con el carácter thousands_sep.

Ejemplos

Archivo de opciones:

num 4

Línea de mandatos:

-numberformat=4

Esta opción es válida en la línea de mandatos inicial y en modalidad interactiva. Si utiliza esta opción en modalidad interactiva, sólo afectará al mandato con el que se especifica. Cuando se complete la ejecución de ese mandato, el valor se revierte al comienzo de la sesión interactiva. Será el valor del archivo dsm.opt, a menos que se haya modificado mediante la línea de mandatos inicial o mediante una opción que el servidor ha forzado.

Optfile

La opción `optfile` especifica el archivo de opciones de cliente que se ha de utilizar cuando inicia una sesión del cliente de copia de seguridad y archivado.

Clientes soportados

Esta opción es válida para todos los clientes.

Sintaxis

►► —OPTFILE =— —*file_name*— ◀◀

Parámetros

nombre_archivo

Especifica un archivo de opciones del cliente alternativo, si utiliza el nombre de vía de acceso cualificado al completo. Si sólo especifica el nombre del archivo, el cliente da por supuesto que el nombre de archivo especificado se encuentra en el directorio de trabajo actual. El valor predeterminado es dsm.opt.

Restricción: especifique la vía de acceso completa cuando utilice esta opción con el daemon de aceptación de clientes (dsmcad), pues éste cambia su directorio de trabajo por el directorio raíz ("/") después de la inicialización.

Ejemplos

Línea de mandatos:

```
dsmc query session -optfile=myopts.opt
```

Daemon de aceptación de clientes:

```
dsmcad -optfile=/usr/tivoli/tsm/client/ba/bin/myopts.opt
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Contraseña

La opción password especifica una contraseña para IBM Spectrum Protect.

Si no se especifica esta opción y el administrador ha establecido la autenticación en 0n, se le solicitará una contraseña al usuario al iniciar una sesión del cliente de copia de seguridad y archivado.

Nota:

1. Si el servidor solicita una contraseña, ésta no se visualizará cuando la escriba. No obstante, si utiliza la opción password en la línea de mandatos, la contraseña se visualizará cuando que la escriba.
2. Si el nombre de servidor de IBM Spectrum Protect cambia o si los clientes de copia de seguridad y archivado se dirigen a otro servidor, todos los clientes deberán autenticarse de nuevo con el servidor, porque se debe volver a generar la contraseña cifrada almacenada.

La opción password no se tiene en cuenta si el valor de passwordaccess es generate.

Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Establezca esta opción en el archivo de opciones de usuario del cliente (dsm.opt).

Sintaxis

►—PASSword— *—password—* ►

Parámetros

password

Especifica la contraseña utilizada para iniciar sesión en el servidor de IBM Spectrum Protect.

Las contraseñas pueden tener una longitud máxima de 63 caracteres. Las restricciones de la contraseña varían, dependiendo de donde se almacenan y gestionan las contraseñas, y en función de la versión del servidor al que el cliente se conecta.

Si el servidor de IBM Spectrum Protect tiene la versión 6.3.3 o posterior y si usa un servidor de directorios LDAP para autenticar contraseñas:

Utilice cualquiera de los siguientes caracteres para crear una contraseña:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ( )
| { } [ ] : ; < > , ? / ~
```

Las contraseñas son sensibles a las mayúsculas y minúsculas, y están sujetas a restricciones adicionales que puedan imponer las políticas de LDAP.

Si el servidor IBM Spectrum Protect está en la versión 6.3.3 o posterior, y si no utiliza un servidor LDAP para gestionar contraseñas

Utilice cualquiera de los siguientes caracteres para crear una contraseña:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ( )
| { } [ ] : ; < > , ? / ~
```

Las contraseñas se almacenan en la base de datos del servidor IBM Spectrum Protect y no distinguen entre mayúsculas y minúsculas.

Si el servidor IBM Spectrum Protect es anterior a la versión 6.3.3

Utilice cualquiera de los siguientes caracteres para crear una contraseña:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9
_ - & + .
```

Las contraseñas se almacenan en la base de datos del servidor IBM Spectrum Protect y no distinguen entre mayúsculas y minúsculas.

Recuerde:

En la línea de mandatos, escriba entre comillas todos los parámetros que contengan uno o varios caracteres especiales. Sin las comillas, los caracteres especiales se pueden interpretar como caracteres de escape, caracteres de redirección de archivos u otros caracteres que tienen importancia para el sistema operativo.

En sistemas AIX, Linux y Solaris:

Escriba los parámetros de mandato entre comillas simples (').

Ejemplo de línea de mandatos:

```
dsmc set password -type=vmguest 'Win 2012 SQL'  
'tssl2dag\administrator' '7@#$$%^&7'
```

Las comillas no son necesarias cuando escribe una contraseña con caracteres especiales en el archivo de opciones.

Ejemplos

Archivo de opciones:

password contraseña

Línea de mandatos:

-password=contraseña

-password='my>pas\$word'

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Passwordaccess

La opción passwordaccess especifica si desea generar la contraseña automáticamente o establecerla mediante una petición al usuario.

El administrador puede solicitar una contraseña para su nodo cliente activando la función de autenticación. Consulte al administrador si se requiere una contraseña para el nodo cliente del usuario.

Si necesita una contraseña, puede seleccionar uno de los métodos siguientes:

- Definir la contraseña del nodo cliente y hacer que el cliente la solicite cada vez que usted solicite servicios.
- Hacer que el cliente genere automáticamente una nueva contraseña para el nodo cliente cada vez que caduque, la cifre y la almacene en un archivo y la recupere del archivo cuando se soliciten los servicios. No se solicita al usuario que especifique la contraseña.
- Si el servidor no está configurado para solicitar una contraseña al iniciar sesión, todavía se le puede solicitar que escriba la contraseña de nodo cuando el cliente de archivado y copia de seguridad establece una conexión con el servidor. Este comportamiento se produce si esta opción, passwordaccess, se permite como valor predeterminado o si la establece en indicador de passwordaccess. La contraseña que proporciona en respuesta a la solicitud se utiliza sólo para cifrar la información de inicio de sesión; no se utiliza para iniciar sesión en el servidor. En esta configuración, puede evitar tener que especificar una contraseña estableciendo esta opción en passwordaccess generate. Al establecer passwordaccess generate el cliente crea, almacena y envía la contraseña en su lugar. Cuando se establece passwordaccess generate, se ignora la opción password.

Debe establecer la opción passwordaccess en generate en las situaciones siguientes:

- Cuando se utilice el cliente de HSM.
- Cuando se utilice el cliente web.
- Cuando se efectúen operaciones NAS.
- Cuando se utilice IBM Spectrum Protect for Workstations.

Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Establezca esta opción en el archivo `dsm.sys` dentro de una sección de servidor. Puede establecer esta opción en el separador **Autorización**, en la sección **Acceso con contraseña** del editor de preferencias.

Sintaxis



Parámetros

prompt

Se le solicitará la contraseña del nodo de cliente cada vez que un cliente se conecte al servidor. Éste es el valor predeterminado.

Para proteger la contraseña del nodo cliente, escriba los mandatos sin la contraseña y espere a que el cliente se la solicite.

Cada usuario debe conocer la contraseña de IBM Spectrum Protect para el nodo cliente. Cualquier usuario que conozca la contraseña del nodo cliente puede obtener acceso a todas las copias de seguridad y todas las copias archivadas que se originan desde el nodo cliente. Por ejemplo: si el usuario especifica el nombre de nodo y la contraseña de un nodo cliente desde otro nodo cliente, el usuario se convierte en un usuario root virtual.

Las aplicaciones API deben proporcionar la contraseña cuando se inicie una sesión. La aplicación es la encargada de obtener la contraseña.

generate

Cifra y almacena la contraseña de forma local y genera una nueva cuando caduca la anterior. El cliente genera aleatoriamente la nueva contraseña. Las restricciones de la contraseña varían, dependiendo de donde se almacenan y gestionan las contraseñas, y en función de la versión del servidor al que el cliente se conecta. Las contraseñas generadas tienen una longitud de 63 caracteres y contienen al menos dos de los caracteres siguientes :

- mayúsculas
- minúsculas
- caracteres numéricos
- caracteres especiales

Además, el primer carácter y el último de una contraseña generada es un carácter alfabético y pueden ser mayúsculas o minúsculas. Las contraseñas generadas no contienen caracteres repetidos.

Aparecerá una solicitud de contraseña al inscribir una estación de trabajo con un servidor utilizando la inscripción abierta, o bien si el administrador cambia manualmente la contraseña.

Cuando se inicia la sesión localmente, los usuarios no necesitan saber la contraseña del nodo cliente. Sin embargo, si se utiliza la opción `nodename` en un nodo remoto,

los usuarios pueden acceder a los archivos de los que son propietarios y a los archivos a los que otro usuario les conceda acceso.

Ejemplos

Archivo de opciones:

`passwordaccess generate`

Línea de mandatos:

No se aplica.

Información relacionada

Si desea obtener información sobre la ubicación en la que se almacena la contraseña, consulte el apartado “`Passworddir`”.

Passworddir

La opción `passworddir` especifica el directorio donde debe almacenarse el archivo de la contraseña cifrada.

El directorio predeterminado para AIX es `/etc/security/adsm` y para otras plataformas UNIX y Linux es `/etc/adsm`. Independientemente de donde se almacene, el archivo de contraseñas creado por el cliente siempre se denomina `TSM.PWD`.

Clientes soportados

Esta opción es válida para todos los clientes UNIX.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor.

Sintaxis

►►—`PASSWORDDIR`— *directoryname*—◀◀

Parámetros

directoryname

Especifica la vía de acceso en la que se almacenará el archivo de contraseñas cifradas. El nombre del archivo de contraseñas es `TSM.PWD`. Si cualquier parte de la vía de acceso especificada no existe, IBM Spectrum Protect intenta crearla.

Ejemplos

Archivo de opciones:

```
passworddir "/Users/user1/Library/Preferences/Tivoli Storage Manager/"
passworddir /etc/security/tsm
```

Línea de mandatos:

No se aplica.

Pick

La opción `pick` crea la lista de versiones de copia de seguridad o copias archivadas que coinciden con la especificación de archivo que ha especificado.

En esta lista, puede seleccionar las versiones que se desee procesar. Incluya la opción `inactive` para ver los objetos activos e inactivos.

Para las imágenes, si no especifica un espacio de archivos de origen y un espacio de archivos de destino, la lista `pick` contiene todas las imágenes cuya copia de seguridad se ha realizado. En este caso, las imágenes seleccionadas desde la lista `pick` se restauran en su ubicación original. Si especifica el espacio de archivos origen y el espacio de archivos destino, puede seleccionar sólo una entrada de la lista `pick`.

La opción `pick` puede utilizarse con los mandatos siguientes:

- **`delete archive`**
- **`delete backup`**
- **`delete group`**
- **`expire`**
- **`restore`**
- **`restore group`**
- **`restore image`**
- **`restore nas`**
- **`retrieve`**

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Sintaxis

►►—Pick—————◄◄

Parámetros

No hay parámetros para esta opción.

Ejemplos

Línea de mandatos:

```
dsmc restore "/Users/van/Documents/*" -pick -inactive
```

Línea de mandatos:

```
dsmc restore "/home/project/*" -pick -inactive
```

Pitdate

Utilice la opción `pitdate` con la opción `pittime` para establecer un instante específico para visualizar o restaurar la última versión de las copias de seguridad.

Se procesarán los archivos cuya copia de seguridad se ha realizado *en o antes* de la fecha y hora que especifique y que no se han suprimido *antes* de la fecha y la hora que especifique. Las versiones de copia de seguridad que se hayan creado después de esta fecha y hora se pasan por alto.

La opción `pitdate` puede utilizarse con los mandatos siguientes:

- **delete backup**
- **query backup**
- **query group**
- **query image**
- **restore**
- **restore group**
- **restore image**
- **restore nas**

Cuando se utiliza `pitdate`, las opciones `inactive` y `latest` son implícitas.

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Sintaxis

►►—PITDate =— —*date*—————►►

Parámetros

date

Especifica la fecha apropiada. Escriba la fecha en el formato seleccionado con la opción `dateformat`.

Si se incluye la opción `dateformat` con un mandato, ésta debe anteponerse a las opciones `fromdate`, `pitdate` y `todate`.

Ejemplos

Línea de mandatos:

```
dsmc restore "/Volumes/proj4/myproj/*" -sub=y -pitdate=08/01/2003  
-pittime=06:00:00
```

Línea de mandatos:

```
dsmc restore "/fs1/*" -sub=y -pitdate=08/01/2003 -pittime=06:00:00
```

Pittime

Utilice la opción `pittime` con la opción `pitdate` para establecer un instante específico para el cual desea visualizar o restaurar la última versión de las copias de seguridad.

Se procesarán los archivos cuya copia de seguridad se ha realizado *en o antes* de la fecha y hora que especifique y que no se han suprimido *antes* de la fecha y la hora que especifique. Las versiones de copia de seguridad que se hayan creado después de esta fecha y hora se pasan por alto. Esta opción se ignora si no especifica la opción `pitdate`.

La opción `pittime` puede utilizarse con los mandatos siguientes:

- **delete backup**
- **query backup**
- **query image**
- **restore**
- **restore image**
- **restore nas**

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Sintaxis

►►—PITTime =— —*hora*—————►►

Parámetros

hora

Especifica una hora en la fecha indicada. Si no se especifica una hora, se toma el valor predeterminado 23:59:59. Especifique la hora en el formato seleccionado con la opción `timeformat`.

Cuando incluya la opción `timeformat` en un mandato, ésta deberá preceder a las opciones `fromtime`, `pittime` y `totttime`.

Ejemplos

Línea de mandatos:

```
dsmc query backup -pitt=06:00:00 -pitd=08/01/2003  
"/Volumes/proj5/myproj/*"
```

Línea de mandatos:

```
dsmc q b "/fs1/*" -pitt=06:00:00 -pitd=08/01/2003
```

Postschedulecmd/Postnschedulecmd

La opción `postschedulecmd/postnschedulecmd` especifica un mandato que el programa cliente procesa después de ejecutar una planificación.

Si desea que el programa cliente para esperar a que el mandato finalice antes de continuar con otro proceso, utilice la opción `postschedulecmd`. Si no desea esperar a que el mandato finalice antes de que el cliente continúe con otro proceso, especifique la opción `postnschedulecmd`.

El comportamiento del manejo de códigos de retorno y de las acciones planificadas depende de la opción especificada y del tipo de operación que se haya planificado:

- Para operaciones planificadas en las que la acción planificada es distinto de **COMMAND**:

Si el mandato `postschedulecmd` no se completa con el código de retorno 0 (cero), el código de retorno para el evento planificado es 8 o el código de evento para la operación planificada, lo que ocurra antes. Si no desea que esta regla se aplique al mandato `postschedulecmd`, cree un archivo script o por lotes que inicie el mandato y finalice con el código de retorno 0. A continuación, configure `postschedulecmd` de modo que inicie el archivo script o por lotes.

- Para operaciones planificadas en las que la acción planificada es **COMMAND**:

El código de retorno del mandato especificado en la opción `postschedulecmd` no afecta al código de retorno del que se informa al servidor cuando se completa el evento planificado. Si desea que los resultados de las operaciones `postschedulecmd` afecten al código de retorno del evento planificado, incluya las operaciones `postschedulecmd` en el script del mandato de acción planificado en lugar de utilizar la opción `postschedulecmd`.

- Si la acción del planificador no se puede iniciar y el mandato especificado en la opción `preschedulecmd` se completa con un código de retorno de cero (0), se ejecuta el mandato especificado por la opción `postschedulecmd`.
- No se realiza el seguimiento de código de retorno de una operación especificada en la opción `postschedulecmd`, y no afecta al código de retorno del evento planificado.

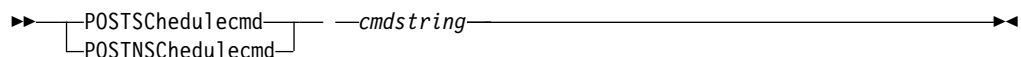
Cientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción. El servidor también puede definir esta opción.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. Puede establecer esta opción en la ficha **Planificador**, en el recuadro de texto **Mandato de planificación** del Editor de preferencias. El servidor también puede definir estas opciones.

Sintaxis



Parámetros

cmdstring

Especifica el mandato que se debe procesar. Con esta opción puede entrarse un mandato para que se ejecute después de una planificación. Utilice únicamente una opción `postschedulecmd`.

Si la serie del mandato contiene espacios en blanco, especifique la serie del mandato entre comillas. Si ya ha colocado la serie del mandato entre comillas, especifique toda la serie del mandato entre comillas simples.

Utilice una serie en blanco, o nula, para *cmdstring* si desea impedir que se ejecute cualquier mandato que el administrador del servidor de IBM Spectrum Protect utiliza para `postschedulecmd` o para `preschedulecmd`. Si especifica una serie en blanco o nula en una de las dos opciones, se impedirá que el administrador pueda utilizar un mandato en ambas opciones.

Si el administrador utiliza una serie en blanco o nula en la opción `postschedulecmd`, el usuario no podrá ejecutar un mandato posterior a la planificación (post-schedule).

En el caso de Mac OS X, si el mandato planificado `postschedulecmd` es un AppleScript, tiene que utilizar el mandato **osascript** para ejecutar el script. Por ejemplo, si "Database Script" es un AppleScript, especifique este mandato:

```
postschedulecmd osascript "/Volumes/La Pomme/Scripting/
Database Script"
```

Ejemplos

Archivo de opciones:

```
Para Mac OS X: postschedulecmd "/Volumes/La Pomme/Scripting/
postsched.sh"
```

Archivo de opciones:

```
postschedulecmd "restart database"
```

La serie del mandato es un mandato válido para arrancar la base de datos.

Línea de mandatos:

```
-postschedulecmd="/Volumes/La Pomme/Scripting/postsched.sh"
```

Línea de mandatos:

```
-postschedulecmd="'restart database'"
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Conceptos relacionados:

Capítulo 8, “Códigos de retorno del cliente”, en la página 297

Referencia relacionada:

 Mandato DEFINE SCHEDULE

Postsnapshotcmd

La opción **postsnapshotcmd** le permite ejecutar scripts o mandatos de shell del sistema operativo después de que el cliente de copia de seguridad y archivado haya iniciado una instantánea durante una operación de copia de seguridad basada en instantánea.

AIX únicamente: esta opción solo se aplica a la copia de seguridad o archivado del archivo JFS2 basada en instantánea y a la copia de seguridad de imagen basada en instantánea. Para una copia de seguridad de archivos basada en instantánea o archivado, utilice esta opción con el mandato **backup**, con la opción `include.fs` o bien en el archivo `dsm.sys`.

Linux únicamente: esta opción sólo es válida si LVM está instalado y configurado en el sistema, lo cual permite realizar una copia de seguridad de imágenes basada en instantánea.

Solo AIX y Linux: para una copia de seguridad de imágenes basada en instantánea, utilice esta opción con el mandato **backup image**, con la opción `include.image` o en el archivo `dsm.sys`.

Si **postsnapshotcmd** falla, la operación continúa pero se anotan los avisos que corresponda.

Clientes soportados

Esta opción solo es válida para los clientes AIX y los clientes Linux x86_64. La API de IBM Spectrum Protect no admite esta opción. El servidor también puede definir esta opción.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. También puede establecer esta opción en la ficha

Image-Snapshot del editor de preferencias.

Sintaxis

►—POSTSNAPshotcmd— —"*cmdstring*"—►

Parámetros

"cmdstring"

Especifica el mandato que ha de procesarse.

Utilice la opción `srvprepostsnapdisabled` para impedir que el administrador del servidor de IBM Spectrum Protect pueda ejecutar mandatos del sistema operativo en el sistema cliente.

Si la cadena del mandato contiene espacios en blanco, debe especificarse entre comillas:

```
"resume database  
myDb"
```

Si ya ha colocado la serie del mandato entre comillas, especifique toda la serie del mandato entre comillas simples:

```
'resume database "myDb"'
```

Ejemplos

Archivo de opciones:

```
postsnapshotcmd "any command"
```

La serie del mandato es un mandato válido para reiniciar la aplicación.

Línea de mandatos:

```
backup image -postsnapshotcmd="any command"
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Información relacionada

“Opciones include” en la página 458

“Srvprepostscheddisabled” en la página 574

Preschedulecmd/Prenschedulecmd

La opción `preschedulecmd` especifica un mandato que el programa cliente procesa antes de ejecutar una planificación.

El programa de cliente espera a que se complete el mandato antes de empezar la planificación. Si no se desea esperar, especifique `prenschedulecmd`.

Nota:

1. La finalización satisfactoria del mandato `preschedulecmd` se considera una condición previa para ejecutar la operación planificada. Si el mandato `preschedulecmd` no finaliza con el código de retorno 0, no se ejecutarán la operación planificada ni los mandatos `postschedulecmd` y `postnschedulecmd`. El cliente notificará que el evento planificado no se ha ejecutado correctamente y el código de retorno será 12. Si no desea que esta regla se aplique al mandato

preschedulecmd, cree un archivo script o por lotes que invoque el mandato y finalice con el código de retorno 0. A continuación, configure preschedulecmd de modo que invoque el archivo script o por lotes. El código de retorno del mandato preschedulecmd no se registra y no afecta al código de retorno del evento planificado.

2. El servidor también puede definir la opción preschedulecmd (y la opción preschedulecmd).

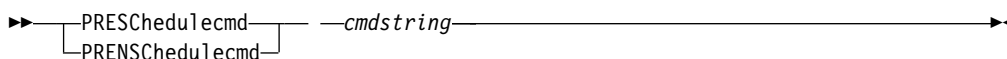
Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción. El servidor también puede definir esta opción.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor. Puede establecer esta opción en el separador **Planificador**, en el recuadro de diálogo **Mandato de planificación** del Editor de preferencias.

Sintaxis



Parámetros

cmdstring

Especifica el mandato que se debe procesar. Utilice sólo una opción preschedulecmd. Con esta opción puede entrarse un mandato para que se ejecute antes de una planificación.

Si la serie del mandato contiene espacios en blanco, especifique la serie del mandato entre comillas. Si ya ha colocado la serie del mandato entre comillas, especifique toda la serie del mandato entre comillas simples.

Utilice espacios en blanco o una cadena nula para *cmdstring* si desea impedir que se ejecuten mandatos que el administrador del servidor de IBM Spectrum Protect utilice para postschedulecmd y preschedulecmd. Si especifica una serie en blanco o nula en una de las dos opciones, se impedirá que el administrador pueda utilizar un mandato en ambas opciones.

Si su administrador utiliza un espacio en blanco o una cadena nula en la opción preschedulecmd, el usuario no puede ejecutar un mandato previo a la planificación.

Para Mac OS X, si el mandato de planificación preschedulecmd es un script de Apple, deberá utilizar el mandato **osascript** para ejecutar el script. Por ejemplo, si `""Database Script""` es un script de Apple, especifique este mandato:

```
preschedulecmd osascript "/Volumes/La Pomme/Scripting/
Database Script"
```

Ejemplos

Archivo de opciones:

```
preschedulecmd "<mandato de detención del producto de base de datos>
base de datos"
```

La serie del mandato es un mandato válido para paralizar la base de datos.

Línea de mandatos:

`-preschedulecmd="'quiesce database'"`

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Conceptos relacionados:

Capítulo 8, “Códigos de retorno del cliente”, en la página 297

PreserveLastAccessDate

Utilice la opción `preserveLastAccessDate` para especificar si una operación de copia de seguridad o de archivado cambia la última hora de acceso.

Una operación de copia de seguridad o archivado puede cambiar la última hora de acceso de un archivo. Tras una operación, el cliente de copia de seguridad y archivado puede restablecer la última hora de acceso al valor anterior a la operación. En lugar de modificarse, el cliente de copia de seguridad-archivado puede conservar la última hora de acceso. El restablecimiento de la última hora de acceso requiere un proceso adicional para cada archivo del que se haga copia de seguridad o se archive.

Si habilita el soporte de archivos abiertos, la última fecha de acceso de los archivos siempre prevalecerá independientemente de los valores de `preserveLastAccessDate`. Cuando está activado el soporte de archivos abiertos, no utilice la opción `preserveLastAccessDate`.

Utilice esta opción con los mandatos **incremental**, **selective** o **archive**.

Nota:

1. Esta opción sólo se aplica a archivos; no se aplica a directorios.
2. El restablecimiento de la última fecha de acceso afecta al rendimiento de la copia de seguridad y el archivado.
3. El restablecimiento de la última fecha de acceso puede afectar a aplicaciones que dependan de últimas fechas de acceso precisas, como es el caso de la aplicación de gestión de recursos de almacenamiento (SRM).
4. En sistemas de archivos que no están gestionados por el cliente IBM Spectrum Protect for Space Management o durante operaciones de copia de seguridad o archivado de usuarios que no sean root, el atributo `ctime` se restablece. El atributo de última fecha y hora cambiada (`ctime`) se restablece a la fecha y hora de la operación de copia de seguridad o archivado.
5. La opción `updateTime` prevalece sobre la opción `preserveLastAccessDate`. Si ambas opciones están establecidas en `yes`, la opción `preserveLastAccessDate` se pasa por alto.
6. En sistemas de archivos que no gestione el cliente IBM Spectrum Protect for Space Management, no utilice `preserveLastAccessDate` y ni el mandato de GPFS `mmbackup`. El mandato **mmbackup** y `preserveLastAccessDate yes` selecciona todos los archivos para cada operación de copia de seguridad.
7. No se puede restablecer la fecha del último acceso de los archivos de sólo lectura. La opción `preserveLastAccessDate` omite los archivos de sólo lectura y no cambia su fecha.

Clientes soportados

Esta opción es válida para todos los clientes.

El servidor también puede definir esta opción.

Archivo de opciones

Coloque esta opción en el archivo de opciones de usuario del cliente (dsm.opt). Puede establecer esta opción en el separador Copia de seguridad del editor de preferencias.

Sintaxis



Parámetros

No Una operación de copia de seguridad o archivado puede cambiar la última fecha de acceso. Este es el valor predeterminado.

Yes

Una operación de copia de seguridad o archivado no cambia la última fecha de acceso.

Ejemplos

Archivo de opciones:

```
preservelastaccessdate yes
```

Línea de mandatos:

```
Incremental /proj/test/test_file -preservelastaccessdate=yes
```

Información relacionada:

- ➡ Mandato mmbackup: Requisitos de IBM Spectrum Protect
- ➡ Orientación para integrar IBM Spectrum Scale AFM con IBM Spectrum Protect
- ➡ Utilización de las opciones de inclusión y exclusión de IBM Spectrum Protect con el mandato mmbackup de IBM Spectrum Scale

Preservepath

La opción `preservepath` especifica qué volumen del directorio origen se reproducirá como parte del directorio destino cuando se restauran o recuperan archivos en una ubicación nueva.

Utilice la opción `-subdir=yes` para incluir el subárbol completo del directorio de origen (los directorios y archivos que se encuentren en el directorio de origen del nivel más bajo) como el origen que debe restaurarse. Si un directorio destino necesario no existe, se crea. Si un archivo destino tiene el mismo nombre que un archivo origen, se graba sobre él. Utilice la opción `-replace=prompt` para que el cliente le pregunte antes de sobrescribir los archivos.

Utilice la opción `preservepath` con los mandatos siguientes:

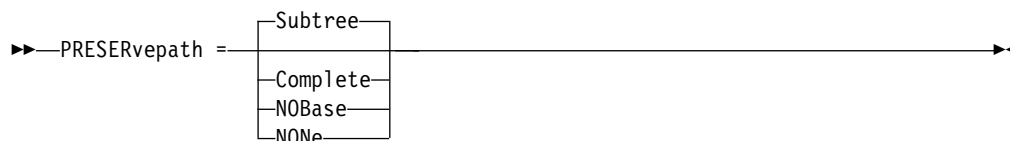
- **restore**

- **restore backupset**
- **restore group**
- **retrieve**

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción. El servidor también puede definir esta opción.

Sintaxis



Parámetros

Subtree

Crea el directorio de origen de más bajo nivel como un subdirectorio del directorio de destino. Los archivos del directorio de origen se almacenan en el nuevo subdirectorio. Éste es el valor predeterminado.

Complete

Restaura toda la vía de acceso, empezando desde el directorio raíz, en el directorio especificado. La vía de acceso completa incluye todos los directorios excepto el nombre del espacio de archivos.

NOBase

Restaura el contenido del directorio de origen sin directorio de nivel inferior, o base, en el directorio de destino especificado.

NONE

Restaura todos los archivos de origen seleccionados en el directorio de destino. Ninguna parte de la vía de acceso de origen al mismo nivel o por encima del directorio de origen se reproduce en el destino.

Si se especifica SUBDIR=yes, el cliente restaura todos los archivos de los directorios de origen en el directorio de destino único.

Ejemplos

Línea de mandatos:

Supongamos que el espacio de archivos del servidor contiene las copias de seguridad siguientes:

```

/fs/h1/m1/file.a
/fs/h1/m1/file.b
/fs/h1/m1/l1/file.x
/fs/h1/m1/l1/file.y
  
```

Este mandato:

```
dsmc res /fs/h1/m1/ /u/ann/ -preser=complete
```

Restaura estos directorios y archivos:

```

/u/ann/h1/m1/file.a
/u/ann/h1/m1/file.b
  
```

Este mandato:

```
dsmc res /fs/h1/m1/ /u/ann/ -preser=nobase
```

Restaura estos directorios y archivos:

```
/u/ann/file.a  
/u/ann/file.b
```

Este mandato:

```
dsmc res backupset /fs/h1/m1/ /u/ann/ -su=yes  
-preser=nobase -loc=file
```

Restaura estos directorios y archivos:

```
/u/ann/file.a  
/u/ann/file.b  
/u/ann/file.x  
/u/ann/file.y
```

Este mandato:

```
dsmc res /fs/h1/m1/ /u/ann/ -preser=subtree
```

Restaura estos directorios y archivos:

```
/u/ann/m1/file.a  
/u/ann/m1/file.b
```

Este mandato:

```
dsmc res /fs/h1/m1/ /u/ann/ -preser=none
```

Restaura estos directorios y archivos:

```
/u/ann/file.a  
/u/ann/file.b
```

Este mandato:

```
dsmc res /fs/h1/m1/ /u/ann/ -su=yes -preser=complete
```

Restaura estos directorios y archivos:

```
/u/ann/h1/m1/file.a  
/u/ann/h1/m1/file.b  
/u/ann/h1/m1/l1/file.x  
/u/ann/h1/m1/l1/file.y
```

Este mandato:

```
dsmc res /fs/h1/m1/ /u/ann/ -su=yes -preser=nobase
```

Restaura estos directorios y archivos:

```
/u/ann/file.a  
/u/ann/file.b  
/u/ann/l1/file.x  
/u/ann/l1/file.y
```

Este mandato:

```
dsmc res /fs/h1/m1/ /u/ann/ -su=yes -preser=subtree
```

Restaura estos directorios y archivos:

```
/u/ann/m1/file.a  
/u/ann/m1/file.b  
/u/ann/m1/l1/file.x  
/u/ann/m1/l1/file.y
```

Este mandato:

```
dsmc res /fs/h1/m1/ /u/ann/ -su=yes -preser=none
```

Restaura estos directorios y archivos:

```
/u/ann/file.a  
/u/ann/file.b  
/u/ann/file.x  
/u/ann/file.y
```

Presnapshotcmd

La opción `presnapshotcmd` le permite ejecutar mandatos del sistema operativo antes de que el cliente de copia de seguridad y archivado inicie una instantánea.

Esto le permite detener una aplicación antes de que el cliente inicie la instantánea durante una operación de copia de seguridad basada en instantánea o archivado.

AIX únicamente: esta opción solo se aplica a la copia de seguridad o archivado del archivo JFS2 basada en instantánea y a la copia de seguridad de imagen basada en instantánea. Para una copia de seguridad de archivos basada en instantánea o archivado, utilice esta opción con el mandato **backup**, con la opción `include.fs` o bien en el archivo `dsm.sys`.

Linux únicamente: esta opción solo es válida si LVM está instalado y configurado en el sistema, lo cual permite realizar una copia de seguridad de imágenes basada en instantánea.

Solo AIX y Linux: para una copia de seguridad de imágenes basada en instantánea, utilice esta opción con el mandato **backup image**, con la opción `include.image` o bien en el archivo `dsm.sys`.

Si la ejecución de `presnapshotcmd` no se realiza correctamente, se da por supuesto que la aplicación no se encuentra en un estado coherente y el cliente detiene la operación y visualiza el mensaje de error adecuado.

Clientes soportados

Esta opción solo es válida para los clientes AIX JFS2 y Linux x86_64. La API de IBM Spectrum Protect no admite esta opción. El servidor también puede definir esta opción.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. También puede establecer esta opción en la ficha **Image-Snapshot** del editor de preferencias.

Sintaxis

►—PRESNAPSHOTcmd— —"*cmdstring*"—◄◄

Parámetros

"*cmdstring*"

Especifica el mandato que ha de procesarse.

Utilice la opción `srvprepostsnapdisabled` para impedir que el administrador del servidor de IBM Spectrum Protect pueda ejecutar mandatos del sistema operativo en el sistema cliente.

Si la cadena del mandato contiene espacios en blanco, debe especificarse entre comillas:

```
"quiesce database myDb"
```

Si ya ha colocado la serie del mandato entre comillas, especifique toda la serie del mandato entre comillas simples:

```
'resume database "myDb"'
```

Ejemplos

Archivo de opciones:

```
presnapshotcmd "any shell command or script"
```

Línea de mandatos:

```
backup image -presnapshotcmd="any shell command or script"
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Información relacionada

“Opciones include” en la página 458

“Srvprepostscheddisabled” en la página 574

Queryschedperiod

La opción `queryschedperiod` especifica el número de horas que se desea que espere el planificador cliente entre los intentos de establecer contacto con el servidor para realizar trabajos planificados.

Esta opción sólo se aplica si el valor de `schedmode` es `polling`. Esta opción sólo se utiliza cuando se está ejecutando el planificador.

El administrador también puede definir esta opción. Si el administrador especifica un valor para esta opción, ese valor altera temporalmente el valor establecido en el archivo de opciones de cliente después de que el nodo de cliente haya establecido contacto correctamente con el servidor.

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción. El servidor también puede definir esta opción.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. Puede establecer esta opción en el separador **Planificador**, en el campo **Intervalo para consultar planificación** del Editor de preferencias.

Sintaxis

►►—QUERYSCedperiod— —horas—►►

Parámetros

horas

Especifica el número de horas que el planificador cliente espera entre intentos de establecer contacto con el servidor para realizar trabajos planificados. El rango de valores es de 1 a 9999, siendo 12 el valor predeterminado.

Ejemplos

Archivo de opciones:

querysch 6

Línea de mandatos:

-queryschedperiod=8

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Querysummary

La opción querysummary proporciona estadísticas sobre los archivos, directorios y objetos que devuelven los mandatos **query backup** o **query archive**.

La opción querysummary proporciona las estadísticas siguientes:

- El número añadido de archivos y directorios devueltos por el mandato query backup o query archive
- El número añadido de datos de los objetos devueltos por el mandato query backup o query archive
- La estimación de uso de memoria de restauración clásica para restaurar objetos devueltos por el mandato query backup o query archive
- El número total de volúmenes de servidor únicos donde residen los objetos devueltos por el mandato query

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Sintaxis

►►—QUERYSUMMARY—◄◄

Parámetros

No hay parámetros para esta opción.

Ejemplos

Línea de mandatos:

dsmc q ba '/usr/fs1/*' -sub=yes -querysummary

[root@kaveri:/home/cpark] \$ dsmc q ba '/kalafs1/*' -sub=yes -querysummary

IBM Spectrum Protect

Interfaz de línea de mandatos del cliente de copia de seguridad/archivado

Versión de cliente 8, release 1, nivel 0.0

Fecha/hora del cliente: 12/09/2016 12:05:35

(c) Copyright by IBM Corporation y otros 1990, 2016. Reservados todos los derechos.

Node Name: KAVERI
 Sesión establecida con el servidor TEMPLAR: AIX-RS/6000
 Versión de servidor 8, release 1, nivel 0.0
 Fecha/hora del servidor: 12/09/2016 12:05:35 Último acceso: 12/07/2016 07:48:59

Tamaño		Fecha copia seg.		Clase gest.		Archivo A/I
----		-----		-----	---	----
4,096	B	08/07/08 12:07:30		BASVT2	A	/kalafs1/
256	B	08/07/08 12:07:30		BASVT2	A	/kalafs1/dir1
10.485.760	B	08/07/08 12:07:30		DEFAULT	A	/kalafs1/info1
5.242.880	B	08/07/08 12:07:30		DEFAULT	A	/kalafs1/info2
1.044	B	08/07/08 12:07:30		DEFAULT	A	/kalafs1/dir1/subfile1
1.044	B	08/07/08 12:07:30		DEFAULT	A	/kalafs1/dir1/subfile2

Estadísticas de resumen

Total arch.	Total dir.	Prom. tam. arch.	Total datos	Est. memoria
-----	-----	-----	-----	-----
4	2	3,75 MB	15,00 MB	1,07 KB

Número estimado de volúmenes: 2

[root@kaveri:/home/cpark] \$

Quiet

La opción quiet limita el número de mensajes que se muestran en la pantalla durante un proceso.

Por ejemplo, cuando ejecuta los mandatos **incremental**, **selective** o **archive**, es posible que aparezca información sobre cada uno de los archivos de los que se realiza una copia de seguridad. Utilice la opción quiet si no desea visualizar esta información.

Si utiliza la opción quiet, aparece información de error y de proceso en la pantalla, mientras que los mensajes se graban en los archivos de anotaciones. Si no especifica quiet, se utiliza la opción predeterminada, verbose.

Clientes soportados

Esta opción es válida para todos los clientes. El servidor también puede definir la opción quiet y hacer que prevalezca sobre el valor del cliente. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Establezca esta opción en el archivo de opciones de usuario del cliente (dsm.opt). Puede establecer esta opción en la ficha **Línea de mandatos**, en el recuadro de selección **No mostrar información de proceso en pantalla** del Editor de preferencias.

Sintaxis

►►—QUIET—◄◄

Parámetros

No hay parámetros para esta opción.

Ejemplos

Archivo de opciones:

quiet

Línea de mandatos:

-quiet

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Quotesareliteral

La opción `quotesareliteral` especifica si las comillas simples (') o las comillas dobles (") se interpretan literalmente cuando se incluyen en la especificación de una lista de archivos en una opción `filelist`.

Normalmente, el cliente requiere que se utilicen comillas simples o dobles para delimitar especificaciones de archivos que contienen caracteres de espacios. Algunos sistemas de archivos permiten el uso de comillas simples y dobles en los nombres de archivos y directorios.

Para impedir errores que de lo contrario se podrían producir, cuando se incluyen especificaciones de archivos en una opción `filelist` y contienen comillas simples (') o comillas dobles ("), establezca `quotesareliteral` yes. Cuando `quotesareliteral` se establece en yes, las comillas que se incluyen en una especificación de lista de archivos en una opción `filelist` se interpretan literalmente, como comillas, y no como delimitadores.

Esta opción se aplica a cualquier mandato que acepta una opción `filelist` como un parámetro de mandato.

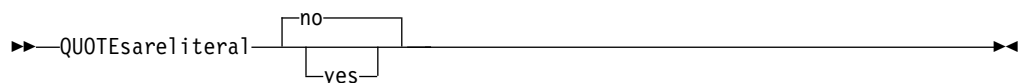
Clientes soportados

Esta opción es válida para todas las plataformas soportadas. La opción se aplica a cualquier mandato que toma una especificación de lista de archivos como parámetro.

Archivo de opciones

Coloque esta opción en el archivo de opciones de usuario del cliente (`dsm.opt`).

Sintaxis



Parámetros

no Especifica que las comillas simples (') y dobles (") se interpretan como delimitadores para las especificaciones de la lista de archivos incluidas en una opción `filelist`. No es el valor predeterminado.

yes

Especifica que las comillas simples (') y dobles (") se interpretan literalmente, y no como delimitadores, para especificaciones de la lista de archivos que se incluyen en una opción `filelist`. Especifique este valor si está realizando la copia de seguridad de archivos desde un sistema de archivos que permite las comillas en nombres de archivo o de directorio.

Ejemplos

Archivo de opciones:

```
QUOTESARELITERAL YES
```

Línea de mandatos:

Suponiendo que el sistema de archivos permita comillas en las vías de acceso, lo siguiente son ejemplos de archivos en una especificación de lista de archivos que se pueden procesar correctamente si `QUOTESARELITERAL` se establece en `YES`

Supongamos que el mandato que se emite es `dsmc sel`
`-filelist=/home/user1/important_files`, donde `important_files.txt` contiene la lista de archivos a procesar.

```
/home/user1/myfiles/"file"1000  
/home/user1/myfiles/'file'  
/home/user1/myfiles/file'ABC  
/home/user1/myfiles/ABC"file"
```

Información relacionada

Para obtener información acerca de la opción `filelist`, consulte “`Filelist`” en la página 439.

Para obtener información sobre la sintaxis para especificaciones de archivo, consulte “Especificación de cadenas de entrada que contengan espacios en blanco o comillas” en la página 145.

“`Wildcardsareliteral`” en la página 651

Removeoperandlimit

La opción `removeoperandlimit` especifica que el cliente elimina el límite de 20 operandos.

Si especifica la opción `removeoperandlimit` con los mandatos **incremental**, **selective** o **archive**, no se aplicará el límite de 20 operandos, y las únicas restricciones serán los recursos disponibles u otros límites del sistema operativo.

La opción `removeoperandlimit` puede ser útil si genera scripts que puedan invocar el cliente de línea de mandatos con un gran número de operandos. Por ejemplo, puede examinar previamente un árbol de directorios para buscar los archivos de los que debe realizarse una copia de seguridad. A medida que se descubre cada uno de los archivos *eligibles*, el archivo se agrega a la lista de operandos de un mandato **selective**. Posteriormente, este mandato **selective** se envía mediante un script de control. En este caso, al especificar la opción `removeoperandlimit` se elimina el límite de 20 operandos.

Nota:

1. La opción `removeoperandlimit` *debe* especificarse inmediatamente después del mandato **incremental**, **selective** o **archive** antes de cualquier especificación de archivo.
2. Esta opción no acepta ningún valor. Si se especifica esta opción en un mandato, se elimina el límite de 20 operandos.
3. Dado que ello afecta negativamente al rendimiento para permitir que el shell expanda caracteres comodín, es aconsejable utilizar la opción `removeoperandlimit` en las operaciones de copia de seguridad o archivado en las que no se utilizan caracteres comodín.
4. La opción `removeoperandlimit` sólo es válida en los mandatos **incremental**, **selective** o **archive** en modalidad por lotes. No es válida en el archivo de opciones de cliente (`dsm.opt`) o en el archivo `dsm.sys`.

Clientes soportados

Esta opción es válida para todos los clientes UNIX y Linux.

Sintaxis

►►—`REMOVEOperandlimit`—————►►

Parámetros

No hay parámetros para esta opción.

Ejemplos

Línea de mandatos:

`-removeoperandlimit`

Replace

La opción `replace` especifica si ha de grabarse encima de los archivos existentes en la estación de trabajo o si ha de solicitarse al usuario que realice la selección deseada al restaurar o recuperar archivos.

Importante: La opción `replace` no afecta a la recuperación de los objetos de directorios. Los objetos de directorios siempre se recuperan, aunque se haya especificado `replace=no`. Para impedir que sobrescriban los directorios existentes, utilice la opción `filesonly`.

Puede utilizar esta opción con los mandatos siguientes:

- **restore**
- **restore backupset**
- **restore group**
- **retrieve**

Nota: la solicitud de sustitución no se produce durante una operación planificada. Si establece la opción `replace` para `prompt`, el cliente de copia de seguridad y archivado pasará por alto los archivos sin realizar ninguna solicitud durante una operación planificada.

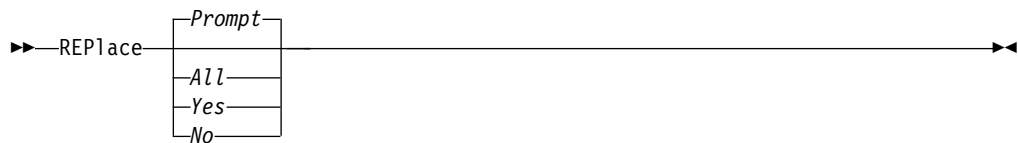
Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Establezca esta opción en el archivo de opciones de usuario del cliente (dsm.opt). Puede establecer esta opción en la ficha **Restaurar**, en la sección **Acción para archivos ya existentes** del Editor de preferencias.

Sintaxis



Parámetros

Prompt

Para las operaciones no planificadas, especifica si ha de grabarse encima de los archivos existentes. Para operaciones planificadas, los archivos existentes no se sobrescriben y no se muestran solicitudes. Éste es el valor predeterminado.

All

Se graba sobre todos los archivos existentes, incluidos los archivos de sólo lectura. Si se deniega el acceso a un archivo, se le solicitará si desea pasarlo por alto o grabar encima. No se emprende ninguna acción sobre el archivo hasta que haya una respuesta a la solicitud.

Yes

Se graba sobre todos los archivos existentes, *excepto* los archivos de sólo lectura. Para las operaciones no planificadas, especifica si ha de grabarse encima de los archivos de sólo lectura existentes. Para operaciones planificadas, los archivos existentes de sólo lectura no se sobrescriben y no se muestran solicitudes. Si se deniega el acceso a un archivo, se pasará por alto.

No No se graba encima de ningún archivo ya existente. No aparece ninguna solicitud.

Ejemplos

Archivo de opciones:

```
replace all
```

Línea de mandatos:

```
-replace=no
```

Esta opción es válida en la línea de mandatos inicial y en modalidad interactiva. Si utiliza esta opción en modalidad interactiva, sólo afectará al mandato con el que se especifica. Cuando se complete la ejecución de ese mandato, el valor se revierte al comienzo de la sesión interactiva. Será el valor del archivo dsm.opt, a menos que se haya modificado mediante la línea de mandatos inicial o mediante una opción que el servidor ha forzado.

Replserverguid

La opción `replserverguid` especifica el GUID (Globally Unique Identifier) que se utiliza cuando el cliente se conecta al servidor secundario durante la migración tras error. El GUID se utiliza para validar el servidor secundario para asegurarse de que es el servidor esperado.

El GUID de réplica es distinto del GUID de máquina del servidor. Se genera una vez para un servidor que está realizando la réplica y no cambia nunca.

Esta opción se debe especificar dentro de una stanza **replservername** en el archivo de opciones del cliente. La stanza **replservername** contiene información de conexión sobre el servidor secundario.

Esta opción se establece mediante el administrador del servidor de IBM Spectrum Protect para el nodo cliente. Durante el proceso de inicio de sesión normal (no migración tras error), la opción se envía al cliente y se guarda en el archivo de opciones del cliente.

No edite esta opción durante las operaciones normales.

Edite esta opción sólo durante situaciones como las siguientes:

- El servidor primario está fuera de línea y la información para el servidor secundario no se encuentra en el archivo de opciones.
- La información del servidor secundario está caducada o es incorrecta.

Todos los valores que edite se eliminarán o se actualizarán la próxima vez que inicie sesión en el servidor primario.

Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Esta opción se coloca en el archivo `dsm.sys` dentro de la stanza `replservername`.

Sintaxis

►►—`replserverguid—serverguid`—————►►

Parámetros

serverguid

Especifica el GUID del servidor secundario que se utiliza durante una migración tras error.

Ejemplos

Archivo de opciones:

REPLSERVERGUID 91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.02

Línea de mandatos:

No se aplica.

Archivo de opciones:

En el ejemplo siguiente se muestra cómo especificar opciones para tres

servidores distintos en el archivo `dsm.sys`, y cómo hacer referencia al servidor secundario. La información de conexión para varios servidor secundario se presenta en stanzas. Cada stanza se identifica mediante la opción **replservername** y el nombre del servidor secundario. La stanza **servername** debe contener la opción **myreplicationserver**, que apunta al servidor secundario que se especifica mediante la stanza **replservername**. Sólo se puede especificar un servidor secundario por stanza **servername**.

```
REPLSERVERNAME      TargetReplicationServer1
REPLTCPSERVERADDRESS TargetReplicationServer1
REPLTCPPOrt         1505
REPLSSLPORT          1506
REPLSERVERGUID       91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00
```

```
REPLSERVERNAME      TargetReplicationServer2
REPLTCPSERVERADDRESS TargetReplicationServer2
REPLTCPPOrt         1505
REPLSSLPORT          1506
REPLSERVERGUID       91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.02
```

```
SErvername          server_a
COMMMethod           TCPip
TCPPOrt              1500
TCPServeraddress     server_hostname1.example.com
PASSWORDAccess       prompt
MYREPLICATIONServer TargetReplicationServer1
```

```
SErvername          server_b
COMMMethod           TCPip
TCPPOrt              1500
TCPServeraddress     server_hostname2.example.com
PASSWORDAccess       generate
INCLExcl             /adm/tsm/archive.excl
MYREPLICATIONServer TargetReplicationServer2
```

```
SErvername          server_c
COMMMethod           TCPip
TCPPOrt              1500
TCPServeraddress     server_hostname3.example.com
PASSWORDAccess       generate
MYREPLICATIONServer TargetReplicationServer1
```

Conceptos relacionados:

“Configuración y uso de la migración tras error automática del cliente” en la página 94

Tareas relacionadas:

“Configuración del cliente de migración automática tras error” en la página 98

Replservername

La opción **replservername** especifica el nombre del servidor secundario al que se conecta el cliente durante una migración tras error.

La opción **replservername** empieza una stanza en el archivo de opciones del cliente que contiene información de conexiones sobre el servidor secundario.

Esta opción se establece mediante el administrador del servidor de IBM Spectrum Protect para el nodo cliente. Durante el proceso de inicio de sesión normal (no migración tras error), la opción se envía al cliente y se guarda en el archivo de opciones del cliente.

No edite esta opción durante las operaciones normales.

Edite esta opción sólo durante situaciones como las siguientes:

- El servidor primario está fuera de línea y la información para el servidor secundario no se encuentra en el archivo de opciones.
- La información del servidor secundario está caducada o es incorrecta.

Todos los valores que edite se eliminarán o se actualizarán la próxima vez que inicie sesión en el servidor primario.

Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Esta opción se coloca en las opciones del sistema cliente `dsm.sys`.

Sintaxis

►—`replservername`—`repl_servername`—►

Parámetros

repl_servername

Especifica el nombre del servidor secundario que se utilizará durante una migración tras error. Este valor es normalmente el nombre del servidor secundario, no el nombre de host del servidor.

Ejemplos

Archivo de opciones:

```
REPLSERVERNAME    TargetReplicationServer1
```

Línea de mandatos:

No se aplica.

Archivo de opciones:

En el ejemplo siguiente se muestra cómo especificar opciones para tres servidores distintos en el archivo `dsm.sys`, y cómo hacer referencia al servidor secundario. La información de conexión para varios servidor secundario se presenta en stanzas. Cada stanza se identifica mediante la opción **replservername** y el nombre del servidor secundario. La stanza **servername** debe contener la opción **myreplicationserver**, que apunta al servidor secundario que se especifica mediante la stanza **replservername**. Sólo se puede especificar un servidor secundario por stanza **servername**.

```
REPLSERVERNAME    TargetReplicationServer1
REPLTCPSERVERADDRESS TargetReplicationServer1
REPLTCPPOORT      1505
REPLSSLPORT       1506
REPLSERVERGUID    91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00

REPLSERVERNAME    TargetReplicationServer2
REPLTCPSERVERADDRESS TargetReplicationServer2
REPLTCPPOORT      1505
REPLSSLPORT       1506
REPLSERVERGUID    91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.02
```

```
SErvername        server_a
COMMMethod         TCPip
TCPPOort           1500
```

TCPServeraddress	server_hostname1.example.com
PASSWORDAccess	prompt
MYREPLICATIONServer	TargetReplicationServer1
SErvername server_b	
COMMMethod	TCPip
TCPPort	1500
TCPServeraddress	server_hostname2.example.com
PASSWORDAccess	generate
INCLExcl	/adm/tsm/archive.excl
MYREPLICATIONServer	TargetReplicationServer2
SErvername server_c	
COMMMethod	TCPip
TCPPort	1500
TCPServeraddress	server_hostname3.example.com
PASSWORDAccess	generate
MYREPLICATIONServer	TargetReplicationServer1

Conceptos relacionados:

“Configuración y uso de la migración tras error automática del cliente” en la página 94

Tareas relacionadas:

“Configuración del cliente de migración automática tras error” en la página 98

Replsslport

La opción `replsslport` especifica el puerto TCP/IP en el servidor secundario que está habilitado para SSL. La opción `replsslport` se utiliza cuando el cliente se conecta al servidor secundario durante una migración tras error.

La opción `replsslport` se envía al cliente mediante el servidor primario sólo si el servidor secundario está configurado para SSL.

Esta opción sólo es aplicable cuando el cliente está configurado para utilizar SSL para proteger las comunicaciones entre el servidor y el cliente de IBM Spectrum Protect. Si el cliente no está configurado para utilizar SSL, se utilizará el puerto especificado por la opción `repltcpport`. Puede determinar si el cliente utiliza SSL verificando la opción de cliente SSL.

Esta opción se debe especificar dentro de una stanza **`replservername`** en el archivo de opciones del cliente. La stanza **`replservername`** contiene información de conexión sobre el servidor secundario.

Durante el proceso de inicio de sesión normal (no migración tras error), esta opción se envía al cliente y se guarda en el archivo de opciones del cliente.

No edite esta opción durante las operaciones normales.

Edite esta opción sólo durante situaciones como las siguientes:

- El servidor primario está fuera de línea y la información para el servidor secundario no se encuentra en el archivo de opciones.
- La información del servidor secundario está caducada o es incorrecta.

Todos los valores que edite se eliminarán o se actualizarán la próxima vez que inicie sesión en el servidor primario.

Cientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Esta opción se coloca en el archivo `dsm.sys` dentro de la stanza `replservername`.

Sintaxis

►►—`replsslport—port_address`—————►►

Parámetros

port_address

Especifica la dirección del puerto TCP/IP que está habilitada para SSL y que se utiliza para comunicarse con el servidor secundario.

Ejemplos

Archivo de opciones:

REPLSSLPORT 1506

Línea de mandatos:

No se aplica.

Archivo de opciones:

En el ejemplo siguiente se muestra cómo especificar opciones para tres servidores distintos en el archivo `dsm.sys`, y cómo hacer referencia al servidor secundario. La información de conexión para varios servidor secundario se presenta en stanzas. Cada stanza se identifica mediante la opción **replservername** y el nombre del servidor secundario. La stanza **servername** debe contener la opción **myreplicationserver**, que apunta al servidor secundario que se especifica mediante la stanza **replservername**. Sólo se puede especificar un servidor secundario por stanza **servername**.

```
REPLSERVERNAME      TargetReplicationServer1
REPLTCPSEVERADDRESS TargetReplicationServer1
REPLTCPPOrt         1505
REPLSSLPORT          1506
REPLSERVERGUID       91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00
```

```
REPLSERVERNAME      TargetReplicationServer2
REPLTCPSEVERADDRESS TargetReplicationServer2
REPLTCPPOrt         1505
REPLSSLPORT          1506
REPLSERVERGUID       91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.02
```

```
SErvername          server_a
COMMMethod           TCPip
TCPPOrt              1500
TCPSEveraddress       server_hostname1.example.com
PASSWORDAccess       prompt
MYREPLICATIONServer  TargetReplicationServer1
```

```
SErvername          server_b
COMMMethod           TCPip
TCPPOrt              1500
TCPSEveraddress       server_hostname2.example.com
PASSWORDAccess       generate
INCLExcl             /adm/tsm/archive.excl
MYREPLICATIONServer  TargetReplicationServer2
```

SErvername	server_c	
COMMMethod		TCPip
TCPPort		1500
TCPServeraddress		server_hostname3.example.com
PASSWORDAccess		generate
MYREPLICATIONServer		TargetReplicationServer1

Conceptos relacionados:

“Configuración y uso de la migración tras error automática del cliente” en la página 94

Tareas relacionadas:

“Configuración del cliente de migración automática tras error” en la página 98

Repltcpport

La opción `repltcpport` especifica el puerto TCP/IP en el servidor secundario que se utilizará cuando el cliente se conecta al servidor secundario durante una migración tras error.

Esta opción se debe especificar dentro de una stanza **replservername** en el archivo de opciones del cliente. La stanza **replservername** contiene información de conexión sobre el servidor secundario.

Esta opción se establece mediante el administrador del servidor de IBM Spectrum Protect para el nodo cliente. Durante el proceso de inicio de sesión normal (no migración tras error), la opción se envía al cliente y se guarda en el archivo de opciones del cliente.

No edite esta opción durante las operaciones normales.

Edite esta opción sólo durante situaciones como las siguientes:

- El servidor primario está fuera de línea y la información para el servidor secundario no se encuentra en el archivo de opciones.
- La información del servidor secundario está caducada o es incorrecta.

Todos los valores que edite se eliminarán o se actualizarán la próxima vez que inicie sesión en el servidor primario.

Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Esta opción se coloca en el archivo `dsm.sys` dentro de la stanza `replservername`.

Sintaxis

►► `repltcpport—port_address—` ◀◀

Parámetros

port_address

Especifica la dirección del puerto TCP/IP que se utiliza para comunicarse con el servidor secundario.

Ejemplos

Archivo de opciones:

REPLTCPPort 1500

Línea de mandatos:

No se aplica.

Archivo de opciones:

En el ejemplo siguiente se muestra cómo especificar opciones para tres servidores distintos en el archivo `dsm.sys`, y cómo hacer referencia al servidor secundario. La información de conexión para varios servidor secundario se presenta en stanzas. Cada stanza se identifica mediante la opción **replservername** y el nombre del servidor secundario. La stanza **servername** debe contener la opción **myreplicationserver**, que apunta al servidor secundario que se especifica mediante la stanza **replservername**. Sólo se puede especificar un servidor secundario por stanza **servername**.

```
REPLSERVERNAME      TargetReplicationServer1
REPLTCPSEVERADDRESS TargetReplicationServer1
REPLTCPPOST         1505
REPLSSLPORT         1506
REPLSERVERGUID      91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00
```

```
REPLSERVERNAME      TargetReplicationServer2
REPLTCPSEVERADDRESS TargetReplicationServer2
REPLTCPPOST         1505
REPLSSLPORT         1506
REPLSERVERGUID      91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.02
```

```
SErvername      server_a
COMMMethod      TCPip
TCPPost         1500
TCPSEVERaddress  server_hostname1.example.com
PASSWORDAccess  prompt
MYREPLICATIONServer TargetReplicationServer1
```

```
SErvername      server_b
COMMMethod      TCPip
TCPPost         1500
TCPSEVERaddress  server_hostname2.example.com
PASSWORDAccess  generate
INCLExcl        /adm/tsm/archive.excl
MYREPLICATIONServer TargetReplicationServer2
```

```
SErvername      server_c
COMMMethod      TCPip
TCPPost         1500
TCPSEVERaddress  server_hostname3.example.com
PASSWORDAccess  generate
MYREPLICATIONServer TargetReplicationServer1
```

Conceptos relacionados:

“Configuración y uso de la migración tras error automática del cliente” en la página 94

Tareas relacionadas:

“Configuración del cliente de migración automática tras error” en la página 98

Repltcpserveraddress

La opción `repltcpserveraddress` especifica la dirección TCP/IP del servidor secundario que se utilizará cuando el cliente se conecta al servidor secundario durante una migración tras error.

Esta opción se debe especificar dentro de una stanza **replservername** en el archivo de opciones del cliente. La stanza **replservername** contiene información de conexión sobre el servidor secundario.

Esta opción se establece mediante el administrador del servidor de IBM Spectrum Protect para el nodo cliente. Durante el proceso de inicio de sesión normal (no migración tras error), la opción se envía al cliente y se guarda en el archivo de opciones del cliente.

No edite esta opción durante las operaciones normales.

Edite esta opción sólo durante situaciones como las siguientes:

- El servidor primario está fuera de línea y la información para el servidor secundario no se encuentra en el archivo de opciones.
- La información del servidor secundario está caducada o es incorrecta.

Todos los valores que edite se eliminarán o se actualizarán la próxima vez que inicie sesión en el servidor primario.

Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Esta opción se coloca en el archivo `dsm.sys` dentro de la stanza **replservername**.

Sintaxis

►►—REPLTCPServeraddress—*server_address*—————►►

Parámetros

server_address

Especifica una dirección TCP/IP para un servidor que tiene entre 1 y 64 caracteres de longitud. Especifique un nombre de dominio TCP/IP o una dirección IP numérica. La dirección IP numérica puede ser una dirección TCP/IP v4 o TCP/IP v6. Sólo puede utilizar direcciones IPv6 si ha especificado la opción `commethod V6Tcpi`.

Ejemplos

Archivo de opciones:

```
REPLTCPServeraddress dsmchost.example.com
```

Línea de mandatos:

No se aplica.

Archivo de opciones:

En el ejemplo siguiente se muestra cómo especificar opciones para tres servidores distintos en el archivo `dsm.sys`, y cómo hacer referencia al servidor secundario. La información de conexión para varios servidor secundario se presenta en stanzas. Cada stanza se identifica mediante la opción **replservername** y el nombre del servidor secundario. La stanza **servername** debe contener la opción **myreplicationserver**, que apunta al servidor secundario que se especifica mediante la stanza **replservername**. Sólo se puede especificar un servidor secundario por stanza **servername**.

```

REPLSERVERNAME      TargetReplicationServer1
REPLTCPSERVERADDRESS TargetReplicationServer1
REPLTCPPOST         1505
REPLSSLPORT         1506
REPLSERVERGUID      91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00

REPLSERVERNAME      TargetReplicationServer2
REPLTCPSERVERADDRESS TargetReplicationServer2
REPLTCPPOST         1505
REPLSSLPORT         1506
REPLSERVERGUID      91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.02

SErvername          server_a
COMMMethod           TCPip
TCPPost             1500
TCPServeraddress     server_hostname1.example.com
PASSWORDAccess       prompt
MYREPLICATIONServer TargetReplicationServer1

SErvername          server_b
COMMMethod           TCPip
TCPPost             1500
TCPServeraddress     server_hostname2.example.com
PASSWORDAccess       generate
INCLExcl            /adm/tsm/archive.excl
MYREPLICATIONServer TargetReplicationServer2

SErvername          server_c
COMMMethod           TCPip
TCPPost             1500
TCPServeraddress     server_hostname3.example.com
PASSWORDAccess       generate
MYREPLICATIONServer TargetReplicationServer1

```

Conceptos relacionados:

“Configuración y uso de la migración tras error automática del cliente” en la página 94

Tareas relacionadas:

“Configuración del cliente de migración automática tras error” en la página 98

Resourceutilization

Utilice la opción `resourceutilization` con el archivo de opciones para regular el nivel de recursos que el servidor y el cliente de IBM Spectrum Protect pueden utilizar durante el proceso.

Cientes soportados

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Establezca esta opción en el archivo `dsm.sys` dentro de una sección de servidor. Puede establecer esta opción en el separador **General**, en el campo **Uso de recursos** del editor de preferencias.

Sintaxis

►—RESOURCEUTILIZATION— *number* —►

Parámetros

number

Especifica el nivel de recursos que el servidor y el cliente de IBM Spectrum Protect pueden utilizar durante el proceso. El rango de valores válidos es de 1 a 10.

Ejemplos

Archivo de opciones:

`resourceutilization 7`

Línea de mandatos:

`-resourceutilization=7`

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Regulación de las sesiones de copia de seguridad/archivado

Si solicita una operación de copia de seguridad o archivado, el cliente puede utilizar más de una sesión del servidor.

El valor predeterminado es utilizar dos sesiones como máximo; una para consultar al servidor y la otra para enviar datos de archivo. El cliente sólo puede utilizar una sesión de servidor si establece la opción **resourceutilization** en 1.

Un cliente puede utilizar más del número predeterminado de sesiones cuando se conecta al servidor de IBM Spectrum Protect. Por ejemplo, `resourceutilization 10` permite hasta ocho sesiones con el servidor. Pueden utilizarse varias sesiones para consultar al servidor y enviar datos de archivo.

Se utilizan varias sesiones de consulta cuando se utilizan distintas especificaciones de archivo en un mandato de copia de seguridad o de archivado. Por ejemplo, si especifica los siguientes mandatos y especifica `resourceutilization 5`, puede que el cliente inicie una segunda sesión para consultar los archivos en el espacio de archivos B.

`inc /Volumes/filespaceA /Volumes/filespaceB`

Si se inicia la segunda sesión depende del tiempo que se tarda en consultar al servidor sobre los archivos de los que se realiza copia de seguridad en el espacio de archivos A. Puede que el cliente también intente leer datos del sistema de archivos y enviarlos al servidor en varias sesiones.

Nota: Durante una operación de copia de seguridad, si especifica varias especificaciones de archivo, el resultado podría ser que archivos de una especificación de archivo se almacenen en varias cintas y que se entremezclen con archivos de distintas especificaciones de archivo. Esto puede afectar negativamente al rendimiento de la restauración. El establecimiento de la opción **collocatebyfilespec** en yes eliminará la entremezcla de archivos de distintas especificaciones de archivo, limitando al cliente a una única sesión de servidor por especificación de archivo. Por consiguiente, si almacena los datos en una cinta, los archivos para cada especificación de archivo se almacenan conjuntamente en una cinta (a menos que se necesite otra para mayor capacidad).

Referencia relacionada:

“Collocatebyfilespec” en la página 365

Regulación de las sesiones de restauración

Si solicita una restauración, el valor predeterminado consiste en utilizar un máximo de una sesión.

Las sesiones de restauración adicionales se basan en:

- el valor **resourceutilization**
- cuántas cintas en las que están almacenados los datos solicitados
- cuántas unidades de disco están disponibles
- el número máximo de puntos de montaje permitidos para el nodo

Nota:

1. Si todos los archivos están en el disco, sólo se utiliza una sesión. No se pueden utilizar varias sesiones para una restauración de agrupación de almacenamiento en disco. Sin embargo, si está realizando una restauración en la que los archivos estén en 4 cintas y otros estén en disco, puede utilizar hasta 5 sesiones durante la restauración.
2. El servidor de IBM Spectrum Protect puede establecer el número máximo de puntos de montaje que un nodo puede utilizar en el servidor con el parámetro **MAXNUMMP**. Si el valor de la opción **resourceutilization** excede el valor de **MAXNUMMP** del servidor para un nodo, la copia de seguridad podría fallar y se generaría un mensaje Error del sistema desconocido.
3. Puede conseguir una restauración multisesión desde un único mandato **restore**, y desde un único volumen en el servidor, si ese volumen es una clase de dispositivo FILE.

Por ejemplo, si los datos que desea restaurar se encuentran en 5 volúmenes de cintas diferentes, el número máximo de puntos de montaje será 5 para el nodo, y si **resourceutilization** se establece en 3, se utilizarán 3 sesiones para la restauración. Si aumenta el valor de **resourceutilization** a 5, se utilizarán 5 sesiones para la restauración. Existe una relación unívoca entre el número de sesiones de restauración que están permitidas y el valor **resourceutilization**. Sólo se permiten varias sesiones de restauración para operaciones de restauración sin consulta.

Consideraciones relacionadas con la utilización de varias sesiones de cliente

En este tema se indican diversos aspectos que deben tenerse en cuenta al trabajar con varias sesiones de cliente.

Los factores siguientes pueden afectar al rendimiento de varias sesiones:

- La capacidad del servidor de gestionar varias sesiones de cliente. ¿Existe suficiente memoria, varios volúmenes de almacenamiento y potencia de procesador para aumentar el rendimiento de la copia de seguridad?
- La capacidad del cliente para dirigir varias sesiones (suficiente procesador, memoria, etc.).
- La configuración del subsistema de almacenamiento del cliente. Los sistemas de archivos que ocupan varios discos, ya sea mediante la subdivisión en bandas por software o mediante RAID-5, pueden gestionar mejor un aumento en las peticiones de lectura aleatorias que un sistema de archivos que se encuentra en una única unidad. Además, es posible que el rendimiento no mejore en un sistema de archivos de unidad única si intenta gestionar varias solicitudes de lectura aleatorias concurrentes.
- Suficiente ancho de banda en la red para dar soporte a un aumento de tráfico.

Entre los aspectos negativos que pueden darse al ejecutar varias sesiones destacan los siguientes:

- El cliente puede generar varios registros de contabilidad.
- El servidor puede no iniciar suficientes sesiones simultáneas. Para evitarlo, el parámetro *maxsessions* del servidor debe revisarse y posiblemente modificarse.
- Un mandato de consulta de nodo puede no resumir la actividad del cliente.
- Es posible que se restauren archivos en lugar de enlaces fijos.

La restauración de archivos en lugar de enlaces puede producirse cuando los siguiente criterios son verdaderos:

- Restaura todo un sistema de archivos
- Durante la operación de restauración, el valor de la opción *resourceutilization* es mayor que 1.
- El sistema de archivos contenía enlaces fijos cuando se realizaba la copia de seguridad del sistema de archivos.

La probabilidad de restaurar archivos enlazados en lugar de enlaces fijos aumentará cuanto mayor sea el número de sesiones. Al restaurar un sistema de archivos que contenía enlaces fijos cuando se realizaba la copia de seguridad del sistema de archivos, establezca *resourceutilization=1* para garantizar que se restauren los enlaces fijos.

Retryperiod

La opción *retryperiod* especifica el número de minutos que debe esperar el planificador cliente entre intentos de procesar un mandato planificado que da error, o entre intentos infructuosos de informar al servidor de los resultados. Utilice esta opción sólo si el planificador se encuentra en ejecución.

El administrador también puede definir esta opción. Si el administrador especifica un valor para esta opción, ese valor modificará temporalmente el valor del archivo de opciones del cliente opciones del sistema cliente después de que el nodo cliente haya establecido contacto correctamente con el servidor.

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (*dsm.sys*) en una stanza de servidor. Puede establecer esta opción en el separador **Planificador**, en el campo **Período entre reintentos** del Editor de preferencias.

Sintaxis

►►—RETRYPeriod— —*minutos*—►►

Parámetros

minutos

Especifica el número de minutos que el planificador cliente espera entre

intentos de establecer contacto con el servidor o para procesar un mandato planificado que da error. El rango de valores es de 1 a 9999, siendo 20 el valor predeterminado.

Ejemplos

Archivo de opciones:

`retry 10`

Línea de mandatos:

`-retryperiod=10`

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Revokeremoteaccess

La opción `revokeremoteaccess` impide que un administrador con privilegio de acceso a cliente acceda a una estación de trabajo cliente donde se esté ejecutando el cliente web.

Esta opción no impide que los administradores con privilegio de propietario de cliente, de sistema o de políticas tengan acceso a la estación de trabajo a través del cliente web.

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. Puede establecer esta opción en la ficha **Cliente web** del Editor de preferencias.

Sintaxis



Parámetros

None

No revoca el acceso a los administradores que disponen de autorización de acceso a cliente. Éste es el valor predeterminado.

Access

Revoca el acceso a los administradores que disponen de autorización de acceso a cliente.

Ejemplos

Archivo de opciones:

`revokeremoteaccess none`

Línea de mandatos:

No se aplica.

Schedcmddisabled

La opción `schedcmddisabled` especifica si ha de desactivarse la planificación de los mandatos mediante la opción `action=command` del servidor en el mandato de servidor **define schedule**.

Esta opción no desactiva los mandatos `preschedulecmd` y `postschedulecmd`. No obstante, puede especificar `preschedulecmd` o `postschedulecmd` con un espacio en blanco o una serie nula para desactivar la planificación de estos mandatos.

Puede desactivar la planificación de los mandatos que ha definido el administrador de IBM Spectrum Protect estableciendo la opción `schedcmddisabled` en `yes`.

Utilice el mandato **query schedule** para consultar las planificaciones definidas por el administrador.

Clientes soportados

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Establezca esta opción en el archivo `dsm.sys` en una stanza de servidor.

Sintaxis



Parámetros

Yes

Especifica que el servidor inhabilita la planificación de los mandatos mediante la utilización de la opción `action=command` en el mandato de servidor **DEFINE SCHEDULE**.

No Especifica que el servidor no inhabilita la planificación de los mandatos mediante la utilización de la opción `action=command` en el mandato de servidor **DEFINE SCHEDULE**. Éste es el valor predeterminado.

Ejemplos

Archivo de opciones:

`schedcmddisabled no`

Línea de mandatos:

No se aplica.

Información relacionada

“Query Schedule” en la página 738

Schedcmdexception

La opción `schedcmdexception` se utiliza conjuntamente con la opción `schedcmddisabled` para desactivar la planificación de mandatos mediante la opción

action=**command** del servidor en el mandato del servidor DEFINE SCHEDULE, excepto para series de mandatos específicas.

Debe especificar la serie exacta que coincide con la definición de “objects” en la planificación para que el mandato del servidor planificado se acepte. Si la serie no coincide exactamente (por ejemplo, contiene un espacio adicional o el uso de las mayúsculas es diferente), la acción del mandato planificado se bloqueará.

Puede proporcionar varias opciones schedcmexception en el archivo de opciones. Esta opción no se cumple si schedcmddisabled no está habilitado. El establecimiento de esta opción en el archivo de opciones es independiente del establecimiento de la opción schedcmddisabled.

Clientes soportados

Esta opción es válida para todos los clientes. Esta opción no es válida en el conjunto de opciones del cliente del servidor de IBM Spectrum Protect.

Archivo de opciones

Establezca esta opción en el archivo dsm.sys dentro de una stanza de servidor.

Sintaxis

►—SCHEDCMException—serie—◄

Parámetros

serie

Para mandatos planificados por la opción action=command en el mandato de servidor DEFINE SCHEDULE, este parámetro indica que se active el patrón de objetos si se especifica la opción schedcmddisabled=yes. Este parámetro es sensible a mayúsculas y minúsculas y debe coincidir con la serie del mandato en la definición de planificación del servidor de IBM Spectrum Protect.

Ejemplo

Archivo de opciones:

```
schedcmddisabled yes  
schedcmexception "start echo hello, world!"
```

Información relacionada

“Schedcmddisabled” en la página 544

Schedlogmax

La opción schedlogmax especifica el tamaño máximo del registro de planificación (dsm.sched.log) y de registro del cliente web (dsm.webcl.log), en megabytes.

Esta opción hace que los archivos de registro creados para sucesos del planificador (dsm.sched.log) y los eventos de cliente web (dsm.webcl.log) se ajusten cuando alcanzan su tamaño máximo. A medida que se registran los sucesos del cliente del planificador y el cliente web, los registros se añaden al final de los archivos de registro hasta que se alcanza el tamaño máximo especificado. Cuando se alcanza el tamaño máximo especificado, se coloca como último registro del archivo un

registro de anotaciones que indica `Continued at beginning of file`. Las anotaciones subsiguientes se reanudan al comienzo del archivo. El final de las anotaciones acomodadas se indica mediante un registro que indica `END OF DATA`.

Al establecer la opción `schedlogmax`, los mensajes de registro del planificador y del cliente web no se guardan en ningún archivo de eliminación. Si desea borrar registros y guardar las entradas de registro eliminadas en otro archivo, consulte la opción `schedlogretention`.

Si cambia de ajuste de registro (opción `schedlogmax`) a eliminación de registro (opción `schedlogretention`), se guardan todas las entradas de registro existentes y el registro se depura mediante el nuevo criterio `schedlogretention`.

Si cambia de eliminación de registro (opción `schedlogretention`) a ajuste de registro (opción `schedlogmax`), todos los registros existentes se copian a un archivo que contiene las entradas eliminadas. Por ejemplo, los registros eliminados del archivo `dsmsched.log` se copian en `dsmsched.pru`. Los registros eliminados de `dsmwebcl.log` se copian a `dsmwebcl.pru`. Los registros (`dsmsched.log` y `dsmwebcl.log`) existentes se vacían, y el registro comienza utilizando el nuevo criterio de ajuste.

Si simplemente cambia el valor de la opción `schedlogmax`, las anotaciones existentes se amplían o reducen para ajustarse al nuevo tamaño. Si el valor se reduce, las entradas más antiguas se suprimen para reducir el tamaño del nuevo archivo.

Si no se especifica `schedlogmax` ni `schedlogretention`, la anotación de registro cronológico de errores puede crecer sin límite de tamaño. Debe gestionar el contenido de los registros manualmente para evitar que el registro agote los recursos del disco. Cuando se ha creado el registro sin ninguna opción especificada, si posteriormente emite un mandato y especifica la opción `schedlogretention`, se elimina el registro mediante el valor de retención especificado. Cuando se ha creado el registro sin ninguna opción especificada, si posteriormente emite un mandato y especifica la opción `schedlogmax`, el registro existente se trata como si fuera un registro eliminado. Es decir, el contenido del archivo `dsmsched.log` se copia en un archivo llamado `dsmsched.pru`, el contenido de `dsmwebcl.log` se copia en `dsmwebcl.pru`, y las entradas de registro nuevas se crean en `dsmsched.log` y en `dsmwebcl.log` y ambos archivos se ajustan cuando alcanzan su tamaño máximo.

Nota: Si especifica un valor distinto de cero para `schedlogmax` (que permite la acomodación de anotaciones), no puede utilizar la opción `schedlogretention` para crear registros eliminados. Los registros pueden ser eliminados o ajustados, pero no las dos cosas.

Los registros creados con la opción `schedlogmax` contienen un registro de cabecera de registro que contiene información similar a este registro de ejemplo:

```
LOGHEADERREC 661 104857600 IBM Spectrum Protect 8.1.0.0 Fri Dec 9 06:46:53 2014
```

Tenga en cuenta que las fechas y las indicaciones de la hora del texto `LOGHEADERREC` no se convierten o formatean utilizando los valores especificados en las opciones `dateformat` o `timeformat`.

Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor.

También puede establecer esta opción en la ficha **Preferencias de cliente > Planificador** en la GUI, seleccionando **Habilitar ajuste de archivo registro de planificador** y especificando un valor distinto de cero para el **tamaño máximo** para el archivo de anotaciones cronológicas. Para impedir el ajuste del archivo de anotaciones, establezca el valor de **tamaño máximo** a cero. Cuando el ajuste máximo se establece en cero, borrar o establecer la opción **Habilitar ajuste de archivo de registro de planificador** no tiene ningún efecto; el ajuste de anotaciones no se produce si el **tamaño máximo** se establece en cero.

Sintaxis

►►—SCHEDLOGMAX— *size*—————►►

Parámetros

size

Especifica el tamaño máximo, en megabytes, del archivo de anotaciones. El rango de valores es de 0 a 2047; el valor predeterminado es 0, que desactiva la acomodación del archivo de anotaciones y deja que el archivo crezca indefinidamente.

Ejemplos

Archivo de opciones:

`schedlogmax 100`

Línea de mandatos:

`-schedlogmax=100`

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Schedlogname

La opción `schedlogname` especifica la vía de acceso y el nombre del archivo donde desea que se almacene la información de las anotaciones de planificación.

Utilice esta opción sólo cuando desee almacenar información de las anotaciones de planificación. Esta opción sólo se aplica cuando se ejecuta el planificador.

Si no se utiliza esta opción, el archivo `dsmsched.log` se crea en el mismo directorio que el archivo `dsmerror.log`.

Si ejecuta el mandato **schedule**, la salida de los mandatos planificados aparecerá en la pantalla. También se envía la información de salida al archivo especificado con esta opción. Si no existe ninguna parte de la ruta que especifica, el cliente intenta crearla.

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor. Puede establecer esta opción en el separador **Planificador**, en el recuadro de texto **Anotaciones de planificación** del Editor de preferencias.

Nota: Establezca la variable de entorno DSM_LOG en el nombre de un directorio en el que se deben colocar las anotaciones. El directorio especificado debe tener permisos que permitan el acceso de grabación desde la cuenta en la que se está ejecutando el cliente. El directorio raíz no es un valor válido para DSM_LOG.

Sintaxis

►—SCHEDLOGName— *filespec*—►

Parámetros

filespec

Especifica la vía de acceso y el nombre de archivo en el que desea restaurar la información de anotaciones de planificación cuando se procesa el trabajo planificado. Si no existe ninguna parte de la ruta que especifica, el cliente intenta crearla.

Si se especifica únicamente un nombre de archivo, el archivo se almacena en el directorio actual. El valor predeterminado es el directorio de trabajo actual que tiene el nombre de archivo dsm Sched.log. El archivo dsm Sched.log *no puede* ser un vínculo simbólico.

En Mac OS X, si sólo especifica un nombre de archivo, el archivo se almacenará en la carpeta predeterminada. Los directorios predeterminados son:

```
~/Library/Logs/tivoli/tsm  
/Library/Logs/tivoli/tsm
```

Ejemplos

Archivo de opciones:

```
SCHEDLOGN /Users/user1/Library/Logs/schedlog.jan  
schedlogname /home/mydir/schedlog.jan
```

Línea de mandatos:

```
-schedlogname=/Users/user1/Library/Logs/schedlog.jan
```

Línea de mandatos:

```
-schedlogname=/home/mydir/schedlog.jan
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Información relacionada

Consulte el tema “Errorlogname” en la página 422 para obtener más información acerca de la ubicación del archivo dsm Sched.log.

Schedlogretention

La opción `schedlogretention` especifica el número de días que se mantienen las entradas en el registro de planificación (`dsmsched.log`) y el registro del cliente web (`dsmwebcl.log`), y si deben guardarse las entradas eliminadas en otro archivo.

El registro de planificación (`dsmsched.log`) se elimina cuando se inicia el planificador y después de que finalice un evento planificado. Las entradas eliminadas se graban en un archivo llamado `dsmsched.pru`.

El registro de cliente web (`dsmwebcl.log`) se elimina durante el primer inicio de `acceptor daemon` de cliente. Las entradas eliminadas se graban en un archivo llamado `dsmwebcl.pru`.

Si cambia de eliminación (opción `schedlogretention`) por el ajuste de registro (opción `schedlogmax`), todos los registros del registro existente se copian en el registro eliminado (`dsmsched.pru` and `dsmwebcl.pru`), y los registros existentes (`dsmsched.log` y `dsmwebcl.log`) se vacían, y el registro comienza utilizando el nuevo criterio de ajuste.

Si cambia de ajuste de registro (opción `schedlogmax`) a eliminación de registro (opción `schedlogretention`), se guardan todas las entradas de registro existentes y el registro se depura mediante el nuevo criterio `schedlogretention`. Las entradas eliminadas se guardan en sus archivos `*.pru` correspondientes.

Si no se especifica `schedlogmax` ni `schedlogretention`, los registros pueden crecer sin límite de tamaño. Debe gestionar el contenido de los registros manualmente para evitar que el registro agote los recursos del disco. Cuando se ha creado el registro sin ninguna opción especificada, si posteriormente emite un mandato y especifica la opción `schedlogretention`, se elimina el registro mediante el valor de retención especificado. Cuando se ha creado el registro sin ninguna opción especificada, si posteriormente emite un mandato y especifica la opción `schedlogmax`, el registro existente se trata como si fuera un registro eliminado. Es decir, el contenido del archivo `dsmsched.log` se copia en un archivo llamado `dsmsched.pru`, el contenido de `dsmwebcl.log` se copia en `dsmwebcl.pru`, y las entradas de registro nuevas se crean en `dsmsched.log` y en `dsmwebcl.log`, y ambos archivos se ajustan cuando alcanzan su tamaño máximo.

Nota: Si especifica la opción `schedlogretention` para crear registros eliminados, no podrá especificar la opción `schedlogmax`. Los registros pueden ser eliminados o ajustados, pero no las dos cosas.

Clientes soportados

Esta opción es válida para todos los clientes.

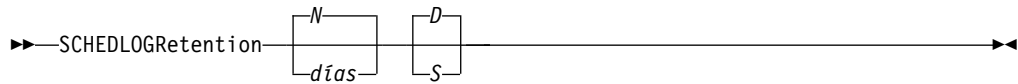
Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor.

También puede establecer esta opción en la ficha **Preferencias de cliente > Planificador** en la GUI seleccionando **Eliminar entradas antiguas** y especificando un valor para **Eliminar entradas más antiguas que**. Al seleccionar la opción **Guardar entradas eliminadas** se guardan las entradas de registro de planificador eliminadas en el archivo de registro `dsmsched.pru`. Al seleccionar **Guardar entradas**

eliminadas también se guardan las entradas de cliente web en el archivo de registro `dsmwebcl.pru`.

Sintaxis



Parámetros

N *days*

Especifica cuánto tiempo se debe esperar antes de eliminar las anotaciones.

N No se eliminarán las anotaciones. Esto hace que las anotaciones crezcan indefinidamente. Éste es el valor predeterminado.

days

Especifica el número de días que se conservarán las entradas del archivo de anotaciones antes de eliminarlas. El rango de valores oscila entre 0 y 9999.

DoS

Especifica si se deben guardar las entradas eliminadas. Utilice un espacio o una coma para separar este parámetro del anterior.

D Elimina las entradas de las anotaciones al eliminarlas. Éste es el valor predeterminado.

S Guarda las entradas de anotaciones al eliminarlas.

Las entradas eliminadas se copian en el archivo de las entradas eliminadas (`dsmsched.pru` o `dsmsched.pru`), que se encuentra almacenado en el mismo directorio que las anotaciones.

Ejemplos

Archivo de opciones:

```
schedlogretention 30 S
```

Línea de mandatos:

```
-schedlogretention=30,S
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Schedmode

La opción `schedmode` especifica si se desea utilizar la modalidad de sondeo de cliente (el nodo cliente periódicamente consulta al servidor sobre los trabajos planificados), o bien la modalidad de petición de servidor (el servidor contacta con el nodo cliente en el momento de iniciar una operación planificada).

Todos los métodos de comunicación pueden utilizar la modalidad de sondeo de cliente, pero sólo TCP/IP puede utilizar la modalidad de petición de servidor.

Esta opción sólo se aplica si utiliza el método de comunicación TCP/IP y se ejecuta el mandato **schedule**.

El administrador puede especificar que el servidor dé soporte a ambas modalidades o sólo a una de ellas. Si el administrador especifica que se dé soporte a ambas modalidades, podrá seleccionar la que desee. Si el administrador sólo ha especificado una única modalidad, deberá especificar esa modalidad en el archivo `dsm.sys`, o el trabajo planificado no se procesará.

Si especifica la modalidad `prompted`, debe considerar la posibilidad de proporcionar valores para las opciones `tcpclientaddress` y `tcpclientport` en el archivo `dsm.sys` o en el mandato de planificación; a continuación, podrá establecerse contacto con el cliente en la dirección o en el puerto deseados (esto es útil para los sistemas cliente que tienen varias tarjetas de interfaz de red).

Nota:

1. Cuando cambie el valor de esta opción en el archivo `dsm.sys`, deberá detener y reiniciar el servicio de planificador para que el valor entre en vigor.
2. El servidor también puede definir esta opción.

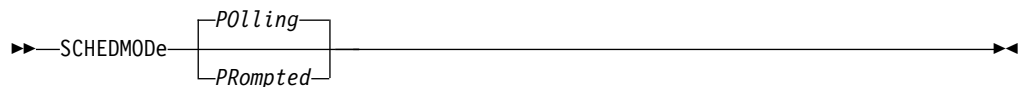
Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. Puede establecer esta opción en el separador **Planificador**, en la sección **Modalidad de planificación** del Editor de preferencias.

Sintaxis



Parámetros

POLLing

El planificador cliente consulta al servidor sobre el trabajo planificado en intervalos de tiempo determinados. Éste es el valor predeterminado. Puede establecer los intervalos de tiempo utilizando la opción `querryschedperiod`.

PRompted

El planificador cliente espera que el servidor establezca contacto con el nodo cliente cuando se tenga que realizar el trabajo planificado.

Nota:

1. Si utiliza el mandato **dsmc schedule** y se han especificado las opciones `schedmode prompted` y `commethod V6Tcpip`, el cliente y el servidor de IBM Spectrum Protect deberán configurarse para IPv6. Asimismo, el nombre de host del cliente deberá configurarse para la dirección IPv6.

Ejemplos

Archivo de opciones:

```
schedmode prompted
```

Línea de mandatos:

-schedmod=po

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Referencia relacionada:

"Cadlistenonport" en la página 362

"Tcpclientaddress" en la página 587

"Tcpclientport" en la página 588

Schedrestretrdisabled

La opción schedrestretrdisabled especifica si se debe inhabilitar la ejecución de las operaciones de restauración o recuperación planificadas.

Clientes soportados

Esta opción es válida para todos los clientes. El servidor no puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Especifique esta opción en el archivo dsm.sys dentro de una stanza de servidor para el planificador. Puede establecer esta opción en el separador **Planificador** en la sección de **Mandato de planificación** del Editor de preferencias.

Sintaxis



Parámetros

No Especifica que el cliente no inhabilita la ejecución de las operaciones de planificación de restauración ni de recuperación. Este parámetro es el predeterminado.

Yes

Especifica que el cliente inhabilita la ejecución de las operaciones de planificación de restauración ni de recuperación.

Ejemplos

Archivo de opciones:

schedrestretrdisabled yes

Línea de mandatos:

No se aplica.

Scrolllines

La opción scrolllines especifica el número de líneas de información que deben aparecer en pantalla a la vez.

Utilice esta opción cuando establezca la opción scrollprompt en *Yes*.

La opción `scrolllines` sólo puede utilizarse con los mandatos siguientes:

- **delete filespace**
- **query archive**
- **query backup**
- **query backupset**
- **query filespace**
- **query group**
- **query image**
- **query nas**
- **query node**
- **query options**

Clientes soportados

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Establezca esta opción en el archivo de opciones de usuario del cliente (`dsm.opt`). Puede establecer esta opción en **Línea de mandatos > Número de líneas que mostrar** en el Editor de preferencias.

Sintaxis

►►—`SCROLLLines`— *number*—►►

Parámetros

number

Especifica el número de líneas de información que deben aparecer en pantalla a la vez. El rango de valores es de 1 a 80, siendo 20 el valor predeterminado.

Ejemplos

Archivo de opciones:

`scrolllines 25`

Línea de mandatos:

`-scroll=25`

Esta opción es válida en la línea de mandatos inicial y en modalidad interactiva. Si utiliza esta opción en modalidad interactiva, sólo afectará al mandato con el que se especifica. Cuando se complete la ejecución de ese mandato, el valor se revierte al comienzo de la sesión interactiva. Será el valor del archivo `dsm.opt`, a menos que se haya modificado mediante la línea de mandatos inicial o mediante una opción que el servidor ha forzado.

Scrollprompt

La opción `scrollprompt` especifica si desea que el cliente de copia de seguridad y archivado se detenga y espere después de visualizar el número de líneas de información especificado en la opción `scrolllines`, o desea que se desplace hasta el final de la lista de información.

La opción `scrollprompt` sólo puede utilizarse con los mandatos siguientes:

- **delete filespace**

- query archive
- query backup
- query backupset
- query filespace
- query group
- query image
- query nas
- query node
- query options

Clientes soportados

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Establezca esta opción en el archivo de opciones de usuario del cliente (dsm.opt). Puede establecer esta opción en la ficha **Línea de mandatos**, en el campo **Detenerse tras mostrar el número de líneas siguiente** del Editor de preferencias.

Sintaxis



Parámetros

No Se desplaza hasta el final de la lista y se detiene. Éste es el valor predeterminado.

Yes

Se detiene y espera después de mostrar el número de líneas indicado en la opción scrolllines. Se mostrará la siguiente solicitud en la pantalla:

Pulse 'Q' para salir, 'C' para desplazamiento continuo o 'Intro' para continuar.

Ejemplos

Archivo de opciones:

scrollprompt yes

Línea de mandatos:

-scrollp=yes

Esta opción es válida en la línea de mandatos inicial y en modalidad interactiva. Si utiliza esta opción en modalidad interactiva, sólo afectará al mandato con el que se especifica. Cuando se complete la ejecución de ese mandato, el valor se revierte al comienzo de la sesión interactiva. Será el valor del archivo dsm.opt, a menos que se haya modificado mediante la línea de mandatos inicial o mediante una opción que el servidor ha forzado.

Servername

En el archivo `dsm.sys`, la opción `servername` especifica el nombre que desea utilizar para identificar un servidor y para iniciar una sección que contenga opciones para ese servidor. Puede identificar y especificar opciones para varios servidores.

En el ejemplo siguiente se muestra cómo especificar opciones para dos servidores diferentes:

```
SErvername      server_a
COMMMethod      TCPip
TCPPort         1500
TCPServeraddress server_hostname2.domain.company.com
PASSWORDAccess  prompt
GRoups          tsm
USERS           sullivan mushock tallan
INCLExcl        /adm/tsm/backup.excl

SErvername      server_b
COMMMethod      SHAREdmem
shmport         1520
PASSWORDAccess  generate
GRoups          system tsm
INCLExcl        /adm/tsm/archive.excl
```

En el archivo de opciones del usuario cliente (`dsm.opt`), la opción `servername` especifica con qué servidor, de los que se especifican en el archivo `dsm.sys`, debe establecerse contacto para obtener los servicios de copia de seguridad/archivado. Cuando se especifica en un archivo de opciones del usuario cliente (`dsm.opt`) o en la línea de mandatos, la opción `servername` modifica temporalmente el servidor predeterminado que se ha especificado en el archivo de opciones del sistema cliente.

Nota:

1. No se puede utilizar la opción `servername` para modificar temporalmente el servidor de migración especificado en el archivo de opciones del sistema cliente.
2. si el nombre de servidor de IBM Spectrum Protect cambia o si los clientes de copia de seguridad y archivado se dirigen a un servidor de IBM Spectrum Protect diferente, deberá inicializarse una nueva contraseña para todos los clientes para el nuevo nombre de servidor.

Clientes soportados

Esta opción es válida para todos los clientes UNIX y Linux.

Archivo de opciones

Establezca esta opción en el archivo de opciones del usuario cliente (`dsm.opt`) y en el archivo de opciones de sistema de cliente (`dsm.sys`). En el archivo `dsm.sys`, la opción `servername` es el comienzo de una stanza de servidor.

No modifique esta opción en `dsm.opt` cuando ejecute el cliente de archivado y copia de seguridad en una sesión de línea de mandatos o cuando ejecute la interfaz gráfica de usuario del cliente de archivado y copia de seguridad.

Sintaxis

►—Servername—servername—◄

Parámetros

servername

En el archivo `dsm.sys`, especifique el nombre que desea asignar a un servidor en particular. En el archivo de opciones del usuario cliente (`dsm.opt`) o en la línea de mandatos, especifique el nombre del servidor con el que desea establecer contacto para los servicios de copia de seguridad/archivado. El valor de *servername* en `dsm.opt` debe coincidir con un valor de *servername* en `dsm.sys`, o el cliente no podrá ponerse en contacto con el servidor.

Un nombre de servidor no es sensible a mayúsculas y minúsculas y puede tener hasta 64 caracteres.

Ejemplos

Archivo de opciones:

```
servername server_a
```

Línea de mandatos:

```
-se=server_b
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Sessioninitiation

Utilice la opción `sessioninitiation` para controlar si el servidor o el cliente ha de iniciar las sesiones a través de un cortafuegos. El valor predeterminado especifica que el cliente ha de iniciar las sesiones. Puede utilizar esta opción con el mandato `schedule`.

Para el planificador del cliente, no es necesario abrir ningún puerto en el cortafuegos. Si establece la opción `sessioninitiation` en `serveronly`, el cliente no intentará establecer contacto con el servidor. La planificación por petición de servidor debe iniciar todas las sesiones en el puerto que se ha definido en el cliente con la opción `tcpclientport`. La opción `sessioninitiation` sólo afecta al comportamiento del planificador cliente que se ejecuta en modalidad por petición. Si establece la opción `sessioninitiation` en `serveronly`, a excepción de los planificadores gestionados por `daemon` del aceptador de cliente, el cliente de la línea de mandatos, la GUI del cliente de archivado y copia de seguridad y la GUI del cliente web seguirán intentando iniciar sesiones.

Atención: No puede utilizar `dsmcad` para la planificación cuando establece la opción `sessioninitiation` en `serveronly`.

Nota: Si establece la opción `sessioninitiation` en `serveronly`, el asistente para la configuración del cliente y el servicio del planificador no podrán autenticarse para el servidor de IBM Spectrum Protect. En este caso, puede ejecutar el planificador desde la línea de mandatos (`dsmc schedule`) y especificar la contraseña del nodo cuando se le solicite.

Se puede producir un problema similar si se necesita una clave de cifrado para las operaciones de copia de seguridad. En este caso, puede ejecutar el planificador

desde la línea de mandatos (`dsmc schedule`) y entrar la clave de cifrado cuando se le solicite. Después de actualizar la contraseña y la clave de cifrado, debe reiniciar el planificador.

Si establece la opción `sessioninitiation` en `client`, el cliente inicia sesiones con el servidor comunicándose en el puerto TCP/IP definido con la opción de servidor `tcpport`. Éste es el valor predeterminado. La planificación por petición de servidor puede utilizarse para solicitar al cliente que se conecte con el servidor.

Nota:

1. El servidor de IBM Spectrum Protect puede especificar `SESSIONINITiation=clientorserver` o `SESSIONINITiation=serveronly` en los mandatos **register node** y **update node**. Si el servidor especifica `SESSIONINITiation=clientorserver`, el cliente puede decidir qué método utilizar. Si el servidor especifica `SESSIONINITiation=serveronly`, el servidor iniciará todas las sesiones.
2. Si `sessioninitiation` se establece en `serveronly`, el valor de la opción de cliente `tcpclientaddress` debe ser igual al valor de la opción `HLAddress` del mandato de servidor **update node** o **register node**. El valor de la opción de cliente `tcpclientport` debe ser igual al valor de la opción `LLAddress` del mandato de servidor **update node** o **register node**.

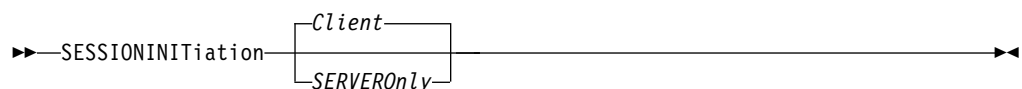
Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Establezca esta opción en el archivo `dsm.sys` dentro de una stanza de servidor. Puede establecer esta opción en la ficha **Planificador**, en el campo **Iniciación de sesión** del Editor de preferencias.

Sintaxis



Parámetros

Client

Especifica que el cliente iniciará sesiones con el servidor comunicándose en el puerto TCP/IP definido con la opción de servidor `TCPPORT`. Éste es el valor predeterminado. La planificación por petición de servidor puede utilizarse para solicitar al cliente que se conecte con el servidor.

SERVEROnly

Especifica que el servidor no aceptará las peticiones de sesiones del cliente. La planificación por petición de servidor debe iniciar todas las sesiones en el puerto que se ha definido en el cliente con la opción `tcpclientport`. A excepción de los planificadores que el daemon de aceptación de clientes gestiona, el cliente de línea de mandatos, la GUI del cliente de copia de seguridad-archivado y la GUI del cliente web seguirán intentando el inicio de las sesiones.

Si la opción AUTHENTICATION del servidor está definida como LDAP, no defina la opción sessioninitiation del cliente como serveronly; de hacerlo, las planificaciones no se podrán ejecutar.

Ejemplos

Archivo de opciones:

sessioninitiation serveronly

Línea de mandatos:

schedule -sessioninitiation=serveronly

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Información relacionada

“Configuración del planificador” en la página 66

“Tcpclientport” en la página 588

Shmport

La opción shmport especifica la dirección del puerto TCP/IP de un servidor al utilizar la memoria compartida. Todas las comunicaciones de memoria compartida comienzan con una conexión TCP/IP.

Nota: El valor que se especifica en la opción shmport en el archivo dsm.sys debe coincidir con el valor que se ha especificado para shmport en el archivo de opciones de servidor.

Clientes soportados

Esta opción es válida para clientes de AIX, Linux y Oracle Solaris.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor.

Sintaxis

►►—SHMPort— —*número_puerto*—————►►

Parámetros

port_number

Especifica el número de puerto. Puede especificar un valor de 1000 a 32767. El valor predeterminado es 1510.

Ejemplos

Archivo de opciones:

shmport 1580

Línea de mandatos:

No se aplica.

Showmembers

Utilice la opción `showmembers` para visualizar todos los miembros de un grupo.

Puede utilizar la opción `showmembers` con los mandatos **`query group`** y **`restore group`**.

La opción `showmembers` no es válida con la opción `inactive`. Si desea visualizar los miembros de un grupo que actualmente no están activos, utilice las opciones `pitdate` y `pittime`.

Clientes soportados

Esta opción es válida para todos los clientes UNIX y Linux, a excepción de Mac OS X.

Sintaxis

►►—SHOWMembers—◄◄

Parámetros

No hay parámetros para esta opción.

Ejemplos

Línea de mandatos:

```
restore group /virtfs/* -pick -showmembers
```

Skipacl

La opción `skipacl` permite incluir o excluir datos de la lista de control de acceso (ACL) durante una operación de copia de seguridad o archivado; se incluyen los datos de ACL de forma predeterminada.

Cuando esta opción está establecida en `yes`, el cliente de copia de seguridad y archivado no incluye los datos de ACL cuando realiza una copia de seguridad o archiva archivos y directorios. El valor predeterminado es `no`, que permite que los datos de ACL sean incluidos cuando los objetos se copian en el servidor. Sólo debe establecer `skipacl` en `yes` cuando las ACL no están definidas en el sistema de archivos, o cuando está seguro de que no necesita los datos de ACL cuando se recuperan o restauran los archivos.

Clientes soportados

Esta opción es válida para todos los clientes UNIX y Linux. En sistemas Linux y AIX, establecer `skipacl` en `yes` también omite los atributos ampliados.

Archivo de opciones

Establezca esta opción en el archivo de opciones del usuario cliente (`dsm.opt`).

Sintaxis



Parámetros

No Si especifica *No*, se realizará copia de seguridad de los datos de ACL. Éste es el valor predeterminado.

Yes

Si especifica *Yes*, no se realiza copia de seguridad de los datos de ACL, y por lo tanto no pueden restaurarse. `skipacl=yes` modifica los valores de `skipaclupdatecheck`.

Ejemplos

Archivo de opciones:

```
skipacl yes
```

Skipaclupdatecheck

La opción `skipaclupdatecheck` desactiva la suma de comprobación y las comparaciones de tamaño de los datos de ACL.

Cuando se establece en *yes* (el valor predeterminado es *no*), el cliente de copia de seguridad y archivado no realizará la comparación de sumas de comprobación ni de tamaños antes o después de la copia de seguridad y durante el proceso incremental (suma de comprobación de ACL de copia de seguridad anterior y ACL actual) para detectar actualizaciones de ACL. Sin embargo, se hará copia de seguridad de los datos de ACL actuales si el archivo se selecciona para la copia de seguridad por otras razones. Si en un archivo sólo se actualizan las ACL, la copia de seguridad incremental siguiente no reconocerá esta actualización de ACL y no se realizará la copia de seguridad del archivo.

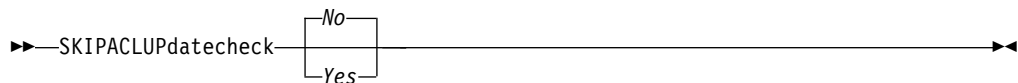
Clientes soportados

Esta opción es válida para todos los clientes UNIX y Linux.

Archivo de opciones

Establezca esta opción en el archivo de opciones del usuario cliente (`dsm.opt`).

Sintaxis



Parámetros

No Si especifica *No*, el cliente lleva a cabo la comparación de sumas de comprobación y tamaños de los datos de ACL, antes y después de la copia de seguridad y durante el proceso incremental. Éste es el valor predeterminado.

Yes

Si especifica Yes, el cliente no realizará la suma de comprobación y las comparaciones de tamaño de los datos de ACL.

Ejemplos

Archivo de opciones:

skipaclup yes

Snapdiff

Si se utiliza la opción **snapdiff** con el mandato **incremental** el proceso de copia de seguridad a incrementos se realiza de forma transparente. El mandato ejecuta una copia de seguridad a incrementos de los archivos modificados, según los informes de NetApp, en lugar de explorar todo el volumen en busca de archivos modificados.

Debe configurar un ID de usuario y una contraseña en el cliente de copia de seguridad y archivado para habilitar el proceso de diferencia de instantánea. Para obtener más información sobre cómo configurar la opción **snapdiff**, consulte “Configuración de NetApp y IBM Spectrum Protect para copias de seguridad incrementales de diferencia de instantánea” en la página 114.

Utilice esta opción con una copia de seguridad incremental de un volumen de archivador NAS, en lugar de una copia incremental simple o incremental con la opción **snapshotroot**, siempre que el servidor de archivos NAS se ejecute en ONTAP 7.3.0, o posterior. No utilice al mismo tiempo las opciones **snapdiff** y **snapshotroot**.

Restricción: Las copias de seguridad incrementales con procesamiento de diferencia de instantáneas solo están disponibles con el cliente de archivado y copia de seguridad de Linux x86_64.

La primera vez que realice una copia de seguridad incremental con la opción de diferencia de instantáneas, se crea una instantánea (la instantánea base) y se ejecuta una copia de seguridad incremental tradicional utilizando esta instantánea como origen. El nombre de la instantánea creada se registra en la base de datos del servidor de IBM Spectrum Protect. La copia de seguridad incremental inicial debe finalizar sin errores para que la siguiente operación de copia de seguridad utilice el proceso de diferencia de instantáneas.

La segunda vez que se ejecuta una copia de seguridad incremental con esta opción, se crea una instantánea más nueva o se utiliza una instantánea existente (en función del valor establecido para la opción **diffsnapshot**) a fin de encontrar las diferencias entre estas dos instantáneas. Esta segunda instantánea se denomina *diffsnapshot*, o instantánea de diferencia. A continuación, el cliente realiza una copia de seguridad incremental de los archivos que se han notificado como cambiados por NetApp en el servidor de IBM Spectrum Protect. El sistema de archivos seleccionado para el proceso de diferencias de instantánea debe estar montado en la raíz del volumen. No puede utilizar la opción **snapdiff** para ningún sistema de archivos que no esté montado en la raíz del volumen. Una vez que haya realizado la copia de seguridad de los datos con la opción **snapdiff**, la instantánea que se ha utilizado como la instantánea base se suprime del directorio de instantánea.

En sistemas Linux, el directorio de instantáneas está en **.snapshot**.

El cliente no suprime ninguna instantánea que no ha creado.

Cuando se completa una operación de copia de seguridad incremental diferencial de instantánea, el cliente asegura que sólo persista la instantánea base registrada más recientemente en el volumen de gestor de archivos. Todas las instantáneas creadas por una copia de seguridad incremental diferencial de instantáneas en el cliente de archivado y copia de seguridad empiezan con los caracteres "TSM_". Si utiliza una herramienta de instantánea distinta del cliente de copia de seguridad y archivado para producir instantáneas, asegúrese de no utilizar la serie "TSM_" al principio del nombre de instantánea. Si los nombres de la instantánea empiezan por "TSM_", los archivos se suprimen cuando el cliente inicia la siguiente operación de copia de seguridad incremental diferencial de instantáneas.

Para ejecutar una copia de seguridad de diferencial de instantánea de volúmenes de archivador de NetApp de sólo lectura, se debe especificar la opción `useexistingbase` para impedir un intento de crear una instantánea en el volumen de sólo lectura. Además, especifique el nombre de la instantánea base a utilizar (la opción `basesnapshotname`) y el nombre de la instantánea diferencial a utilizar (la opción `diffsnapshotname`).

Para los servidores de archivos NAS y N-Series que ejecutan ONTAP 7.3.0, o posterior, puede utilizar la opción `createnewbase` para realizar una copia de seguridad de los archivos que se han omitido debido a los siguientes motivos:

- Se excluye un archivo porque el archivo de inclusión-exclusión tiene una regla de exclusión en vigor. Se excluye un archivo cuando no ha modificado el archivo de inclusión/exclusión, pero ha eliminado la regla que ha excluido el archivo. La API de NetApp detecta los cambios de archivos sólo entre dos instantáneas, no cambios en el archivo de inclusión/exclusión.
- Si ha añadido una sentencia de inclusión en el archivo de opciones, dicha opción de inclusión no entra en vigor a menos que NetApp detecte que se han producido cambios en el archivo. El cliente no inspecciona cada uno de los archivos del volumen durante la copia de seguridad.
- Ha utilizado el mandato **`dsmdc delete backup`** para suprimir explícitamente un archivo del inventario del servidor de IBM Spectrum Protect. NetApp no detecta que un archivo se ha suprimido manualmente del servidor. Por consiguiente, el archivo sigue sin protección en el almacenamiento de IBM Spectrum Protect hasta que se cambia en el volumen y NetApp detecta el cambio, lo que indica al cliente que vuelva a hacer una copia de seguridad del mismo.
- Los cambios de políticas como, por ejemplo, de `mode=modified` a `mode=absolute` no se detectan.
- El espacio de archivo entero se suprime del inventario IBM Spectrum Protect. Esta acción hace que la opción de diferencia de instantáneas cree una instantánea para que se utilice como origen, y ejecuta una copia de seguridad incremental completa.
- Se excluye un archivo de la instantánea debido a que el nombre de archivo contiene un carácter que no está incluido en el juego de caracteres ASCII de 7 bits. La opción `createnewbase` crea una instantánea base y la utiliza como fuente para ejecutar una copia de seguridad incremental completa. NetApp controla qué es lo que constituye un objeto modificado.

Consejo: Puede utilizar la opción `snaptiffhttps` para ejecutar copias de seguridad incrementales diferenciales de instantánea de los gestores de archivos NetApp con una conexión HTTPS segura. Para ejecutar correctamente las copias de seguridad incrementales diferenciales de instantáneas, los releases anteriores del cliente de archivado de la copia de seguridad requerían acceso administrativo de HTTP para habilitarse en el archivador de NetApp. Con la opción `snaptiffhttps`, puede

establecer una sesión de administración segura con el archivador NetApp independientemente de si está habilitado o no el acceso de administración de HTTP en el archivador.

En la lista de opciones que utiliza el mandato **incremental** tradicional, la última columna muestra la interacción de cada opción con la opción `snapdiff`. En la información siguiente se describen las definiciones de *válido*, *no válido* y *sin efecto*:

Válido

El proceso se ejecuta normalmente cuando se utiliza la opción.

No válido

Si la opción se utiliza con `snapdiff`, se genera un mensaje de error.

Sin efecto

La opción se puede utilizar, pero no se tiene en cuenta.

Tabla 75. Mandato Incremental: opciones relacionadas

Opción	Donde se especifica	Con <code>snapdiff</code>
<code>asnodename</code> “Asnodename” en la página 349	En el archivo de opciones del sistema cliente (<code>dsm.sys</code>) o en la línea de mandatos.	Válido
<code>automount</code> “Automount” en la página 358	Archivo de opciones del cliente (<code>dsm.opt</code>).	Sin efecto
<code>basesnapshotname</code> “Basesnapshotname” en la página 361	Archivo de opciones del cliente (<code>dsm.opt</code>) o línea de mandatos.	Válido
<code>changingretries</code> “Changingretries” en la página 363	En el archivo de opciones del sistema cliente (<code>dsm.sys</code>) o en la línea de mandatos.	Sin efecto
<code>compressalways</code> “Compressalways” en la página 369	Archivo de opciones del cliente (<code>dsm.opt</code>) o línea de mandatos.	Válido
<code>compression</code> “Compression” en la página 370	Archivo de opciones del sistema cliente (<code>dsm.sys</code>) dentro de una stanza de servidor o línea de mandatos.	Válido
<code>createnewbase</code> “Createnewbase” en la página 373	Sólo línea de mandatos.	Válido
<code>diffsnapshot</code> “Diffsnapshot” en la página 387	Sólo línea de mandatos.	Válido
<code>diffsnapshotname</code> “Diffsnapshotname” en la página 388	Archivo de opciones del cliente (<code>dsm.opt</code>) o línea de mandatos.	Válido
<code>dirsonly</code> “Dirsonly” en la página 390	Sólo línea de mandatos.	Válido
<code>domain</code> “Domain” en la página 394	Archivo de opciones del sistema cliente (<code>dsm.sys</code>), archivo de opciones del usuario cliente (<code>dsm.opt</code>), o línea de mandatos.	Válido
<code>efsdecrypt</code> “Efsdecrypt” en la página 410	Archivo de opciones del sistema cliente (<code>dsm.sys</code>), archivo de opciones del usuario cliente (<code>dsm.opt</code>), o línea de mandatos.	Sin efecto

Tabla 75. Mandato Incremental: opciones relacionadas (continuación)

Opción	Donde se especifica	Con snapdiff
enablelanfree "Enablelanfree" en la página 416	En el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos.	Válido
encryptiontype "Encryptiontype" en la página 417	Archivo de opciones del sistema (dsm.sys) dentro de una stanza de servidor.	Válido
encryptkey "Encryptkey" en la página 418	Archivo de opciones del sistema (dsm.sys) dentro de una stanza de servidor.	Válido
exclude.fs.nas "Opciones exclude" en la página 425	Archivo de opciones del sistema cliente (dsm.sys).	Sin efecto
filelist "Filelist" en la página 439	Sólo línea de mandatos.	No válido
filesonly "Filesonly" en la página 443	Sólo línea de mandatos.	Válido
followsymboliclink "Followsymbolic" en la página 444	Archivo de opciones del cliente (dsm.opt).	Sin efecto
include.fs.nas "Opciones include" en la página 458	En el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos.	Sin efecto
inclexcl "Inclexcl" en la página 456	Archivo de opciones del sistema cliente (dsm.sys).	Válida, pero solo cuando NetApp detecta un cambio de archivo.
incrbydate "Incrbydate" en la página 474	Sólo línea de mandatos.	No válido
memoryefficientbackup "Memoryefficientbackup" en la página 491	Esta opción se admite en dsm.sys y dsm.opt, pero el valor de dsm.opt se pasa por alto si también se encuentra en dsm.sys. También puede incluir esta opción en una stanza del servidor o en la línea de mandatos inicial.	Sin efecto
monitor "Monitor" en la página 496	Sólo línea de mandatos.	No válido
nojournal "Nojournal" en la página 502	Sólo línea de mandatos.	No válido
postsnapshotcmd "Postsnapshotcmd" en la página 516	Archivo de opciones del sistema cliente (dsm.sys) o con la opción include.fs.	Válido
preservelastaccessdate "Preservelastaccessdate" en la página 519	Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.	Válido
presnapshotcmd "Presnapshotcmd" en la página 523	Archivo de opciones del sistema cliente (dsm.sys) o con la opción include.fs.	Válido
removeoperandlimit "Removeoperandlimit" en la página 528	Sólo línea de mandatos.	Válido
skipaclupdatecheck "Skipaclupdatecheck" en la página 560	Archivo de opciones del cliente (dsm.opt).	Válido

Tabla 75. Mandato Incremental: opciones relacionadas (continuación)

Opción	Donde se especifica	Con snapdiff
snapdiffhttps "Snapdiffhttps" en la página 566	Sólo línea de mandatos.	Válido
snapshotcachesize "Snapshotcachesize" en la página 567	Archivo de opciones del sistema cliente (dsm.sys) o con la opción include.fs.	Sin efecto
snapshotproviderfs "Snapshotproviderfs" en la página 569	Archivo de opciones del sistema (dsm.sys) en una stanza del servidor o con la opción include.fs.	No válido
snapshotproviderimage "Snapshotproviderimage" en la página 570	Archivo de opciones del sistema cliente (dsm.sys) o con la opción include.image.	No válido
snapshotroot "Snapshotroot" en la página 571	Sólo línea de mandatos.	No válido
subdir "Subdir" en la página 581	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.	No válido
tapeprompt "Tapeprompt" en la página 583	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.	Válido
toc "Toc" en la página 596	Sólo línea de mandatos.	No válido
useexistingbase "Useexistingbase" en la página 601	Sólo línea de mandatos.	Válido
virtualfsname "Virtualfsname" en la página 606	Sólo línea de mandatos.	No válido
virtualmountpoint "Virtualmountpoint" en la página 606	Archivo de opciones del sistema cliente (dsm.sys).	No válido

Clientes soportados

Esta opción es válida para clientes de Linux x86_64.

Sintaxis

►►—SNAPDiff—◄◄

Parámetros

No hay parámetros para esta opción.

Ejemplos

Línea de mandatos:

Realice una copia de seguridad incremental diferencial de instantánea de un sistema de archivos NFS montado /vol/vol1 alojado en el servidor de archivos homestore.example.com, donde /net/home1 es el punto de montaje de /vol/vol1.

```
incremental -snapdiff -diffsnapshot=latest /net/home1
```

Línea de mandatos:

Ejecute una copia de seguridad incremental completa única tras detectar que el servidor de NetApp ha migrado a un servidor de archivos habilitado para Unicode de un servidor que no soportaba nombres de archivos Unicode.

```
dsmc incremental -snapdiff -createnewbase=migrate /net/home1
```

Ejecute una copia de seguridad incremental diferencial de instantáneas tras detectar que el servidor de NetApp ha migrado a un servidor de archivos habilitado por Unicode de un servidor que no soportaba los nombres de archivos Unicode. Este mandato suprime el mensaje de aviso.

```
dsmc incremental -snapdiff -createnewbase=ign /net/home1
```

Realice una copia de seguridad incremental completa debido a que ha realizado algunos cambios de inclusión o exclusión:

```
dsmc incremental -snapdiff -createnewbase=yes /net/home1
```

Conceptos relacionados:

“Copia de seguridad diferencial de la instantánea con una conexión HTTPS” en la página 178

“Soporte de SnapMirror para la copia de seguridad a incrementos progresivos asistida por instantáneas NetApp (snapdiff)” en la página 120

Tareas relacionadas:

“Configuración de NetApp y IBM Spectrum Protect para copias de seguridad incrementales de diferencia de instantánea” en la página 114

Referencia relacionada:

“Snapdiffhttps”

“Basesnapshotname” en la página 361

“Diffsnapshotname” en la página 388

“Useexistingbase” en la página 601

“Diffsnapshot” en la página 387

“Establecer contraseña” en la página 784

Snapdiffhttps

Especifique la opción `snapdiffhttps` para utilizar una conexión HTTPS segura para comunicarse con un archivador NetApp durante una copia de seguridad diferencial de instantáneas.

Al especificar esta opción, el cliente de archivado de copia de seguridad puede establecer una sesión de administración segura con el archivador de NetApp independientemente de si está habilitado o no el acceso de administración de HTTP en el archivador NetApp.

Importante: El protocolo de comunicación predeterminado que utiliza el cliente de archivado de copia de seguridad para establecer la sesión de administración con el archivador NetApp es HTTP. Para utilizar una conexión HTTPS segura, debe especificar la opción `snapdiffhttps` siempre que se ejecuta una copia de seguridad diferencial de instantáneas.

Restricciones:

Las siguientes restricciones se aplican a copias de seguridad diferencias instantáneas con HTTPS:

- La conexión HTTPS sólo se utiliza para transmitir datos de forma segura a través de la sesión de administración entre el cliente de archivado de copia de seguridad y el archivador de NetApp. Los datos de la sesión de administración incluyen información como credenciales del archivador, información de instantánea y los nombres de archivo y los atributos que se generan mediante el proceso de diferenciación de instantáneas. La conexión HTTPS no se utiliza para transmitir datos de archivos normales a los que se accede en el archivador mediante el cliente a través del compartimiento de archivos. La conexión HTTPS tampoco se aplica a los datos de archivos normales transmitidos mediante el cliente al servidor de IBM Spectrum Protect a través del protocolo cliente/servidor de IBM Spectrum Protect normal.
- La opción **snappdiffhttps** no se aplica a vFilers porque el protocolo HTTPS no está admitido en NetApp vFiler.
- La opción **snappdiffhttps** sólo está disponible utilizando la interfaz de línea de mandatos. No está disponible para su utilización con la GUI del cliente de archivado de copia de seguridad.

Clientes soportados

Esta opción es válida para clientes de Linux x86_64.

Archivo de opciones

Esta opción sólo es válida en la interfaz de línea de mandatos. No puede especificarla en un archivo de opciones del cliente.

Sintaxis

►►—SNAPDIFFHTTPS—◄◄

Parámetros

No hay parámetros para esta opción.

Ejemplos

Línea de mandatos:

Emita el mandato siguiente en un sistema Linux, con un sistema de archivos montado en NFS /vol/vol1 alojado en el servidor de archivos homestore.example.com, donde /net/home1 es el punto de montaje de /vol/vol1.

```
dsmc incr /net/home1 -snapdiff -snappdiffhttps
```

Conceptos relacionados:

“Copia de seguridad diferencial de la instantánea con una conexión HTTPS” en la página 178

Referencia relacionada:

“Snapdiff” en la página 561

Snapshotcachesize

Utilice la opción **snapshotcachesize** para especificar un tamaño adecuado para crear una instantánea.

Se necesita una estimación de tamaño adecuada para almacenar los bloques de datos originales de los datos modificados y eliminados del instante específico en que se tomó la instantánea.

Para archivado o copia de seguridad de archivos basados en instantánea, utilice la opción `snapshotcachesize` con la opción `include.fs`, o bien en la sección del servidor en el archivo `dsm.sys`.

Para realizar copias de seguridad de imagen basada en instantánea, utilice la opción `snapshotcachesize` con el mandato **backup image**, la opción `include.image` o bien en el archivo `dsm.sys`.

Clientes soportados

Esta opción *sólo* es válida para los clientes AIX y Linux. La API de IBM Spectrum Protect no admite esta opción. El servidor también puede definir esta opción.

Archivo de opciones

Especifique esta opción en la stanza de servidor, en el archivo `dsm.sys`. Puede establecer esta opción en la ficha **Imagen-Instantánea** del editor de preferencias.

Sintaxis

►►—SNAPSHOTCACHESize— —size—►►

Parámetros

size

Especifica un tamaño adecuado para crear la instantánea con el fin de almacenar los bloques de datos originales de los datos modificados y eliminados del instante específico en que se tomó la instantánea. El valor es el porcentaje del tamaño del sistema de archivos que se cambia debido a la actividad del sistema de archivos. El rango de valores oscila entre 1 y 100 por cien. Para AIX JFS2 y Linux el valor predeterminado es el 100 por cien del tamaño del sistema de archivos. Si no se dispone de una cantidad suficiente de espacio libre para crear la instantánea, el mandato fallará y mostrará un mensaje de error. A continuación, podrá incrementar el tamaño del grupo de volúmenes o bien volver a intentar la operación. Si la práctica le ha demostrado que para la actividad del sistema de archivos JFS2 de AIX no necesitará un tamaño de instantánea del 100 por cien, puede ajustar el valor con más precisión.

Ejemplos

Archivo de opciones:

```
snapshotcachesize 95
AIX only: include.fs /kalafs1
          snapshotproviderfs=JFS2 snapshotcachesize=95
AIX only: include.image /kalafs2
          snapshotcachesize=95
Linux only: include.image /linuxfs1
           snapshotcachesize=100
```

Línea de mandatos:

```
-snapshotcachesize=95
```

Información relacionada

Consulte el tema “Opciones include” en la página 458 para obtener más información acerca de `include.fs`.

Snapshotproviderfs

Utilice la opción `snapshotproviderfs` para habilitar las operaciones de archivado y copia de seguridad de archivo basadas en instantáneas, y para especificar un proveedor de instantáneas.

Debe ser un usuario root para poder realizar una operación de archivado o de copia de seguridad de archivos basada en instantáneas. Si no es usuario root, la operación fallará y mostrará un mensaje de error.

Clientes soportados

Esta opción es válida solo para los clientes AIX. La API de IBM Spectrum Protect no admite esta opción. El servidor también puede definir esta opción.

Archivo de opciones

Especifique esta opción en la stanza del servidor del archivo de opciones del sistema, `dsm.sys`, con el fin de habilitar instantáneas para todos los sistemas de archivos JFS2 del cliente. Puede alterar temporalmente la opción para todos los clientes de una operación específica si indica esta opción en la línea de mandatos de archivado y copia de seguridad. También puede alterar temporalmente la opción para todos los clientes de un sistema de archivos específico mediante la sentencia `include.fs` en el archivo `dsm.sys`. También puede establecer esta opción mediante el editor de preferencias.

Sintaxis

►►—SNAPSHOTPROVIDERFS— —*value*—————►►

Parámetros

value

Especifique uno de los valores siguientes:

JFS2

Especifica que desea realizar una operación de archivado o copia de seguridad de archivos basada en instantáneas mientras el sistema de archivos está disponible para otras aplicaciones del sistema. *Sólo* es válido para los sistemas de archivos JFS2 en clientes AIX.

NONE

Especifica que no se deben utilizar instantáneas. De este modo se realizará una operación de archivado o copia de seguridad de archivos mediante el sistema de archivos especificado. Éste es el valor predeterminado.

Ejemplos

Archivo de opciones:

```
snapshotproviderfs JFS2
include.fs /kalafs1 snapshotproviderfs=JFS
```

Línea de mandatos:
-SNAPSHOTPROVIDERFs=JFS2

Snapshotproviderimage

Utilice la opción snapshotproviderimage para activar la copia de seguridad de imágenes basada en instantánea y para especificar un proveedor de instantáneas.

Debe ser usuario root para realizar una operación de copia de seguridad de imagen basada en instantáneas. Si no es usuario root, la operación fallará y mostrará un mensaje de error.

Clientes soportados

Esta opción es válida solo para los clientes AIX y Linux. La API de IBM Spectrum Protect no admite esta opción. El servidor también puede definir esta opción.

Archivo de opciones

Especifique esta opción en la stanza del servidor del archivo de opciones del sistema, dsm.sys, con el fin de habilitar instantáneas para todos los sistemas de archivos del cliente. Puede alterar temporalmente la opción para todos los clientes de una operación específica si indica esta opción para el mandato **backup image** en la línea de mandatos. También puede alterar temporalmente la opción para todos los clientes de un sistema de archivos específico mediante la sentencia include.image en el archivo dsm.sys. También puede establecer esta opción mediante el editor de preferencias.

Sintaxis

►►—SNAPSHOTPROVIDERImage— *value* —————►►

Parámetros

value

Especifique uno de los valores siguientes:

JFS2

Especifica que desea realizar una copia de seguridad de imágenes basada en instantánea mientras el sistema de archivos está disponible para otras aplicaciones del sistema. Éste es el valor predeterminado para los sistemas de archivos JFS2. *Sólo* es válido para los clientes AIX.

LINUX_LVM

Especifica que desea realizar una copia de seguridad de imágenes basada en instantánea mientras el sistema de archivos está disponible para otras aplicaciones del sistema. Es el valor predeterminado para los sistemas de archivos que residen en los volúmenes lógicos que ha creado el Gestor de volúmenes lógicos de Linux. *Sólo* es válido para los clientes Linux.

NONE

Especifica que no desea realizar una operación de copia de seguridad de imágenes basada en instantánea. De este modo se realizará una operación de copia de seguridad de imágenes estática mediante el sistema de archivos especificado. Es el valor predeterminado para los sistemas de archivos distintos de JFS2 de AIX y LVM de Linux.

Ejemplos

Archivo de opciones:

```
snapshotprovideri JFS2  
include.image /kalafs1 snapshotprovideri=JFS2
```

Línea de mandatos:

```
-SNAPSHOTPROVIDERImage=NONE
```

Snapshotroot

Utilice la opción `snapshotroot` con los mandatos **incremental**, **selective** o **archive** con una aplicación de un proveedor de software independiente que proporcione una instantánea de un volumen lógico para asociar los datos de la instantánea local a los datos del espacio de archivos reales que se almacenan en el servidor de IBM Spectrum Protect.

La opción `snapshotroot` puede utilizarse para realizar la copia de seguridad de los sistemas de archivos montados NFS. Tanto la especificación de copia de seguridad (origen) como el valor `snapshotroot` pueden ser una especificación de archivo montado en NFS. Por ejemplo, la opción `snapshotroot` puede utilizarse para realizar la copia de seguridad de un sistema de archivos NFS alojado en un almacenamiento conectado a red (NAS) que dé soporte a las instantáneas.

Esta opción debe utilizarse con una copia de seguridad incremental del volumen de archivador NAS en lugar de una copia incremental simple o incremental con `snapshotroot` siempre que el archivador NAS esté ejecutando ONTAP V7.3 por motivos de rendimiento. Las opciones `snappdiff` y `snapshotroot` no deben utilizarse conjuntamente.

En el siguiente ejemplo, `filesystem test495` se ha montado en NFS desde un archivador NAS `philo` y `/philo/test945/.snapshot/backupsnap` representa la instantánea que se ha creado en el archivador NAS.

```
dsmc i /philo/test945 -snapshotroot=/philo/test945/.snapshot/backupsnap
```

También puede especificar un directorio con la opción `snapshotroot` al realizar la copia de seguridad de cada juego de archivos como un espacio de archivos individual.

La opción `snapshotroot` no proporciona ningún recurso para tomar una instantánea de volumen, solo para gestionar los datos que ha creado una instantánea de volumen.

Por ejemplo, imaginemos que una aplicación toma una instantánea del sistema de archivos `/usr` y que la monta como `/snapshot/day1`. Si realiza la copia de seguridad de estos datos mediante la utilización del siguiente mandato, en el servidor se creará un espacio de archivos exclusivo denominado `/snapshot/day1`.

```
dsmc incremental /snapshot/day1
```

Sin embargo, puede que desee asociar los datos de la instantánea a los datos que ya se han procesado para el sistema de archivos `/usr`. Mediante la utilización de la opción `snapshotroot`, puede asociar los datos al espacio de archivos que corresponde al sistema de archivos `/usr` en el servidor de IBM Spectrum Protect:

```
dsmc incremental /usr -snapshotroot=/snapshot/day1
```

Con posterioridad, otro día, puede realizar la copia de seguridad de una instantánea grabada en una ubicación alternativa, pero gestionada en el mismo espacio de archivos en el servidor:

```
dsmc incremental /usr -snapshotroot=/snapshot/day2
```

Puede realizar copias de seguridad incrementales, copias de seguridad selectivas u operaciones de archivado de un único directorio, de una estructura de directorios o de un único archivo utilizando la opción `snapshotroot`. En todos los casos, la opción `snapshotroot` debe identificar la raíz del volumen lógico que la instantánea ha creado. Por ejemplo:

```
dsmc incremental /usr/dir1/* -subdir=yes
-snapshotroot=/snapshot/day1
dsmc selective /usr/dir1/sub1/file.txt
-snapshotroot=/snapshot/day1
dsmc archive /usr/dir1/sub1/*.txt
-snapshotroot=/snapshot/day1
```

Si desea incluir o excluir especificaciones de archivo concretas, las sentencias de inclusión y exclusión deben contener el nombre del sistema de archivos que era el origen de la instantánea (el sistema de archivos `/usr` y no el nombre del destino de la instantánea (`/snapshot/day1`). Esto le permite conservar un conjunto de sentencias de inclusión y exclusión en el que no se considera el nombre del volumen lógico en el que se graba la instantánea. A continuación, se muestran ejemplos de sentencias de inclusión y exclusión.

```
include /usr/dir1/*.txt 1yrmgmtclass
exclude /usr/mydocs/*.txt
```

Las sentencias de inclusión/exclusión siguientes no son válidas, pues contienen el nombre de la instantánea:

```
include /snapshot/day1/dir1/*.txt 1yrmgmtclass
exclude /snapshot/day1/mydocs/*.txt
```

Para una copia de seguridad incremental o selectiva, o para una operación de archivado, debe utilizar la opción `snapshotroot` con una única especificación de archivo. No puede especificar varias especificaciones de archivo o ninguna especificación de archivo. Por ejemplo, estos mandatos son válidos:

```
dsmc incremental /usr -snapshotroot=/snapshot/day1
dsmc incremental /usr/dir1/* -snapshotroot=/snapshot/day1
```

El mandato siguiente no es válido porque contiene dos especificaciones de archivo:

```
dsmc incremental /usr/dir1/* /home/dir2/*
-snapshotroot=/snapshot/day1
```

El mandato siguiente no es válido porque no contiene ninguna especificación de archivo:

```
dsmc incremental -snapshotroot=/snapshot/day1
```

Notas:

1. Asegúrese de que la opción `snapshotroot` haga referencia a una instantánea del volumen correcto. Asegúrese de que la ubicación `snapshotroot` haga referencia a la raíz de la instantánea. Si no se siguen estas reglas, es posible que se produzcan resultados imprevisibles, como la caducidad incorrecta de los archivos.
2. Si especifica la opción `filelist` y la opción `snapshotroot`, se asumirá que todos los archivos especificados en la opción `filelist` están en el mismo sistema de archivos. Si hay entradas en `filelist` en un sistema de archivos

diferente, serán ignoradas y se registrará un error. Si `filelist` contiene archivos creados en el sistema de archivos después de tomar la instantánea, se ignorarán dichas entradas y se registrará el error.

3. No puede utilizar la opción `snapshotroot` con la opción `snappdiff`.
4. Puede utilizar la opción `snapshotroot` con las opciones `preschedulecmd` y `postschedulecmd` o en un script automatizado que se ejecute con el planificador de cliente.

Clientes soportados

Esta opción es válida para los clientes siguientes:

- Clientes UNIX y Linux excepto Mac OS X.

Sintaxis

►►—SNAPSHOTRoot =— —*snapshot_volume_name*—————►►

Parámetros

snapshot_volume_name

Especifica la raíz del volumen lógico que ha creado la aplicación de instantáneas de otro proveedor.

Ejemplos

Línea de mandatos:

```
dsmc incremental /usr -SNAPSHOTRoot=/snapshot/day1
```

Srvoptsetencryptiondisabled

La opción `srvoptsetencryptiondisabled` permite que el cliente ignore las opciones de cifrado en el conjunto de opciones del cliente desde el servidor de IBM Spectrum Protect.

Si la opción está establecida en `yes` en el archivo de opciones del cliente, el cliente ignorará las siguientes opciones en un conjunto de opciones del cliente desde el servidor:

- `encryptkey generate`
- `exclude.encrypt`
- `include.encrypt`

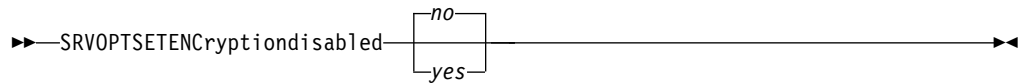
Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Especifique esta opción en el archivo de opciones del cliente (`dsm.sys`) de una stanza de servidor.

Sintaxis



Parámetros

yes

El cliente de copia de seguridad y archivado pasa por alto los valores de las opciones de cifrado listadas en un conjunto de opciones del cliente desde el servidor de IBM Spectrum Protect.

no

El cliente de copia de seguridad y archivado procesa los valores de las opciones de cifrado listadas en un conjunto de opciones del cliente desde el servidor de IBM Spectrum Protect. Éste es el valor predeterminado.

Ejemplos

Archivo de opciones:

`srvoptsetencryptiondisabled no`

Línea de mandatos:

No se aplica.

Srvprepostscheddisabled

La opción `srvprepostscheddisabled` especifica si ha de impedirse que los mandatos de preplanificación y de postplanificación que ha especificado el administrador de IBM Spectrum Protect se ejecuten en el sistema cliente al realizar operaciones planificadas.

La opción `srvprepostscheddisabled` puede utilizarse con las opciones `schedcmddisabled` y `srvprepostscheddisabled` para desactivar la posibilidad de que el administrador de IBM Spectrum Protect ejecute mandatos del sistema operativo no deseados en un nodo cliente.

Clientes soportados

Esta opción es válida para todos los clientes de copia de seguridad y archivado que utilizan el planificador cliente de IBM Spectrum Protect. El servidor no puede definir esta opción.

Archivo de opciones

Especifique esta opción en el archivo `dsm.sys` dentro de una stanza de servidor para el planificador. Puede establecer esta opción en el separador **Planificador** del editor de preferencias, en la sección de **Mandato de planificación**.

Sintaxis



Parámetros

No

Especifica que el cliente ha de permitir que los mandatos de preplanificación y de postplanificación que ha definido el administrador de IBM Spectrum Protect

se ejecuten en el sistema cliente al realizar operaciones planificadas. Si el cliente y el administrador de IBM Spectrum Protect, ambos, han definido un mandato de preplanificación o de postplanificación, el mandato que ha definido el administrador modificará temporalmente el mandato correspondiente que se ha definido en el archivo de opciones del cliente. Éste es el valor predeterminado.

Yes

Especifica que el cliente ha de impedir que los mandatos de preplanificación y de postplanificación que ha definido el administrador de IBM Spectrum Protect se ejecuten en el sistema cliente al realizar operaciones planificadas. Si el cliente y el administrador de IBM Spectrum Protect, ambos, han definido un mandato de preplanificación o de postplanificación, el mandato que ha definido el administrador *no* modificará temporalmente el mandato correspondiente que se ha definido en el archivo de opciones del cliente. Esta opción se puede utilizar conjuntamente con las opciones `schedcmddisabled` y `srvprepostscheddisabled`.

Ejemplos

Archivo de opciones:

`srvprepostscheddisabled yes`

Línea de mandatos:

No se aplica.

Srvprepostsnapdisabled

La opción `srvprepostsnapdisabled` especifica si ha de impedirse que los mandatos de previos y posteriores a la instantánea que ha especificado el administrador de IBM Spectrum Protect se ejecuten en el sistema cliente al realizar operaciones planificadas de copia de seguridad de instantánea.

La opción `srvprepostsnapdisabled` puede utilizarse con las opciones `schedcmddisabled` y `srvprepostsnapdisabled` para desactivar la posibilidad de que el administrador de IBM Spectrum Protect ejecute mandatos del sistema operativo no deseados en un nodo cliente.

Clientes soportados

Esta opción es válida para los clientes Linux que admiten el mandato de copia de seguridad de instantánea. El servidor no puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Especifique esta opción en el archivo `dsm.sys` dentro de una stanza de servidor para el planificador. Puede establecer esta opción en el separador **Instantánea** del editor de preferencias, en la sección **Opciones de instantáneas**.

Sintaxis



Parámetros

No Especifica que el cliente ha de permitir que los mandatos previos y posteriores a la instantánea que ha definido el administrador de IBM Spectrum Protect se ejecuten en el sistema cliente al realizar operaciones planificadas de copia de seguridad de instantánea. Si el cliente y el administrador de IBM Spectrum Protect, ambos, han definido un mandato previo o posterior a la instantánea, el mandato que ha definido el administrador modificará temporalmente el mandato correspondiente que se ha definido en el archivo de opciones del cliente. Éste es el valor predeterminado.

Yes

Especifica que el cliente ha de impedir que los mandatos previos y posteriores a la instantánea que ha definido el administrador de IBM Spectrum Protect se ejecuten en el sistema cliente al realizar operaciones planificadas de copia de seguridad de instantánea. Si el cliente y el administrador de IBM Spectrum Protect, ambos, han definido un mandato previo o posterior a la instantánea, el mandato que ha definido el administrador *no* modificará temporalmente el mandato correspondiente que se ha definido en el archivo de opciones del cliente. Esta opción puede utilizarse junto con las opciones `schedcmddisabled` y `srvprepostsnapdisabled`.

Ejemplos

Archivo de opciones:

`srvprepostsnapdisabled yes`

Línea de mandatos:

No se aplica.

Ssl

Utilice la opción `ssl` para habilitar Secure Sockets Layer (SSL) para proporcionar comunicaciones de servidor y de cliente seguro.

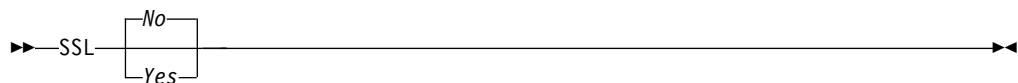
Clientes soportados

Esta opción es válida para todos los clientes soportados.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. También puede establecer esta opción en el separador **Comunicación** del editor de preferencias.

Sintaxis



Parámetros

No Especifica que el cliente de copia de seguridad y archivado no utiliza SSL para cifrar la información. No es el valor predeterminado.

Yes

Especifica que el cliente de copia de seguridad y archivado utiliza SSL para cifrar la información.

Para habilitar SSL, especifique `ssl yes` y cambie el valor de la opción `tcpport`. Cambiar el valor de la opción `tcpport` es normalmente necesario porque el servidor de IBM Spectrum Protect normalmente está configurado para escuchar conexiones SSL en un puerto distinto.

Ejemplos

Archivo de opciones:

`ssl yes`

Línea de mandatos:

No se aplica.

Información relacionada

“Configuración de las comunicaciones cliente/servidor de IBM Spectrum Protect con Secure Sockets Layer” en la página 74.

“`Sslrequired`” en la página 578

“`Tcpport`” en la página 590

Sslfipsmode

La opción `sslfipsmode` especifica si el cliente utiliza la modalidad de SSL Federal Information Processing Standards (FIPS) para comunicaciones de capa segura de sockets (SSL) con el servidor. El valor predeterminado es `no`.

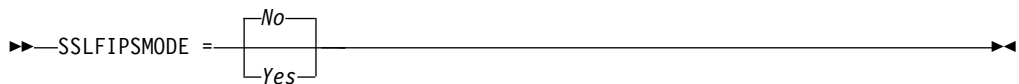
Clientes soportados

Esta opción se soporta en todos los clientes.

Archivo de opciones

Establezca esta opción en el archivo de opciones del cliente. No se puede especificar como un parámetro de línea de mandatos y no se puede establecer esta opción en un conjunto de opciones de cliente.

Sintaxis



Parámetros

No Especifica que el cliente no utiliza la modalidad SSL FIPS para comunicaciones seguras con el cliente. La modalidad SSL FIPS solo se admite en la versión 6.3 y en versiones posteriores del servidor. Establezca esta opción de cliente en `no` si el cliente utiliza SSL para conectarse a un servidor que no sea V6.3 o posterior.

Yes

Especifica que el cliente utiliza la modalidad SSL FIPS para comunicaciones seguras con el cliente. Establecer esta opción en `yes` restringe la negociación de la sesión SSL para que utilice sólo suites de cifrado aprobadas por FIPS. La modalidad SSL FIPS solo se admite en el servidor V6.3 (o posterior).

Ejemplo

Para habilitar la modalidad SSL FIPS en el cliente:

SSLFIPSMODE yes

Sslrequired

La opción `sslrequired` especifica las condiciones en que SSL es o no necesario cuando el cliente inicia la sesión en el servidor o en los agentes de almacenamiento de IBM Spectrum Protect. Para habilitar realmente SSL para que las comunicaciones de cliente a servidor y de cliente a almacenamiento sean seguras, debe configurar la opción de cliente `ssl` en yes.

Clientes soportados

Esta opción está soportada para todos los clientes.

Archivo de opciones

Coloque esta opción en el archivo de opciones del cliente o en la GUI, en la ficha Comunicaciones. No puede establecer esta opción en la línea de mandatos.

Sintaxis



Parámetros

Default

Este valor indica que el SSL es necesario para proteger las comunicaciones entre el cliente y el servidor, y entre el cliente y los agentes de almacenamiento, si `AUTHENTICATION=LDAP` se configura en el servidor. Para proteger las comunicaciones utilizando SSL, también debe establecer `ssl=yes` en el cliente.

Si `AUTHENTICATION=LOCAL` se configura en el servidor, este valor indica que el SSL no es necesario. Aunque el SSL no es obligatorio cuando `AUTHENTICATION=LOCAL` y `sslrequired=default`, puede utilizar SSL estableciendo la opción de cliente `ssl` en yes.

Yes

Indica que siempre se necesita SSL para proteger las comunicaciones entre el cliente y el servidor, y entre el cliente y el almacenamiento de agentes.

`sslrequired=yes` no tiene ninguna dependencia en la opción del servidor `AUTHENTICATION`. Si configura `sslrequired=yes` en el cliente, debe configurar también `ssl=yes` en el cliente.

No Indica que no necesita utilizar SSL para proteger las comunicaciones entre el cliente y el servidor o entre el cliente y el almacenamiento de agentes. Elija esta opción solo si utiliza una red privada virtual u otro método para proteger las comunicaciones de la sesión. Todavía puede habilitar SSL configurando `ssl=yes` en el cliente; pero `sslrequired=no` especifica que SSL no es un requisito previo.

SERVERonly

Indica que se necesita SSL para comunicaciones de cliente a servidor y no para comunicaciones de servidor a almacenamiento de agentes. Para utilizar SSL para la comunicación de cliente a servidor, configure `sslrequired=serveronly` y `ssl=yes`. El valor del servidor para la opción `AUTHENTICATION` puede ser `LOCAL` o `LDAP`.

Para las comunicaciones de cliente a almacenamiento de agentes, utilice la opción de cliente `lanfreessl` para habilitar SSL.

En la tabla siguiente se describen las situaciones en las que la autenticación se realiza satisfactoriamente o presenta anomalías dependiendo de los valores de la opción `SSLREQUIRED` en el servidor, y el cliente, y el valor de la opción `ssl` en el cliente. Los resultados de la tabla presuponen que se proporcionan credenciales válidas.

Tabla 76. Efectos de los valores SSL de servidor y cliente en el éxito o el fracaso de los intentos de inicio de sesión

opción SSLREQUIRED (valor de servidor)	opción sslrequired (valor de cliente)	opción ssl (valor de cliente)	Éxito o anomalía de autenticación
Yes	Yes	Yes	Autenticación satisfactoria
Yes	Yes	No	Autenticación anómala; el cliente rechaza la sesión
Yes	No	Yes	Autenticación satisfactoria
Yes	No	No	Autenticación anómala; el servidor rechaza la sesión
No	Yes	Yes	Autenticación satisfactoria
No	Yes	No	Autenticación anómala; el cliente rechaza la sesión
No	No	Yes	Autenticación satisfactoria
No	No	No	Autenticación satisfactoria

En el texto siguiente se describe cómo la configuración de `SSLREQUIRED=DEFAULT` y `SSLREQUIRED=SERVERONLY` en el servidor afecta a la opción `ssl` en el cliente.

Si el servidor se configura con `SSLREQUIRED=DEFAULT` y `AUTHENTICATION=LDAP`, el cliente debe configurarse como `ssl=yes`, si no, la autenticación falla.

Si el servidor se configura con `SSLREQUIRED=DEFAULT` y `AUTHENTICATION=LOCAL`, el cliente debe configurarse como `ssl=yes` o `ssl=no`.

Si el servidor se configura con `SSLREQUIRED=SERVERONLY`, debe configurarse `ssl=yes` en el cliente. La opción de cliente `lanfreessl` se puede establecer en `yes`, para proteger la comunicación con un almacenamiento de agentes, o en `no` si las comunicaciones seguras con los almacenamientos de agentes no son necesarias.

Ejemplos

Archivo de opciones:

```
sslrequired yes
sslrequired no
sslrequired default
sslrequired serveronly
```

Línea de mandatos:

No aplicable; no se puede establecer esta opción en la línea de mandatos.

Ssldisablelegacytls

Utilice la opción `ssldisablelegacytls` para no permitir el uso de protocolos SSL que son inferiores a TLS 1.2.

Clientes soportados

Esta opción es válida para todos los clientes soportados.

Archivo de opciones

Establezca esta opción en el archivo `dsm.sys`. También puede establecer esta opción en la GUI seleccionando el recuadro de selección **Requerir TLS 1.2 o superior** en el separador **Comunicación** del editor Preferencias. No puede establecer esta opción en la línea de mandatos.

Sintaxis



Parámetros

No Especifica que el cliente de copia de seguridad y archivado no necesita TLS 1.2 para sesiones de SSL. Permite la conexión en TLS 1.1 y protocolos SSL inferiores. No es el valor predeterminado.

Yes

Especifica que el cliente de copia de seguridad y archivado requiere que todas las sesiones de SSL utilicen el protocolo de TLS 1.2 (o superior).

Ejemplos

Archivo de opciones:

```
ssldisablelegacytls yes
```

Línea de mandatos:

No se aplica.

Información relacionada

“Ssl” en la página 576.

“Sslrequired” en la página 578

“Tcpport” en la página 590

Stagingdirectory

La opción `stagingdirectory` define la ubicación donde el cliente mantiene los datos que genera a fin de realizar sus operaciones. Una vez finalizado el proceso se suprimen los datos.

Esta opción se utiliza durante las operaciones de copia de seguridad de diferencia de instantáneas.

Clientes soportados

Esta opción es válida para los clientes de Linux. El servidor también puede definir esta opción.

Archivo de opciones

Coloque esta opción en el archivo de opciones del cliente (`dsm.opt`). Cuando `stagingdirectory` se especifica en la línea de mandatos, modifica los valores especificados en el archivo de opciones.

Sintaxis

►►—STAGINGDIRectory—ruta—◄◄

Parámetros

vía de acceso

Especifica la vía de acceso del directorio donde el cliente graba los datos de transición. Si no se especifica ningún directorio intermedio, el cliente almacena datos temporales en el sistema de archivos temporales (normalmente `/tmp`).

Ejemplos

Archivo de opciones:

`stagingdirectory /usr/tsmdata`

`stagingdirectory /private/tmp`

Línea de mandatos:

`-stagingdir="/tmp/tsmtempdata"`

Referencia relacionada:

“Diffsnapshot” en la página 387

“Snapdiff” en la página 561

Subdir

La opción `subdir` especifica si desea incluir subdirectorios de los directorios especificados para el proceso.

Puede utilizar la opción `subdir` con los mandatos siguientes:

- **archive**
- **delete archive**
- **delete backup**
- **incremental**
- **query archive**
- **query backup**
- **restore**

- **restore backupset**
- **restore group**
- **retrieve**
- **selective**

Si establece la opción `subdir` en `yes` al realizar la copia de seguridad de una vía de acceso y un archivo específicos, el cliente de copia de seguridad y archivado busca de forma recursiva en todos los subdirectorios de esa vía de acceso las instancias del archivo especificado que existan en los subdirectorios. Por ejemplo, supongamos que existe un archivo denominado `myfile.txt` en un cliente en los siguientes directorios:

```
//myfile.txt
/dir1/myfile.txt
/dir1/dir_a/myfile.txt
/dir1/dir_b/myfile.txt
```

Si se realiza una copia de seguridad selectiva del archivo, como se muestra a continuación, se realiza una copia de seguridad de todas las instancias de `myfile.txt`:

```
dsmc sel /myfile.txt -subdir=yes
```

De forma parecida, el siguiente mandato muestra todas las instancias de `myfile.txt` si especifica `subdir=yes` en el archivo de opciones de cliente o en un conjunto de opciones de cliente.

```
dsmc restore /myfile.txt -pick
```

Clientes soportados

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Establezca esta opción en el archivo de opciones de usuario del cliente (`dsm.opt`).

Sintaxis



Parámetros

No Los subdirectorios no se procesan. Éste es el valor predeterminado.

Yes

Los subdirectorios se procesan. Debido a que el programa de cliente busca en todos los subdirectorios de un directorio que se está procesando, el proceso puede tardar más tiempo en completarse. Especifique *yes* sólo cuando sea necesario.

Si utiliza la opción `preserve-path` además de `subdir=yes`, ello puede afectar a qué subdirectorios han de procesarse.

Si un subdirectorio es un sistema de archivos montado, éste no se procesará, aunque haya especificado `subdir=yes`.

Nota:

1. Cuando ejecuta el cliente en modalidad interactiva, si utiliza la opción `-subdir=yes`, el valor persiste para todos los mandatos especificados en modalidad interactiva hasta que finalice la modalidad interactiva especificando `Quit`.
2. Si `subdir=yes` se aplica cuando restaura varios archivos, coloque un carácter delimitador de directorios al final de la especificación del archivo de destino. Si se omite el delimitador, el cliente muestra un mensaje indicando que la especificación del archivo de destino no es válida.
3. Se recomienda incluir sólo el valor predeterminado de `subdir` (No) en un archivo de opciones de cliente o un conjunto de opciones de cliente.

Ejemplos**Archivo de opciones:**

```
subdir no
```

Línea de mandatos:

Para restaurar la estructura:

```
/Users/mike/dir1
/Users/mike/dir1/file1
/Users/mike/dir1/dir2
/Users/mike/dir1/dir2/file1
```

especifique alguno de los mandatos siguientes:

```
dsmc rest "/Users/van/dir1/*" /Users/mike/ -su=yes
dsmc rest "/Users/van/dir1/file*" /Users/mike/ -su=yes
dsmc rest "/Users/van/dir1/file1*" /Users/mike/ -su=yes
```

Para restaurar la estructura:

```
/via2/dir1
/via2/dir1/arch1
/via2/dir1/dir2
/via2/dir1/dir2/arch1
```

especifique alguno de los mandatos siguientes:

```
dsmc rest "/via/dir1/*" /via2/ -su=yes
dsmc rest "/via/dir1/arch*" /via2/ -su=yes
dsmc rest "/via/dir1/arch1*" /via2/ -su=yes
```

Esta opción es válida en la línea de mandatos inicial y en modalidad interactiva. Si utiliza esta opción en modalidad interactiva, sólo afectará al mandato con el que se especifica. Cuando se complete la ejecución de ese mandato, el valor se revierte al comienzo de la sesión interactiva. Será el valor del archivo `dsm.opt`, a menos que se haya modificado mediante la línea de mandatos inicial o mediante una opción que el servidor ha forzado.

Información relacionada

“`Preservepath`” en la página 520

Tapeprompt

La opción `tapeprompt` especifica si el cliente de copia de seguridad y archivado debe esperar el montaje de la cinta cuando éste sea necesario en un proceso de copia de seguridad, archivado, restauración o recuperación, o si se debe preguntar al usuario.

En la GUI del cliente de copia de seguridad y archivado, el cuadro de diálogo Montaje de medio puede visualizar el valor Información no disponible en los campos Dispositivo y Etiqueta de volumen si se realiza una operación de restauración o recuperación estándar (también conocida como clásica). Este valor significa que la información sólo está disponible para operaciones de restauración o recuperación sin consulta; no en caso de una operación de restauración o recuperación estándar. El campo **Dispositivo** muestra el nombre del dispositivo en el que debe montarse el medio para procesar un objeto. El campo **Etiqueta de volumen** muestra el nombre del volumen necesario para procesar un objeto.

No se producirá ninguna solicitud de cinta durante una operación planificada, independientemente del valor especificado en la opción tapeprompt.

La opción tapeprompt puede utilizarse con los mandatos siguientes:

- **archive**
- **delete archive**
- **delete backup**
- **incremental**
- **restore**
- **retrieve**
- **selective**

Nota: El servidor también puede definir esta opción.

Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Establezca esta opción en el archivo de opciones de usuario del cliente (dsm.opt). Puede establecer esta opción en el separador **General**, en la casilla de verificación **Preguntar antes de montar cintas** del Editor de preferencias.

Sintaxis



Parámetros

No No se preguntará al usuario. El servidor espera a que la cinta apropiada esté montada. Éste es el valor predeterminado.

Nota: En el caso de las aplicaciones API, permite realizar copias de seguridad directamente en cinta.

Yes

Se solicita al usuario el montaje de la cinta cuando éste es necesario en una operación de copia de seguridad, archivado, restauración o recuperación. Al recibir el mensaje de solicitud, el usuario tiene la opción de esperar a que la cinta apropiada se monte, esperar siempre a que se monte una cinta, omitir un objeto determinado, omitir todos los objetos de una sola cinta, omitir todos los objetos de todas las cintas o cancelar toda la operación.

Ejemplos

Archivo de opciones:

tapeprompt yes

Línea de mandatos:

-tapep=yes

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Tcpadminport

Utilice la opción `tcpadminport` para especificar un número de puerto TCP/IP por separado en el que el servidor está a la espera de las peticiones de sesiones de cliente de administración, lo que permite establecer sesiones de administración seguras dentro de una red privada.

El valor `tcpadminport` del cliente depende de cómo se hayan configurado las opciones `tcpadminport` y `adminonclientport` del servidor de IBM Spectrum Protect. El servidor tiene un valor `tcpadminport` que indica en qué puerto debe estar el servidor a la escucha de las sesiones de administración, y el valor `adminonclientport`, que puede ser `yes` o `no`.

Si no se establece `tcpadminport` en el servidor entonces las sesiones administrativas estarán permitidas en el mismo puerto que las sesiones cliente.

Si `tcpadminport` se establece en el servidor, se permitirán las sesiones administrativas en el puerto que especifique ese valor. En este caso, si `adminonclientport yes` está en vigor, las sesiones administrativas se pueden conectar en el puerto de cliente normal o el puerto especificado por `tcpadminport`. Si `adminonclientport` no está en vigor, las sesiones de administración sólo pueden conectarse en el puerto que especifica `tcpadminport`.

Clientes soportados

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Establezca esta opción en el archivo `dsm.sys` dentro de una sección de servidor. Puede establecer esta opción en el separador **Comunicación**, en el campo **Puerto de administración** del editor de preferencias.

Sintaxis

►►—TCPADMINPort—┐
└─*admin_port_address*—┘

Parámetros

admin_port_address

Especifica el número de puerto del servidor. El valor predeterminado es el valor de la opción `tcppport`.

Ejemplos

Archivo de opciones:
tcpadminport 1502

Tcpbuffsize

La opción `tcpbuffsize` especifica el tamaño del almacenamiento intermedio de comunicaciones TCP/IP interno utilizado para transferir datos entre el nodo cliente y el servidor. Aunque utilice más memoria, un almacenamiento intermedio de mayor tamaño puede mejorar el rendimiento en las comunicaciones.

Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. Puede establecer esta opción en el separador **Comunicación**, en el campo **Tamaño de almacenamiento intermedio** del editor de preferencias.

Sintaxis

►—TCPBuffsize— *size*—►

Parámetros

size

Especifica el tamaño en kilobytes que se desea utilizar para la memoria intermedia de comunicaciones TCP/IP interno. El rango de valores válidos comprende los valores 1 a 512; el valor predeterminado es 32.

Según los valores de comunicación del sistema operativo, es posible que el sistema no acepte todos los valores comprendidos entre 1 y 512.

Ejemplos

Archivo de opciones:
tcpb 32

Línea de mandatos:
-tcpbuffsize=32

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Tcpcadaddress

La opción `tcpcadaddress` especifica una dirección TCP/IP para `dsmcad`. Esta opción no suele ser necesaria. Utilice esta opción sólo si el nodo cliente tiene más de una dirección TCP/IP o bien si TCP/IP no es el método de comunicación predeterminado.

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Establezca esta opción en el archivo `dsm.sys` dentro de una sección de servidor.

Sintaxis

►—TCPCADAddress— *cad_address*—◄

Parámetros

cad_address

Especifica un nombre de dominio TCP/IP de Internet o una dirección IP numérica. Si especifica una dirección IPv6, debe especificarse la opción `commethod V6Tcpip`.

Ejemplos

Archivo de opciones:

```
tcpcada dsmclnt.example.com
```

Línea de mandatos:

```
-tcpcadaddress=192.0.2.0  
-tcpcadaddress=mycompany.example.com  
-tcpcadaddress=2001:0DB8:0:0:0:0:0:0
```

Esta opción sólo es válida en la línea de mandatos inicial del programa `dsmcad`. No es válida con otros módulos `dsm`.

Información relacionada

Consulte el tema “`Commmethod`” en la página 366 para determinar si el nodo cliente tiene más de una dirección TCP/IP o si TCP/IP no es el método de comunicación predeterminado.

Tcpclientaddress

La opción `tcpclientaddress` especifica una dirección TCP/IP si el nodo cliente tiene más de una dirección y quiere que el servidor contacte con una dirección distinta de la utilizada para realizar el primer contacto del servidor.

El servidor utilizará esta dirección cuando comience la operación planificada por petición de servidor.

Utilice esta opción sólo si especifica el parámetro `prompted` con la opción `schedmode`.

Si `sessioninitiation` se ha establecido en `serveronly`, el valor de la opción de cliente `tcpclientaddress` debe ser igual que el valor del servidor `HLAddress`.

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Incluya esta opción en el archivo `dsm.sys` *dentro* de una sección de servidor. Puede establecer esta opción en la ficha **Planificador**, en el campo **Su dirección TCP/IP** del Editor de preferencias.

Sintaxis

►—TCPCLIENTAddress— *—client_address—*►

Parámetros

client_address

Especifica la dirección TCP/IP que se desea que utilice el servidor para establecer contacto con el nodo cliente. Especifique un nombre de dominio Internet TCP/IP o una dirección IP numérica. La dirección IP numérica puede ser una dirección TCP/IPv4 o TCP/IPv6. Sólo puede utilizar direcciones IPv6 si ha especificado la opción `commmethod V6Tcpi`.

Ejemplos

Archivo de opciones:

```
tcpclienta dsmclnt.example.com
o bien
tcpclienta 192.0.2.21
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Tcpclientport

La opción `tcpclientport` especifica un número de puerto TCP/IP para que el servidor contacte con el cliente cuando el servidor comience la operación planificada por petición de servidor.

Utilice esta opción sólo si especifica el parámetro `prompted` con la opción `schedmode`.

Si `sessioninitiation` se ha establecido en `serveronly`, el valor de la opción de cliente `tcpclientport` debe ser igual al valor de la opción de servidor `LLAddress`.

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Establezca esta opción en el archivo `dsm.sys` dentro de una sección de servidor. Puede establecer esta opción en el separador **Planificador**, en el campo **Su puerto TCP/IP** del editor de preferencias.

Sintaxis

►►—TCPCLIENTPort— —*client_port_address*—►►

Parámetros

dirección_puerto_cliente

Especifica la dirección de puerto TCP/IP que se desea que utilice el servidor para establecer contacto con el nodo cliente. El rango de valores es de 1 a 32767; siendo 1501 el valor predeterminado.

Ejemplos

Archivo de opciones:

tcpclientp 1502

Línea de mandatos:

-tcpclientport=1492

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Tcpnodelay

La opción tcpnodelay especifica si el cliente desactiva la demora de enviar paquetes pequeños consecutivos en la red, por transacción.

Sólo deberá cambiar el valor predeterminado yes cuando se den las condiciones siguientes:

- El soporte técnico de IBM le ha indicado que debe cambiar la opción.
- Comprende bien los efectos del algoritmo TCP Nagle en las transmisiones en la red. Si se establece la opción en el valor no se activará el algoritmo Nagle, que retrasa el envío de paquetes consecutivos pequeños.

Clientes soportados

Esta opción es válida para todos los clientes UNIX y Linux.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor. Puede establecer esta opción en el separador

Communication del editor de preferencias. Seleccione **Enviar transacción al servidor inmediatamente**.

Sintaxis

►►—TCPNodeLay—

Yes
No

—►►

Parámetros

No Especifica que el servidor no permite enviar paquetes pequeños consecutivos de forma inmediata por la red. Si establece esta opción en no, el rendimiento puede verse afectado negativamente.

Yes

Especifica que el servidor o el cliente permiten enviar paquetes pequeños consecutivos de forma inmediata por la red. El valor predeterminado es yes.

Ejemplos

Archivo de opciones:

tcpnodelay yes

Línea de mandatos:

No se aplica.

Tcpport

La opción tcpport especifica una dirección de puerto TCP/IP para el servidor de IBM Spectrum Protect. Puede obtenerse esta dirección del administrador.

Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor. Puede establecer esta opción en el separador **Comunicación**, en el campo **Puerto de servidor** del editor de preferencias.

Sintaxis

►—TCPPort— —*port_address*—————►

Parámetros

port_address

Especifica la dirección de puerto TCP/IP que se utiliza para la comunicación con un servidor. El rango de valores es de 1 a 32767, siendo 1500 el valor predeterminado.

Ejemplos

Archivo de opciones:

tcpp 1501

Línea de mandatos:

No se aplica.

Tcpserveraddress

La opción tcpserveraddress especifica la dirección TCP/IP del servidor de IBM Spectrum Protect. Puede obtener esta dirección de servidor solicitándosela al administrador.

Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor. Puede establecer esta opción en el separador **Comunicación**, en el campo **Dirección de servidor** del editor de preferencias.

Si no se especifica esta opción, el cliente intentará establecer contacto con un servidor que se ejecute en el mismo sistema que el cliente de copia de seguridad y archivado.

Sintaxis

►—TCPServeraddress— —server_address—►

Parámetros

server_address

Especifica una dirección TCP/IP de 1 a 64 caracteres para un servidor. Especifique un nombre de dominio TCP/IP o una dirección IP numérica. La dirección IP numérica puede ser una dirección TCP/IP v4 o TCP/IP v6. Sólo puede utilizar direcciones IPv6 si ha especificado la opción commmethod V6TcpiP.

Ejemplos

Archivo de opciones:

tcps dsmchost.example.com

Línea de mandatos:

No se aplica.

Tcpwindow size

Utilice la opción tcpwindow size para especificar el tamaño en kilobytes que desea que tenga la ventana deslizante de TCP/IP para el nodo cliente.

El host que envía los datos no puede enviar más datos hasta que recibe un acuse de recibo y una actualización de la ventana de recepción de TCP. Cada paquete TCP contiene la ventana de recepción de TCP indicada en la conexión. Una ventana más grande permite al remitente continuar enviando datos y puede mejorar el rendimiento de las comunicaciones.

Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor. Puede establecer esta opción en la ficha **Comunicación**, en el campo **Tamaño de ventana** del Editor de preferencias.

Sintaxis

►—TCPWindow size— —window_size—►

Parámetros

window_size

Especifica el tamaño en kilobytes que se desea utilizar para la ventana deslizante de TCP/IP del nodo cliente. El rango de valores comprende los valores 0 a 2048. El valor 0 permite que el cliente utilice el tamaño de ventana de TCP predeterminado del sistema operativo. Los valores del 1 al 2048 indican que el tamaño de ventana oscila entre 1 KB y 2 MB. Si especifica un valor menor que 1, el tamaño de la ventana de TCP utilizará el valor predeterminado 1. Si especifica un valor mayor que 2048, el tamaño de la ventana de TCP utilizará el valor predeterminado 2048.

Para los clientes de copia de seguridad- archivado, el valor predeterminado para este parámetro es 63 KB.

Para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware, el valor predeterminado para este parámetro es 512 KB.

Notas:

- La ventana de TCP actúa como un almacenamiento intermedio en la red. No está relacionada con la opción `tcpbuffsize` ni con los almacenamientos intermedios de envío y recepción asignados en la memoria del cliente o del servidor.
- Un tamaño de ventana mayor que el espacio de almacenamiento intermedio en el adaptador de red podría reducir el rendimiento debido al reenvío de paquetes que se perdieron en el adaptador.
- Según los valores de comunicación del sistema operativo, es posible que el sistema no acepte todos los valores del rango.
- La opción `tcpwindowsize` altera temporalmente los tamaños de ventana de envío y recepción de sesión TCP/IP predeterminados del sistema operativo.

Ejemplos

Archivo de opciones:

```
tcpwindowsize 63
```

Línea de mandatos:

```
-tcpw=63
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Timeformat

La opción `timeformat` especifica el formato en el que desea ver y especificar la hora del sistema.

De manera predeterminada, los clientes de copia de seguridad/archivado y de administración obtienen la información de formato de la definición del entorno regional que esté en funcionamiento en el momento en que se llama al cliente. Consulte la documentación del sistema local para obtener más detalles sobre la configuración del entorno regional.

Nota: La opción `timeformat` no afecta al cliente web. El cliente web utiliza el formato de hora para el entorno regional en el que se está ejecutando el navegador. Si un navegador no se está ejecutando en un entorno regional que admite el cliente, el cliente web utiliza el formato de hora de inglés de Estados Unidos.

Puede utilizar la opción `timeformat` con los mandatos siguientes:

- **delete archive**
- **delete backup**
- **expire**
- **query archive**
- **query backup**
- **query filespace**
- **query image**
- **query nas**
- **restore**
- **restore image**
- **restore nas**
- **retrieve**
- **set event**

Si incluye la opción `timeformat` con un mandato, ésta deberá preceder a las opciones `fromtime`, `pittime` y `totime`.

Cientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Establezca esta opción en el archivo de opciones de usuario del cliente (`dsm.opt`). Puede establecer esta opción en la ficha **Configuración regional**, en el campo **Formato de hora** del Editor de preferencias.

Sintaxis

►►—`TIMEformat`— *—número_formato—*————►►

Parámetros

número_formato

Visualiza la hora en uno de los formatos listados aquí. Seleccione el número que se corresponda con el formato que desee utilizar. Si incluye la opción `timeformat` en un mandato, ésta deberá preceder a las opciones `fromtime`, `pittime` y `totime`.

- 0** Utilice el formato de hora definido para el entorno regional (no se aplica a Mac OS X). Este es el valor predeterminado si el formato que especifica el entorno regional consta de dígitos, caracteres de separación y, si se aplica, la serie AM o PM.
- 1** 23:00:00

Este es el valor predeterminado si el formato que especifica el entorno regional no consta de dígitos, de caracteres de separación ni, si se aplica, de la serie AM o PM.
- 2** 23,00,00
- 3** 23.00.00
- 4** 12:00:00A/P
- 5** A/P 12:00:00

Ejemplos

Archivo de opciones:

timeformat 4

Línea de mandatos:

-time=3

Esta opción es válida en la línea de mandatos inicial y en modalidad interactiva. Si utiliza esta opción en modalidad interactiva, sólo afectará al mandato con el que se especifica. Cuando se complete la ejecución de ese mandato, el valor se revierte al comienzo de la sesión interactiva. Será el valor del archivo dsm.opt, a menos que se haya modificado mediante la línea de mandatos inicial o mediante una opción que el servidor ha forzado.

Consideraciones adicionales para especificar los formatos de fecha y hora

El formato de fecha y hora que especifique con esta opción debe utilizarse en las opciones que acepten una entrada de fecha y hora. Por ejemplo: totime, fromtime, todate, fromdate y pittime.

Por ejemplo, si especifica la opción timeformat como TIMEFORMAT 4, el valor que proporciona en la opción fromtime o totime debe especificarse como una hora, por ejemplo, 12:24:00pm. Si especifica 13:24:00, no será válido porque TIMEFORMAT 4 necesita un entero de hora menor o igual a 12. Si desea especificar valores de hasta 24 horas en una opción y utilizar comas como separadores, debe especificar TIMEFORMAT 2.

Configuración de los formatos de fecha y hora en el archivo de configuración del entorno regional del sistema

Puede especificar formatos de fecha y hora configurándolos en el archivo de entorno regional del sistema. Si especifica formatos de fecha y hora en el archivo del entorno regional, deben definirse utilizando un subconjunto de especificadores de formato de producción de números soportados por la función strftime() del lenguaje C. Puede utilizar los siguientes especificadores para establecer los formatos de fecha y hora en los valores de configuración del entorno regional.

Especificadores de fecha

- %Y - el año, en cuatro dígitos. Por ejemplo, 2011.
- %y - el año, solo con los dos últimos dígitos. Por ejemplo, 11; no 2011.
- %m - el mes, como un número decimal (1-12).
- %d - el día del mes (1-31).

En los especificadores de fecha, sólo puede especificar un especificador de año. No especifique %Y ni %y. El modificador E (un E en mayúsculas) puede preceder los especificadores de fecha para crear la forma alternativa del entorno local para el año, mes o día. Si no existe ningún formato alternativo, el modificador E se ignora. Separe los especificadores con un carácter ASCII de 7 bits. Los separadores más utilizados son los dos puntos (:), las comas (,), los puntos (.), (.), guiones (-) o barras diagonales (/). No utilice caracteres de varios bytes como separadores.

Especificadores de hora

- %H - la hora, en formato de 24 horas (00-23).
- %I - la hora, en formato de 12 horas (00-12).

- %M - minutos después de la hora (00-59).
- %S - segundos después del minuto (00-59)
- %p - añade el indicador AM (antes de mediodía) o PM (después de mediodía).

En los especificadores de hora, sólo puede especificar un especificador de hora. No especifique %I y %H a la vez.

El modificador O (una O mayúscula) puede ir antes que los especificadores de hora para producir el formato alternativo del entorno regional para la hora, los minutos o los segundos. El modificador O no puede ir antes que el especificador %p. Separe los especificadores con un carácter ASCII de 7 bits. Los separadores más utilizados son los dos puntos (:), las comas (,) o los puntos (.). No utilice caracteres de varios bytes como separadores. No especifique un separador entre el especificador %p y el separador que le precede o le sigue.

Ejemplos de formato de hora, configurados en los valores de entorno regional

Para establecer un formato de hora en particular, edite el archivo de configuración del entorno regional que utiliza y modifique la línea `t_fmt` en función de sus necesidades. Sea cual sea el formato de hora seleccionado, se aplica tanto a la salida como a la entrada. Una vez editado el archivo de configuración del entorno regional, debe ejecutarse el mandato **localedef** para crear el archivo del entorno regional final.

Tabla 77. Valores del formato de hora de ejemplo en la configuración del entorno regional (línea `t_fmt`)

Ejemplo	Resultado
"%H:%M:%S"	Muestra la hora en el formato <i>hh:mm:ss</i> , siendo valores válidos para <i>hh</i> el rango de 0 a 23.
"%H,%M,%S"	Muestra la hora en el formato <i>hh,mm,ss</i> , siendo valores válidos para <i>hh</i> el rango de 0 a 23.
"%I,%M,13p"	Muestra la hora en el formato <i>hh,mm,ssA/P</i> , donde <i>hh</i> puede estar entre 1 y 12, y donde <i>A/P</i> es la abreviatura local de antemeridiano (AM en inglés) o postmeridiano (PM en inglés).

Ejemplos de formato de fecha, configurados en los valores de entorno regional

Para establecer un formato de fecha en particular, edite el archivo de configuración y modifique la línea `d_fmt` en función de sus necesidades. Sea cual sea el formato de fecha seleccionado, se aplica tanto a la salida como a la entrada.

Tabla 78. Valores del formato de fecha de ejemplo en la configuración del entorno regional (línea `d_fmt`)

Ejemplo	Resultado
"%m/%d/%y"	Visualiza la fecha con el formato MM/DD/AA.
"%d.%m.%Y"	Visualiza la fecha con el formato DD.MM.AAAA.

Toc

Utilice la opción `toc` con el mandato **backup nas** o la opción `include.fs.nas` para especificar si el cliente de copia de seguridad y archivado ha de guardar la información de la tabla de contenido (TOC) para cada copia de seguridad del sistema de archivos.

Tenga en cuenta las consideraciones siguientes cuando decida si desea guardar la información de TOC:

- Si guarda la información de la TOC, podrá utilizar el mandato de servidor `QUERY TOC` para determinar el contenido de la copia de seguridad de un sistema de archivos junto con el mandato de servidor `RESTORE NODE` para restaurar archivos individuales o árboles de directorios.
- También puede utilizar el cliente web para examinar todo el árbol del sistema de archivos y seleccionar los archivos y directorios que han de restaurarse.
- Para crear una TOC, debe definir el atributo `TOCDESTINATION` en el grupo de copias de seguridad para la clase de gestión a la que se vincula esta imagen de copia de seguridad. Tenga en cuenta que, para crear una tabla de contenido, se necesitan un proceso adicional, recursos de red, espacio de agrupación de almacenamiento y, posiblemente, un punto de montaje durante la operación de copia de seguridad.
- Si no guarda la información de las TOC, podrá restaurar archivos individuales o árboles de directorios utilizando el mandato de servidor `RESTORE NODE`, siempre que conozca el nombre calificado al completo de cada archivo o directorio y sepa en qué imagen se ha realizado la copia de seguridad de ese objeto.

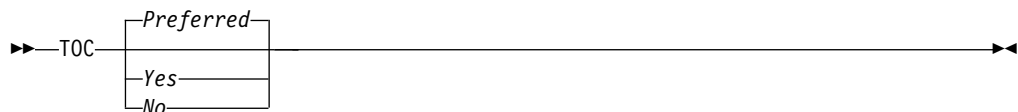
Clientes soportados

Esta opción solo es válida para los clientes AIX y Solaris. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Especifique la sentencia `include.fs.nas` que contiene el valor `toc` en el archivo `dsm.sys` dentro de una stanza de servidor.

Sintaxis



Parámetros

Yes

Especifica que el cliente ha de guardar la información de las TOC durante la realización de una copia de seguridad de imagen del sistema de archivos NAS. Sin embargo, la copia de seguridad no se realizará correctamente si se produce un error durante la creación de la TOC.

No Especifica que el cliente no ha de guardar la información de las TOC durante la realización de una copia de seguridad de imagen del sistema de archivos NAS.

Preferred

Especifica que el cliente ha de guardar la información de las TOC durante la realización de una copia de seguridad de imagen del sistema de archivos NAS. La copia de seguridad no falla si se produce un error durante la creación de la TOC. Éste es el valor predeterminado.

Nota: Si la opción `mode` se ha establecido en `differential` y establece la opción `toc` en `preferred` o `yes`, pero la última imagen completa no dispone de una tabla de contenido, el cliente realizará una copia de seguridad de imágenes completa y creará una tabla de contenido.

Ejemplos

Archivo de opciones:

```
include.fs.nas netappsj/vol/vol0 homemgmtclass toc=yes
```

Línea de mandatos:

```
backup nas -nasnodename=netappsj /vol/vol0 -toc=yes
```

Todate

Utilice la opción `todate` con la opción `totime` para especificar una fecha y una hora finales hasta las que desea buscar copias de seguridad o copias archivadas durante una operación de restauración, recuperación o consulta.

Utilice las opciones `todate` y `totime` con las opciones `fromtime` y `fromdate` para solicitar una lista de copias de seguridad o archivadas realizadas durante un período de tiempo determinado. Por ejemplo, puede solicitarse una lista de archivos cuya copia de seguridad se realizó entre las 6:00 del 1 de julio de 2002 y las 23:59 del 30 de julio de 2002.

La opción `todate` puede utilizarse con los mandatos siguientes:

- **delete backup**
- **query archive**
- **query backup**
- **restore**
- **restore group**
- **retrieve**

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Sintaxis

►► —TODate =— —date— ◀◀

Parámetros

date

Especifica una fecha final. Escriba la fecha en el formato seleccionado con la opción `dateformat`.

Si se incluye la opción `dateformat` con un mandato, ésta debe anteponerse a las opciones `fromdate`, `pitdate` y `todate`.

Ejemplos

Línea de mandatos:

```
dsmc restore "/Users/agordon/Documents/*" -todate=12/11/2003
```

Línea de mandatos:

```
dsmc restore "/home/user1/*" -todate=12/11/2003
```

Totime

Utilice la opción `totime` con la opción `todate` para especificar una fecha y una hora finales hasta las que desea buscar copias de seguridad o copias archivadas durante una operación de restauración, recuperación o consulta. El cliente de copia de seguridad y archivado pasa por alto esta opción si no especifica la opción `todate`.

Utilice las opciones `totime` y `todate` con las opciones `fromtime` y `fromdate` para solicitar una lista de archivos cuyas copias de seguridad se realizaron durante un período de tiempo determinado. Por ejemplo, puede solicitarse una lista de archivos cuya copia de seguridad se realizó entre las 6:00 del 1 de julio de 2003 y las 23:59 del 30 de julio de 2003.

La opción `totime` puede utilizarse con los mandatos siguientes:

- **delete backup**
- **query archive**
- **query backup**
- **restore**
- **restore group**
- **retrieve**

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Sintaxis

►►—TOTime =— —hora—————►►

Parámetros

hora

Especifica una hora final. Si no se especifica una hora, se toma el valor predeterminado 23:59:59. Especifique la hora en el formato seleccionado con la opción `timeformat`.

Si incluye la opción `timeformat` en un mandato, ésta deberá preceder a las opciones `fromtime`, `pittime` y `totime`.

Ejemplos

Línea de mandatos:

```
dsmc restore "/Users/van/Documents/myfiles/*" -todate=09/17/2003  
-totime=23:00:00
```

Línea de mandatos:

```
dsmc restore "/home/user1/*" -todate=09/17/2003 -totime=23:00:00
```

Txnbytelimit

La opción `txnbytelimit` especifica el número de kilobytes que el programa de cliente guarda en el almacenamiento intermedio antes de enviar una transacción al servidor.

Una *transacción* es la unidad de trabajo que se ha intercambiado entre el cliente y el servidor. Una transacción puede contener más de un archivo o directorio, llamado *grupo de transacción*.

Puede controlar la cantidad de datos enviados entre el cliente y el servidor antes de que el servidor valide los datos y cambios en la base de datos del servidor, utilizando la opción `txnbytelimit`. Controlando la cantidad de datos enviados, cambia la velocidad del cliente para realizar las transacciones. La cantidad de datos enviados se utiliza cuando los archivos se procesan por lotes durante una copia de seguridad o cuando se reciben archivos del servidor durante un procedimiento de restauración.

Una vez que `txngroupmax` ha alcanzado este número, el cliente envía los archivos al servidor, aunque el límite de bytes de transacción no se ha alcanzado.

Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. Puede establecer esta opción en el separador **General**, en el campo **Tamaño de almacenamiento intermedio de transacción** en el editor de preferencias.

Sintaxis

►►—TXNBytelimit— *number* —————◀◀

Parámetros

number

Especifica el número de kilobytes que el programa cliente envía al servidor antes de enviar una transacción. El rango de valores va de 300 a 34359738368 (32 GB). El valor predeterminado es 25600 KB. Se puede especificar el número como número entero o como número entero con uno de los siguientes cualificadores de unidad:

K o k (kilobytes)
M o m (megabytes)
G o g (gigabytes)

Si no se especifica la unidad del cualificador, el número entero está en kilobytes.

Restricción: La opción `txnbytelimit` no admite números decimales, y sólo se permiten letras de una unidad. Por ejemplo: K, M o G.

Ejemplos

Archivo de opciones:

```
txnb 25600  
  
txnb 2097152  
  
txnb 2097152k  
  
txnb 2048m  
  
txnb 2g  
  
txnb 32G
```

Línea de mandatos:

```
-txnb=25600  
  
-txnb=16G
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Type

Utilice la opción **type** con el mandato **query node** para especificar el tipo de nodo que ha de consultarse. Utilice esta opción con el mandato **set event** para activar, retener o liberar.

Clientes soportados

Esta opción también es válida para el mandato **set password** con el tipo TSM en clientes AIX.

Esta opción solo es válida para los clientes AIX y Solaris. La API de IBM Spectrum Protect no admite esta opción.

Sintaxis



Parámetros

nas

Especifica todos los nodos NAS inscritos en el servidor.

servidor

Especifica nodos cliente que se encuentran en otros servidores de IBM Spectrum Protect.

client

Especifica nodos cliente que son clientes de copia de seguridad/archivado.

Ejemplos

Línea de mandatos:

```
query node -type=nas
```

Updatectime

Utilice la opción `updatectime` para comprobar el atributo para cambio de hora (`ctime`) durante una operación de copia de seguridad o archivado.

Utilice esta opción con los mandatos **incremental**, **selective** o **archive**.

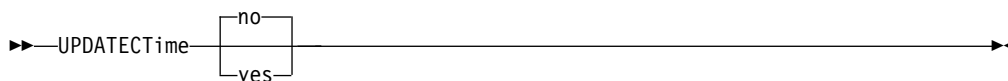
Clientes soportados

Esta opción es válida para clientes de AIX y Linux sólo en sistemas de archivos GPFS. El servidor también puede definir esta opción.

Archivo de opciones

Coloque esta opción en el archivo de opciones de usuario del cliente (`dsm.opt`).

Sintaxis



Parámetros

no El cliente de copia de seguridad y archivado no comprueba el cambio de hora (atributo `ctime`) durante una operación de copia de seguridad o archivado. Este es el valor predeterminado.

yes

El cliente de copia de seguridad y archivado comprueba el cambio de hora (atributo `ctime`) durante una operación de copia de seguridad o archivado. Si el atributo `ctime` ha cambiado desde la última operación de copia de seguridad o archivado, el atributo `ctime` se actualizará en el servidor de IBM Spectrum Protect. No se hace copia de seguridad del objeto ni se archiva. El cliente comprueba los archivos y directorios.

Ejemplos

Archivo de opciones:

```
updatect yes
```

Línea de mandatos:

```
dsmc incr /proj/gpfs/test/ -updatectime=yes
```

Useexistingbase

La opción `useexistingbase` se utiliza cuando se hacen copias de seguridad de instantáneas que se encuentran en volúmenes de archivador NetApp. La opción `useexistingbase` indica que la instantánea más reciente que existe en el volumen del que se está realizando una copia de seguridad, debe utilizarse como la instantánea base durante una operación de copia de seguridad diferencial de instantáneas.

Si no se especifica esta opción, se crea una nueva instantánea en el volumen del que se está realizando una copia de seguridad. Debido a que los volúmenes de archivador de destino son de sólo lectura, debe especificarse `useexistingbase` cuando se realizan copias de seguridad diferenciales de instantáneas de volúmenes de archivador de destino. Si no se especifica `useexistingbase`, las copias de

seguridad diferenciales de instantáneas de un volumen de archivador de destino muestran una anomalía porque la instantánea nueva no puede crearse en el volumen de sólo lectura.

Cuando realice una copia de seguridad de volúmenes de archivador de destino, utilice las opciones `useexistingbase` y `diffsnapshot=latest` para asegurarse de utilizar la base más reciente y las instantáneas de diferencial más recientes durante la copia de seguridad de volumen.

Clientes soportados

Esta opción puede utilizarse con clientes Linux x86_64 soportados.

Archivo de opciones

Esta opción sólo es válida en la línea de mandatos.

Sintaxis

►►—USEEXISTINGBase—◄◄

Parámetros

Esta opción no tiene parámetros

Ejemplos

Archivo de opciones:

No se aplica.

Línea de mandatos:

```
dsmc incr \\DRFiler\UserDataVol_Mirror_Share -snapdiff  
-useexistingbase -basenameshotname="nightly.?"
```

Información relacionada

Basesnapshotname

Usereplicationfailover

La opción `usereplicationfailover` especifica si se produce la migración tras error automatizada del cliente de un nodo cliente.

Utilice esta opción para permitir que un nodo cliente para migración tras error o para impedir que migre tras error en el servidor secundario. Esta opción altera temporalmente la configuración que se proporciona mediante los valores del administrador del servidor de IBM Spectrum Protect en el servidor primario.

Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Coloque esta opción dentro de una stanza del servidor en el archivo `dsm.sys`.

Sintaxis



Parámetros

Yes

Especifica que desea que el cliente migre tras error automáticamente al servidor secundario si el servidor primario no está disponible. El cliente utiliza la configuración proporcionada por el servidor primario para conectarse al servidor secundario. Este es el valor predeterminado.

No Especifica que el cliente no migra tras error automáticamente al servidor secundario.

Ejemplos

Archivo de opciones:

USEREPLICATIONFailover no

Línea de mandatos:

No se aplica.

Conceptos relacionados:

“Configuración y uso de la migración tras error automática del cliente” en la página 94

Tareas relacionadas:

“Configuración del cliente de migración automática tras error” en la página 98

Usuarios (obsoleto)

Esta opción está obsoleta.

Para obtener información sobre cómo restringir el acceso de los usuarios que no son administradores al cliente de copia de seguridad y archivado mediante un grupo de usuarios, consulte el apartado “Restricción del acceso a IBM Spectrum Protect a un grupo de usuarios” en la página 52.

V2archive

Utilice la opción **v2archive** con el mandato **archive** para realizar el archivado sólo de los archivos en el servidor.

El cliente de copia de seguridad y archivado no procesará los directorios que existen en la ruta de la especificación de archivo de origen.

Esta opción difiere de la opción **filesonly** en que la opción **filesonly** archiva los directorios existentes en la vía de acceso de la especificación de archivos origen.

Las opciones **v2archive** y **dirsonly** se excluyen mutuamente, y se visualizará un mensaje de error si utiliza ambas opciones en el mismo mandato **archive**.

Si utiliza esta opción también debe tener en cuenta las consideraciones siguientes:

- Puede experimentar problemas de rendimiento al recuperar grandes cantidades de datos archivados con esta opción.

- Plantéese utilizar esta opción únicamente si le preocupa el rendimiento de la función de caducidad en un servidor que ya contenga cantidades ingentes de datos archivados.
- Si hay varios archivos con el mismo nombre para la opción `v2archive`, los archivos se archivan varias veces, con su estructura de directorios. La opción `v2archive` sólo archiva los archivos.

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Sintaxis

►►—V2archive—◄◄

Parámetros

No hay parámetros para esta opción.

Ejemplos

Este mandato:

```
dsmc archive "/Users/user2/Documents/*" -v2archive -su=y.
```

Realiza el archivado de los archivos siguientes:

```
/Users/user2/Documents/file1
/Users/user2/Documents/file2
/Users/user2/Documents/file3
/Users/user2/Documents/dir2/file4
/Users/user2/Documents/dir2/file5
```

Nota: El cliente no archiva `/Users/user2/Documents` ni `/Users/user2/Documents/dir2`.

Este mandato:

```
dsmc archive "/home/relx/dir1/*" -v2archive -su=y.
```

Realiza el archivado de los archivos siguientes:

```
/home/relx/dir1/archivo1
/home/relx/dir1/archivo2
/home/relx/dir1/archivo3
/home/relx/dir1/dir2/archivo4
/home/relx/dir1/dir2/archivo5
```

Nota: El cliente no archiva `/home/relx/dir1` ni `/home/relx/dir1/dir2`.

Verbose

La opción `verbose` especifica que se desea visualizar información detallada de proceso en la pantalla. Éste es el valor predeterminado.

Cuando se ejecutan los mandatos **incremental**, **selective** o **archive**, se visualiza información acerca de cada archivo del que se hace copia de seguridad. Utilice la opción `quiet` si no desea visualizar esta información.

El siguiente comportamiento se aplica cuando se utilizan las opciones `verbose` y `quiet`.

- Si el servidor especifica la opción **quiet** o la opción **verbose** en el conjunto de opciones del cliente del servidor, los valores del servidor modificarán temporalmente los valores del cliente, aunque **force** se haya establecido en *no* en el servidor.
- Si especifica **quiet** en el archivo `dsm.opt` y especifica **-verbose** en la línea de mandatos, prevalecerá **-verbose**.
- Si especifica tanto **-quiet** como **-verbose** en el mismo mandato, prevalecerá la última opción detectada durante el proceso de las opciones. Si especifica **-quiet -verbose**, prevalecerá **-verbose**. Si especifica **-verbose -quiet**, prevalecerá **-quiet**.

La información aparece en la pantalla en la ventana de estado del planificador. Esta opción sólo se aplica si se está ejecutando el planificador y el cliente está llevando a cabo un trabajo planificado.

Clientes soportados

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Establezca esta opción en el archivo de opciones de usuario del cliente (`dsm.opt`). Puede establecer esta opción en la ficha **Línea de mandatos**, en el recuadro de selección **No mostrar información de proceso en pantalla** del Editor de preferencias.

Sintaxis

►►—VErbose—◄◄

Parámetros

No hay parámetros para esta opción.

Ejemplos

Archivo de opciones:
verbose

Línea de mandatos:
-verbose

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Verifyimage

Utilice la opción **verifyimage** con el mandato **restore image** para especificar que desea activar la detección de los sectores defectuosos en el volumen de destino.

Si se detectan sectores defectuosos en el volumen de destino, el cliente de copia de seguridad y archivado emite un mensaje de aviso en la consola y en el registro de errores.

Clientes soportados

Esta opción solo es válida para clientes de AIX, Oracle Solaris y todos los de Linux. La API de IBM Spectrum Protect no admite esta opción.

Sintaxis

►►—VERIFYImage—————►►

Parámetros

No hay parámetros para esta opción.

Ejemplos

Línea de mandatos:

```
dsmc restore image /usr -verifyimage
```

Virtualfsname

Utilice la opción **virtualfsname** con el mandato **backup group** para especificar el nombre del espacio de archivos virtual para el grupo en el que desea realizar la operación. El valor de la opción **virtualfsname** no puede ser igual a un nombre de espacio de archivos existente.

Clientes soportados

Esta opción es válida para todos los clientes UNIX y Linux, a excepción de Mac OS X.

Sintaxis

►►—VIRTUALFsname =— —fsname—————►►

Parámetros

nombre_espacio_archivos

Especifica el nombre del contenedor del grupo en el que desea realizar la operación.

Ejemplos

Línea de mandatos:

```
backup group -filelist=/Users/van/Documents/filelist1 -groupname=group1  
-virtualfsname=/virtfs -mode=full  
backup group -filelist=/home/dir1/filelist1 -groupname=group1  
-virtualfsname=/virtfs -mode=full
```

Virtualmountpoint

La opción **virtualmountpoint** define un punto de montaje virtual para un sistema de archivos, si desea que se realice una copia de seguridad de los archivos que empiezan en un directorio determinado de dicho sistema de archivos.

La utilización de la opción **virtualmountpoint** para identificar un directorio dentro de un sistema de archivos proporciona una vía de acceso directa a los archivos de

los que se quiere efectuar copia de seguridad, ahorrando tiempo de proceso. Es más eficaz definir un punto de montaje virtual en un sistema de archivos que definir dicho sistema de archivos utilizando la opción `domain` y después utilizar la opción `exclude` de la lista de opciones de inclusión/exclusión para excluir los archivos de los que no desea realizar una copia de seguridad.

Utilice la opción `virtualmountpoint` para definir puntos de montaje virtuales en varios sistemas de archivos, para sistemas de archivos locales y remotos y para definir varios puntos de montaje virtuales en el mismo espacio de archivos. Los puntos de montaje virtual no pueden utilizarse en un sistema de archivos gestionado por el montador automático.

Puede utilizar la opción `virtualmountpoint` para hacer copias de seguridad de los sistemas de archivos no soportados, con ciertas limitaciones. Para obtener información sobre cómo utilizar `virtualmountpoint` con sistemas de archivos no soportados, consulte "Soporte para sistemas de archivos y ACL" en la página 162.

Nota: si el directorio que desea especificar como punto de montaje virtual es un vínculo simbólico, establezca la opción `followsymbolic` en *Yes*. Si esta opción se establece en *no* (valor predeterminado), no se le permitirá utilizar un vínculo simbólico como punto de montaje virtual. Asimismo, si hace una copia de seguridad del sistema de archivos, agrega un punto de montaje virtual, y después efectúa otra copia de seguridad incremental en el sistema de archivos, los archivos y directorios del directorio del punto de montaje virtual caducarán, porque se incluyen de forma lógica en el directorio del punto de montaje virtual y no en el sistema de archivos.

Después de definir un punto de montaje virtual, podrá definir la vía de acceso y nombre de directorio con la opción `domain` en el archivo de opciones del cliente predeterminado o en el mandato **incremental** para incluirlo en los servicios de copia de seguridad incremental. Cuando realice una operación de copia de seguridad o archivado con la opción `virtualmountpoint`, el mandato **query filesystem** mostrará el punto de montaje virtual en su respuesta junto con otros sistemas de archivos. Generalmente, los directorios que se definen como puntos de montaje virtuales se tratan como sistemas de archivos reales y requieren que se especifique la opción `virtualmountpoint` en el archivo `dsm.sys` para restaurar o recuperar los datos.

Nota: cuando se especifica una opción `virtualmountpoint`, la vía de acceso que se especifica se agrega al dominio de copia de seguridad predeterminado (`domain all-local`). La vía de acceso `virtualmountpoint` siempre se considera un "punto de montaje" local independientemente del tipo de sistema de archivos real al que haga referencia.

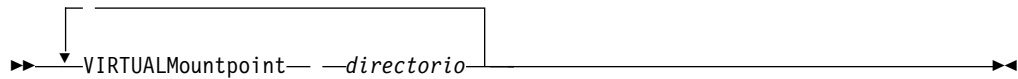
Clientes soportados

Esta opción es válida para todos los clientes UNIX, a excepción de Mac OS X. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor.

Sintaxis



Parámetros

directorio

Especifica la vía de acceso y el nombre del directorio que desea utilizar como punto de montaje virtual para un sistema de archivos. No puede utilizar caracteres comodín en la vía de acceso ni en el nombre de directorio.

Defina solo un punto de montaje virtual con cada opción `virtualmountpoint` que incluya en el archivo de opciones del sistema cliente. Utilice la opción `virtualmountpoint` tantas veces como sea necesario para definir todos los puntos de montaje virtuales que desee utilizar.

Ejemplos

Archivo de opciones:

```
virtualmountpoint /afs/xyzcorp.com/home/ellen  
virtualmountpoint /afs/xyzcorp.com/home/ellen/test/data
```

Línea de mandatos:

No se aplica.

Virtualnodename

La opción `virtualnodename` especifica el nombre de nodo de la estación de trabajo cuando desea restaurar o recuperar archivos en una estación de trabajo diferente.

Cuando utilice la opción `virtualnodename` en el archivo de opciones del cliente o con un mandato:

- Debe especificar el nombre que ha especificado con la opción `nodename` en el archivo de opciones del sistema cliente (`dsm.sys`). Este nombre debe ser distinto del nombre que devuelve el mandato **hostname** en la estación de trabajo.
- El cliente solicita la contraseña asignada al nodo que se especifique, en caso de que se requiera una contraseña (incluso cuando la opción `passwordaccess` se ha establecido en `generate`). Si se escribe la contraseña correcta, se tendrá acceso a todas las copias de seguridad y copias archivadas que se originaron en el nodo especificado.

Al conectarse a un servidor, el cliente debe identificarse ante el servidor. Esta identificación de conexión se determina de los modos siguientes:

- Si no se especifican las opciones `nodename` y `virtualnodename` o si no se especifica un nombre de nodo virtual en la línea de mandatos, el identificador de conexión predeterminado será el nombre que devolverá el mandato **hostname**.
- Si se especifica la opción `nodename`, el nombre que se especifique con la opción `nodename` modificará temporalmente el nombre que devuelve el mandato **hostname**.
- Si se especifica la opción `virtualnodename` o se especifica un nombre de nodo virtual en la línea de mandatos, este nombre no podrá ser igual al nombre que devuelve el mandato **hostname**.

Clientes soportados

Esta opción es válida para todos los clientes.

Archivo de opciones

Establezca esta opción en el archivo de opciones de usuario del cliente (dsm.opt).

Sintaxis

►►—VIRTUALNodename— —nodename—►►

Parámetros

nodename

Especifica un nombre de 1 a 64 caracteres que identifica el nodo para el que se desea solicitar servicios de IBM Spectrum Protect. No hay valor predeterminado.

Ejemplos

Archivo de opciones:

virtualnodename pilar

Línea de mandatos:

-virtualn=marisa

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

Vmbackdir

La opción `vmbackdir` especifica la ubicación del disco temporal en el que el cliente guarda los archivos de control que se han creado durante las operaciones de copia de seguridad y restauración de las máquinas virtuales VMware e Hyper-V de Microsoft.

Clientes soportados



Las operaciones de máquina virtual solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments.

Cuando un cliente en un nodo transportador de datos inicia una copia de seguridad de máquina virtual completa, el cliente crea los metadatos en los archivos asociados con la copia de seguridad de máquina virtual y sus datos. Los archivos que contienen los metadatos se conocen como *archivos de control*.

Durante las operaciones de copia de seguridad de VM completas, los metadatos se guardan en un disco en el nodo transportador de datos hasta que la copia de seguridad termina y tanto los datos de la máquina virtual como los archivos de control se guardan en el almacenamiento del servidor. Durante una operación de restauración de máquina virtual completa, los archivos de control se copian desde el servidor y se guardan temporalmente en el disco del transportador de datos, donde se utilizan para restaurar la máquina virtual y sus datos. Cuando termina

una copia de seguridad o una operación de restauración, los archivos de control ya no son necesarios y el cliente los suprime desde la ubicación de disco temporal.

El directorio especificado por esta opción debe encontrarse en una unidad con suficiente espacio libre para contener la información de control de una copia de seguridad de máquina virtual completa.

Esta opción es válida para clientes Linux instalados en un servidor de copia de seguridad vStorage.

Archivo de opciones

Establezca esta opción en el archivo de opciones del cliente, en la línea de mandatos como una opción para los mandatos **backup vm** o **restore vm**.

Sintaxis

►►—VBACKDir—directorio—►►

Parámetros

directorio

Especifica la vía de acceso en la que se guardan los archivos de control en el servidor de copia de seguridad.

El valor predeterminado es /tmp/tsmvmbbackup/fullvm/

Ejemplos

Archivo de opciones:

```
VBACKD /tmp/tsmvmbbackup/
```

Línea de mandatos:

```
dsmc backup vm -VBACKUPT=fullvm -VBACKD=/home/vmware/control_files
```

```
dsmc restore vm -VBACKUPT=fullvm -VBACKD=/home/mine/bkup_ctrl
```

Vmbakupmailboxhistory

La opción `vmbakupmailboxhistory` especifica si el historial del buzón se debe cargar automáticamente con la copia de seguridad de la máquina virtual (VM) si se detecta IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server en una VM.

Clientes soportados

Esta opción es válida para los clientes que actúan como nodos de movimiento de datos para copias de seguridad de huésped VMware.



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor.

Sintaxis



Parámetros

Yes

El historial del buzón se carga automáticamente con la copia de seguridad de la VM si se detecta IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server en una VM.

No El historial del buzón no se carga automáticamente con la copia de seguridad de la VM.

Ejemplos

Archivo de opciones:

```
vmbakupmailboxhistory yes
```

Vmbackuptype

Utilice la opción `vmbackuptype` con el mandato **backup VM** o **restore VM** para especificar el tipo de copia de seguridad de máquina virtual para completar. También puede utilizar esta opción en mandatos **query VM** para filtrar los resultados de la consulta e incluir solo máquinas virtuales cuya copia de seguridad haya sido realizada por un tipo de copia de seguridad específico. Para obtener ejemplos, consulte la descripción del mandato **query VM**.



Las operaciones de máquina virtual solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments.

Puede especificar una copia de seguridad completa de la máquina virtual VMware.

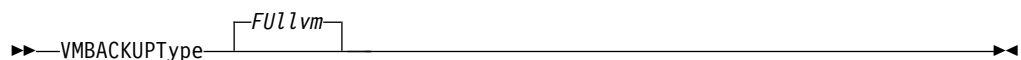
Clientes soportados

Esta opción es válida en clientes Linux instalados en un servidor de copia de seguridad vStorage. El servidor también puede definir esta opción.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor.

Sintaxis



Parámetros

Fullvm

Especifique este valor para ejecutar una copia de seguridad de la máquina

virtual completa tradicional de una máquina virtual VMware. Este es el tipo de copia de seguridad predeterminada para clientes Linux.

Ejemplos

Archivo de opciones:

```
VMBACKUPT full
```

Línea de mandatos:

```
dsmc backup vm vm1 -VMBACKUPT=full -vmchost=virtctr  
-vmcuser=virtctr_admin -vmcpw=xxxxx
```

Realiza una copia de seguridad de máquina virtual completa de vm1.example.com utilizando la máquina de VMware VirtualCenter virtctr.example.com, en el servidor de IBM Spectrum Protect, utilizando el nombre de máquina vm1.

Vmchost

Utilice la opción `vmchost` con los mandatos **backup VM**, **restore VM** o **query VM** para especificar el nombre de host de VMware VirtualCenter o del servidor ESX que desea restaurar, consultar o del que desea hacer una copia de seguridad.

Utilice VirtualCenter si está disponible. Si no puede utilizar un servidor de VirtualCenter y necesita realizar copias de seguridad de varios sistemas de archivos en varios servidores de ESX, no especifique esta opción; en lugar de ello, especifique la opción con el mandato para que pueda cambiarse en función de cada servidor de ESX.



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Clientes soportados

Este mandato es válido para los clientes que están configurados para realizar una copia de seguridad consolidada de una máquina virtual VMware. El servidor también puede definir esta opción.

Archivo de opciones

Coloque esta opción en el archivo de opciones del cliente (`dsm.opt`), en el archivo de opciones del sistema del cliente (`dsm.sys`) o en la línea de mandatos.

Sintaxis

►►—VMCHost— —*hostname*—►►

Parámetros

nombre_host

Especifica el nombre de host de VMware VirtualCenter o del servidor ESX que desea restaurar, consultar o del que desea hacer una copia de seguridad.

Ejemplos

Archivo de opciones:

```
VMCH vcenter.storage.usca.example.com
```

Línea de mandatos:

```
-VMCH=esx1.storage.usca.example.com
```

Vmcpw

Utilice la opción `vmcpw` con los mandatos **backup VM**, **restore VM** o **query VM** para especificar la contraseña del ID de usuario de VMware VirtualCenter o de ESX que se ha especificado con la opción `vmcuser`.

Utilice VirtualCenter si está disponible. Si no puede utilizar un servidor de VirtualCenter y necesita realizar copias de seguridad de varios sistemas de archivos en varios servidores de ESX, no especifique esta opción; en lugar de ello, especifique la opción con el mandato para que pueda cambiarse en función de cada servidor de ESX.



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Clientes soportados

Esta opción sólo es válida en clientes Linux soportados que estén instalados en un servidor de copia de seguridad vStorage utilizado para realizar copias de seguridad de una máquina virtual de VMware.

Archivo de opciones

Coloque esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) o en la línea de mandatos.

1. Pulse **Editar > Preferencias del cliente > Copia de seguridad de máquina virtual**. En el campo **Contraseña**, escriba la contraseña que desea guardar.
2. Pulse en **Aceptar**.

Como alternativa al editor de preferencias, puede almacenar la contraseña localmente usando el mandato **set password**. Por ejemplo:

```
dsmc SET PASSWORD -type=vm  
vcenter.us.ibm.com Administrator secret
```

Sintaxis

►►—VMCPw— —pwname—◄◄

Parámetros

nombre_contraseña

Especifica la contraseña de VMware VirtualCenter o del servidor ESX que desea restaurar, consultar o del que desea hacer una copia de seguridad.

Ejemplos

Archivo de opciones:

VMCPw SECRET

Línea de mandatos:

-VMCPw=SECRET

Referencia relacionada:

“Establecer contraseña” en la página 784

Vmctlmc

Esta opción especifica la clase de gestión que utilizar al hacer copias de seguridad archivos de control de máquina virtual.



Las operaciones de máquina virtual solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments.

De forma predeterminada, los archivos de control de máquina virtual están vinculados a la clase de gestión predeterminada. La opción `vmmc` se puede usar para especificar una clase de gestión diferente a la que estén vinculados los datos de virtual y los datos de control de máquina virtual. La opción `vmctlmc` altera temporalmente la clase de gestión predeterminada y la opción `vmmc` para los archivos de control de máquina virtual.

En determinadas condiciones, es posible que sea deseable o necesario vincular los archivos de control a una clase de gestión diferente a los archivos de datos.

La opción `vmctlmc` es necesaria si se realiza una copia de seguridad de los archivos de datos de máquina virtual en cinta. Debe realizarse una copia de seguridad de los archivos de control de máquina virtual en una agrupación de almacenamiento basada en disco que no migre a una cinta. La agrupación de almacenamiento puede estar compuesta de volúmenes de acceso aleatorios y volúmenes de archivos secuenciales; también puede ser una agrupación desduplicada. Utilice la opción `vmctlmc` para especificar una clase de gestión que almacene datos en dicha agrupación de almacenamiento.

Restricción: La clase de gestión que especifica la opción `vmctlmc` sólo determina la agrupación de almacenamiento de destino para los archivos de control de máquina virtual. La retención de los archivos de control viene determinada por la opción `vmmc`, si está especificada, o por la clase de gestión predeterminada. La retención de los archivos de control de máquina virtual siempre coincide con la retención de los archivos de datos de máquina virtual.

Clientes soportados

Esta opción es válida para los clientes que son nodos de movimiento de datos que protegen las máquinas virtuales de VMware.

La opción sólo se puede utilizar para copias de seguridad de máquina virtual que utilizan una modalidad de copia de seguridad incremental, constante.

Esta opción solo está disponible si tiene licencia para utilizar IBM Spectrum Protect for Virtual Environments: Data Protection for VMware o IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V.

Archivo de opciones

Coloque esta opción en el archivo de opciones del sistema `dsm.sys`.

Sintaxis

►►—VMCTLmc—*class_name*—◄◄

Parámetros

nombre_clase

Especifica una clase de gestión que se aplica para realizar copia de seguridad de los archivos de control de máquina virtual. Si no establece esta opción, se utiliza la clase de gestión que se especifica en la opción `vmmc`. Si no establece esta opción y no está establecida la opción `vmmc`, se utilizará la clase de gestión predeterminada del nodo.

Ejemplos

Archivo de opciones:

`vmctlmc diskonlymc`

Línea de mandatos:

No se aplica.

Vmcuser

Utilice la opción `vmcuser` con los mandatos **backup VM**, **restore VM** o **query VM** para especificar el nombre de usuario de VMware VirtualCenter o del servidor ESX que desea restaurar, consultar o del que desea hacer una copia de seguridad.

Utilice VirtualCenter si está disponible. Si no puede utilizar un servidor de VirtualCenter y necesita realizar copias de seguridad de varios sistemas de archivos en varios servidores de ESX, no especifique esta opción; en lugar de ello, especifique la opción con el mandato para que pueda cambiarse en función de cada servidor de ESX.



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Clientes soportados

Esta opción es válida para los clientes que están configurados para realizar una copia de seguridad consolidada de máquinas virtuales VMware. El servidor también puede definir esta opción.

Archivo de opciones

Coloque esta opción en el archivo de opciones del cliente (`dsm.opt`), en el archivo de opciones del sistema del cliente (`dsm.sys`) o en la línea de mandatos.

Sintaxis

►►—VMCUser— *username* —◄◄

Parámetros

nombre_usuario

Especifica el nombre de usuario de VMware VirtualCenter o del servidor ESX que desea restaurar, consultar o del que desea hacer una copia de seguridad.

Cuando se trabaja con un centro virtual, es necesario un ID de usuario con acceso al sistema Windows que aloja el centro virtual. Este ID de usuario debe tener privilegios de administrador o los privilegios mínimos que se identifican en la nota técnica 1659544.

Ejemplos

Archivo de opciones:

```
VMCUser administrator
```

Línea de mandatos:

```
backup vm -VMCUser=nombredominio\administrador
```

Línea de mandatos:

Ejemplo de conexión a un servidor de ESX:

```
backup vm -VMCUser=root
```

Vmdatastorethreshold

Utilice la opción `vmdatastorethreshold` para establecer el porcentaje de umbral de uso de espacio de cada almacén de datos de VMware de una máquina virtual.

Cuando especifica esta opción, el uso de espacio se comprueba antes de que se cree una instantánea de máquina virtual. Si se excede el umbral, no se hace una copia de seguridad de la máquina virtual. Si establece esta opción, puede evitar errores de falta de espacio cuando realice copias de seguridad de máquinas virtuales.



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Clientes admitidos

Puede utilizar esta opción con clientes x86_64 Linux admitidos.

Archivo de opciones

Puede especificar esta opción en el archivo de opciones del sistema cliente (`dsm.sys`) o en la línea de mandatos mediante el mandato **backup vm**. También puede incluir esta opción en el servidor de IBM Spectrum Protect 7.1.5 o posterior en un conjunto de opciones de cliente. No puede establecer esta opción en el Editor de preferencias.

Sintaxis

►►—VMDATASTOREThreshoId—*porcentaje*—————►►

Parámetros

porcentaje

Especifica el porcentaje de umbral de cada almacén de datos de VMware de la

máquina virtual de la que se va a realizar una copia de seguridad. Puede especificar un entero comprendido entre 0 y 100. El valor predeterminado es 100. Si no establece esta opción, el cliente inicia la copia de seguridad de máquina virtual sin verificar primero el uso de espacio existente.

Requisitos:

- Asegúrese de que el umbral sea lo suficientemente bajo para que la instantánea no utilice todo el espacio disponible en los almacenes de datos de VMware. De lo contrario, se quedará sin espacio en los almacenes de datos de VMware y la instantánea no se creará.
- Si utiliza varios clientes que actúan como nodos de transportador de datos, debe añadir esta opción al archivo de opciones para cada transportador de datos.
- El cliente comprueba el uso de datos del almacén de datos de VMware que contiene las instantáneas de disco de máquina virtual. De forma predeterminada, las instantáneas se crean en el mismo directorio que el del archivo de disco virtual (.vmdk).

Si cambia la ubicación de la instantánea a un directorio nuevo en el mismo almacén de datos o a otro almacén de datos con la opción `workingDir` en el archivo de configuración de la máquina virtual, asegúrese de que la ruta del directorio de trabajo sea correcta. Si la ruta es incorrecta, el cliente podría validar el uso de datos del almacén de datos erróneo.

Si utiliza la opción `EXCLUDE.VMDISK` para excluir uno o varios discos de una copia de seguridad, la comprobación de umbral continúa ejecutándose en esos discos. Aunque no se realice la copia de seguridad de esos discos, VMware continúa realizando una instantánea de ellos.

Los discos independientes no se comprueban durante la verificación de espacio porque una instantánea de estos discos no utiliza espacio de ningún almacén de datos de VMware.

Ejemplo 1

La máquina virtual `vm1` abarca `datastore1` y `datastore2`. Establezca la opción `vmdatastorethreshold` en 90 para asegurarse de que ambos almacenes de datos de VMware estén al 90% de su capacidad antes de que se realice la copia de seguridad de la máquina virtual.

Archivo de opciones:

```
vmdatastorethreshold 90
```

Línea de mandatos:

```
dsmc backup vm vm1 -vmdatastorethreshold=90
```

Ejemplo 2

El umbral del almacén de datos de `datastore2` está establecido en 85. El umbral del almacén de datos se ha superado durante la copia de seguridad de la máquina virtual `vm5`. Se visualiza el siguiente mensaje de error:

```
ANS14200E No se ha podido realizar una copia de seguridad de la máquina virtual
'vm5' porque el
uso de datos del almacén de datos 'datastore2' ha excedido el
umbral de almacén de datos
del 85%.
```

Aumente el valor de la opción `vmdatastorethreshold` a 95 y reinicie la copia de seguridad.

Archivo de opciones:

`vmdatastorethreshold 95`

Línea de mandatos:

`dsmc backup vm vm5 -vmdatastorethreshold=95`

Referencia relacionada:

“Backup VM” en la página 683

Vmdefaultdvportgroup

Utilice esta opción para especificar el grupo de puertos que utilizarán las NIC durante las operaciones **restore vm** para una máquina virtual que estaba conectada a un grupo de puertos virtuales distribuidos cuando se realizó la copia de seguridad, pero el host de destino para la operación de restauración no contiene un grupo de puerto virtual distribuido similar.



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Esta opción no se aplica a operaciones de copia de seguridad o restauración para máquinas virtuales Microsoft Hyper-V.

Clientes soportados

Esta opción es válida para clientes Linux instalados en un servidor de copia de seguridad vStorage.

Archivo de opciones

Coloque esta opción en el archivo de opciones de cliente (`dsm.opt`), en el archivo de opciones del sistema cliente (`dsm.sys`), o bien especifíquela como parámetro de línea de mandatos en el mandato **restore vm**.

Sintaxis

►►—VMDEFAULTDVPORTGROUP—*portgroup_name*—————◄◄

Parámetros

portgroup name

Especifica el nombre del grupo de puertos que se utilizará. El nombre de grupo de puertos distingue entre mayúsculas y minúsculas.

Ejemplos

Archivo de opciones:

`VMDEFAULTDVPORTGROUP dvPortGroup`

Línea de mandatos:

`dsmc restore vm vm123 -VMDEFAULTDVPORTGROUP=dvPortGroup`

Referencia relacionada:

"Vmdefaultnetwork"
"Vmdefaultdvswitch"

Vmdefaultdvswitch

Utilice esta opción para especificar el conmutador virtual distribuido (dvSwitch) que contiene el grupo de puertos que establezca en la opción `vmdefaultdvportgroup`. La opción no tiene efecto a menos que también especifique la opción `vmdefaultdvportgroup`.



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Esta opción no se aplica a operaciones de copia de seguridad o restauración para máquinas virtuales Microsoft Hyper-V.

Clientes soportados

Esta opción es válida para clientes Linux instalados en un servidor de copia de seguridad vStorage.

Archivo de opciones

Coloque esta opción en el archivo de opciones de cliente (`dsm.opt`), en el archivo de opciones del sistema cliente (`dsm.sys`), o bien especifíquela como parámetro de línea de mandatos en el mandato **restore vm**.

Sintaxis

►►—VMDEFAULTDVSWITCH—*dvSwitch*—————►►

Parámetros

dvSwitch

Especifica el nombre del conmutador virtual que se utilizará. El nombre de conmutador virtual distingue entre mayúsculas y minúsculas.

Ejemplos

Archivo de opciones:

```
VMDEFAULTDVSWITCH dvSwitch
```

Línea de mandatos:

```
dsmc restore vm vm123 -VMDEFAULTDVSWITCH=dvSwitch -VMDEFAULTDVPORTGROUP=dvPortGroup
```

Referencia relacionada:

"Vmdefaultdvportgroup" en la página 618

Vmdefaultnetwork

Utilice esta opción para especificar la red para que utilizarán las NIC durante una operación **restore vm**, para una máquina virtual que se había conectado a un grupo de puertos virtuales distribuidos cuando se realizó la copia de seguridad, pero el host de destino para la operación de restauración no tiene ningún grupo de puerto conmutador distribuido configurado.



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Esta opción no se aplica a operaciones de restauración para máquinas virtuales Microsoft Hyper-V.

Clientes soportados

Esta opción es válida para clientes Linux instalados en un servidor de copia de seguridad vStorage.

Archivo de opciones

Coloque esta opción en el archivo de opciones de cliente (`dsm.opt`), en el archivo de opciones del sistema cliente (`dsm.sys`), o bien especifíquela como parámetro de línea de mandatos en el mandato **restore vm**.

Sintaxis

►►—VMDEFAULTNETWORK—*vm_network_name*—————►►

Parámetros

vm_network_name

Especifica el nombre de la red de máquina virtual que se utilizará. El nombre de red distingue entre mayúsculas y minúsculas. Si el nombre contiene caracteres de espacio, ciérrelo entre comillas.

Ejemplos

Archivo de opciones:

```
VMDEFAULTNETWORK "VM Network"
```

Línea de mandatos:

```
dsmc restore vm vm123 -VMDEFAULTNETWORK="VM Network"
```

Referencia relacionada:

“Vmdefaultdvportgroup” en la página 618

“Vmdefaultdvswitch” en la página 619

Vmenabletemplatebackups

La opción `vmenabletemplatebackups` especifica si el cliente realiza una copia de seguridad de máquinas virtuales de plantillas de VMware cuando protege máquinas virtuales en un servidor vCenter. No se puede realizar la copia de seguridad de las máquinas virtuales de plantillas de VMware cuando éstas están en un host ESXi porque ESXi no soporta plantillas.

Cuando esta opción está habilitada, puede incluir máquinas plantilla de VMware en las operaciones de copia de seguridad de máquina virtual completa. Puede utilizar el mandato **Backup VM** existente y la opción `DOMAIN.VMFULL` para especificar las máquinas virtuales que se incluirán en la operación de copia de seguridad.



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

No se admiten las copias de seguridad incrementales y no se toman instantáneas, por lo que debe utilizar `MODE=IFFULL`. Utilice `MODE=IFFULL` para forzar una copia de seguridad nueva de las máquinas virtuales de plantilla de VMware, incluso si no se han modificado desde la última copia de seguridad.

Si se habilita la opción `vmenabletemplatebackups`, cualquier proceso de copia de seguridad iniciado utilizando `MODE=IFINCREMENTAL` se procesa mediante `MODE=IFFULL`. Las máquinas virtuales de plantilla de VMware se incluyen en una copia de seguridad sólo si se han modificado desde que se produjo la última copia de seguridad.

Con esta opción habilitada, asegúrese de que las opciones de `vmvstortransport` incluyen `NBDSSL` o `NBD`. Si sólo se utilizan las modalidades de transporte `SAN` o `HOTADD` con esta opción habilitada, las copias de seguridad de las máquinas de plantilla fallarán.

Clientes soportados

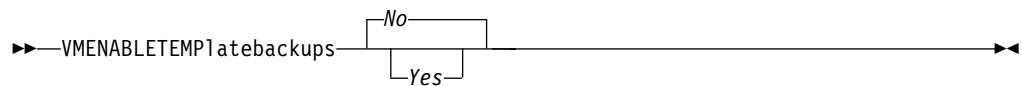
Esta opción puede utilizarse con clientes Linux x86_64 soportados.

Archivo de opciones

Puede definir esta opción en la línea de mandatos, el archivo de opciones de sistema de cliente (`dsm.sys`), el archivo de opciones de cliente (`dsm.opt`) o en un conjunto de opciones de cliente del servidor.

También puede establecerla en el editor de preferencias en la ficha **Copia de seguridad de la máquina virtual** (seleccione la opción **Plantillas de máquina virtual para copia de seguridad**).

Sintaxis



Parámetros

No Especifica que las máquinas virtuales de plantilla no se incluyen en las operaciones de copia de seguridad de máquina virtual completa; este es el valor predeterminado.

Yes

Especifica que las máquinas virtuales de plantilla se incluyen en las operaciones de copia de seguridad de máquina virtual completa.

Ejemplos

Archivo de opciones

```
vmenabletemplatebackups yes
```

Línea de mandatos

Realizar una copia de seguridad de una máquina virtual de plantilla de VMware

```
dsmc backup vm vmname -VMENABLETEMPLATEBACKUPS=YES
```

donde *vmname* es el nombre de la máquina de plantilla.

Línea de mandatos

Restaurar una máquina virtual de plantilla de VMware en la misma ubicación y con el mismo nombre

```
dsmc restore vm vmname -VMENABLETEMPLATEBACKUPS=YES
```

donde *vmname* es el nombre de la máquina de plantilla.

Línea de mandatos

Restaurar una máquina virtual de plantilla en una ubicación nueva

```
dsmc restore vm nombre_máquina_virtual -vmname=win7x64  
-datastore=datastore22 -host=supersht.labx.com  
-datacenter="Lab Center" -VMENABLETEMPLATEBACKUPS=YES
```

donde *vmname* es el nombre de la máquina de plantilla. “win7x64” es el nuevo nombre de máquina virtual de plantilla. También se incluirán el centro de datos, el host y el almacén de datos nuevos.

Referencia relacionada:

“Backup VM” en la página 683

“Restore VM” en la página 764

“Domain.vmfull” en la página 401

Vmlimitperdatastore

La opción `vmlimitperdatastore` especifica el número de máquinas virtuales (VM) y discos virtuales de un almacén de datos que se pueden procesar en paralelo durante una operación de seguridad optimizada.

Una operación de seguridad optimizada es aquella en la que se habilita la funcionalidad de copia de seguridad en paralelo a nivel de máquina virtual, disco virtual o subdisco.

La opción `vmlimitperdatastore` funciona con las opciones `vmmaxparallel`, `vmmaxbackupsessions` y `vmlimitperhost` para optimizar las operaciones de copia de seguridad y ayudar a controlar la cantidad de recursos que puede crear la copia de seguridad en un host de la infraestructura vSphere. Ajuste los valores de estas opciones para encontrar los valores que proporcionen un rendimiento óptimo para las copias de seguridad del entorno.



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

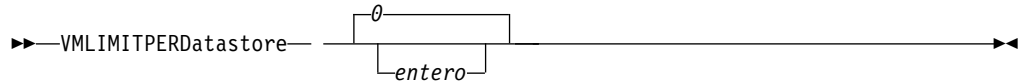
Clientes soportados

Esta opción puede utilizarse con clientes Linux x86_64 soportados.

Archivo de opciones

Esta opción es válida en el archivo de opciones del sistema del cliente `dsm.sys`), en el archivo de opciones del cliente (`dsm.opt`) o en la línea de mandatos para **Backup VM**. También puede incluirse en el servidor en un conjunto de opciones del cliente. No puede establecerse en el Editor de preferencias.

Sintaxis



Parámetros

entero

Especifica el número máximo en cualquier almacén de datos de máquinas virtuales que se incluyen durante una operación de seguridad optimizada. El máximo que puede especificar es 50 máquinas virtuales. El valor predeterminado es 0 (cero).

Si se especifica 0, se indica que no está preocupado por la cantidad de máquinas virtuales (VM) de las que se pueden hacer copias de seguridad en paralelo desde un almacén de datos. En lugar de ello, quiere limitar el número máximo de máquinas virtuales que incluir en una copia de seguridad utilizando el valor que se especifique en la opción `vmmaxparallel`. La opción `vm-limitperdatastore` se impone incluso cuando existen datos de máquina virtual en dos o más almacenes de datos.

Ejemplos

Archivo de opciones

```
VMLIMITPERD 5
```

Línea de mandatos:

```
dsmc backup vm -VMLIMITPERD=5
```

Referencia relacionada:

“Backup VM” en la página 683


“Domain.vmfull” en la página 401

“Vmmaxbackupsessions” en la página 625

“Vmmaxparallel” en la página 627

“Vmlimitperhost”

Información relacionada:

 Realización de copias de seguridad de varias máquinas virtuales en paralelo

Vmlimitperhost

La opción `vmlimitperhost` especifica el número de máquinas virtuales (VM) y discos virtuales de un host que se pueden procesar en paralelo durante una operación de seguridad optimizada.

Una operación de seguridad optimizada es aquella en la que se habilita la funcionalidad de copia de seguridad en paralelo a nivel de máquina virtual, disco virtual o subdisco.

La opción `vmlimitperhost` funciona con las opciones `vmmaxparallel`, `vmmaxbackupsessions` y `vmlimitperdatastore` para optimizar las operaciones de copia de seguridad y ayudar a controlar la cantidad de recursos que puede crear la copia de seguridad en un host de la infraestructura vSphere. Ajuste los valores de estas opciones para encontrar los valores que proporcionen un rendimiento óptimo para las copias de seguridad del entorno.



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Clientes soportados

Esta opción puede utilizarse con clientes Linux x86_64 soportados.

Archivo de opciones

Esta opción es válida en el archivo de opciones del sistema del cliente (`dsm.sys`), en el archivo de opciones del cliente (`dsm.opt`) o en la línea de mandatos para **Backup VM**. También puede incluirse en el servidor en un conjunto de opciones del cliente. No puede establecerse en el Editor de preferencias.

Sintaxis



Parámetros

entero

Especifica el número máximo de máquinas virtuales en cualquier servidor ESX que se pueden incluir en una operación de seguridad optimizada. El máximo que puede especificar es 50 máquinas virtuales. El valor predeterminado es 0 (cero).

Si se especifica 0 se indica que no está preocupado por la cantidad de máquinas virtuales (VM) de las que se pueden hacer copias de seguridad en paralelo desde un servidor ESX. En lugar de ello, quiere limitar el número máximo de máquinas virtuales que incluir en una copia de seguridad utilizando el límite especificado en la opción `vmmaxparallel`.

Ejemplos

Archivo de opciones

```
VMLIMITPERH 5
```


Línea de mandatos:

```
dsmc backup vm -VMLIMITPERH=5
```

Referencia relacionada:

- “Backup VM” en la página 683
- “Domain.vmfull” en la página 401
- “Vmmaxparallel” en la página 627
- “Vmlimitperhost” en la página 623

Información relacionada:

 Realización de copias de seguridad de varias máquinas virtuales en paralelo

Vmmaxbackupsessions

La opción `vmmaxbackupsessions` especifica el número máximo de sesiones de Servidor de IBM Spectrum Protect que trasladan de la máquina virtual (VM) al servidor datos que se pueden incluir en una operación de seguridad optimizada.

Una operación de seguridad optimizada es aquella en la que se habilita la funcionalidad de copia de seguridad en paralelo a nivel de máquina virtual, disco virtual o subdisco.

La opción `vmmaxbackupsessions` funciona con las opciones `vmmaxparallel`, `vmlimitperdatastore` y `vmlimitperhost` para optimizar las operaciones de copia de seguridad y ayudar a controlar la cantidad de recursos que puede crear la copia de seguridad en un host de la infraestructura vSphere. Ajuste los valores de estas opciones para encontrar los valores que proporcionen un rendimiento óptimo para las copias de seguridad del entorno.

Clientes admitidos



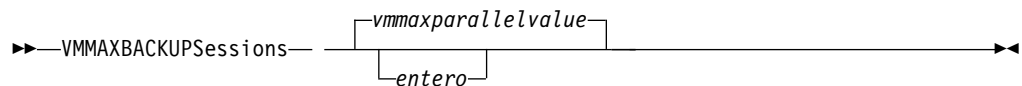
Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Esta opción puede utilizarse con clientes Linux x86_64 soportados.

Archivo de opciones

Esta opción es válida en el archivo de opciones del sistema del cliente (`dsm.sys`), en el archivo de opciones del cliente (`dsm.opt`) o en la línea de mandatos para **Backup VM**. También puede incluirse en el servidor en un conjunto de opciones del cliente. No puede establecerse en el Editor de preferencias.

Sintaxis



Parámetros

entero

Especifica el número máximo de sesiones de Servidor de IBM Spectrum Protect que se pueden crear durante la operación de seguridad.

Revise la información siguiente para utilizar la opción `vmmaxbackupsessions` junto con la opción `vmmaxparallel` o el parámetro de servidor `maxnumpp`:

vmmaxparallel

La opción `vmmaxparallel` especifica el número máximo de máquinas virtuales de las que se puede realizar copia de seguridad en el Servidor de IBM Spectrum Protect en un momento dado. El valor de la opción `vmmaxbackupsessions` tiene que ser igual o superior al valor de la opción `vmmaxparallel`.

Si el valor es inferior al valor de la opción `vmmaxparallel`, se devuelve el siguiente mensaje y el valor cambia al mismo valor que la opción `vmmaxparallel`:

ANS9995W El valor de la opción `VMMAXBACKUPSESSIONS` es *valor_número*. Este valor debe ser mayor o igual que el valor de la opción `VMMAXPARALLELM`, que es *valor_número*. El valor se establecerá en el valor de la opción `VMMAXPARALLEL`.

maxnummp

El parámetro de servidor `maxnummp` especifica el número máximo de puntos de montaje que un nodo puede utilizar en el servidor cuando el destino de la copia de la agrupación de almacenamiento es `FILE` o `TAPE`. El parámetro `maxnummp` tiene que ser igual o mayor que los valores de opción `vmmaxparallel` y `vmmaxbackupsessions`. Cuando varias instancias del cliente están realizando copias de seguridad de archivos o cuando un único cliente realiza copias de seguridad paralelas, pueden ser necesarios más puntos de montaje.

Si los valores de `vmmaxparallel` o `vmmaxbackupsessions` superan el valor de `maxnummp`, se mostrarán los mensajes `ANS0266I` y otros. Según el mensaje, el cliente reduce el valor de la opción `vmmaxparallel` para que coincida con el número especificado por el parámetro `maxnummp` o prohíbe que se abran sesiones adicionales para la máquina virtual especificada. En cualquiera de estas situaciones, la operación de seguridad continúa.

Si se detectan errores `ANS0266I` adicionales, el cliente reduce el valor `vmmaxparallel` en 1 e intenta continuar con la copia de seguridad. Si `vmmaxparallel` se reduce a 1 y el cliente recibe más errores `ANS0266I`, el cliente finaliza la copia de seguridad y emite el error siguiente:

ANS5228E Una operación de copia de seguridad ha fallado porque `VMMAXPARALLEL` fue reducida a 1 y el cliente todavía no puede obtener un punto de montaje del servidor.

Póngase en contacto con el administrador del servidor si quiere que el valor actualmente definido para `maxnummp` aumente, con el fin de que el nodo pueda dar soporte a sesiones adicionales de copias de seguridad paralelas.

El valor máximo que puede especificar es de 100 sesiones. El predeterminado es el valor definido para la opción `vmmaxparallel`.

Ejemplos

Archivo de opciones

`VMMAXBACKUPS 10`

Línea de mandatos:

`dsmc backup vm -VMMAXBACKUPS=10`

Referencia relacionada:

“Backup VM” en la página 683
“Domain.vmfull” en la página 401
“Vmmaxparallel” en la página 627
“Vmlimitperdatastore” en la página 622
“Vmlimitperhost” en la página 623

Información relacionada:

➡ Realización de copias de seguridad de varias máquinas virtuales en paralelo

Vmmaxparallel

La opción `vmmaxparallel` se utiliza para configurar copias de seguridad optimizadas de varias máquinas virtuales utilizando una única instancia del cliente de archivado y copia de seguridad. Esta opción especifica el número máximo de máquinas virtuales de las que se pueden efectuar copias de seguridad en Servidor de IBM Spectrum Protect en cualquier momento.

Una operación de seguridad optimizada es aquella en la que se habilita la funcionalidad de copia de seguridad en paralelo a nivel de máquina virtual, disco virtual o subdisco.

La opción `vmmaxparallel` funciona con las opciones `vmmaxbackupsessions`, `vmlimitperhost` y `vmlimitperdatastore` para optimizar las operaciones de copia de seguridad y controlar la cantidad de recursos que puede crear la copia de seguridad en un host de la infraestructura vSphere. Ajuste los valores de estas opciones para encontrar los valores que proporcionen un rendimiento óptimo para las copias de seguridad del entorno.



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

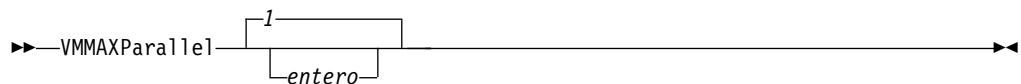
Clientes soportados

Esta opción puede utilizarse con clientes Linux x86_64 soportados.

Archivo de opciones

Esta opción es válida en el archivo de opciones del sistema cliente (`dsm.sys`) o en la línea de mandatos para el mandato **Backup VM**. También puede incluirse en el servidor en un conjunto de opciones del cliente. No puede establecerse en el Editor de preferencias.

Sintaxis



Parámetros

entero

Especifica el número máximo de máquinas virtuales de las que se pueden realizar copias de seguridad en cualquier momento durante una operación de seguridad optimizada. El valor predeterminado es 1. El máximo es 50.

Nota: Cuando utilice la eliminación de duplicados de datos del lado del cliente, se inicia una sesión de eliminación de duplicados de datos para cada máquina virtual. Esta sesión de eliminación de duplicados de datos no se cuenta como una de las sesiones `vmmaxparallel`.

Revise la información siguiente para utilizar la opción `vmmaxparallel` junto con la opción `vmmaxbackupsessions` o el parámetro de servidor `maxnummp`:

vmmaxbackupsessions

vmmaxbackupsessions especifica el número máximo de sesiones que trasladan datos de la máquina virtual al servidor que se pueden incluir en una operación de seguridad optimizada. El valor de la opción vmmaxbackupsessions tiene que ser igual o superior al valor de la opción vmmaxparallel.

maxnummp

El parámetro de servidor maxnummp especifica el número máximo de puntos de montaje que un nodo puede utilizar en el servidor cuando el destino de la copia de la agrupación de almacenamiento es FILE o TAPE. El parámetro maxnummp tiene que ser igual o mayor que los valores de opción vmmaxparallel y vmmaxbackupsessions. Cuando varias instancias del cliente están realizando copias de seguridad de archivos o cuando un único cliente realiza copias de seguridad paralelas, pueden ser necesarios más puntos de montaje.

Si los valores de vmmaxparallel o vmmaxbackupsessions superan el valor de maxnummp, se mostrarán los mensajes ANS0266I y otros. Según el mensaje, el cliente reduce el valor de la opción vmmaxparallel para que coincida con el número especificado por el parámetro maxnummp o prohíbe que se abran sesiones adicionales para la máquina virtual especificada. En cualquiera de estas situaciones, la operación de seguridad continúa.

Si se detectan errores ANS0266I adicionales, el cliente reduce el valor vmmaxparallel en 1 e intenta continuar con la copia de seguridad. Si vmmaxparallel se reduce a 1 y el cliente recibe más errores ANS0266I, el cliente finaliza la copia de seguridad y emite el error siguiente:

ANS5228E Una operación de copia de seguridad ha fallado porque VMMAXPARALLEL fue reducida a 1 y el cliente todavía no puede obtener un punto de montaje del servidor.

Póngase en contacto con el administrador del servidor si quiere que el valor actualmente definido para maxnummp aumente, con el fin de que el nodo pueda dar soporte a sesiones adicionales de copias de seguridad paralelas.

Ejemplos

Archivo de opciones

VMMAXP 10

Referencia relacionada:


“Backup VM” en la página 683

“Domain.vmfull” en la página 401

“Vmlimitperhost” en la página 623

“Vmlimitperdatastore” en la página 622

Información relacionada:

 Realización de copias de seguridad de varias máquinas virtuales en paralelo


Vmmaxrestoresessions

La opción vmmaxrestoresessions especifica el número máximo de sesiones de Servidor de IBM Spectrum Protect que se pueden incluir en una operación de restauración optimizada para una máquina virtual (VM).

Una operación de restauración optimizada es aquella en la que se ha habilitado la prestación de restauración paralela en el nivel de subdisco de un disco virtual.

Clientes admitidos

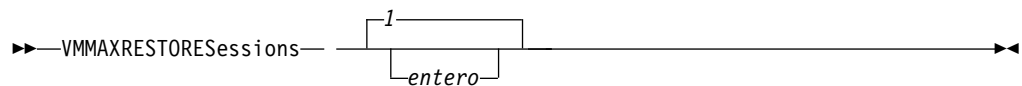
Esta opción puede utilizarse con clientes Linux x86_64 soportados.

 Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Archivo de opciones

Esta opción es válida en el archivo de opciones del sistema del cliente (`dsm.sys`), en el archivo de opciones del cliente (`dsm.opt`) o en la línea de mandatos para **Restore VM**. También puede incluirse en el servidor en un conjunto de opciones del cliente. No puede establecerse en el Editor de preferencias.

Sintaxis



Parámetros

entero

Especifica el número de sesiones de Servidor de IBM Spectrum Protect que se crean durante la operación de restauración. El valor predeterminado es 1. El máximo es 10.

Ejemplos

Archivo de opciones


VMMAXRESTORES 10

Referencia relacionada:

“Restore VM” en la página 764

Vmmaxvirtualdisks

La opción `vmmaxvirtualdisks` especifica el tamaño máximo de los discos de máquina virtual VMware (VMDK) para incluir en una operación de copia de seguridad.

 Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Utilice la opción `vmmaxvirtualdisks` con la opción `vmskipmaxvirtualdisks` para especificar cómo el cliente procesa VMDK grandes durante una operación de copia de seguridad.

- Establezca la opción `vmmaxvirtualdisks` para especificar el tamaño máximo de los VMDK a incluir.

- Establezca la opción `vmskipmaxvirtualdisks` para hacer copias de seguridad de los VMDK que no exceden el tamaño máximo (y excluir los VMDK que sí lo exceden) o la operación fallará.

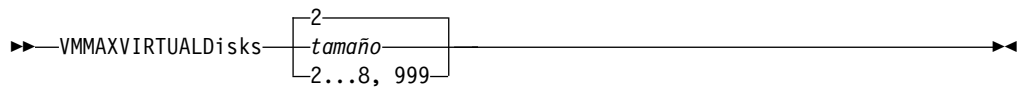
Clientes soportados

Esta opción es válida para clientes de Linux de 64 bits que se configuran como transportadores de datos que realizan copias de seguridad de máquinas virtuales VMware.

Archivo de opciones

Establezca la opción `vmmxvirtualdisks` en el archivo de opciones de sistema de cliente (`dsm.sys`). También puede especificar esta opción como un parámetro de línea de mandato en el mandato **backup vm**.

Sintaxis



Parámetros

tamaño

Especifica el tamaño máximo, en terabytes, de los VMDK a incluir en una operación de copia de seguridad. El rango es un entorno entre 2 y 8; el valor predeterminado es 2. El máximo es 8.

Para asegurarse de que el tamaño de VMware VMDK que está incluido en operaciones de copia de seguridad siempre es el tamaño máximo, especifique 999. Utilice este valor como el método más eficaz para asegurarse de que siempre está establecido el valor máximo. Este valor evita la necesidad de modificar de forma continuada los archivos de opciones.

Cuando también se especifica la opción `vmskipmaxvirtualdisks yes`, se excluyen los VMDKs que tienen el tamaño máximo especificado o menor de los que se han hecho copias de seguridad y los VMDK que superan que el tamaño máximo especificado.

Cuando también se especifica la opción `vmskipmaxvirtualdisks no`, las operaciones de copia de seguridad fallan si un VMDK supera el tamaño máximo especificado.

Ejemplos

Archivo de opciones:

```
vmmxvirtualdisks 3
```

Línea de mandatos:

Haga una copia de seguridad de los VMDK que tienen 5 TB o menos y excluya los VMDK que tienen más de 5 TB:

```
backup vm VM1 -vmmxvirtualdisks=5 -vmskipmaxvirtualdisks=yes
```

Haga una copia de seguridad de los VMDK que tienen 3 TB o menos y haga fallar la operación de copia de seguridad si un VMDK tiene más de 3 TB:

```
backup vm VM1 -vmmxvirtualdisks=3 -vmskipmaxvirtualdisks=no
```

Haga una copia de seguridad de los VMDK que tienen 8 TB o menos y excluya los VMDK que tienen más de 8 TB:

```
backup vm VM1 -vmmxvirtualdisks=8 -vmskipmaxvirtualdisks=yes
```

o bien

```
backup vm VM1 -vmmxvirtualdisks=999 -vmskipmaxvirtualdisks=yes
```

Vmmc

Utilice la opción `vmmc` para almacenar las copias de seguridad de máquina virtual con una clase de gestión distinta a la clase de gestión predeterminada. La opción `vmmc` sólo es válida si está establecida la opción `vmbackuptype=fullvm` o `vmbackuptype=hypervfull`.

Clientes soportados



Las operaciones de máquina virtual solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments.

Esta opción es válida para clientes que estén configurados para realizar copia de seguridad de las máquinas virtuales VMware. El servidor también puede definir esta opción.

Archivo de opciones

Coloque esta opción en el archivo de opciones de cliente `dsm.opt`, el archivo de opciones de sistema de cliente `dsm.sys` o la línea de mandatos.

Sintaxis

►►—VMMC—*management_class_name*—►►

Parámetros

mgmtclassname

Especifica una clase de gestión que se aplica a la copia de seguridad de los datos de la máquina virtual. Si no se define esta opción, se utiliza la clase de gestión predeterminada del nodo.

Ejemplos

Tarea: Ejecute una copia de seguridad de la máquina virtual denominada `myVirtualMachine` y guarde la copia de seguridad de acuerdo con la clase de gestión denominada `myManagmentClass`.

```
dsmc backup vm "myVirtualMachine" -vmmc=myManagmentClass
```

Vmnoprmdisks

Esta opción permite al cliente restaurar la información de configuración para los volúmenes pRDM que están asociados con una máquina virtual VMware, aunque no se puedan encontrar las LUN que estaban asociadas con los volúmenes. Dado que los volúmenes pRDM no se incluyen en la instantánea de máquina virtual, solo se puede restaurar la información de configuración y no los datos que estaban en los volúmenes.



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Esta opción no se aplica a copias de seguridad de máquinas virtuales Microsoft Hyper-V.

Clientes soportados

Esta opción es válida para los clientes Windows y Linux que están instalados en un servidor de copia de seguridad de vStorage.

Archivo de opciones

Coloque esta opción en el archivo de opciones de cliente (dsm.opt), en el archivo de opciones del sistema cliente (dsm.sys), o bien especifíquela como parámetro de línea de mandatos en el mandato **restore vm**.

Sintaxis



Parámetros

YES

Especifique este valor si debe restaurar una máquina virtual de la que ha hecho copia de seguridad con `-vmprocesswithprdm=yes` y las LUN originales que se han correlacionado mediante el archivo de correlaciones de dispositivo en bruto no se pueden ubicar. Este valor hace que el cliente omita los intentos de localizar las LUN que faltan utilizadas por los volúmenes pRDM y restaure la información de configuración (etiquetas de disco) que estaba asociada a ellos. Los volúmenes pRDM se restauran como VMDK VMFS con suministro fino. Entonces puede utilizar el cliente vSphere para crear las correlaciones pRDM necesarias.

NO El establecimiento de `-vmnoprdmdisk=no` hace que fallen las operaciones de restauración para máquinas virtuales de las que se ha hecho copia de seguridad con `-processvmwithprdm=yes` si no se pueden ubicar las LUN originales con las que el archivo de correlaciones de dispositivo en bruto las ha correlacionado. Este valor es el valor predeterminado.

Ejemplos

Archivo de opciones:

```
VMNOPRMDISKS YES
```

Línea de mandatos:

```
dsmc restore vm vm123 -vmnoprdmdisks=yes
```

Información relacionada

“Vmprocessvmwithindependent” en la página 634

“Vmprocessvmwithprdm” en la página 636

Vmnovrmdisks

Esta opción permite al cliente restaurar la información de configuración y los datos para volúmenes de pRDM asociados a una máquina virtual VMware virtual, incluso si no se encuentran los LUN que estaban asociados a los volúmenes.



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Esta opción no se aplica a las copias de seguridad de máquinas virtuales Microsoft Hyper-V.

Clientes soportados

Esta opción es válida para clientes Windows y Linux instalados en un servidor de copia de seguridad vStorage.

Archivo de opciones

Coloque esta opción en el archivo de opciones de cliente (dsm.opt), en el archivo de opciones del sistema cliente (dsm.sys), o bien especifíquela como parámetro de línea de mandatos en el mandato **restore vm**.

Sintaxis



Parámetros

YES

Especifique este valor si tiene que restaurar una máquina virtual con copia de seguridad realizada, y no se puedan localizar los LUN originales correlacionados por el archivo Raw Device Mappings. Este valor provoca que el cliente omita intentos de localizar los LUN que faltan utilizados por los volúmenes vRDM, y restaura la información de configuración (etiquetas de disco) y los datos con copia de seguridad. Los volúmenes vRDM se restauran como VMFS VMDKs de aprovisionamiento fino.

NO Establecer `-vmnovrmdisk=no` provoca que las operaciones de restauración para máquinas virtuales que tenían un volumen vRDM fallen si no se pueden localizar los LUN originales correlacionados por el archivo Raw Device Mappings. Este valor es el valor predeterminado.

Ejemplos

Archivo de opciones:

```
VMNOVRMDISKS YES
```

Línea de mandatos:

```
dsmc restore vm vm123 -vmnovrmdisks=yes
```

Información relacionada

“Vmprocessvmwithprdm” en la página 636

Vmpreferdagpassive

La opción `vmpreferdagpassive` especifica si se debe realizar una copia de seguridad de una copia activa o pasiva de una base de datos que forma parte de un grupo de disponibilidad de base de datos (DAG) de Microsoft Exchange Server.

Esta opción se aplica a cargas de trabajo de Microsoft Exchange Server que se ejecutan dentro de sistemas invitados de máquina virtual de VMware protegidos por IBM Spectrum Protect for Virtual Environments.

Utilice la opción `vmpreferdagpassive` con el mandato **backup vm** .

Clientes soportados

Esta opción es válida para los clientes que actúan como nodos de movimiento de datos para copias de seguridad de huésped VMware.

Archivo de opciones

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor.

Sintaxis



Parámetros

No Realice una copia de seguridad de la base de datos de Microsoft Exchange Server de un DAG independientemente de si se trata de una copia activa o pasiva. Este es el valor predeterminado.

Yes

Omita la copia de seguridad para una copia de la base de datos activa de un DAG si dispone de una copia pasiva válida en otro servidor. Si no dispone de ninguna copia pasiva válida, se hace una copia de seguridad de la copia de la base de datos activa.

Ejemplos

Archivo de opciones:

```
vmpreferdagpassive yes
```

Vmprocessvmwithindependent

Utilice esta opción para controlar si las copias de seguridad completas de máquinas virtuales de VMware son procesadas si la máquina se suministra con uno o más volúmenes de discos independientes.

Los volúmenes de discos independientes no dan soporte a instantáneas. Cualquier volumen de disco independiente en una máquina virtual no será procesado como parte de la operación de copia de seguridad. Cuando se restaure la máquina virtual, el cliente de copia de seguridad y archivado recupera la máquina virtual y sólo se restaurarán los volúmenes que han participado en las operaciones de instantáneas. La información de configuración y contenido de los volúmenes de

disco independientes no se conserva en la información almacenada en el servidor de IBM Spectrum Protect. Los usuarios deben recrear los volúmenes de disco independientes en la máquina restaurada.

Si la máquina virtual también contiene uno o más volúmenes de correlación de dispositivos RAW (RDM), utilice la opción `vmprocessvmwithprdm` para controlar si el cliente realiza cualquier copia de seguridad en la máquina virtual si hay presente un disco independiente.



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Esta opción sólo es válida para copias de seguridad de VMware y no para copias de seguridad de Microsoft Hyper-V.

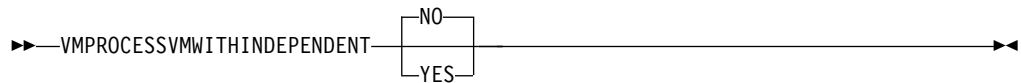
Clientes soportados

Esta opción es válida para clientes Windows y Linux configurados como servidores de copia de seguridad de VMware. El servidor también puede definir esta opción.

Archivo de opciones

Coloque esta opción en el archivo de opciones del cliente (`dsm.opt`), en el archivo de opciones del sistema (`dsm.sys`) o en la línea de mandatos.

Sintaxis



Parámetros

No La copia de seguridad de a máquina virtual falla si se detecta uno o más volúmenes de discos independientes. No es el valor predeterminado.

Sí Las máquinas virtuales que contienen uno o más volúmenes de discos independientes se incluyen en la copia de seguridad. Sin embargo, los volúmenes de discos independientes no se procesan como parte de la operación de copia de seguridad de máquinas virtuales.

Si la máquina virtual también contiene uno o más discos RDM (correlación de dispositivos RAW) proporcionados en modalidad de compatibilidad física, deberá especificarse también la opción `VMPROCESSVMWITHPRDM`.

Ejemplos

Archivo de opciones:

```
VMPROCESSVMWITHINDEPENDENT Yes
```

Línea de mandatos:

```
dsmc backup vm vmlocal -vmbackuptype=fullvm  
-vmprocessvmwithindependent=yes
```

Información relacionada

"Vmprocessvmwithprdm"

Vmprocessvmwithprdm

Utilice esta opción para controlar si las copias de seguridad de máquina virtual de VMware completa son procesadas si la máquina tiene uno o más volúmenes RDM (dispositivos de correlación RAW) proporcionados en modalidad de compatibilidad física (pRDM).

Los volúmenes pRDM no dan soporte a instantáneas. Cualquier volumen pRDM que se encuentre en una máquina virtual no será procesado como parte de la operación de copia de seguridad. Cuando se restaure la máquina virtual, el cliente de copia de seguridad y archivado recupera la máquina virtual y sólo se restaurarán los volúmenes que han participado en las operaciones de instantáneas. La información de configuración y contenido de los volúmenes pRDM no se conserva en la información almacenada en el servidor de IBM Spectrum Protect. Los usuarios deben recrear los volúmenes pRDM en la máquina restaurada.

Esta opción no se aplica a las máquinas virtuales que tengan uno o más volúmenes RDM proporcionados en modalidad de compatibilidad virtual (vRDM). Puesto que los volúmenes vRDM no dan soporte a operaciones de instantáneas, se incluyen en una copia de seguridad de máquina virtual de VMware completa.

Si la máquina virtual también contiene uno o más discos independientes, utilice la opción `vmprocessvmwithindependent` para controlar si el cliente realiza cualquier copia de seguridad en la máquina virtual si hay presente un disco independiente.



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Esta opción sólo es válida para copias de seguridad de VMware y no para copias de seguridad de Microsoft Hyper-V.

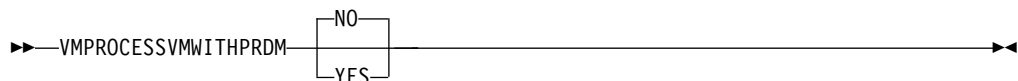
Clientes soportados

Esta opción es válida para clientes Windows y Linux configurados como servidores de copia de seguridad de VMware. El servidor también puede definir esta opción.

Archivo de opciones

Coloque esta opción en el archivo de opciones de cliente(`dsm.opt`), el archivo de opciones de sistema de cliente (`dsm.sys`) o la línea de mandatos.

Sintaxis



Parámetros

No La copia de seguridad de a máquina virtual falla si se detecta uno o más volúmenes pRDM. No es el valor predeterminado.

Yes

Las máquinas virtuales que contengan uno o más volúmenes RDM (correlación de dispositivos RAW) proporcionados en modalidad de compatibilidad física (pRDM) serán incluidos en la copia de seguridad. Sin embargo, los volúmenes pRDM no se procesan como parte de la operación de copia de seguridad de máquinas virtuales.

Si la máquina virtual también contiene uno o más discos independientes, deberá también especificarse la opción `vmprocessvmwithindependentdisk`.

Ejemplos

Archivo de opciones:

```
VMPROCESSVMWITHPRDM Yes
```

Línea de mandatos:

```
dsmc backup vm vmlocal -vmbackuptype=fullvm -vmprocessvmwithprdm=yes
```

Información relacionada

“Vmprocessvmwithindependent” en la página 634

Vmskipctlcompression

Utilice la opción `vmskipctlcompression` para copias de seguridad de máquina virtual para especificar si los archivos de control (*.ctl) se comprimen durante una copia de seguridad de máquina virtual. La opción no afecta a la compresión de los archivos de datos (*.dat)

Puede comprimir archivos de control de máquina virtual y archivos de datos sólo cuando los archivos se almacenan en una agrupación de almacenamiento habilitada para optimización del cliente. Utilice la siguiente configuración de opciones para comprimir los archivos de datos y no comprimir los archivos de control:

```
compression yes  
vmskipctlcompression yes
```

Debe dirigir los archivos de datos a una agrupación de almacenamiento habilitada para la optimización del cliente. Puede dirigir los archivos de control a una agrupación de almacenamiento que no esté habilitado para la optimización del cliente

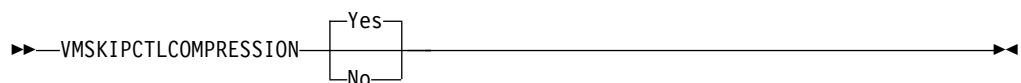
Debe tener licencia para utilizar IBM Spectrum Protect for Virtual Environments para utilizar esta opción.

Clientes soportados

Archivo de opciones

Coloque esta opción en el archivo de opciones del cliente (`dsm.opt`) o en la línea de mandatos.

Sintaxis



Parámetros

Yes

No comprimir archivos de control (*.ctl) durante una copia de seguridad de máquina virtual. La opción no afecta a la compresión de archivos de datos (*.dat).

No Los archivos de control (*.ctl) se pueden comprimir durante la copia de seguridad de máquina virtual. Si los archivos de control se comprimen depende del valor de la opción `compression`.

Vmskipmaxvirtualdisks

La opción `vmskipmaxvirtualdisks` especifica cómo la operación de copia de seguridad procesa discos de máquina virtual VMware (VMDKs) que exceden el tamaño máximo de disco.



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Utilice la opción `vmskipmaxvirtualdisks` con la opción `vmmaxvirtualdisks` para especificar cómo el cliente procesa VMDK grandes durante una operación de copia de seguridad:

- Establezca la opción `vmskipmaxvirtualdisks` para hacer copias de seguridad de los VMDKs que no exceden el tamaño máximo (y excluir los VMDK que sí lo exceden) o la operación fallará.
- Establezca la opción `vmmaxvirtualdisks` para especificar el tamaño máximo de los VMDK a incluir.

En V7.1.3 y anterior, la opción `vmskipmaxvirtualdisks` se llamaba `vmskipmaxvmdks`. En V7.1.4 y posteriores, `vmskipmaxvirtualdisks` es el nombre de opción preferido. Sin embargo, el cliente sigue procesando operaciones de copia de seguridad con el nombre `vmskipmaxvmdks`.

Clientes soportados

Esta opción es válida para clientes de Linux de 64 bits que se configuran como transportadores de datos que realizan copias de seguridad de máquinas virtuales VMware.

Archivo de opciones

Establezca la opción `vmskipmaxvirtualdisks` en el archivo de opciones de sistema de cliente (`dsm.sys`). También puede especificar esta opción como un parámetro de línea de mandato en el mandato **backup vm**.

Sintaxis



Parámetros

No Especifica que las operaciones de copia de seguridad fallan si una máquina virtual VMware tiene uno o más VMDK que superan el tamaño máximo. Éste es el valor predeterminado.

Yes

Especifica que las operaciones de copia de seguridad incluyen VMware VMDK que tienen el tamaño máximo (o menos) y excluyen los VMDK que superan el tamaño máximo.

Ejemplos

Archivo de opciones:

```
vmskipmaxvirtualdisks yes
```

Línea de mandatos:

La operación copia de seguridad falla si un VMDK es mayor de 2 TB:

```
backup vm VM1 -vmskipmaxvirtualdisks=no
```

La operación copia de seguridad falla si un VMDK es mayor de 5 TB:

```
backup vm VM1 -vmskipmaxvirtualdisks=no -vmmxvirtualdisks=5
```

Haga una copia de seguridad de los VMDK que tienen 8 TB o menos y excluya los VMDK que tienen más de 8 TB:

```
backup vm VM1 -vmskipvirtualdisks=yes -vmmxvirtualdisks=8
```

Vmskipmaxvmdks

La opción `vmskipmaxvmdks` especifica cómo la operación de copia de seguridad procesa discos de máquina virtual VMware (VMDK) que exceden el tamaño máximo de disco.

En V7.1.4 y posteriores, `vmskipmaxvmdks` se renombra a `vmskipmaxvirtualdisks`. Aunque `vmskipmaxvirtualdisks` es el nombre preferido, el cliente sigue procesando las operaciones de copia de seguridad con el nombre `vmskipmaxvmdks`.



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Consulte “`Vmskipmaxvirtualdisks`” en la página 638 si desea más información sobre cómo establecer esta opción.

Vmtagdefaultdatamover

Utilice la opción `vmtagdefaultdatamover` para proteger las máquinas virtuales, definidas en una planificación, que no tengan un código y una categoría Data Mover asignados o heredados.



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Si especifica un nodo de transportador de datos con la opción `vmtagdefaultdatamover` y la opción `vmtagdatamover yes`, el transportador de datos realiza una copia de seguridad de todas las máquinas virtuales nuevas añadidas a

cualquier contenedor del centro de datos, si el contenedor ya se encuentra en un conjunto de protección. Un conjunto de protección consta de las máquinas virtuales de un contenedor asignado al código y la categoría Schedule (IBM Spectrum Protect). El transportador de datos predeterminado también realiza copias de seguridad de las máquinas virtuales del conjunto de protección a las que no se ha asignado el código Data Mover.

Si hay más de un transportador de datos asociado a una planificación, defina un transportador de datos como el predeterminado con la opción `vmtagdefaultdatamover`. Si solo hay un transportador de datos asociado a una planificación, asígnelo como predeterminado.

Consejo: Para cada planificación, especifique como predeterminado solo un transportador de datos de la lista de transportadores de datos asociados. En caso contrario, se realizará más de una copia de seguridad de las máquinas virtuales nuevas y de aquellas a las que no se les haya asignado el código Data Mover.

Se pueden asignar códigos de protección de datos al inventario de vSphere para gestionar la protección de máquinas virtuales. Para obtener una lista de los códigos y categorías admitidos, consulte el apartado “Códigos de protección de datos admitidos” en la página 793.

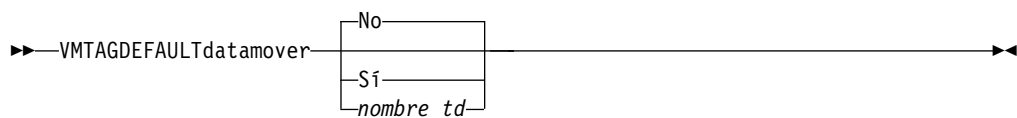
Cientes admitidos

Esta opción se puede utilizar con los transportadores de datos admitidos de Linux x86_64.

Archivo de opciones

Puede especificar esta opción en el archivo de opciones del sistema cliente (`dsm.sys`) o en la línea de mandatos mediante el mandato **backup vm**. También puede incluir esta opción en el servidor de IBM Spectrum Protect en un conjunto de opciones de cliente. No puede establecer esta opción en el Editor de preferencias.

Sintaxis



Parámetros

- No** El transportador de datos local no funciona como un transportador de datos predeterminado. Las máquinas virtuales a las que no se haya asignado el código Data Mover no serán protegidas por este transportador de datos. Este es el valor predeterminado.
- Sí** Especifica que el transportador de datos local (el transportador de datos donde se especifica esta opción) funciona como transportador de datos predeterminado.

Tiene que habilitar también el transportador de datos para que dé soporte a la codificación especificando la opción `vmtagdatamover yes`.

nombre_td

Nombre del transportador de datos que se quiere utilizar como transportador de datos predeterminado. Esta opción solo es necesaria si quiere definirla en el archivo de opciones para el transportador de datos predeterminado. Esta opción se omite en el caso de cualquier transportador de datos que no sea el transportador de datos predeterminado.

Es posible transmitir esta opción a todos los transportadores de datos del mandato de planificación del servidor o incluirla en todos los archivos de opción del transportador de datos. Solo el transportador de datos predeterminado utiliza esta opción. Por lo tanto, defina solo un transportador de datos.

También tiene que especificar la opción `vmtagdatamover` yes en el archivo de opciones del transportador de datos que quiere designar como transportador de datos predeterminado.

Ejemplo

La configuración de Data Protection for VMware de Windows utiliza dos transportadores de datos, `VC1_DC1_DM1` y `VC1_DC1_DM2`. Para designar el transportador de datos `VC1_DC1_DM1` como transportador de datos predeterminado, complete los pasos siguientes:

1. En el archivo de opciones del transportador de datos `VC1_DC1_DM1` (`dsm.VC1_DC1_DM1.opt`), añada las sentencias siguientes:

```
vmtagdatamover yes  
vmtagdefaultdatamover yes
```

o bien

```
vmtagdatamover yes  
vmtagdefaultdatamover VC1_DC1_DM1
```

2. En el archivo de opciones del transportador de datos `VC1_DC1_DM2` (`dsm.VC1_DC1_DM2.opt`), añada las sentencias siguientes:

```
vmtagdatamover yes  
vmtagdefaultdatamover VC1_DC1_DM1
```

La opción `vmtagdefaultdatamover` también se puede pasar a un mandato o una definición de planificación para asignar el transportador de datos predeterminado. Si el transportador de datos predeterminado está definido en la definición de planificación, todos los transportadores de datos asociados a la planificación podrán identificar el transportador de datos predeterminado del conjunto de protección.

Por ejemplo: `dsmc backup vm -vmtagdefaultdatamover=VC1_DC1_DM1`

Tareas relacionadas:

 **Habilitación del soporte de codificación**

Referencia relacionada:

“Domain.vmfull” en la página 401

“Vmtagdatamover”

“Set Vmtags” en la página 790

Vmtagdatamover

Utilice la opción `vmtagdatamover` para habilitar el soporte de codificación en el cliente de copia de seguridad y archivado (transportador de datos). Si esta opción

está habilitada, el cliente gestiona las copias de seguridad de las máquinas virtuales en los objetos de inventario de VMware de acuerdo con los códigos de protección de datos definidos por la Extensión de IBM Spectrum Protect del cliente web vSphere o por herramientas como como VMware vSphere PowerCLI versión 5.5 R2 o posteriores.



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Para obtener más información sobre los códigos de protección de datos, consulte el apartado “Visión general de los códigos de protección de datos” en la página 792.

El transportador de datos procesa los códigos de protección de datos si la opción `vmtagdatamover` está establecida en `yes`. Asegúrese de que se cumplan los siguientes requisitos.

Requisitos:

- Para el transportador de datos:
 - VMware vCenter Server debe estar en la Versión 6.0 Actualización 1 o posterior.
 - Se necesitan permisos adicionales para la cuenta que se utiliza para operaciones de copia de seguridad o restauración. Estos nuevos permisos de vCenter se necesitan para realizar las operaciones de codificación y de categoría. Asegúrese de que los siguientes permisos están establecidos en el servidor vCenter raíz:
 - Inventory Service > vSphere Tagging > Assign or Unassign vSphere Tag
 - Inventory Service > vSphere Tagging > Create vSphere Tag
 - Inventory Service > vSphere Tagging > Create vSphere Tag Category
 - Inventory Service > vSphere Tagging > Delete vSphere Tag
 - Inventory Service > vSphere Tagging > Delete vSphere Tag Category
 - Inventory Service > vSphere Tagging > Modify UsedBy Field For Tag
 - Inventory Service > vSphere Tagging > Modify UsedBy Field For Category
 - Para obtener más información sobre la configuración de permisos de vCenter para operaciones de copia de seguridad y restauración, consulte la nota técnica 7047438.
 - Para que la GUI de Data Protection for VMware vSphere funcione correctamente con el soporte para códigos, asegúrese de que se cumplan los requisitos siguientes durante la instalación de la GUI:
 - Es necesario instalar al menos un transportador de datos y la GUI de Data Protection for VMware vSphere en el mismo servidor. Es necesario configurar este nodo de transportador de datos para guardar las credenciales de servidor de vCenter. Puede guardar las credenciales ejecutando el asistente de configuración para guardar la contraseña del nodo de transportador de datos, o bien mediante el mandato **`dsmc set password`** de la línea de mandatos del transportador de datos.
- Si utiliza otros transportadores de datos, que se ejecuten en máquinas virtuales o máquinas físicas como transportadores de datos adicionales, puede instalarlos en otros servidores. En lo relativo al soporte de codificación, es necesario configurar también todos estos transportadores de datos con la opción `vmtagdatamover=yes`. Estos transportadores de datos adicionales no requieren que la GUI de Data Protection for VMware vSphere esté instalada en el mismo servidor para funcionar correctamente como transportadores de datos basados en códigos.

- En el caso de transportadores de datos de Linux, asegúrese de especificar el directorio de instalación del transportador de datos y la biblioteca compartida de Java™ libjvm.so en la variable de entorno LD_LIBRARY_PATH. La vía de acceso a libjvm.so se utiliza para el soporte de codificación cuando se habilita la opción vmtagdatamover en el transportador de datos. Para obtener instrucciones, consulte la publicación Configuración de los nodos transportadores de datos en un entorno de vSphere.
- En sistemas operativos Linux, la GUI de Data Protection for VMware vSphere se debe instalar utilizando el nombre de usuario predeterminado (tdpvmware).
- En los nodos transportadores de datos Linux, se debe utilizar el archivo de contraseñas predeterminado (/etc/adsm/TSM.PWD).

Cientes admitidos

Esta opción puede utilizarse con clientes Linux x86_64 soportados.

Archivo de opciones

Puede especificar esta opción en el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos mediante el mandato **backup vm**. También puede incluir esta opción en el servidor de IBM Spectrum Protect en un conjunto de opciones de cliente. No puede establecer esta opción en el Editor de preferencias.

Sintaxis



Parámetros

No El cliente no tiene en cuenta los valores de protección de datos ni los códigos que se atribuyen al activo VMware. Este es el valor predeterminado.

Yes

El cliente gestiona las copias de seguridad en función de los valores de protección de datos de la Extensión de IBM Spectrum Protect o en función de los valores de los códigos atribuidos al activo VMware.

Si el soporte a la codificación está habilitado, algunas opciones de cliente podrían verse afectadas por los valores de protección de datos. Para obtener información sobre las opciones que se ven afectadas, consulte el apartado “Códigos de protección de datos admitidos” en la página 793.

En los ejemplos siguientes se muestra cómo se pueden ver afectadas las opciones de cliente por los códigos de protección de datos:

- Cuando se utilizan los valores o códigos de protección de datos para controlar las máquinas virtuales VMware de las que se realiza una copia de seguridad, los valores de código se pueden solapar con el valor de la opción del cliente `domain.vmfull`. Aunque la opción `domain.vmfull` define las máquinas virtuales que protege el cliente, los códigos `Excluded` e `Included` sustituyen a lo que se ha definido con la opción `domain.vmfull`.

Por ejemplo, la siguiente sentencia del archivo de opciones especifica lo que se copia durante operaciones de copia de seguridad completa de la máquina virtual:

DOMAIN.VMFULL VMHOSTCLUSTER=cluster01,cluster02;VM=Dept20*

Si utiliza valores o códigos de protección de datos para excluir la máquina virtual Dept204, no se realizará una copia de seguridad de la máquina virtual Dept204.

- El valor de la política de retención de la Extensión de IBM Spectrum Protect o el valor del código correspondiente a la categoría Management Class (IBM Spectrum Protect) prevalece sobre las opciones de cliente `include.vm` y `vmmc`, pero no sustituye la opción `vmctlmc`.

Consejo: Si quiere configurar un transportador de datos como el predeterminado, consulte el apartado “`Vmtagdefaultdatamover`” en la página 639.

Ejemplos

Archivo de opciones:

`vmtagdat yes`

Línea de mandatos:

`-vmtagdat=yes`

Tareas relacionadas:



Habilitación del soporte de codificación

Referencia relacionada:

“`Vmtagdefaultdatamover`” en la página 639

“`Domain.vmfull`” en la página 401

“`Include.vm`” en la página 466

“`Vmmc`” en la página 631

“`Vmctlmc`” en la página 614

“**Set Vmtags**” en la página 790

Vmverifyfaction

Utilice esta opción para especificar la acción a realizar si el transportador de datos detecta problemas de integridad con los archivos CTL y bitmap más recientes para una máquina virtual.

Esta opción afecta al proceso de copia de seguridad de un huésped de máquina virtual solo cuando todas las condiciones siguientes son verdaderas:

- La operación de copia de seguridad anterior para el huésped de máquina virtual era una copia de seguridad incremental-constante-incremental (`mode=ifincremental`)
- La operación de copia de seguridad actual para el huésped de máquina virtual es una copia de seguridad incremental-constante-incremental
- El transportador de datos ha detectado un problema de integridad con los datos CTL y bitmap de una operación de copia de seguridad incremental-constante-incremental anterior
- La opción `vmverifyflatest` está establecida en `yes`

Si todas estas condiciones no son verdaderas para una máquina virtual, la copia de seguridad se produce como habitualmente; la acción especificada por esta opción no se inicia.



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Clientes soportados

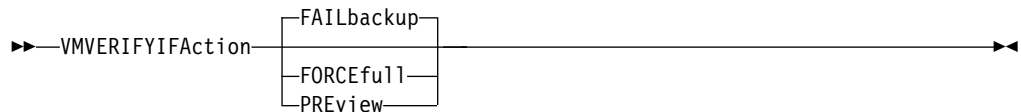
Esta opción es válida para clientes Linux que son nodos de movimiento de datos para copias de seguridad de huésped VMware.

Archivo de opciones

Establezca esta opción en el archivo de opciones de cliente (dsm.opt) o el archivo de opciones del sistema del cliente (dsm.sys).

Esta opción también se puede incluir en un conjunto de opciones de cliente, como parámetro en un mandato **backup vm**, o en la definición del parámetro **options**.

Sintaxis



Parámetros

FAILbackup

Esta acción falla en la operación de copia de seguridad. Se escriben los siguientes mensajes en el archivo de registro de errores del transportador de datos (dsmerror.log):

```
ANS9921E Disco de máquina virtual, nombre_mv (etiqueta_disco),  
ha fallado la comprobación de verificación (xxx/yyy).
```

xxx/yyy en el mensaje indican el tamaño de los archivos bitmap (*xxx*) y CTL (*yyy*).

```
ANS9919E No se han podido encontrar los archivos de control esperados  
para nombre_mv
```

Realice una copia de seguridad de máquina virtual completa (establezca `-mode=IFFull` para las máquinas virtuales afectadas en el momento que elija. Una alternativa es utilizar `-vmverifyifaction=forcefull` en la siguiente operación de incremental-constante-incremental planificada para forzar una copia de seguridad completa de dichas máquinas virtuales, si determina que la ventana de copia de seguridad planificada puede contener las copias de seguridad de máquina virtual completas para estas máquinas virtuales. Este valor es el valor de acción predeterminado.

FORCEfull

Esta acción cambia la modalidad de copia de seguridad de `-mode=ifincremental` a `-mode=iffull`; la copia de seguridad actual se convierte en una copia de seguridad de máquina virtual completa. Se inicia la copia de seguridad de máquina virtual completa. Se escriben los siguientes mensajes en el archivo de registro de errores del transportador de datos (dsmerror.log):

```
ANS9921E Disco de máquina virtual, nombre_mv (etiqueta_disco),  
ha fallado la comprobación de verificación (xxx/yyy)
```

xxx/yyy en el mensaje indican el tamaño de los archivos bitmap (xxx) y CTL (yyy).

ANS9919E No se han podido encontrar los archivos de control esperados para *nombre_mv*

ANS9922I VMVERIFYIFlatest está habilitado para *nombre_mv* (acción: FORCEFULL).

ANS9920W Forzando una copia de seguridad de máquina virtual completa para *nombre_mv*

Utilice esta opción si la ventana de copia de seguridad actual puede contener una copia de seguridad de máquina virtual completa de las máquinas virtuales afectadas.

PREview

Esta acción no realiza ninguna copia de seguridad. En cambio, los datos CTL y bitmap para cada huésped de máquina virtual que procesa el mandato **backup vm** se almacena en una ubicación temporal, donde se comprueba la integridad. Si la comprobación de integridad falla, se escriben los siguientes mensajes en el archivo de registro de errores del transportador de datos (dsmerror.log):

ANS9921E Disco de máquina virtual, *nombre_mv* (*etiqueta_disco*), ha fallado la comprobación de verificación (xxx/yyy)

xxx/yyy en el mensaje indican el tamaño de los archivos bitmap (xxx) y CTL (yyy).

ANS9919E No se han podido encontrar los archivos de control esperados para *nombre_mv*

ANS9922I VMVERIFYIFlatest está habilitado para *nombre_mv* (acción: PREVIEW)

Utilice esta opción para validar la integridad de copias de seguridad incrementales-constantes-incrementales (-mode=ifincremental) que haya creado previamente para una o más máquinas virtuales.

Si los mensajes indican que ha fallado la comprobación de integridad en algunas máquinas virtuales, inicie una copia de seguridad de máquina virtual completa (-mode=iffull) en el momento que elija. Como alternativa, establezca -vmverifyifaction=forcefull en la siguiente operación incremental-constante-incremental planificada para forzar una copia de seguridad completa de esas máquinas virtuales. La ventana de copia de seguridad debe ser lo bastante grande para acomodar una o más copias de seguridad de máquina virtual completas.

Vmverifyiflatest

Esta opción solo se aplica a operaciones de copia de seguridad de máquina virtual VMware que utilicen la modalidad de copia de seguridad incremental-constante-incremental (es decir, un mandato a **backup vm** con **-mode=IFIncremental** especificado). Si se habilita esta opción **vmverifyiflatest**, el transportador de datos ejecuta una comprobación de integridad en los archivos CTL y bitmap que se crearon en un servidor durante la última copia de seguridad, si la última copia de seguridad fue una copia de seguridad incremental-constante-incremental.

Si los archivos pasan las pruebas de integridad, la máquina virtual es restaurable. La copia de seguridad actual continúa y añade otra instantánea a la cadena de instantáneas para la máquina virtual.

Si los archivos fallan las pruebas de integridad, la máquina virtual no es restaurable. En este caso, el transportador de datos realiza otra acción, que ha especificado en la opción (vmverifyifaction). Puede establecer vmverifyifaction

para crear una copia de seguridad de máquina virtual completa inmediatamente, o puede fallar toda la copia de seguridad y ejecutar una copia de seguridad de máquina virtual completa en otro momento. Se puede establecer un tercer parámetro para verificar los archivos CTL y bitmap para una máquina virtual, sin crear una nueva instantánea de copia de seguridad.

La verificación solo se puede realizar si la operación de copia de seguridad anterior para la verificación utilizó `mode=IFIncr`, y si la operación de copia de seguridad actual también utiliza `mode=IFIncr`. Esta opción no tiene efecto en las otras modalidades de copia de seguridad de máquina virtual.

Importante:

Si esta opción se establece en `no`, el proceso de copia de seguridad de máquina virtual continuará sin ninguna prueba de verificación. Los recursos de procesamiento implicados en realizar las comprobaciones de integridad no tienen valor. Para garantizar la integridad continuada de la cadena de copia de seguridad incremental-constante-incremental, establezca o utilice el valor predeterminado (`vmverifyiflatest yes`). No establezca esta opción en `no`, a menos que así se lo indique el soporte de IBM.



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Clientes soportados

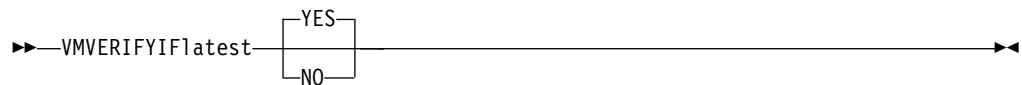
Esta opción es válida para clientes Linux que son nodos de movimiento de datos para copias de seguridad de huésped VMware.

Archivo de opciones

Establezca esta opción en el archivo de opciones de cliente (`dsm.opt`) o el archivo de opciones del sistema del cliente (`dsm.sys`).

Esta opción también se puede incluir en un conjunto de opciones de cliente, como parámetro en un mandato **backup vm**, o en la definición del parámetro **options**.

Sintaxis



Parámetros

YES

Este valor especifica que la validación de los datos CTL y bitmap se realiza para cada máquina virtual procesada por la operación actual de copia de seguridad incremental-constante-incremental (`mode=IFIncr`), si la operación de copia de seguridad anterior para la máquina virtual también era una copia de seguridad incremental-constante-incremental. Este valor es el valor predeterminado.

NO Este valor especifica que la validación de datos CTL y bitmap no se produce

durante el proceso de copia de seguridad incremental-constante-incremental.
No establezca este valor a menos que así se lo indique el soporte de IBM.

Ejemplos

Archivo de opciones:

```
vmverifyiflatest yes
```

Línea de mandatos:

```
dsmc backup vm vml -mode=ifincremental -vmverifyiflatest=yes
```

Vmstortransport

La opción `vmstortransport` especifica el orden de transportes preferido (jerarquía) que utilizar cuando se realizan copias de seguridad de o restaurar máquinas virtuales de VMware. Si no incluye un transporte determinado utilizando esta opción, se excluirá el transporte y no se utilizará para transferir los datos.

El orden de transporte que especifique determina cómo accede VMware API for Data Protection (VADP) a los datos en los discos virtuales, pero no afecta a la vía de acceso de datos utilizada entre el cliente de copia de seguridad y archivado y el servidor de IBM Spectrum Protect. Los transportes válidos incluyen cualquier orden o combinación de las opciones siguientes:

- nbd** Transferencia de datos basada en la red. Acceda a los datos del disco virtual utilizando la LAN. Esta vía de transporte suele estar disponible en todas las configuraciones.
- nbdssl** Igual que `nbd`, pero los datos se cifran antes de enviarlos por la LAN. El cifrado puede reducir el rendimiento.
- san** Transferencia de red de área de almacenamiento: Acceda a los datos del disco virtual utilizando la SAN.
- hotadd** Si utiliza un cliente de archivado-copia de seguridad en una máquina virtual, el transporte `hotadd` permite el transporte de datos de los que se haya realizado una copia de seguridad a almacenamiento añadido dinámicamente.

Separe cada opción de transporte de las demás con dos puntos, por ejemplo, `san:nbd:nbdssl:hotadd`.

Si no especifica una jerarquía de transporte, el orden de selección de transporte predeterminado es `san:hotadd:nbdssl:nbd`.

El primer transporte que está disponible se utiliza para transferir los datos. Si impedir el transporte de datos sobre una determinada vía de acceso, no la incluya en la lista de transportes. Por ejemplo, si es importante no interrumpir el tráfico de la LAN, omita los transportes `nbd` de la jerarquía.



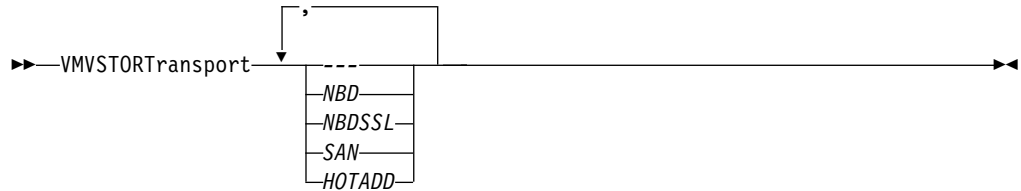
Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Establezca esta opción en `dsm.sys`.

Clientes soportados

Esta opción es válida para clientes Linux configurados para realizar copias de seguridad de o restaurar máquinas virtuales utilizando VDAP.

Sintaxis



Ejemplos

Si la SAN está disponible, no transporte copias de seguridad ni restauraciones sobre la LAN

```
VMVSTORTRANSPORT san
```

El cliente de archivado-copia de seguridad se ejecuta en una máquina virtual, pero no utilice el transporte hotadd

```
VMVSTORTRANSPORT nbdssl:nbd
```

Utilice el transporte de LAN, incluso si nbdssl está disponible, para obtener un rendimiento superior

```
VMVSTORTRANSPORT nbd
```

Es preferible utilizar el transporte SAN, pero utilice nbd cuando SAN no esté disponible, y no utilice nbdssl u hotadd

```
VMVSTORTRANSPORT san:nbd
```

Vmtimeout

VMTIMEOut especifica el tiempo máximo, en segundos, que debe esperarse antes de abandonar una operación **backup vm**, cuando se utiliza la opción INCLUDE.VMTSMVSS para proporcionar protección de aplicaciones. Para utilizar esta opción, la licencia de IBM Spectrum Protect for Virtual Environments debe estar instalada.

Las operaciones **backup vm** realizadas en una máquina virtual protegida por una opción INCLUDE.VMTSMVSS están sujetas a un temporizador. El valor del temporizador determina cuántos segundos debe esperar el cliente para pausar la actividad de la aplicación y truncar sus registros para poder realizar la copia de seguridad. El valor de tiempo predeterminado es suficiente para la mayoría de los entornos. Sin embargo, si no se puede realizar copia de seguridad de los datos de la aplicación porque la aplicación necesita tiempo adicional para preparar la instantánea, puede aumentar el valor de tiempo de espera. Este temporizador sólo se aplica a operaciones **backup vm** cuando se establece la opción INCLUDE.VMTSMVSS para una máquina virtual.

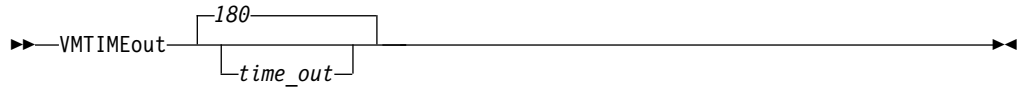
Clientes soportados

Esta opción puede utilizarse con clientes Linux x86_64 soportados.

Archivo de opciones

Coloque esta opción en el archivo de opciones del cliente. No puede establecerse en la línea de mandatos ni el editor de preferencias.

Sintaxis



Parámetros

tiempo_espera

Especifica el tiempo, en segundos, que hay que dejar para que finalicen las operaciones de copia de seguridad cuando una máquina virtual está protegida por la opción de protección de aplicaciones, INCLUDE.VMTSMVSS. El valor especificado debe ser un número entero entre 180 y 500. El valor predeterminado es de 180 segundos.

Ejemplos

Archivo de opciones

VMTIMEout 500

Línea de mandatos

No aplicable; esta opción no puede establecerse en la línea de mandatos.

Referencia relacionada:

“INCLUDE.VMTSMVSS” en la página 472

Webports

La opción webports habilita el uso del cliente web fuera de un cortafuegos.

La opción webports permite utilizar el cliente web fuera de un cortafuegos mediante la especificación del número de puerto TCP/IP que utilizan el servicio de aceptación de clientes de IBM Spectrum Protect y el servicio del agente de cliente web para las comunicaciones con el cliente web.

Es necesario especificar valores para el aceptador de clientes y para el servicio del agente de cliente web.

Si no especifica esta opción, se utiliza el valor predeterminado, cero (0), en ambos puertos. Esto da lugar a que TCP/IP asigne aleatoriamente un número de puerto libre para el aceptador de clientes y el servicio del agente de cliente web.

Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

Archivo de opciones

Establezca esta opción en el archivo dsm.sys dentro de una stanza de servidor. Para establecer esta opción en el editor Preferencias del cliente, pulse **Editar** > **Preferencias del cliente** > **Cliente web** y especifique los puertos en los campos **Puerto del agente web** y **Puerto del aceptador de clientes web**.

Sintaxis

►►—WEBPorts— —*cadport*— —*agentport*—►►

Parámetros

cadport

Especifica el número de puerto necesario del aceptador de clientes. El rango de valores oscila entre 1000 y 32767. Si no se especifica ningún valor, el valor predeterminado, cero (0), hace que TCP/IP asigne al azar un número de puerto libre.

puerto_agente

Especifica el número de puerto necesario del servicio del agente de cliente web. El rango de valores oscila entre 1000 y 32767. Si no se especifica ningún valor, el valor predeterminado, cero (0), hace que TCP/IP asigne al azar un número de puerto libre.

Ejemplos

Archivo de opciones:

webports 2123 2124

Línea de mandatos:

No se aplica.

Wildcardsareliteral

La opción `wildcardsareliteral` especifica si los signos de interrogación (?) y los asteriscos (*) se interpretan literalmente, cuando están incluidos en una especificación de una lista de archivos en una opción `filelist`.

Normalmente, el cliente no acepta caracteres comodín (? y *) en una especificación de lista de archivos que se incluye en una opción `filelist`. Algunos sistemas de archivos permiten el uso de comillas simples y dobles en los nombres de archivos y directorios. Para impedir errores que de lo contrario se podrían producir, cuando se incluyen especificaciones de archivos en una opción `filelist` y contienen caracteres comodín, establezca `wildcardsareliteral yes`. Cuando `wildcardsareliteral` tiene el valor `yes`, los signos de interrogación (?) y los asteriscos (*) que se incluyen en una especificación de lista de archivos en la opción `filelist` se interpretan literalmente, y no como caracteres comodín.

Esta opción se aplica a cualquier mandato que acepta una opción `filelist` como un parámetro de mandato.

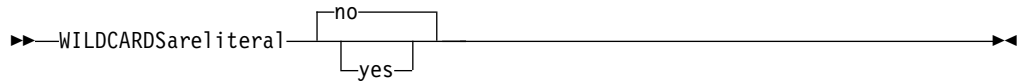
Clientes soportados

Esta opción es válida para todas las plataformas soportadas. La opción se aplica a cualquier mandato que toma una especificación de lista de archivos como parámetro.

Archivo de opciones

Coloque esta opción en el archivo de opciones de usuario del cliente (`dsm.opt`).

Sintaxis



Parámetros

no Especifica que las interrogaciones y los asteriscos se interpretan como comodines cuando se utilizan en una especificación de lista de archivos que se incluye en una opción `filelist`. No es el valor predeterminado. Si una especificación de lista de archivos en una opción `filelist` incluye una interrogación o un asterisco, se produce un error y no se puede procesar la especificación de archivo.

yes

Especifica que los asteriscos y las interrogaciones en una especificación de lista de archivos que se incluye en una opción `filelist` se interpretan literalmente, y no como caracteres comodín. Especifique este valor si está realizando la copia de seguridad de archivos desde un sistema de archivos que permite los caracteres comodín en nombres de archivo o de directorio.

Ejemplos

Archivo de opciones:

```
WILDCARDSARELITERAL YES
```

Línea de mandatos:

Suponiendo que el sistema de archivos permita caracteres comodín en las vías de acceso, los siguientes son ejemplos de archivos de una especificación de lista de archivos que se pueden procesar correctamente si `WILDCARDSARELITERAL` se establece en `YES`.

Supongamos que el mandato emitido es `dsmc sel -filelist=/home/user1/important_files`, donde `important_files.txt` contiene la lista de archivos a procesar.

`important_files.txt` contiene la siguiente lista de archivos:

```
/home/user1/myfiles/file?9000
/home/user1/myfiles/?file
/home/user1/myfiles/**README**version2
/home/user1/myfiles/ABC?file*
```

Si `WILDCARDSARELITERAL` y `QUOTESARELITERAL` se establecen en `YES`, las siguientes copias de seguridad se pueden procesar satisfactoriamente:

```
/home/user1/myfiles/"file?
/home/user1/myfiles/?file'
/home/user1/myfiles/**"README Tomorrow"**
/home/user1/myfiles/file*
```

Información relacionada

Para obtener información acerca de la opción `filelist`, consulte “`Filelist`” en la página 439.

Para obtener información sobre la sintaxis para especificaciones de archivo, consulte “Especificación de cadenas de entrada que contengan espacios en blanco o comillas” en la página 145.

“Quotesareliteral” en la página 527

Capítulo 11. Utilización de los mandatos

El cliente de copia de seguridad y archivado proporciona una interfaz de línea de mandatos (CLI) que puede utilizar como alternativa a la interfaz gráfica de usuario (GUI). En este tema se describe cómo iniciar o finalizar una sesión de mandatos de cliente y cómo escribir los mandatos.

A continuación se muestra una lista de tareas relacionadas con la especificación de mandatos.

- “Inicio y finalización de una sesión de mandatos de cliente” en la página 658
- “Especificación de los nombres, opciones y parámetros de los mandatos de cliente” en la página 660
- “Caracteres comodín” en la página 663

En la siguiente tabla se muestran una lista alfabética de los mandatos y una breve descripción.

Tabla 79. Mandatos

Mandato	Descripción
archive “Archive” en la página 664	Archiva los archivos de una estación de trabajo en el almacenamiento de IBM Spectrum Protect.
backup fastback “Copia de seguridad de FastBack” en la página 669	Volúmenes de copias de seguridad especificados por las opciones <code>fbpolicyname</code> , <code>fbclientname</code> y <code>fbvolumename</code> para una retención larga.
backup group “Backup Group” en la página 672	Crea y realiza una copia de seguridad de un grupo que contiene una lista de archivos de uno o más orígenes de espacio de archivos en un espacio de archivos virtual en el servidor de IBM Spectrum Protect.
backup image “Backup Image” en la página 674	Crea una copia de seguridad de imágenes de uno o varios sistemas de archivos o volúmenes lógicos que especifique.
backup nas “Backup NAS” en la página 680	Crea una copia de seguridad de imágenes de uno o varios sistemas de archivos pertenecientes a un servidor de archivos NAS (Almacenamiento conectado en red).
backup vm “Backup VM” en la página 683	Realiza una copia de seguridad de máquinas virtuales especificadas en la opción <code>vm list</code> .
cancel process “Cancel Process” en la página 691	Visualiza una lista de los procesos actuales de copia de seguridad de imágenes y de restauración NAS (si se ha activado el soporte de NDMP) para los que el usuario de administración dispone de autorización.
cancel restore “Cancel Restore” en la página 692	Muestra una lista de sesiones de restauración reiniciables donde puede seleccionar una para cancelarla.
delete access “Delete Access” en la página 692	Suprime reglas de autorización para archivos que se han almacenado en el servidor. En los clientes que admiten la copia de seguridad de imágenes, este mandato suprime reglas de autorización para imágenes que se han almacenado en el servidor.
delete archive “Delete Archive” en la página 693	Suprime copias archivadas del almacenamiento del servidor de IBM Spectrum Protect.

Tabla 79. Mandatos (continuación)

Mandato	Descripción
delete backup “Delete Backup” en la página 694	Suprime archivos de copia de seguridad activos e inactivos del almacenamiento del servidor de IBM Spectrum Protect.
delete filespace “Delete Filespace” en la página 698	Suprime los espacios de archivos del almacenamiento del servidor de IBM Spectrum Protect.
delete group “Delete Group” en la página 699	Suprime una copia de seguridad de grupo en el servidor de IBM Spectrum Protect.
expire “Expire” en la página 701	Desactiva los objetos de copia de seguridad indicados en la especificación de archivo o mediante la opción <code>filelist</code> .
help “Help” en la página 703	Muestra una tabla de contenido de los temas de ayuda para el cliente de línea de mandatos.
incremental “Incremental” en la página 704	Realiza la copia de seguridad de todos los archivos o directorios nuevos o cambiados del dominio de cliente predeterminado o de los sistemas de archivos, directorios o archivos que ha especificado, a menos que los haya excluido de los servicios de copia de seguridad.
loop “Loop” en la página 712	Inicia una sesión interactiva de mandatos.
macro “Macro” en la página 713	Ejecuta mandatos dentro del archivo de macro que especifique.
monitor process “Monitor Process” en la página 714	Visualiza una lista de los procesos actuales de copia de seguridad de imagen y de restauración NAS desde la que puede seleccionar el proceso que desea cancelar.
preview archive “Preview Archive” en la página 715	Simula un mandato de archivado sin enviar datos al servidor.
preview backup “Previsualizar copia de seguridad” en la página 716	Simula un mandato de copia de seguridad sin enviar datos al servidor.
query access “Query Access” en la página 717	Visualiza una lista de las reglas actuales de autorización.
query archive “Query Archive” en la página 718	Visualiza una lista de las copias archivadas.
query backup “Query Backup” en la página 720	Visualiza una lista de las versiones de copia de seguridad.
query backupset “Query Backupset” en la página 723	Consulta un juego de copias de seguridad de un archivo local o del servidor de IBM Spectrum Protect. En los clientes que admiten dispositivos de cinta, este mandato puede consultar un juego de copias de seguridad de un dispositivo de cinta.
query filespace “Query Filespace” en la página 727	Visualiza una lista de los espacios de archivos del almacenamiento de IBM Spectrum Protect. También puede especificar un único nombre de espacio de archivos para su consulta.
query group “Query Group” en la página 729	Visualiza información acerca de las copias de seguridad de grupo y sus miembros.
query image “Query Image” en la página 731	Visualiza información acerca de las copias de seguridad de imagen.
query inclexcl “Query Inclexcl” en la página 733	Visualiza una lista de sentencias de inclusión/exclusión en el orden en que se procesan durante las operaciones de copia de seguridad/archivado.

Tabla 79. Mandatos (continuación)

Mandato	Descripción
query mgmtclass “Query Mgmtclass” en la página 734	Muestra información sobre las clases de gestión disponibles.
query node “Query Node” en la página 735	Muestra todos los nodos en los que un identificador de usuario de administración dispone de autorización para realizar operaciones.
query options “Query Options” en la página 736	Muestra todas o parte de las opciones y sus valores actuales.
query restore “Query Restore” en la página 737	Visualiza una lista de las sesiones de restauración reiniciables de la base de datos del servidor.
query schedule “Query Schedule” en la página 738	Muestra información sobre los eventos planificados para el nodo.
query session “Query Session” en la página 738	Muestra información acerca de la sesión como, por ejemplo, el nombre de nodo actual, cuándo se ha establecido la sesión, información del servidor e información de conexión del servidor.
query systeminfo “Query Systeminfo” en la página 739	Recopila información del sistema de IBM Spectrum Protect y envía esta información a un archivo o la visualiza en la consola.
query vm “Query VM” en la página 741	Verifica las copias de seguridad correctas de las máquinas virtuales del servidor de copia de seguridad vStorage.
restart restore “Restart Restore” en la página 743	Muestra una lista de sesiones de restauración reiniciables donde puede seleccionar una para reiniciarla.
restaurar “Restore” en la página 744	Restaura copias de versiones de copias de seguridad de los archivos desde el servidor de IBM Spectrum Protect.
restore backupset “Restore Backupset” en la página 749	Restaura un juego de copias de seguridad desde el servidor de IBM Spectrum Protect o un archivo local. En los clientes que admiten dispositivos de cinta, este mandato puede restaurar un conjunto de copias de seguridad de un dispositivo de cinta.
restore group “Restore Group” en la página 756	Restaura miembros específicos o todos los miembros de una copia de seguridad de grupo.
restore image “Restore Image” en la página 758	Restaura un sistema de archivos o una copia de seguridad de imágenes de volumen RAW.
restore nas “Restore NAS” en la página 762	Restaura la imagen de un sistema de archivos que pertenece a un servidor de archivos NAS (Network Attached Storage).
restore vm “Restore VM” en la página 764	Restaura una copia de seguridad de la máquina virtual completa y devuelve los archivos de copia de seguridad de la máquina virtual completa al directorio vmbackdir del servidor de copia de seguridad vStorage.
retrieve “Retrieve” en la página 770	Recupera copias archivadas del servidor de IBM Spectrum Protect.
schedule “Schedule” en la página 773	Inicia el planificador cliente de la estación de trabajo.
selective “Selective” en la página 775	Realiza copia de seguridad de los archivos seleccionados.

Tabla 79. Mandatos (continuación)

Mandato	Descripción
set access “Set Access” en la página 778	Otorga autorización a otro usuario para que éste pueda acceder a sus versiones de copia de seguridad o a sus copias archivadas. En los clientes que admiten la copia de seguridad de imágenes, este mandato puede establecer reglas de autorización para imágenes que se han almacenado en el servidor.
set event “Set Event” en la página 781	Permite especificar las circunstancias que se deben dar cuando se suprimen datos archivados.
set netappsvm Set Netappsvm	Asocia las credenciales de inicio de sesión para un servidor de gestión de clústeres con una máquina virtual de almacenamiento NetApp y el nombre del SVM de datos (Vserver de datos). Este mandato debe especificarse antes de crear una copia de seguridad incremental por diferencia de instantánea de un volumen de NetApp en clúster.
set password “Establecer contraseña” en la página 784	Cambia la contraseña de IBM Spectrum Protect de la estación de trabajo.

Para que el funcionamiento sea correcto, el nodo was debe restaurarse en la misma ubicación y con el mismo nombre.

Importante: Para evitar problemas, restaure los datos sólo en el nodo de Network Deployment Manager o en el nodo de Application Server.

Referencia relacionada:

“Lectura de diagramas de sintaxis” en la página xiv

Inicio y finalización de una sesión de mandatos de cliente

Una sesión de mandatos de cliente se puede iniciar o finalizar en modalidad de proceso por lotes o en modalidad interactiva.

Utilice la modalidad de proceso por lotes si desea entrar un *único* mandato de cliente. El cliente de copia de seguridad y archivado procesa el mandato y vuelve al indicador de mandatos.

Utilice la modalidad interactiva si desea entrar una *serie* de mandatos. Puesto que el cliente establece una sola vez la conexión con el servidor para la modalidad interactiva, el conjunto de mandatos se puede procesar más rápidamente. El cliente procesa los mandatos y vuelve al indicador de Protect>.

Proceso de mandatos en modalidad por lotes

Algunas opciones *sólo* son válidas en la línea de mandatos inicial pero no en modalidad interactiva. Por lo general, estas opciones afectan al funcionamiento de toda la sesión.

Por ejemplo, el mandato **dsmc query session -errorlogname=myerror.log** se acepta y asigna un nombre a la anotación de errores. Sin embargo, se acepta solamente porque aparece en el mandato inicial, aunque la opción no es válida para el mandato de consulta.

También hay algunas opciones que son siempre válidas en la línea de mandatos inicial, así como en mandatos individuales en la modalidad interactiva. Por ello, algunas opciones se aceptan en la línea de mandatos inicial aunque no tienen efecto en el mandato que se especifica. Por ejemplo, **dsmc query session -subdir=yes** es un mandato válido, pero en este caso la opción *-subdir* no tiene efecto en el mandato que se ha especificado.

Si especifica un *único* mandato en modalidad de proceso por lotes, deberá incluir, delante de éste, el nombre del programa ejecutable, **dsmc**. Por ejemplo, para procesar el mandato **incremental** en la modalidad por lotes, escribiría:

```
dsmc incremental
```

Cada vez que especifique un mandato, el cliente de copia de seguridad y archivado le preguntará si la opción *passwordaccess* se ha establecido en *prompt* y si la autenticación del servidor se ha establecido en *On*. Escríbala y pulse Intro.

También se puede entrar la contraseña mediante la opción *password* con un mandato, pero la contraseña aparece en la pantalla. Por ejemplo, si la contraseña es *secreto*, se entra:

```
dsmc incremental -password=secreto
```

Si establece la opción *passwordaccess* en *generate* en el archivo *dsm.opt*, no es necesario que especifique la contraseña con el mandato. El cliente solo solicita la contraseña si el usuario está inscribiendo la estación de trabajo en un servidor o si está modificando manualmente la contraseña.

Conceptos relacionados:

Capítulo 10, “Opciones de proceso”, en la página 313

Proceso de mandatos en modalidad interactiva

Utilice la modalidad *interactiva* (o la modalidad de *bucle*) para especificar series de mandatos.

Escriba **dsmc** en la línea de mandatos y pulse Intro. Cuando aparezca el indicador de mandatos *Protect>*, escriba el nombre del mandato y pulse Intro. No preceda cada mandato con el nombre del programa ejecutable, **dsmc**. Otra alternativa consiste en escribir **dsmc loop** en la línea de mandatos para iniciar una sesión de mandatos de cliente en modalidad interactiva. **Loop** es el mandato predeterminado de **dsmc**.

Si se necesita una contraseña, el cliente de copia de seguridad y archivado la solicita antes de que entre el primer mandato.

Escriba el identificador de usuario y la contraseña y pulse Intro.

También puede especificar la contraseña mediante la utilización de la opción *password* con el mandato **loop**, pero la contraseña aparecerá en la pantalla. Por ejemplo, si la contraseña es *secreto*, se entra:

```
dsmc loop -password=secreto
```

Para finalizar una sesión interactiva, escriba *quit* en el indicador.

Nota para los clientes UNIX y Linux:

En la modalidad de bucle, después de una operación de restauración directamente desde cinta, el punto de montaje no se libera por si se realizan solicitudes de restauración adicionales de dicho volumen. Si solicita una operación de copia de seguridad en la misma sesión y dicho punto de montaje es el único que está disponible, la operación de copia de seguridad se interrumpirá con el mensaje siguiente:

Esperando a que se monte un medio fuera de línea.

En este caso, el punto de montaje no se libera hasta que se cumple una de las condiciones siguientes:

- Se satisface el límite MOUNTRETENTION de la clase de dispositivo.
- Se satisface el período de inactividad (idletimeout) del cliente.
- La sesión de bucle dsmc se cierra una vez que ha finalizado la operación de restauración, lo que permite iniciar otra sesión en modalidad de bucle para realizar la operación de copia de seguridad.

Especificación de los nombres, opciones y parámetros de los mandatos de cliente

Un mandato de cliente incluye uno o varios de estos componentes: *nombre del mandato*, *opciones* y *parámetros*. Las secciones que aparecen a continuación describen cada uno de estos componentes.

Nombre de mandato

La primera parte de un mandato es el nombre de mandato. El nombre de mandato consiste en una única palabra, como **help** o **schedule** o una palabra de acción y un objeto para esa acción, tal como **query archive**.

Escriba el nombre completo del mandato o la abreviatura mínima.

Por ejemplo, puede entrar cualquiera de las siguientes versiones del mandato **query schedule**:

```
query schedule
q sc
q sched
query sc
```

Opciones

Cuando escriba opciones con un mandato, anteponga siempre un guión (-) a la opción. No incluya ningún espacio entre el guión y el nombre de la opción.

Pueden entrarse las opciones de los mandatos en cualquier orden, antes o después de la especificación de archivo. Separe las diferentes opciones con un espacio en blanco.

Existen dos grupos de opciones que puede utilizar con los mandatos: opciones del cliente (se establecen en el archivo de opciones) u opciones de mandatos de cliente (se utilizan en la línea de mandatos).

- **Opciones de cliente:** grupo de opciones que se establecen en el archivo de opciones del cliente. Puede modificar temporalmente una opción en el archivo de opciones del cliente cuando especifica la opción con un mandato en la línea de mandatos.

- **Opciones de línea de mandatos:** utilice una opción de mandato de cliente *sólo* cuando especifique la opción con un mandato en la línea de mandatos. No puede establecer estas opciones en un archivo de opciones.

Conceptos relacionados:

“Consulta de opciones del cliente” en la página 345

Opciones en la modalidad interactiva

En la modalidad interactiva, las opciones que especifique en la línea de mandatos inicial modificarán temporalmente el valor que ha especificado en el archivo de opciones.

Este valor seguirá aplicándose durante toda la sesión interactiva a menos que un valor distinto lo modifique en un mandato interactivo determinado.

Por ejemplo, si establece la opción `subdir` en *yes* en el archivo `dsm.opt` o en el archivo `dsm.sys` y especifica `-subdir=no` en la línea de mandatos inicial, el valor `-subdir=no` seguirá en vigor durante la totalidad de la sesión interactiva a menos que lo modifique temporalmente mediante el valor `-subdir=yes` en un mandato interactivo determinado. Sin embargo, si el valor `subdir=yes` sólo se especifica en la sesión interactiva, sólo afectará al mandato en el que se ha especificado. Cuando ese mandato se haya completado, el valor volverá a establecerse en `subdir=no`, el valor que tenía al inicio de la sesión interactiva.

Parámetros

Los mandatos pueden tener parámetros obligatorios, parámetros optativos o pueden no tener parámetros.

Los obligatorios proporcionan la información necesaria para realizar una tarea. El que más se utiliza es la especificación de archivo.

Por ejemplo, si desea realizar el archivado de un archivo denominado `budget.fin` desde el directorio `project`, debe especificar lo siguiente:

```
dsmc archive /project/budget.fin
```

Algunos mandatos tienen parámetros optativos. Si no se entra el valor de un parámetro opcional, el cliente de copia de seguridad y archivado utiliza el valor predeterminado. Por ejemplo, el mandato **restore** tiene un parámetro obligatorio, **especificaciónarchivoorigen**, que indica la vía de acceso y el nombre de archivo del almacenamiento que desea restaurar. El parámetro opcional, **destinationfilespec**, especifica la vía de acceso donde desea colocar los archivos restaurados. Si no se especifica una **especificaciónarchivodestino**, el cliente restaura los archivos en la vía de acceso de origen. Si desea restaurar los archivos en un directorio *distinto*, especifique un valor para **especificaciónarchivodestino**.

Ejemplo: restaurar el archivo /project/budget.fin en la nueva ruta /newproj/newbudg.fin

```
dsmc restore /project/budget.fin /newproj/
```

Los parámetros deben entrarse según el orden indicado en el diagrama de sintaxis del mandato.

Sintaxis de especificación de archivo

A continuación se presentan diversas reglas de sintaxis que deberá conocer al especificar parámetros de especificación de archivo, como **filespec**, **sourcefilespec** y **destinationfilespec**.

A continuación se muestran las reglas de sintaxis:

- No utilice caracteres comodín como parte del nombre de espacio de archivos ni al indicar **espacioarchivosdestino**. La única excepción a esta regla es el mandato **set access**, donde se permiten caracteres comodín en los dos niveles más inferiores de la especificación de archivo.

Ejemplo: Permitir el acceso a todos los archivos de todos los directorios dentro y subordinados en el directorio /home:

```
set access backup /home/* * *  
set access backup /home/*/* * *
```

Con los clientes UNIX, no utilice caracteres comodín para el nombre de la ruta del directorio, por ejemplo:

```
/home/j*asler/file1.c
```

- Existe un número máximo de especificaciones de archivo por mandato:
 - Los mandatos **Query** sólo admiten una especificación de archivo.
 - Los mandatos **restore** y **retrieve** pueden aceptar una especificación de archivo de origen y una especificación de archivo de destino.
 - Existe un límite de 20 operandos en algunos mandatos. Este límite es para evitar un número excesivo de sesiones causado cuando el procesador de mandatos de shell de UNIX expande los caracteres comodín.

Puede impedir que la expansión del shell supere el límite de 20 operandos especificando entre comillas los caracteres de expansión de la especificación de archivo de origen para los mandatos restore.

Nota: El efecto secundario de la utilización de comillas es la generación de una restauración sin consulta.

Puede utilizar la opción `removeoperandlimit` para especificar que el cliente de copia de seguridad y archivado ha de eliminar el límite de 20 operandos. Si especifica la opción `removeoperandlimit` con los mandatos **incremental**, **selective** o **archive**, no se aplicará el límite de 20 operandos, y las únicas restricciones serán los recursos disponibles u otros límites del sistema operativo.

- La longitud de una especificación de archivo está limitada.
 - En AIX, Solaris y Mac: el número máximo de caracteres en un nombre de archivo es 255. La longitud máxima combinada del nombre del archivo y del nombre de la ruta es de 1024 caracteres. La representación Unicode de un carácter puede ocupar varios bytes, de modo que el número máximo de caracteres que un nombre de archivo contiene puede variar.
 - En Linux: la longitud máxima de un nombre de archivo es 255 bytes. La longitud máxima combinada del nombre del archivo y del nombre de la vía de acceso es de 4096 bytes. Esta longitud coincide con el valor `PATH_MAX` soportado por el sistema operativo. La representación Unicode de un carácter puede ocupar varios bytes, por lo tanto, el número máximo de caracteres de los que consta un nombre de vía de acceso y de archivo puede variar. La limitación real es el número de bytes de los componentes de vía de acceso y archivo, que podría corresponder a un número de caracteres igual.
- En Linux: para las operaciones de archivado o recuperación, la longitud máxima que puede especificar para un nombre de vía de acceso y de archivo (combinado) sigue siendo de 1024 bytes.

- Cuando especifique **sourcefilespec**, si el nombre del directorio acaba con `/`, entonces se presupone `/*`.

Cuando se especifica una **destinationfilespec**, si el nombre finaliza con `/`, se considera que es un directorio; de otro modo, se considera que es un archivo.

En el ejemplo siguiente se muestran estas dos reglas: Aunque mydir y yourdir son directorios, el mandato no se ejecutará correctamente porque se presupone /* a continuación de mydir, y se considera que yourdir es un archivo.

```
restore /home/mydir/ /away/yourdir
restore c:\home\mydir\ c:\away\yourdir
```

- Si una especificación de archivo no comienza con un delimitador de directorio, se presupone que la especificación de archivo es un subdirectorio del directorio de trabajo actual. El cliente añade la especificación de archivo al directorio de trabajo para crear la vía de acceso completa.

Por ejemplo, si el directorio de trabajo actual es /home/me y el mandato es dsmc res "/fs/dir1/*" mydir/, la vía de acceso de restauración completa es la siguiente: /home/me/mydir

- El único mandato que acepta un nombre de espacio de archivos simple es el mandato **incremental**. El ejemplo siguiente es válido:

```
dsmc i /Users
```

El ejemplo siguiente no es válido, ya que el mandato es el mandato **selective**:

```
dsmc sel /Users
```

Referencia relacionada:

"Filelist" en la página 439

"Removeoperandlimit" en la página 528

Caracteres comodín

Utilice los caracteres comodín cuando quiera especificar varios archivos con nombres similares en *un* mandato. Si no los utiliza, tendrá que repetir el mandato para cada archivo.

En un mandato, los caracteres comodín pueden utilizarse *sólo* en el nombre o la extensión del archivo. No puede utilizarlos para especificar archivos de destino, sistemas de archivos o nombres de servidor. No puede especificar un directorio cuyo nombre contenga un asterisco (*) o un signo de interrogación (?).

Los caracteres comodín válidos que pueden utilizarse son los siguientes:

- * Asterisco: representa cero o más caracteres.
- ? Interrogante: representa cualquier único carácter que se encuentre en la posición del comodín.

La tabla siguiente muestra ejemplos de cada carácter comodín.

Tabla 80. Caracteres comodín

Patrón	Coincide con	No coincide con
Asterisco (*)		
ab*	ab, abb, abxxx	a, b, aa, bb
ab*rs	abrs, abtrs, abrsrs	ars, aabrs, abrss
ab*ef*rs	abefrs, abefghrs	abefr, abers
abcd.*	abcd.c, abcd.txt	abcd, abcdc, abcdtxt
Signo de interrogación (?)		
ab?	abc	ab, abab, abzzz
ab?rs	abfrs	abrs, abllrs

Tabla 80. Caracteres comodín (continuación)

Patrón	Coincide con	No coincide con
ab?ef?rs	abdefjrs	abefrs, abdefrs, abefjrs
ab??rs	abcdrs, abzzrs	abrs, abjrs, abkkrs

Importante: Utilice un asterisco (*) en lugar de una interrogación (?) como carácter comodín cuando intente buscar la coincidencia de un patrón en una página de códigos de varios bytes con el fin de evitar que se produzcan resultados no esperados.

Nota: En la modalidad de proceso por lotes, especifique entre comillas los valores que contengan caracteres comodín. De lo contrario, los shells de UNIX expanden los caracteres comodín que no están entrecomillados y es fácil exceder el límite de 20 operandos. Es más eficiente dejar que el cliente procese las especificaciones de archivo comodín porque se necesitan menos interacciones de servidor para completar la tarea. Por ejemplo:

```
dsmc selective "/home/me/*.c"
```

Consulta de mandatos de cliente

Las secciones que figuran a continuación contienen información detallada sobre cada uno de los mandatos del cliente de copia de seguridad y archivado.

La información sobre cada mandato incluye lo siguiente:

- Una descripción del mandato.
- Un diagrama de sintaxis del mandato.
- Descripciones detalladas de los parámetros del mandato. Si el parámetro es una constante (un valor que no cambia), la abreviatura mínima aparece en letras mayúsculas.
- Ejemplos de cómo utilizar el mandato.

Archive

El mandato **archive** archiva un solo archivo, los archivos seleccionados o todos los archivos de un directorio y sus subdirectorios en un servidor.

Las copias archivadas que desee conservar en su condición actual. Para liberar espacio de almacenamiento de la estación de trabajo, suprima los archivos según los vaya archivando mediante la opción `deletfiles`. Recupere las copias archivadas en la estación de trabajo siempre que las necesite de nuevo.

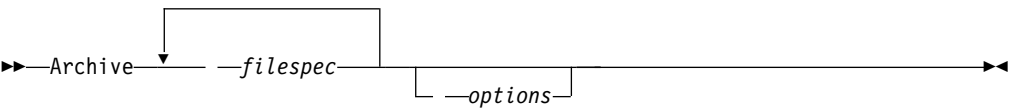
Utilice la opción `snapshotroot` con el mandato **archive** junto con una aplicación de otro proveedor de software independiente que proporcione una instantánea de un volumen lógico para asociar los datos de la instantánea local con los datos del espacio de archivos reales que se almacenan en el servidor de IBM Spectrum Protect. La opción `snapshotroot` no proporciona ningún recurso para tomar una instantánea de volumen, solo para gestionar los datos que ha creado una instantánea de volumen.

Sólo AIX: puede activar el archivado de archivos basado en instantáneas mediante la utilización de la opción `snapshotproviderfs=JFS2`.

Clientes soportados

Este mandato es válido para todos los clientes.

Sintaxis



Parámetros

filespec

Especifica la vía de acceso y el nombre del archivo que se desea archivar. Utilice caracteres comodín para incluir un grupo de archivos o todos los archivos de un directorio.

Para incluir varias especificaciones de archivos, separe cada parámetro de *filespec* con un carácter de espacio. Si se incluyen varias especificaciones de archivo, y dos o más de las especificaciones tienen directorios padre comunes, entonces es posible archivar los objetos de directorio comunes más de una vez. Las condiciones bajo las que este comportamiento ocurre son dependientes del tiempo de ejecución, pero el comportamiento por sí mismo no tiene efectos adversos.

Por ejemplo, si la especificación de archivo es `/home/amr/ice.doc` `/home/amr/fire.doc`, entonces se pueden archivar `/home` y `/home/amr` dos veces. Los objetos de archivo `ice.doc` y `fire.doc` se archivan solo una vez.

Si desea evitar incluir el directorio padre compartido más de una vez, utilice separar, no superponer mandatos **archive** para archivar cada especificación de archivo.

Si archiva un sistema de archivos, incluya una barra inclinada final (`/home/`).

Existe un límite de 20 operandos. Este límite previene un número excesivo de sesiones cuando el procesador de mandatos de shell de UNIX expande los caracteres comodín. Puede impedir que la expansión del shell supere el límite de 20 operandos colocando entre comillas las especificaciones de archivo que contienen caracteres comodín ("`home/docs/*`").

Puede utilizar la opción **removeoperandlimit** para especificar que se elimina el límite de 20 operandos. Si especifica la opción **removeoperandlimit**, el límite de 20 operandos no se aplica y queda restringido únicamente a los recursos disponibles u otros límites del sistema operativo. Por ejemplo, elimine el límite de 20 operandos para archivar 21 especificaciones de archivo:

```
selective -removeoperandlimit filespec1 filespec2 ... filespec21
```

Puede utilizar la opción **filelist**, en lugar de las especificaciones de archivo, para identificar qué archivos se han de incluir en esta operación. Sin embargo, estos dos métodos se excluyen mutuamente. No puede incluir parámetros de especificación de archivo y utilizar la opción **filelist**. Si se especifica la opción **filelist**, cualquiera de las especificaciones de archivo que se incluyen se ignoran.

Tabla 81. mandato Archive: opciones relacionadas

Opción	Dónde se utiliza
archmc	Sólo línea de mandatos.

Tabla 81. mandato Archive: opciones relacionadas (continuación)

Opción	Dónde se utiliza
archsylinksfile	Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
autofsrename	Sólo archivo de opciones del cliente (dsm.opt).
changingretries	Archivo de opciones del sistema cliente o línea de mandatos.
compressalways	Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
compression	Archivo dsm.sys de una stanza del servidor o línea de mandatos.
deletefiles	Sólo línea de mandatos.
description	Sólo línea de mandatos.
dirsonly	Sólo línea de mandatos.
encryptiontype	Archivo dsm.sys dentro de una stanza de servidor.
encryptkey	Archivo dsm.sys dentro de una stanza de servidor.
filelist	Sólo línea de mandatos.
filesonly	Sólo línea de mandatos.
preservelastaccessdate	Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
removeoperandlimit	Sólo línea de mandatos.
snapshotcachesize	Archivo de opciones del cliente (dsm.opt) o con la opción include.fs.
snapshotroot	Sólo línea de mandatos.
subdir	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
tapeprompt	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
v2archive	Sólo línea de mandatos.

Ejemplos

Tarea Realizar el archivado de un único archivo denominado budget en el directorio /home/proj1.

Mandato: archive /home/proj1/budget

Tarea Realizar el archivado de todos los archivos en el directorio /home/proj1 que tienen la extensión de archivo .txt.

Mandato: archive "/home/proj1/*.txt"

Tarea Realizar el archivado de todos los archivos en el árbol de directorios que encabeza el directorio /home.

Mandato: archive -subdir=yes "/home/*"

Tarea Realizar el archivado, dándose por supuesto que ha iniciado una instantánea del sistema de archivos /usr y que ha montado la instantánea como /snapshot/day1, del árbol de directorios /usr/dir1/sub1 desde la instantánea local y gestionar éste en el servidor de IBM Spectrum Protect, en el nombre de espacio de archivos /usr.

Mandato: `dsmc archive /usr/dir1/sub1/ -subdir=yes
-snapshotroot=/snapshot/day1`

Conceptos relacionados:

“Soporte para sistemas de archivos y ACL” en la página 162

Referencia relacionada:

“Snapshotproviderfs” en la página 569

Archivado de FastBack

Utilice el mandato **archive fastback** para archivar volúmenes de Tivoli Storage Manager FastBack especificados por las opciones `fbpolicyname`, `fbclientname` y `fbvolumename` para una retención a largo plazo.

Antes de utilizar este mandato, configure el cliente para realizar copias de seguridad y archivar datos de Tivoli Storage Manager FastBack. Asimismo, antes de emitir este mandato, debe existir al menos una instantánea en el repositorio de FastBack para la política de FastBack que se archiva o de la que se realiza copia de seguridad.

Si una especificación de política contiene clientes FastBack de Windows y Linux, solo se hará una copia de seguridad de los volúmenes Linux, o bien se archivarán, en el servidor de IBM Spectrum Protect mediante el cliente de copia de seguridad y archivado de Linux.

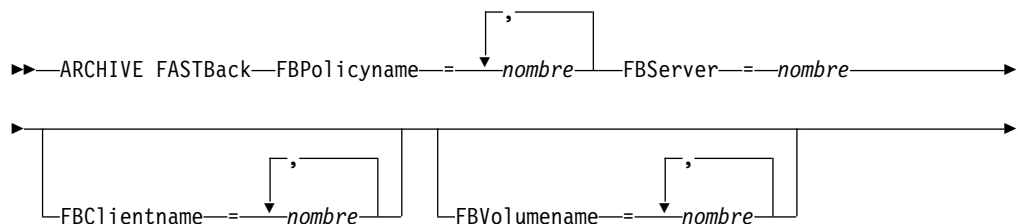
Puede utilizar las opciones de Tivoli Storage Manager FastBack para archivar las últimas instantáneas de los volúmenes siguientes:

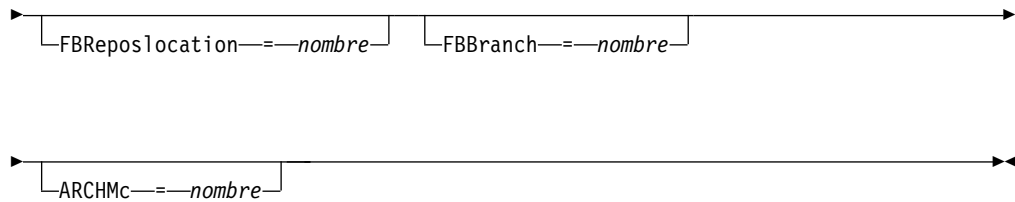
- Todos los clientes y volúmenes asociados a una política específica de FastBack o una lista de políticas de FastBack.
- Todos los volúmenes asociados a un cliente específico de FastBack o una lista de clientes de FastBack para una determinada política de FastBack.
- Un volumen o varios volúmenes específicos asociados a un cliente específico de FastBack para una política de FastBack determinada.

Clientes soportados

Esta opción es válida para clientes de Linux x86_64.

Sintaxis





Importante:

1. Como mínimo es necesario siempre un FBpolicyName.
2. Podrá especificar hasta 10 valores para FBPolicyName, si no se ha especificado ningún valor ni para FBClientName ni para FBVolumeName.
3. Si se especifica un valor de FBClientName, debe haber solo un valor para FBPolicyName.
4. Puede especificar hasta 10 valores para FBClientName si solo se ha especificado un PolicyName y no se ha especificado ningún valor para FBVolumeName.
5. Cuando se especifica la opción FBVolumeName, se puede tener solo un FBPolicy y un FBClientName especificados.
6. Podrá especificar varios FBVolumeNames si se cumple la condición 5.
7. Debe especificar siempre la opción FBReposLocation para Linux.

Parámetros

Tabla 82. mandato Archive Fastback: opciones relacionadas

Opción	Dónde se utiliza
fbpolycname "Fbpolicname" en la página 434	Línea de mandatos y planificador.
fbserver "Fbserver" en la página 436	Línea de mandatos y planificador.
fbclientname "Fbclientname" en la página 432	Línea de mandatos y planificador.
fbvolumename "Fbvolumename" en la página 438	Línea de mandatos y planificador.
fbreposlocation "Fbreposlocation" en la página 435	Línea de mandatos y planificador.
fbbranch "Fbbranch" en la página 431	Línea de mandatos y planificador.
archmc "Archmc" en la página 347	Línea de mandatos y planificador.

Ejemplos

Línea de mandatos:

El cliente de archivado y copia de seguridad está instalado en una

máquina de cliente proxy de Linux. Utilice este mandato para archivar todos los volúmenes de FastBack para todos los clientes FastBack de Linux definidos para policy1 de FastBack:

```
dsmc archive fastback -fbpolicyname=Policy1  
-fbserver=myfbserver -fbreposlocation=myfbserver@WORKGROUP
```

El nombre del servidor de FastBack, -myFbDrHub es el nombre de host abreviado del servidor de FastBack Disaster Recovery Hub donde se encuentra el repositorio.

El parámetro -fbreposlocation especifica la ubicación del repositorio. La ubicación del repositorio es necesaria. Si no proporciona la ubicación del repositorio, se produce un error en el mandato.

En este caso, FBServer debería apuntar al nombre de host abreviado del FastBack DR Hub.

Línea de mandatos:

El repositorio, rep_server1, se encuentra en el FastBack DR Hub, myFbDrHub.

```
dsmc archive fastback -fbpolicyname="Policy 1"  
-fbserver=myFbDrHub -fbreposlocation=\\myFbDrHub\rep_server1
```

La ubicación del repositorio es necesaria. Si no proporciona la ubicación del repositorio, se produce un error en el mandato.

El nombre de servidor de FastBack, -myFbDrHub, es el nombre de host abreviado del FastBack Disaster Recovery Hub donde se encuentra el repositorio.

En este caso, FBServer debería apuntar al nombre de host abreviado del FastBack DR Hub.

Línea de mandatos:

Archivar todos los volúmenes protegidos por la política de FastBack denominada policy1 del servidor de FastBack denominado basil:

```
dsmc archive fastback -fbpolicyname=policy1  
-FBServer=basil -ARCHMC="my_tsm_mgmt_class"  
-fbreposlocation=basil@WORKGROUP
```

Conceptos relacionados:

“Configuración del cliente para realizar una copia de seguridad y archivado de los datos de Tivoli Storage Manager FastBack” en la página 102

Copia de seguridad de FastBack

Utilice el mandato **backup fastback** para realizar copia de seguridad de los volúmenes de Tivoli Storage Manager FastBack especificados por las opciones fbpolicyname, fbclientname y fbvolumename para una retención a largo plazo.

Antes de utilizar este mandato, configure el cliente para realizar copias de seguridad y archivar datos de Tivoli Storage Manager FastBack. Asimismo, antes de emitir este mandato, debe existir al menos una instantánea en el repositorio de Tivoli Storage Manager FastBack para la política de Tivoli Storage Manager FastBack que se archiva o de la que se realiza copia de seguridad.

Si una especificación de política contiene clientes FastBack de Windows y Linux, solo se hará una copia de seguridad de los volúmenes Linux, o bien se archivarán, en el servidor de IBM Spectrum Protect mediante el cliente de copia de seguridad y archivado de Linux.

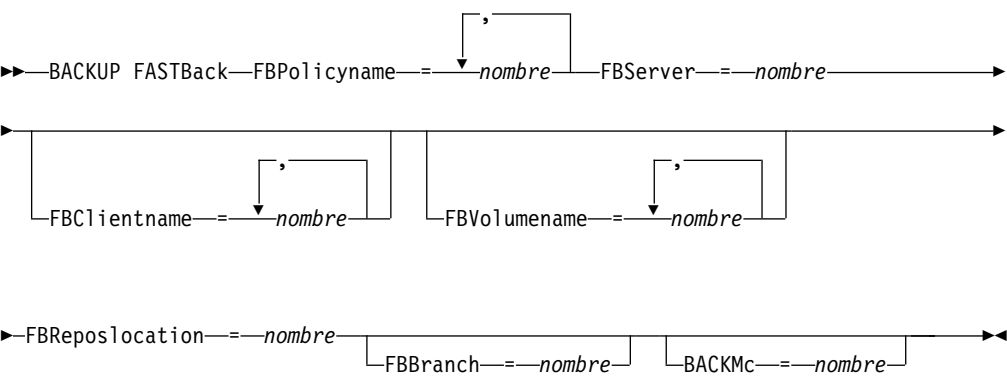
Las opciones de Tivoli Storage Manager FastBack están soportadas para la copia de seguridad incremental de las últimas instantáneas, dependiendo de la opción especificada:

- Todos los clientes y volúmenes asociados a la política de FastBack o una lista de políticas de FastBack.
- Todos los volúmenes asociados a un cliente específico de FastBack o una lista de clientes de FastBack para una determinada política de FastBack.
- Un volumen o varios volúmenes específicos asociados a un cliente específico de FastBack para una política de FastBack determinada.

Cientes soportados

Este mandato es válido para clientes Linux x86_64 configurados como proxies dedicados de Tivoli Storage Manager FastBack.

Sintaxis



Importante:

1. Como mínimo es necesario siempre un FBpolicyName.
2. Podrá especificar hasta 10 valores para FBPolicyName, si no se ha especificado ningún valor ni para FBClientName ni para FBVolumeName.
3. Si se especifica un valor de FBClientName, debe haber solo un valor para FBPolicyName.
4. Podrá especificar hasta 10 valores para FBClientName si se ha especificado solo un valor para PolicyName y ninguno para FBVolumeName.
5. Cuando se especifica la opción FBVolumeName, se puede tener solo un FBPolicy y un FBClientName especificados.
6. Podrá especificar varios FBVolumeNames si se cumple la condición 5.
7. Debe especificar la opción FBReposLocation.

Tabla 83. mandato Backup FastBack: opciones relacionadas

Opción	Dónde se utiliza
fbpolicyname "fbpolicyname" en la página 434	Línea de mandatos y planificador.
fbserver "fbserver" en la página 436	Línea de mandatos y planificador.

Tabla 83. mandato Backup FastBack: opciones relacionadas (continuación)

Opción	Dónde se utiliza
fbclientname "Fbclientname" en la página 432	Línea de mandatos y planificador.
fbvolumename "Fbvolumename" en la página 438	Línea de mandatos y planificador.
fbreposlocation "Fbreposlocation" en la página 435	Línea de mandatos y planificador.
fbbranch "Fbbranch" en la página 431	Línea de mandatos y planificador.
backmc "Backmc" en la página 359	Línea de mandatos y planificador.

Ejemplos

Línea de mandatos:

El cliente de archivado y copia de seguridad está instalado en una máquina de cliente proxy de Linux. Utilice este mandato para realizar una copia de seguridad de todos los volúmenes de FastBack para todos los clientes FastBack de Linux definidos para policy1 de FastBack:

```
dsmc backup fastback -fbpolicyname=Policy1
-fbserver=myfbserver
-fbreposlocation=myfbserver@WORKGROUP
```

La ubicación del repositorio es necesaria. Si no proporciona la ubicación del repositorio, se producirá un error en el mandato.

El nombre de servidor de FastBack, -myfbserver, es el nombre de host abreviado del servidor de FastBack donde se encuentra el repositorio.

Línea de mandatos:

El repositorio, rep_server1, se encuentra en el FastBack Disaster Recovery Hub, myFbDrHub

```
dsmc backup fastback -fbpolicyname="Policy 1"
-fbserver=myFbDrHub -fbreposlocation=\\myFbDrHub\rep_server1
```

El nombre de servidor de FastBack, -myFbDrHub, es el nombre de host abreviado del servidor de FastBack Disaster Recovery Hub donde se encuentra el repositorio.

La opción -fbreposlocation especifica la ubicación del repositorio. La ubicación del repositorio es necesaria. Si no se proporciona la ubicación de repositorio, el mandato falla.

La opción FBServer debe señalar al nombre de host abreviado del FastBack DR Hub en este caso.

Línea de mandatos:

Realizar una copia de seguridad de todos los volúmenes protegidos por la política de FastBack denominada policy1 del servidor de FastBack denominado basil:

```
dsmc backup fastback -Fbpolicyname=policy1
-FBServer=basil -BACKMC="my_tsm_mgmt_class"
-fbreposlocation=basil@WORKGROUP
```

Conceptos relacionados:

“Configuración del cliente para realizar una copia de seguridad y archivado de los datos de Tivoli Storage Manager FastBack” en la página 102

Backup Group

Utilice el mandato **backup group** para crear y realizar la copia de seguridad de un grupo que contenga una lista de archivos de uno o más orígenes de espacio de archivos en un espacio de archivos virtual en el servidor de IBM Spectrum Protect.

Sólo AIX: puede activar la copia de seguridad de grupo basada en instantáneas mediante la utilización de la opción `snapshotproviderfs=JFS2`.

Una copia de seguridad de grupo permite crear una copia de seguridad de punto en el tiempo coherente de un grupo de archivos que se gestiona como una entidad lógica individual. Los objetos del grupo están sujetos a las siguientes reglas:

- Operación de volver a vincular con clase de gestión para objetos agrupados:
 - Durante las copias de seguridad completa, todos los objetos de un grupo de copia de seguridad están asignados a la misma clase de gestión.
 - Durante las copias de seguridad diferenciales, si se especifica una nueva la clase de gestión en una sentencia incluye para un grupo de copia de seguridad existente, el comportamiento será el siguiente:
 - Los objetos nuevos y modificados del grupo de copia de seguridad están vinculados a la nueva clase de gestión.
 - Los objetos de miembro del grupo que no se modifican aparecen como si no se hubiesen vinculado a la nueva clase de gestión. Estos objetos sin modificar no se incluyen en las estadísticas **Número total de objetos revinculados** que se muestran cuando finaliza el mandato **Backup Group**.
 - Los objetos que no se han modificado se vuelven a asignar a un backup group creado recientemente y el nuevo backup group se vincula a la nueva clase de gestión. Sin embargo, el nombre de clase de gestión original todavía se muestra para los objetos de grupo que no se han modificado.
Aunque el nombre de la clase de gestión original continúe apareciendo para los objetos sin modificar, están vinculados con la nueva clase de gestión del grupo de copias de seguridad.
- Las sentencias `exclude` existentes que se aplican a cualquier archivo del grupo se pasan por alto.
- Todos los objetos del grupo se exportan juntos.
- Todos los objetos del grupo caducan al mismo tiempo, tal como se ha especificado en la clase de gestión. Ninguno de los objetos de un grupo caduca hasta que caducan los demás objetos del grupo, incluso cuando caduque otro grupo al que pertenecen.
- Si realiza copias de seguridad de grupo completas o diferenciales en un dispositivo secuencial, durante una restauración, los datos no se encontrarán en más de dos ubicaciones. Para optimizar el tiempo de restauración, realice copias de seguridad completas periódicamente para realizar la copia de seguridad de los datos en una única ubicación en los medios secuenciales.
- Durante una copia de seguridad de grupo completa, todos los datos de la lista de archivos se envían al servidor. Durante una copia de seguridad de grupo diferencial, sólo se envían al servidor los datos que han cambiado desde la última copia de seguridad completa. Los objetos de la lista de archivos que no han cambiado desde las últimas copias de seguridad completas se asignan como

miembros de la copia de seguridad de grupo diferencial. Estos datos no vuelven a enviarse al servidor, con lo que se reduce el tiempo de la copia de seguridad.

El mandato **backup group** necesita las opciones siguientes:

filelist

Especifica una lista de archivos que ha de agregarse a un nuevo grupo.

groupname

Especifica el nombre calificado al completo del grupo que contiene una lista de archivos.

virtualfsname

Especifica el nombre del espacio de archivos virtual del grupo en el que desea realizar la operación. La opción **virtualfsname** no puede ser igual a un nombre de espacio de archivos existente.

mode

Especifica si desea realizar la copia de seguridad de todos los archivos de la lista de archivos o sólo de los archivos que han cambiado desde la última copia de seguridad completa.

Nota:

1. Si falla alguno de los archivos de la copia de seguridad del grupo, fallará toda la copia de seguridad del grupo.
2. Utilice el mandato **query group** para consultar los miembros de una copia de seguridad de grupo en el servidor de IBM Spectrum Protect.
3. Utilice el mandato **restore group** para restaurar miembros específicos o todos los miembros de una copia de seguridad de grupo en el servidor.
4. A menos que esté ejecutando Mac OS X, utilice el mandato **delete group** para suprimir una copia de seguridad de grupo específica del servidor.
5. Utilice el mandato **query filepace** para visualizar nombres de espacios de archivos virtuales para el nodo que se almacenan en el servidor.
6. Una copia de seguridad de grupo puede agregarse a un juego de copias de seguridad.

Clientes soportados

Este mandato es válido para todos los clientes UNIX y Linux, a excepción de Mac OS X.

Sintaxis

►►Backup GRoup— *options* —————►►

Parámetros

Tabla 84. Mandato **backup group**: opciones relacionadas

Opción	Dónde se utiliza
filelist "Filelist" en la página 439	Sólo línea de mandatos.
groupname "Groupname" en la página 449	Sólo línea de mandatos.
mode "Mode" en la página 492	Sólo línea de mandatos.

Tabla 84. Mandato backup group: opciones relacionadas (continuación)

Opción	Dónde se utiliza
snapshotproviderfs "Snapshotproviderfs" en la página 569	Archivo de opciones del sistema (dsm.sys) en una stanza del servidor o con la opción include.fs.
virtualfsname "Virtualfsname" en la página 606	Sólo línea de mandatos.

Ejemplos

Tarea Realizar una copia de seguridad completa de todos los archivos del archivo /home/dir1/filelist1 en el nombre de espacio de archivos virtual accounting que contiene el archivo /home/group1 de líder de grupo.

Mandato:

```
backup group -filelist=/home/dir1/filelist1 -groupname=group1
-virtualfsname=/virtfs -mode=full
```

Información relacionada

"Opciones include" en la página 458

"Query Group" en la página 729

"Restore Group" en la página 756

"Delete Group" en la página 699

"Query Filespace" en la página 727

Backup Image

El mandato **backup image** crea una copia de seguridad de imagen de uno o varios volúmenes del sistema.

Puede utilizar el mandato **backup image** para hacer una copia de seguridad de volúmenes NTFS o ReFS, o bien RAW no formateados. Si un volumen tiene formato NTFS, sólo se realizará copia de seguridad de los bloques que utiliza el sistema de archivos. En volúmenes de ReFS, se realizará copia de seguridad de todos los bloques.

Si establece la opción **imagegapsize** en 0, se realizará copia de seguridad de todos los bloques, incluidos los bloques que no se utilizan situados al final del volumen.

Si especifica un sistema de archivos JFS2 de AIX para la copia de seguridad de imágenes, solo se realizará la copia de seguridad de los bloques que el sistema de archivos utiliza. Si establece la opción **imagegapsize** en cero, se realizará copia de seguridad de todos los bloques, incluidos los bloques no situados al final del volumen.

Nota:

1. Sólo AIX: de forma predeterminada, la copia de seguridad de imágenes basada en instantáneas está activada para los volúmenes JFS2. Para desactivar las

copias de seguridad de imágenes basadas en instantáneas, establezca `-snapshotproviderimage=NONE` en este mandato.

2. Para los clientes Linux, la copia de seguridad de imágenes solo se admite en las particiones que tienen el ID 0x83 o en los volúmenes lógicos creados con el gestor de volúmenes lógicos de Linux. La realización de la copia de seguridad de otras particiones, como las particiones ampliadas que contienen datos de base de datos o sistemas de archivos montados, puede generar datos de copia de seguridad no coherentes si los datos cambian durante la operación de copia de seguridad de imágenes.
3. En el cliente de Linux, no se admiten las copias de seguridad de imágenes de dispositivos DASD con modalidad de acceso de seguimiento raw en Linux on z Systems.
4. La copia de seguridad de imágenes no se admite en ningún sistema de archivos GPFS.
5. La API de IBM Spectrum Protect debe estar instalada para utilizar el mandato **backup image**.
6. Cuando cambie el atributo de un sistema de archivos JFS2 por otro gestionado por HSM, no se realizará una copia de seguridad de imágenes de ese sistema de archivos.

Importante: la hora de la última copia de seguridad incremental hace referencia a la hora del servidor y la hora de modificación de archivo hace referencia a la hora del cliente. Si la hora del cliente y del servidor no están sincronizadas, o si el cliente y el servidor están en distintos husos horarios, esto afectará a la copia de seguridad incremental por fecha y a la copia de seguridad de imagen donde `mode=incremental`.

El cliente hace copia de seguridad de los archivos que tienen fechas y horas de modificación (en el cliente) que son posteriores a la fecha y hora de la última copia de seguridad incremental del sistema de archivos en el que se almacena el archivo (en el servidor).

Si la hora del servidor va por delante de la hora del cliente, las copias de seguridad incrementales por fecha, o la copia de seguridad de imagen con `mode=incremental`, pasan por alto los archivos, que se han creado o modificado tras la última copia de seguridad incremental o de imagen con una fecha de modificación anterior a la última indicación de fecha y hora de copia de seguridad incremental.

Si la hora del cliente es posterior a la hora del servidor, se vuelve a hacer una copia de seguridad de todos los archivos creados o modificados antes de la última copia de seguridad incremental o de la copia de seguridad de imágenes y que tienen una indicación de fecha y hora de modificación posterior a la indicación de fecha y hora de la última copia de seguridad incremental. Normalmente, no se haría ninguna copia de seguridad de estos archivos, porque ya se ha realizado.

La fecha de copia de seguridad puede comprobarse con el mandato **query filespace**.

El cliente de copia de seguridad y archivado debe dar soporte al tipo de dispositivo RAW de la plataforma específica para poder realizar una copia de seguridad de imágenes de un dispositivo RAW. Solamente puede realizar una copia de seguridad de imagen en los dispositivos locales. No se admiten los dispositivos de un clúster ni los sistemas de archivos, ni tampoco los dispositivos ni los sistemas de archivos que compartan dos o varios sistemas. Si se desea

realizar una copia de seguridad de imágenes de un sistema de archivos montado en un dispositivo RAW, debe darse soporte a dicho dispositivo.

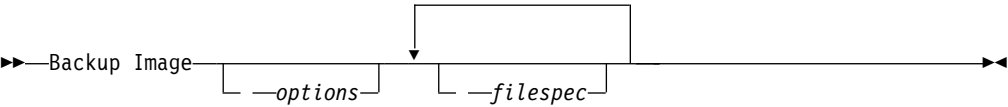
Utilice la opción **include.image** para incluir un sistema de archivos o un volumen lógico en la copia de seguridad de imágenes, o para especificar opciones específicas del volumen para la copia de seguridad de imágenes.

El mandato **backup image** utiliza la opción **compression**.

Cientes soportados

Esta opción es válida para clientes de AIX, Linux y Oracle Solaris.

Sintaxis



Parámetros

filespec

Especifica el nombre de uno o varios volúmenes lógicos. Si desea hacer una copia de seguridad de más de un sistema de archivos, separe los nombres con espacios. No utilice caracteres de coincidencia con patrón. Si no especifica un nombre de volumen, se procesarán los volúmenes lógicos que se especifican con la opción **domain.image**. Si no utiliza la opción **domain.image** para especificar los sistemas de archivos que se procesarán, aparece un mensaje de error y no se lleva a cabo ninguna copia de seguridad de imágenes.

Especifique el espacio de archivos sobre el que se monta el volumen lógico, o el nombre del volumen lógico. Si existe un sistema de archivos configurado en el sistema para un volumen determinado, no puede realizar la copia de seguridad del volumen con el nombre de dispositivo.

Por ejemplo, si el espacio de archivos /dev/lv01 está montado en el volumen /home, puede emitir backup image /home, pero backup image /dev/lv01 falla con un error:

ANS1063E Se ha especificado una vía de acceso no válida

Nota: En sistemas Sun, especifique un nombre de sistema de archivos o un nombre de dispositivos RAW (tipo de dispositivo de bloque).

Tabla 85. Mandato Backup Image: opciones relacionadas

Opción	Dónde se utiliza
asnodename "Asnodename" en la página 349	Archivo de opciones del sistema del cliente (dsm.sys) o línea de mandatos.
compressalways "Compressalways" en la página 369	Archivo de opciones del sistema del cliente (dsm.sys) o línea de mandatos.
compression "Compression" en la página 370	En el archivo de opciones del cliente o en la línea de mandatos.

Tabla 85. Mandato Backup Image: opciones relacionadas (continuación)

Opción	Dónde se utiliza
dynamicimage “Dynamicimage” en la página 410	Utilice esta opción con el mandato backup image o la opción include.image del archivo de opciones.
imagegapsize “Imagegapsize” en la página 454	Utilice esta opción con el mandato backup image , la opción include.image o en el archivo de opciones.
mode “Mode” en la página 492	Sólo línea de mandatos.
postsnapshotcmd “Postsnapshotcmd” en la página 516	Utilice esta opción con el mandato backup image , la opción include.image o en el archivo de opciones.
presnapshotcmd “Presnapshotcmd” en la página 523	Utilice esta opción con el mandato backup image , la opción include.image o en el archivo de opciones.
snapshotcachesize “Snapshotcachesize” en la página 567	Utilice esta opción con el mandato backup image , la opción include.image o en el archivo de opciones.
snapshotproviderimage “Snapshotproviderimage” en la página 570	Archivo de opciones del cliente o con la opción include.image .

Ejemplos

Tarea Realizar una copia de seguridad del espacio de archivos /home/prueba sobre el que está montado el volumen lógico y realizar una copia de seguridad de imágenes incremental que solamente efectúe una copia de seguridad de los archivos nuevos y de los archivos que se han modificado desde la copia de seguridad de imágenes completa más reciente.

```
dsmc backup image /home/test -mode=incremental
```

Tarea Realizar una copia de seguridad de imagen estática del volumen lógico que se ha montado en el directorio /home.

```
dsmc backup image /home -snapshotproviderimage=none
```

Tarea Realizar una copia de seguridad de imagen dinámica del volumen lógico que se ha montado en el directorio /home.

Mandato: dsmc backup image /home -dynamicimage=yes

Tarea Realizar una copia de seguridad de instantánea del directorio /home.

```
AIX client: dsmc backup image /home
             -snapshotproviderimage=JFS2
Cliente LINUX: dsmc backup image /home
             -snapshotproviderimage=LINUX_LVM
```

Tarea Realizar la copia de seguridad del volumen lógico RAW /dev/1v01.

```
dsmc backup image /dev/1v01
```

Información relacionada

“Imagegapsize” en la página 454

“Snapshotproviderimage” en la página 570

“Snapshotcachesize” en la página 567

“Mode” en la página 492

“Comparación de los métodos 1 y 2” en la página 201 Para determinar qué método es el adecuado para el entorno que se utiliza.

Copia de seguridad de imagen estática, dinámica y de instantánea

La copia de seguridad de imagen tradicional impide que durante la operación otras aplicaciones del sistema accedan con permiso de escritura al volumen.

Utilice la opción `dynamicimage` para realizar una copia de seguridad del volumen tal cual sin volver a montarlo como de sólo lectura. La copia de seguridad se puede dañar si las aplicaciones escriben datos en el volumen mientras se está realizando la copia de seguridad. En este caso, ejecute **fsck** después de una restauración.

La opción `dynamicimage` no se admite para volúmenes JFS2.

Solo para clientes Linux x86_64: de forma predeterminada, el cliente de archivado y copia de seguridad ejecuta una copia de seguridad de imágenes de instantánea de sistemas de archivos que residen en un volumen lógico creado por el Gestor de volúmenes lógicos de Linux, durante la cual el volumen está disponible para otras aplicaciones de sistemas. La copia de seguridad de imagen de instantánea necesita la versión 5.1 de un servidor de IBM Spectrum Protect.

Solo para clientes AIX: de forma predeterminada, el cliente de archivado y copia de seguridad ejecuta una copia de seguridad de imágenes de instantánea de volúmenes JFS2 durante la cual el volumen está disponible para otras aplicaciones del sistema. AIX permite la creación de una instantánea de un volumen JFS2 mientras todavía está en línea. La instantánea se crea dentro del mismo grupo de volúmenes que el volumen de origen. Debe asegurarse de que el grupo de volúmenes proporcione el espacio de disco libre suficiente para crear la instantánea. La instantánea contiene los bloques de datos antiguos y los datos modificados se almacenan en el volumen de origen. Utilice la opción `snapshotcachesize` con el mandato de imagen de copia de seguridad, en el archivo `dsm.sys`, o bien con la opción `include.image` para especificar un tamaño de instantánea adecuado para que todos los bloques de datos antiguos se puedan almacenar mientras se realiza la copia de seguridad de imagen..

El gestor de volúmenes lógicos (LVM) de Linux permite crear una instantánea de un volumen lógico mientras el volumen lógico continúa activado. La instantánea se crea dentro del mismo grupo de volúmenes que el volumen lógico de origen. Debe asegurarse de que el grupo de volúmenes proporcione el espacio de disco libre suficiente para crear la instantánea. La instantánea contiene los bloques de datos antiguos y los datos modificados se almacenan en el volumen lógico de origen. Utilice la opción `snapshotcachesize` con el mandato **backup image**, en el archivo `dsm.sys`, o con la opción `include.image` para especificar un tamaño de instantánea adecuado, de modo que todos los bloques de datos antiguos se puedan guardar mientras se realiza la copia de seguridad de imagen. Un tamaño de instantánea del 100% asegurará que la instantánea sea válida.

Utilización de la copia de seguridad de imagen para realizar una copia de seguridad incremental del sistema de archivos

Existen dos métodos de utilizar las copias de seguridad de imágenes para realizar copias de seguridad incrementales eficaces del sistema de archivos. Estos métodos de copia de seguridad permiten realizar restauraciones a un instante específico de los sistemas de archivos y mejorar el rendimiento de las operaciones de copia de seguridad y restauración.

La copia de seguridad sólo la puede realizar en volúmenes con formato y no en volúmenes lógicos RAW. Puede utilizar la *copia de seguridad de imágenes con la copia de seguridad incremental del sistema de archivos* o puede utilizar la *copia de seguridad de imágenes con la modalidad de copia de seguridad incremental de imagen* para realizar las copias de seguridad de los volúmenes que tienen sistemas de archivos montados.

A continuación, se muestran varios ejemplos de la utilización de la *copia de seguridad de imágenes con la copia de seguridad incremental del sistema de archivos*.

- Para realizar una copia de seguridad incremental completa del sistema de archivos: `dsmc incremental /myfilesystem`
- Para realizar una copia de seguridad de imágenes del mismo sistema de archivos: `dsmc backup image /myfilesystem`
- Para realizar copias de seguridad incrementales periódicamente: `dsmc incremental /myfilesystem`

Deberá seguir los siguientes pasos en el orden que se indica para asegurarse de que el servidor registra las adiciones y las supresiones con precisión.

Utilice este mandato para restaurar el sistema de archivos en el estado que tenía exactamente en la última copia de seguridad incremental: `dsmc restore image /myfilesystem -incremental -deletefiles`.

Durante la restauración, el cliente realiza lo siguiente:

- Restaura la imagen más reciente en el servidor.
- Suprime todos los archivos restaurados en el paso anterior que están desactivados en el servidor. Éstos son los archivos que existían en el momento de realizar la copia de seguridad de imágenes pero que después se suprimieron y grabaron en una copia de seguridad incremental.
- Restaura los archivos nuevos y modificados a partir de las copias de seguridad incrementales.

Si no realiza los pasos en el orden exacto, pueden suceder dos cosas:

1. Después de haber restaurado la imagen original, se restaurarán individualmente todos los archivos cuya copia de seguridad se ha realizado con el mandato **incremental**.
2. Si realiza una **copia de seguridad de imágenes** antes de realizar una **copia de seguridad incremental**, los archivos suprimidos de la imagen original *no* se suprimirán del sistema de archivos restaurado final.

A continuación, se muestran varios ejemplos de la utilización de la *copia de seguridad de imágenes con la modalidad de copia de seguridad incremental de imagen*.

- Para realizar una copia de seguridad de imágenes del mismo sistema de archivos: `dsmc backup image /myfilesystem`
- Para realizar una copia de seguridad de imágenes incremental del sistema de archivos: `dsmc backup image /myfilesystem -mode=incremental`

Con ello solamente se envían al servidor los archivos que se han añadido o modificado desde la copia de seguridad de imágenes más reciente.

- Para realizar copias de seguridad de imágenes completas periódicamente: `dsmc backup image /myfilesystem`
- Para restaurar la imagen: `dsmc restore image /misistemaarchivos -incremental`

Durante la restauración, el cliente de copia de seguridad y archivado pasa por alto la opción `deletefiles` cuando se utiliza la técnica de copia de seguridad de imágenes combinada con la copia de seguridad de imágenes incremental. La restauración incluirá los archivos que se suprimieron después de la última copia de seguridad de imágenes completa además de las últimas versiones de los archivos añadidos o modificados después de la copia de seguridad de imágenes más reciente.

Nota: Deberá realizar copias de seguridad de imágenes completas periódicamente en los casos siguientes. De este modo se reducirá el tiempo necesario para la restauración, ya que se aplican menos cambios de las copias de seguridad incrementales.

- Cuando un sistema de archivos ha cambiado sustancialmente (más del 40%).
- Una vez al mes.
- Según sea adecuado en su entorno.

A continuación, se indican las restricciones que tienen aplicación cuando se utiliza la copia de seguridad de imágenes con la modalidad de copia de seguridad incremental de imagen:

- El sistema de archivos no puede tener copias de seguridad incrementales completas anteriores, generadas mediante el mandato **incremental**.
- La copia de seguridad de imágenes incremental por fecha no desactiva los archivos en el servidor; por consiguiente, cuando los archivos se restauren no podrá suprimirse ninguno.
- Si se trata de la primera copia de seguridad de imágenes del sistema de archivos, se realiza una copia de seguridad de imágenes completa.
- La utilización de `mode=incremental` sólo realiza la copia de seguridad de los archivos cuya fecha ha cambiado, no de los archivos cuyos permisos han cambiado.
- Si los sistemas de archivos están funcionando completos o casi completos, puede provocarse una condición de falta de espacio durante la restauración.

Backup NAS

El mandato **backup nas** crea una copia de seguridad de imagen de uno o varios sistemas de archivos pertenecientes a un servidor de archivos NAS (Network Attached Storage), también conocido como copia de seguridad NDMP. Se le solicitará el ID de administrador de IBM Spectrum Protect.

El servidor de archivos NAS realiza el proceso de traspaso de datos externos. Se inicia un proceso del servidor para realizar la copia de seguridad.

Utilice la opción `nasnodename` para especificar el nombre de nodo del servidor de archivos NAS. El nombre del nodo NAS identifica el servidor de archivos NAS ante el servidor de IBM Spectrum Protect. El nombre del nodo NAS debe estar inscrito en el servidor. Especifique la opción `nasnodename` en el archivo de opciones del cliente (`dsm.opt`). El valor del archivo de opciones del cliente es el valor predeterminado, pero puede modificarse temporalmente en la línea de mandatos.

Utilice la opción **toc** con el mandato **backup nas** o la opción **include.fs.nas** para especificar si el servidor de IBM Spectrum Protect ha de guardar la información de la Tabla de contenido (TOC) para cada copia de seguridad del sistema de archivos. Si guarda la información de la TOC, podrá utilizar el mandato de servidor **QUERY TOC** para determinar el contenido de la copia de seguridad de un sistema de archivos con el mandato de servidor **RESTORE NODE** para restaurar archivos individuales o árboles de directorios.

También puede utilizar el cliente web de IBM Spectrum Protect para examinar todo el árbol del sistema de archivos y seleccionar los archivos y los directorios que han de restaurarse. Para crear una tabla de contenido, debe definir el atributo **tocdestination** en el grupo de copias de seguridad para la clase de gestión a la que se vincula esta imagen de copia de seguridad. La creación de TOC necesitan más procesamiento, recursos de red, espacio de agrupación de almacenamiento y, posiblemente, un punto de montaje durante la operación de copia de seguridad. Si no guarda la información de las TOC, podrá restaurar archivos individuales o árboles de directorios utilizando el mandato de servidor **RESTORE NODE**, siempre que conozca el nombre calificado al completo de cada archivo o directorio y sepa en qué imagen se ha realizado la copia de seguridad de ese objeto.

La opción **toc** sólo recibe soporte para las imágenes cuya copia de seguridad ha realizado el cliente y el servidor de la versión 5.2 o posterior.

La especificación de **mode =differential** en el mandato de servidor **BACKUP NODE** o en el mandato **backup nas** donde no exista ninguna imagen completa mostrará que se ha iniciado una copia de seguridad completa. Utilizar el mandato de servidor **QUERY PROCESS** muestra que una copia de seguridad completa está en proceso.

Utilice la opción **mode** para especificar si se realiza una copia de seguridad de imagen NAS diferencial o completa. Una copia de seguridad de imagen completa realiza una copia de seguridad de todo el sistema de archivos. El valor predeterminado es una copia de seguridad de imagen NAS diferencial en los archivos que se han modificado después de la copia de seguridad de imagen completa más reciente. Si no hay una copia de seguridad de imagen completa que pueda seleccionarse, se realiza una copia de seguridad de imagen completa. Si existe una imagen completa, tanto si es restaurable como si está caducada y está siendo mantenida debido a las imágenes diferenciales dependientes, especificar **mode =differential** envía una copia de seguridad de imágenes diferencial. Si una imagen completa se envía durante una copia de seguridad diferencial, esto queda reflejado como una imagen completa utilizando el mandato de servidor **QUERY NASBACKUP**. El mandato de servidor **QUERY NASBACKUP** también muestra imágenes NAS que son restaurables y se mostrarán imágenes completas o imágenes diferenciales como tipo de objeto.

Utilice la opción **monitor** para especificar si desea supervisar una copia de seguridad de imagen del sistema de archivos NAS y visualizar la información sobre el proceso en la pantalla.

Utilice el mandato **monitor process** para visualizar una lista de todos los procesos para los que un ID de usuario de administración tiene autorización. El ID de usuario de administración debe tener como mínimo autorización de propietario de cliente sobre el nodo NAS y sobre el nodo de la estación de trabajo cliente que están utilizando desde la línea de mandatos o desde la Web.

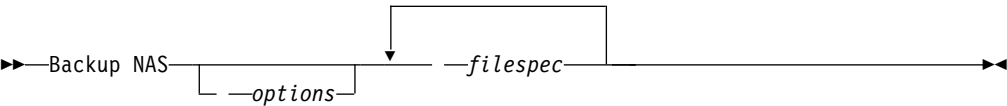
Utilice el mandato **cancel process** para detener el proceso de copia de seguridad de NAS.

Con independencia de la plataforma del cliente utilizada, las especificaciones del sistema de archivos NAS utilizan como separador la barra inclinada (/), como en el ejemplo siguiente: /vol/vol0.

Cientes soportados

Este mandato sólo es válido para los clientes AIX y Solaris.

Sintaxis



Parámetros

filespec
Especifica el nombre de uno o varios sistemas de archivos del servidor de archivos NAS. Si no especifica este parámetro, el cliente de copia de seguridad y archivado procesa todos los sistemas de archivos definidos por la opción `domain.nas`.

Si no especifica la opción *especificaciónarchivo* o la opción `domain.nas`, se utilizará el valor predeterminado **all-nas** para `domain.nas` y se realizará la copia de seguridad de todos los sistemas de archivos del servidor de archivos NAS.

Tabla 86. mandato backup NAS: opciones relacionadas

Opción	Dónde se utiliza
mode “Mode” en la página 492	Sólo línea de mandatos.
monitor “Monitor” en la página 496	Sólo línea de mandatos.
nasnodename “Nasnodename” en la página 498	Archivo de opciones del cliente (dsm.sys) o línea de mandatos.
toc “Toc” en la página 596	Línea de mandatos o con la opción <code>include.fs.nas</code> del archivo de opciones del cliente (dsm.sys).

Ejemplos

- Tarea** Realizar la copia de seguridad de imágenes NAS de todo el sistema de archivos.
Mandato: `backup nas -mode=full -nasnodename=nas1 /vol/vol0 /vol/vol2`
- Tarea** Realizar la copia de seguridad de imagen NAS de todo el servidor de archivos.
Mandato: `backup nas -nasnodename=nas1`
- Tarea** Realizar una copia de seguridad de imágenes NAS de todo el sistema de

archivos y guardar información de la tabla de contenido (TOC) para la copia de seguridad del sistema de archivos.

Mandato: `backup nas -mode=full -nasnodename=netappsj /vol/vol0 -toc=yes`

Información relacionada

“Nasnodename” en la página 498

“Toc” en la página 596

“Mode” en la página 492

“Monitor” en la página 496

“Cancel Process” en la página 691

“Domain.nas” en la página 400

Backup VM

Utilice el mandato **backup vm** para iniciar una copia de seguridad completa de una máquina virtual.



Las operaciones de máquina virtual solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments.

Realización de copia de seguridad de máquinas virtuales VMware

Utilice el mandato **backup vm** para realizar copias de seguridad de máquinas virtuales VMware.

El nodo transportador de datos de IBM Spectrum Protect hace copia de seguridad de una o varias máquinas virtuales. *El nodo transportador de datos* es el nombre que recibe una configuración en la que el cliente de archivado y copia de seguridad se ejecuta en un servidor de copia de seguridad vStorage y está configurado para proteger las máquinas virtuales de un centro virtual o un servidor ESX/ESXi. Debe configurar la máquina virtual VMware antes de utilizar este mandato. Para obtener información sobre cómo configurar la máquina virtual VMware, consulte “Preparación del entorno para copias de seguridad paralelas de máquinas virtuales VMware” en la página 220.

Una copia de seguridad de máquina virtual completa almacena una copia de seguridad de la información de configuración e imágenes de disco virtual completas de una máquina virtual. Las copias de seguridad completas de máquinas virtuales permiten una restauración completa de una máquina virtual, pero llevan más tiempo y necesitan más espacio de servidor que una copia de seguridad incremental.

Si establece la opción `vmenabletemplatebackups` en **yes**, una operación **backup vm** incluye las VM de plantilla, pero sólo si el servidor de copia de seguridad vStorage está conectado a un servidor vCenter y no a un host ESX o ESXi.

Si una instantánea falla durante el copia de seguridad, el cliente intenta realizar la copia de seguridad de la máquina virtual VMware una vez más. Para controlar el número de intentos de instantáneas totales, defina la opción `INCLUDE.VMSNAPSHOTATTEMPTS` en el archivo de opciones de cliente.

Los códigos de protección de datos se utilizan para configurar la política de copia de seguridad de las máquinas virtuales en objetos de VMware. Los códigos y las categorías el usuario utiliza uno de los métodos siguientes:

- Habilita el soporte de codificación en el nodo del transportador de datos con la opción `vmtagdatamover` y ejecuta del mandato **backup vm**.
- Utiliza la Extensión de IBM Spectrum Protect para gestionar copias de seguridad de IBM Spectrum Protect.
- Ejecuta el mandato **set vmtags** en cualquier nodo transportador de datos.

Cuando la opción `vmtagdatamover` se establece en *yes*, se realiza una copia de seguridad de todos los códigos que se asignan a una máquina virtual durante las operaciones **backup vm**. Los códigos se restauran cuando se ejecuta el mandato **restore vm**. No se efectúan copias de seguridad de los códigos que se asignan a otros objetos de inventario, por lo que no se pueden restaurar.

Para obtener más información sobre los códigos de protección de datos, consulte el apartado “Visión general de los códigos de protección de datos” en la página 792.

Una copia de seguridad de VM completa utiliza el CBT (Changed Block Tracking - Seguimiento de bloques cambiados) de VMware para crear copias de seguridad que reconocen el contenido (sólo de bloque utilizado). El cliente permite el seguimiento de bloques cambiados (CBT) en un servidor ESX o ESXi cuando empieza una copia de seguridad. CBT de VMware necesita un host ESX 4.1 (o posterior), con hardware virtual 7 (o posterior). No puede realizar copias de seguridad de VM incrementales o completas en máquinas virtuales que no soportan CBT.

Cuando CBT está habilitado, realiza el seguimiento de los cambios de disco cuando la pila de almacenamiento de servidor ESX o ESXi procesa las operaciones de E/S en los discos siguientes:

- Un disco virtual almacenado en VMFS; el disco puede ser un disco iSCSI, un disco local o un disco que está en una SAN.
- Un disco virtual almacenado en NFS.
- Una RDM que está en modalidad de compatibilidad virtual.

Cuando la pila de almacenamiento ESX o ESXi no procesa las operaciones de E/S, no se puede utilizar el seguimiento de bloques cambiados para hacer el seguimiento de cambios de disco. Los discos siguientes no pueden utilizar CBT:

- Una RDM que está en modalidad de compatibilidad física.
- Un disco al que se accede directamente desde dentro de una máquina virtual. Por ejemplo, vSphere no puede hacer el seguimiento de los cambios realizados en una LUN iSCSI a la que se accede mediante un iniciador iSCSI en la máquina virtual.

La información completa sobre los requisitos de seguimiento de bloques cambiados se describe en la publicación *VMware Virtual Disk API Programming Guide* en la documentación del producto VMware. En la guía, busque “Low Level Backup Procedures” y lea la sección “Changed Block Tracking on Virtual Disks”.

Para servidores VMware que no soporten CBT, se hace una copia de seguridad de las áreas utilizadas y de las no utilizadas del disco y se registra un mensaje informativo en el archivo `dsmerror.log`. Utilice la opción `-preview` en el mandato **backup vm** para ver el estado CBT actual. El estado de CBT tiene tres valores:

Desactivado

Indica que el parámetro de configuración de CBT (**ctkEnabled**) no está habilitado en los parámetros de configuración de la máquina virtual. **Off** es el valor predeterminado.

No soportado

Indica que la máquina virtual no da soporte a CBT. No es posible hacer copias de seguridad sólo de bloques cambiados.

Activado

Indica que la máquina virtual da soporte a CBT y que CBT está habilitado en los parámetros de configuración de la máquina virtual (`ctkEnabled=true`).

El cliente activa la CBT (se establece `ctkEnabled=true`) con cada intento de copia de seguridad. Cuando el cliente activa la CBT, continúa activada, incluso si se suprime la máquina virtual del servidor de IBM Spectrum Protect. Con la CBT habilitada, una vez realizada la primera copia de seguridad de VM completa, sólo se puede hacer una copia de seguridad de o restaurar los bloques cambiados del disco.

Si ya no realiza copias de seguridad de IBM Spectrum Protect de una máquina virtual, puede desactivar la CBT. Para desactivar la CBT, pulse el botón derecho del ratón en la máquina virtual para la que desea desactivar la CBT en el cliente vSphere. Pulse **Editar valores > Opciones > General > Parámetros de configuración**. A continuación, establezca el parámetro de configuración **ctkEnabled** como `false`.

Consejo: Puede utilizar la opción de compresión con copias de seguridad sólo si la copia de seguridad se guarda en una agrupación de almacenamiento habilitada para la eliminación de duplicados.

Especifique las opciones `-vmbackuptype` y `-mode` para indicar cómo deben realizarse las copias de seguridad. Para copias de seguridad completas, utilice `-vmbackuptype=full` y especifique cualquiera de las siguientes modalidades de opciones:

IFFull Modalidad completa-constante-incremental. En esta modalidad, se realiza una copia de seguridad en el servidor de una instantánea de todos los bloques de utilizados en los discos de una máquina virtual. Tiene que tener licencia de uso de IBM Spectrum Protect for Virtual Environments: Data Protection for VMware o IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V para utilizar esta opción.

IFIncremental

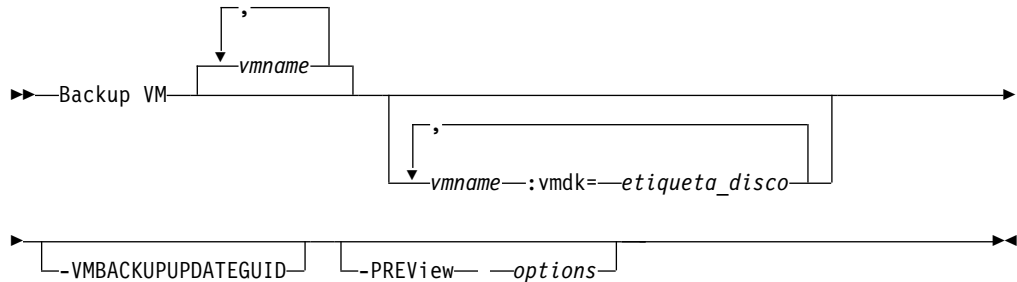
Incremental-constante-incremental. En esta modalidad, se crea una instantánea de los bloques que han cambiado desde la última copia de seguridad. Tiene que tener licencia de uso de IBM Spectrum Protect for Virtual Environments: Data Protection for VMware o IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V para utilizar esta opción.

Para obtener información sobre la estrategia de copia de seguridad incremental-constante, consulte IBM Spectrum Protect for Virtual Environments,

Clientes soportados

Este mandato sólo es válido en clientes Linux soportados instalados en un servidor de copia de seguridad vStorage que protege las máquinas virtuales VMware.

Sintaxis



Parámetros

vmname

Especifique el nombre de las máquinas virtuales de las que quiera realizar copias de seguridad. El nombre es el de visualización de la máquina virtual. Separe los nombres de distintas máquinas virtuales con comas. Si establece la opción `vmenabletemplatebackups` en **yes**, *vmname* puede especificar el nombre de una máquina virtual de plantilla para realiza una copia de seguridad.

vCenter de VMware permite que dos o más máquinas virtuales tengan el mismo nombre de visualización. No obstante, el cliente de copia de seguridad y archivado requiere que todos los nombres de máquina virtual de una configuración de servidor de vCenter sean exclusivos. Para evitar errores durante el proceso, asegúrese de que todas las máquinas virtuales tienen un nombre de visualización exclusivo.

Si no especifica *vmname*, puede identificar la máquina virtual con la opción `domain.vmfull`.

:vmdk=etiqueta_disco

Esta palabra clave es una extensión de *vmname*. Especifica la etiqueta (nombre) del disco de la máquina virtual que hay que incluir en la operación de copia de seguridad. Puede excluir un disco poniendo el operador de exclusión (-) delante de la palabra clave. Para obtener procedimientos adicionales para incluir o excluir los discos de proceso, consulte "Domain.vmfull" en la página 401, "Exclude.vmdisk" en la página 430, "Include.vmdisk" en la página 467.

-VMBACKUPUPDATEGUID

Para utilizar esta opción, tiene que tener un acuerdo de licencia para utilizar IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Esta opción actualiza el identificador exclusivo global (GUID) para la máquina virtual de la cual realiza la copia de seguridad. Este parámetro

está destinado para utilizar sólo en el siguiente caso de ejemplo: Desea restaurar una máquina virtual de la cual previamente se ha realizado una copia de seguridad, llamada ORION. Pero, antes de concluir y sustituir la copia de ORION que está ejecutándose en su entorno de producción, desea verificar la configuración de la máquina virtual restaurada antes de utilizarla para sustituir la ORION existente.

1. Restaura la máquina virtual ORION y le asigna un nombre nuevo: `dsmc restore vm Orion -vmname=Orion2`
2. Actualiza y verifica la máquina virtual ORION2 y determina que está preparada para sustituir la máquina virtual existente denominada ORION.
3. Apaga y suprime ORION.
4. Renombra ORION2, de modo que ahora se llama ORION.
5. La próxima vez que realice una copia de seguridad de ORION, utilizando una copia de seguridad incremental-constante-completa, o incremental-constante-incremental, debe añadir el parámetro **-VMBACKUPUPDATEGUID** al mandato **backup vm**. Esta opción actualizará el GUID, en el servidor IBM Spectrum Protect, de modo que el nuevo GUID se asocie a las copias de seguridad almacenadas para la máquina virtual ORION. La cadena de copias de seguridad incrementales se mantiene; no es necesario suprimir las copias de seguridad existentes y sustituirlas por las nuevas copias de seguridad.

-PREVIEW

Esta opción muestra información sobre una máquina virtual, incluidas las etiquetas de los discos duros de la máquina virtual y la información de clase de gestión de una máquina virtual.

Puede utilizar las etiquetas de disco con las palabras clave `:vmdk=` o `:-vmdk=` para incluir o excluir discos de una operación de copia de seguridad. El texto siguiente es una salida de muestra del parámetro

-preview:

```
backup vm vm1 -preview
BACKUP de VM completo de las máquinas virtuales VM1"

vmName:vm1
VMDK[1]Etiqueta: Disco duro 1
VMDK[1]Nombre: [ds5k_svt_1] tsmcetlnx14/tsmcetlnx14.vmdk
VMDK[1]Estado: Incluido
VMDK[2]Etiqueta: Disco duro 2
VMDK[2]Nombre: [ds5k_svt_1] tsmcetlnx14/tsmcetlnx14_1.vmdk
VMDK[2]Estado: Excluido: usuario,independiente,pRDM
```

Este ejemplo de salida de `-preview` muestra que VMDK 2 se ha excluido de la copia de seguridad anterior. Los discos que se han incluido en una copia de seguridad tienen el estado `Included`. Los discos que se han excluido de la copia de seguridad tienen el estado `Excluded`, seguido de un código de razón. Los códigos de razón pueden ser cualquiera de los siguientes:

usuario

Indica que el disco se ha omitido porque estaba excluido en una sentencia `domain.vmfull`, en la línea de mandatos, o en el archivo de opciones del cliente.

Independiente

Indica que el disco es un disco independiente. Los discos independientes no pueden formar parte de una instantánea, por lo

que son excluidos de las operaciones **backup vm**. Asegúrese de que la opción `vmprocessvmwithindependent` esté establecida en yes o toda la máquina virtual es omitida por la operación de copia de seguridad si contiene uno o más discos independientes.

pRDM

Indica que el disco es un disco pRDM (physical Raw Device Mapped). Los discos pRDM no pueden formar parte de una instantánea, por lo que son excluidos de las operaciones **backup vm**. Asegúrese de que la opción `vmprocessvmwithprdm` esté establecida en yes o toda la máquina virtual es omitida por una operación de copia de seguridad si contiene uno o más volúmenes RDM (Raw Device Mapping, asignación de dispositivos en bruto) suministrados en modo de compatibilidad física (pRDM).

La salida del parámetro **-preview** también muestra el nombre de la clase de gestión que está asociada con la máquina virtual, junto con información sobre el lugar en el que se ha definido la clase de gestión. Esta información puede ayudarle a verificar si los valores de dominio y de código se han definido correctamente para la clase de gestión. Por ejemplo:

`backup vm -preview`
BACKUP de VM completo de las máquinas virtuales especificadas en la opción `DOMAIN.VMFULL`.

```
1. vmName: tag_vm_2
   DomainKeyword: all-vm
   toolsRunningStatus: guestToolsNotRunning
   toolsVersionStatus: guestToolsNotInstalled
   consolidationNeeded: No
   Change Block Tracking: On
   managementClassName: STANDARD
   managementClassLocation: Node Default

   VMDK[1]Etiqueta: 'Hard disk 1' (Hard Disk 1)
   VMDK[1]Nombre: '[Raid1-lannds2] tag_vm_2/tag_vm_2.vmdk'
   VMDK[1]Estado: Incluido
...

12. vmName: vm-jean
   DomainKeyword: all-vm
   toolsRunningStatus: guestToolsNotRunning
   toolsVersionStatus: guestToolsNotInstalled
   consolidationNeeded: No
   Change Block Tracking: On
   managementClassName: MGMTCLASS1 (invalid)
   managementClassLocation: VM Tag Management Class (IBM Spectrum Protect)

   VMDK[1]Etiqueta: 'Hard disk 1' (Hard Disk 1)
   VMDK[1]Nombre: '[Raid1-lannds2] vm-jean/vm-jean.vmdk'
   VMDK[1]Estado: Incluido
```

donde:

managementClassName

Muestra el nombre de la clase de gestión a la que está vinculada la máquina virtual.

Si aparece la etiqueta "(invalid)" junto al nombre de la clase de gestión, significa que el nombre se ha especificado incorrectamente, que la clase de gestión se ha eliminado del servidor de IBM Spectrum Protect o que no se ha encontrado ningún grupo de copias de seguridad en la clase de gestión en el servidor. Si el nombre de la clase de gestión no es válido, la operación de copia de seguridad de la máquina virtual falla.

managementClassLocation

Muestra el lugar en el que se ha definido la clase de gestión. Se permiten las siguientes ubicaciones:

Nodo predeterminado

La clase de gestión se ha definido en el dominio predeterminado del nodo del centro de datos de VMware.

Opción VMMC

La clase de gestión se ha definido con la opción `vmmc`.

Opción VMCTLMC

La clase de gestión se ha definido con la opción `vmctlmc`.

Opción INCLUDE.VM

La clase de gestión se ha definido con la opción `include.vm`.

VM Tag Management Class (IBM Spectrum Protect)

La clase de gestión se ha definido como un valor de código de la categoría de códigos Management Class (IBM Spectrum Protect). Los valores de los códigos se pueden definir con valores de protección de datos en la Extensión de IBM Spectrum Protect del cliente web de vSphere, o bien utilizando herramientas como VMware vSphere PowerCLI versión 5.5 R2 o posterior.

Importante: Para visualizar la información de la clase de gestión definida por los códigos, debe definir la opción `vmtagdatamover yes` en el archivo de opciones del cliente o debe incluir el parámetro **`-vmtagdatamover=yes`** cuando ejecute el mandato **`dsmc backup vm`**. Si no ha establecido la opción `vmtagdatamover` o si se ha establecido en `no`, el cliente pasa por alto cualquier valor de código de clase de gestión y muestra la definición de la clase de gestión establecida en el dominio predeterminado del nodo del centro de datos, en la opción `vmmc` o en la opción `include.vm`.

Códigos de retorno para operaciones de copia de seguridad de máquinas virtuales

Las operaciones de copia de seguridad para máquinas virtuales pueden completarse con los códigos de retorno que se muestran en la siguiente tabla:

Código de retorno	Descripción
0	Un mandato para realizar una copia de seguridad de una o más máquinas virtuales se ha completado correctamente.
8	Un mandato para realizar una copia de seguridad de varias máquinas virtuales se ha realizado correctamente para algunas de las máquinas virtuales para las que se ha ejecutado el mandato. Examine el archivo de registro para determinar el estado de proceso de cada una de las máquinas virtuales de destino.

Código de retorno	Descripción
12	<p>Indica que se ha producido alguna de las siguientes condiciones de error:</p> <ul style="list-style-type: none"> • El mandato de copia de seguridad no ha podido realizar la copia de seguridad de ninguna de las máquinas virtuales que eran destinos de la operación de copia de seguridad. • El mandato backup ha fallado y se ha detenido antes de que se inspeccionaran todas las máquinas virtuales que se han especificado. <p>Examine el archivo de registro para determinar el motivo del error.</p>

Mandatos de ejemplo de protección de datos de vStorage API

Realizar una copia de seguridad IFIncremental de dos máquinas denominadas vm3 y vm4.

```
dsmc backup vm vm3,vm4 -vmbackuptype=fullvm -mode=ifincremental
```

Realizar una copia de seguridad IFFull de una máquina denominada vm1.

```
dsmc backup vm vm1 -vmbackuptype=fullvm -mode=iffull
```

Realizar una copia de seguridad de máquina virtual IFFull de una máquina virtual denominada vm1, pero incluyendo únicamente el disco duro 1 en la operación de copia de seguridad.

```
dsmc backup vm "vm1:vmdk=Hard Disk 1" -vmbackuptype=fullvm -mode=iffull
```

Realizar una copia de seguridad siempre incremental de una máquina virtual llamada vm1, pero excluir el disco duro 1 y el disco duro 4 de la operación de copia de seguridad.

```
dsmc backup vm "vm1:-vmdk=Hard Disk 1:-vmdk=Hard Disk 4"
-vmbackuptype=fullvm -mode=iffull
```

Realizar una copia de seguridad incremental siempre incremental de dos máquinas virtuales llamadas vm1 y vm2. En vm1, realizar una copia de seguridad sólo del disco duro 2 y el disco duro 3. En vm2, realizar una copia de seguridad de todos los discos virtuales.

```
dsmc backup vm "vm1:vmdk=Hard Disk 2:vmdk=Hard Disk 3",
vm2 -vmbackuptype=fullvm -mode=iffull
```

Realizar copias de seguridad paralelas de tipo completa-constante-incremental de las máquinas virtuales VMware que se han seleccionado para copia de seguridad utilizando los criterios de selección (parámetros de dominio) en la sentencia domain.vmfull. Defina el número máximo de copias de seguridad paralelas en 5 máquinas virtuales y 10 sesiones, y limite las copias de seguridad a 5 máquinas virtuales por host y 5 máquinas virtuales por almacén de datos.

```
dsmc backup vm -vmbackuptype=fullvm -mode=iffull -vmmaxparallel=5
-vmmaxbackupsessions=10 -vmlimitperhost=5 -vmlimitperdatastore=5
```

Enlaces relacionados para realizar copias de seguridad de máquinas virtuales VMware

- “Query VM” en la página 741
- “Restore VM” en la página 764
- “Domain.vmfull” en la página 401
- “Include.vm” en la página 466
- “Mbjrefreshthresh” en la página 489

- “Mbpctrefreshthresh” en la página 490
- “Mode” en la página 492
- “Vmbackdir” en la página 609
- “Vmbackuptype” en la página 611
- “Vmchost” en la página 612
- “Vmctlmc” en la página 614
- “Vmcpw” en la página 613
- “Vmouser” en la página 615
- “Vmlimitperdatastore” en la página 622
- “Vmlimitperhost” en la página 623
- “Vmmc” en la página 631
- “Vmmaxbackupsessions” en la página 625
- “Vmmaxparallel” en la página 627
- “Vmtagdatamover” en la página 641
- “Set Vmtags” en la página 790
- “Opciones exclude de la máquina virtual” en la página 429
- “Opciones include de la máquina virtual” en la página 465

Cancel Process

El mandato **cancel process** visualiza una lista de los procesos actuales de copia de seguridad de imagen y de restauración NAS (si se ha activado el soporte de NDMP) para los que el usuario de administración dispone de autorización. Se le solicitará el ID de administrador de IBM Spectrum Protect.

Desde la lista, el usuario de administración puede seleccionar el proceso que desea cancelar. El privilegio de propietario cliente es una autorización suficiente para poder cancelar los procesos de copia de seguridad de imagen o restauración NAS seleccionados.

Clientes soportados

Este mandato sólo es válido para los clientes AIX, Linux, y Solaris.

Sintaxis

►►—Cancel Process—◄◄

Parámetros

No hay parámetros para este mandato.

Ejemplos

Tarea Cancelar los procesos de copia de seguridad de imagen o restauración NAS actuales.

Mandato: cancel process

Cancel Restore

El mandato **cancel restore** visualiza una lista de las sesiones de restauración reiniciables de la base de datos del servidor.

Sólo puede cancelar una única sesión de restauración reinicialable al mismo tiempo. Vuelva a ejecutar el mandato **cancel restore** para cancelar más restauraciones. Para reiniciar sesiones de restauración reiniciables, utilice el mandato **restart restore**.

Utilice el mandato **cancel restore** cuando se den las circunstancias siguientes:

- No se puede hacer una copia de seguridad de archivos afectados por una restauración reinicialable.
- Las sesiones de restauración reiniciables bloquean el espacio de archivos del servidor, por lo que los archivos no se pueden traspasar fuera de los volúmenes secuenciales del servidor.

Clientes soportados

Este mandato es válido para todos los clientes.

Sintaxis

►►—Cancel Restore—◄◄

Parámetros

No hay parámetros para este mandato.

Ejemplos

Tarea Cancelar una operación de restauración.

`cancel restore`

Delete Access

El mandato **delete access** suprime reglas de autorización para los archivos que están almacenados en el servidor.

Cuando se suprime una regla de autorización, se revoca el acceso de usuario a cualquier archivo o imágenes que se haya especificado en dicha regla.

Clientes soportados

Este mandato es válido para todos los clientes.

Sintaxis

►►—Delete— —Access—◄◄

Parámetros

No hay parámetros para este mandato.

Ejemplos

Tarea Mostrar una lista de las reglas de autorización actuales y seleccionar las que se deben suprimir.

`delete access`

Vea el siguiente ejemplo de pantalla:

Índice	Tipo	Nodo	Prop.	Ruta
1	Backup	NOD01	MARTA	home/dev/proja/list/
2	Archive	NOD03	CELIA	home/fin/budg/depta/
3	Backup	NOD04	PILAR	home/plan/exp/deptc/
4	Archive	NOD05	MIGUEL	home/mfg/invn/parta/

Escriba el Índice de regla(s) para suprimir, o quit para cancelar:

Para suprimir las reglas de autorización que permiten a luie y user2s acceder a los archivos e imágenes, escriba 2 4 o 2,4 y pulse Intro.

Delete Archive

El mandato **delete archive** suprime las copias archivadas del almacenamiento del servidor de IBM Spectrum Protect. Su administrador debe concederle la autoridad para suprimir los archivos archivados.

Importante: si suprime archivos archivados, no podrá recuperarlos. Verifique que los archivos están obsoletos antes de suprimirlos.

Clientes soportados

Este mandato es válido para todos los clientes.

Sintaxis

```
➤➤ Delete ARchive [—options] [—filespec] [—{filespace—}—filespec] ➤➤
```

Parámetros

filespec

Especifica la vía de acceso y el nombre del archivo que se desea suprimir del almacenamiento. Utilice caracteres comodín para especificar un grupo de archivos o todos los archivos de un directorio. También puede utilizar la opción **filelist** para procesar una lista de archivos. El cliente de copia de seguridad y archivado abre el archivo que especifique con esta opción y procesa la lista de archivos que contiene de acuerdo con el mandato específico.

Nota: si indica *filespace*, no incluya una letra de unidad en la especificación de archivo.

{filespace}

Especifica el nombre del espacio de archivos (entre llaves) del servidor que contiene el archivo que se desea suprimir. Es el nombre de la unidad de la estación de trabajo desde la que se archivó el archivo.

Utilice el *filespace* si el nombre ha cambiado o si desea suprimir copias archivadas de otro nodo cuyas etiquetas de unidad son distintas de las suyas.

Tabla 87. mandato delete archive: opciones relacionadas

Opción	Dónde se utiliza
dateformat "Dateformat" en la página 376	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
description "Descripción" en la página 384	Sólo línea de mandatos.
filelist "Filelist" en la página 439	Sólo línea de mandatos.
noprompt "Noprompt" en la página 503	Sólo línea de mandatos.
numberformat "Numberformat" en la página 504	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
pick "Pick" en la página 512	Sólo línea de mandatos.
subdir "Subdir" en la página 581	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
tapeprompt "Tapeprompt" en la página 583	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
timeformat "Timeformat" en la página 592	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.

Ejemplos

Tarea Suprimir un archivo denominado budget.

```
dsmc delete archive /user/home/proj1/budget
```

Tarea Suprimir todas las copias archivadas del directorio /user/home/proj1 que tienen la extensión de archivo .txt.

```
dsmc del arch "/user/home/proj1/*.txt"
```

Tarea Suprimir todas las copias archivadas del directorio /user/project mediante la utilización de la opción **pick** para que se visualice una lista de las copias archivadas que coinciden con la especificación de archivo. En esta lista, puede seleccionar las versiones que se desee procesar.

```
dsmc delete archive "/user/project/*" -pick
```

Tarea Suprimir los archivos seleccionados del grupo de copias archivadas que tienen la descripción "Monthly Budgets 2010" y que se encuentran en /user/projects y sus subdirectorios.

```
dsmc delete ar "/user/projects/*" -description="Monthly Budgets 2010" -pick -subdir=yes
```

Información relacionada

Delete Backup

El mandato **delete backup** suprime archivos, imágenes y máquinas virtuales de las que se ha realizado copia de seguridad en el almacenamiento del servidor de IBM Spectrum Protect. El administrador debe otorgar autorización para suprimir objetos.

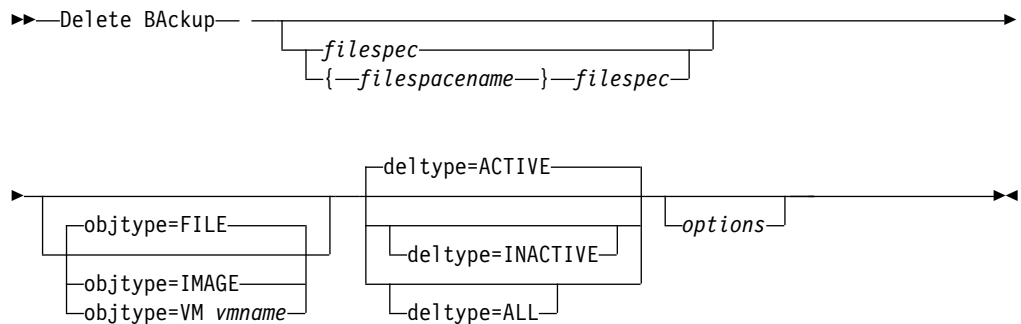
Al suprimir archivos, el servidor de IBM Spectrum Protect toma todos los archivos de copia de seguridad que cumplen las opciones `filespec` y `deltype` específicas y las desactiva. El servidor también asigna una fecha de desactivación de *infinite-minus* de forma que los archivos dejan de estar disponibles para la restauración y se depurarán, inmediatamente en la subsiguiente ejecución de caducidad de archivo. El archivo no se elimina físicamente hasta que se ejecuta el proceso de caducidad.

Importante: Después de suprimir las copias de seguridad, no podrá restaurarlas; verifique que los archivos de copia de seguridad ya no sean necesarios antes de suprimirlos. Se le solicitará si desea continuar con la operación de supresión. Si especifica **yes**, los archivos de copia de seguridad especificados se planifican para su supresión y se eliminan del almacenamiento del servidor.

Clientes soportados

Este mandato es válido para todos los clientes.

Sintaxis



Parámetros

filespace/filespec

filespec

Especifica la vía de acceso y el nombre del archivo que se desea suprimir del almacenamiento. Para especificar un archivo en otro espacio de archivos, preceda el nombre de archivo con el nombre de espacio de archivos. Utilice caracteres comodín para especificar un grupo de archivos o todos los archivos de un directorio. Separe las especificaciones de los archivos con un espacio en blanco. También puede utilizar la opción `filelist` para procesar una lista de archivos. El cliente de copia de seguridad y archivado abre el archivo que se ha especificado con esta opción y procesa la lista de archivos que contiene de acuerdo con el mandato específico.

Nota: si indica *filespace*, no incluya una letra de unidad en la especificación de archivo.

Cuando utilice `-deltype=inactive` o `-deltype=active`, haga uso de los caracteres comodín para especificar un grupo de archivos o todos los archivos de un directorio.

Al utilizar `-deltype=all`, especifique un directorio con caracteres comodín.

objtype

Especifica el tipo de objeto que desea eliminar. Puede especificar uno de los valores siguientes:

FILE

Especifica que se desea suprimir directorios y archivos. Este valor es el tipo de objeto predeterminado.

IMAGE

Especifica que se desea suprimir una copia de seguridad de imagen.

Especifica que se desea suprimir una copia de seguridad de imagen.

Objtype=image no está soportado en Mac OS X.

VM *vmname*

Especifica que desea suprimir una o varias versiones de una copia de seguridad de máquina virtual; la máquina virtual se identifica mediante el parámetro variable *vmname*. El nombre de la máquina virtual no puede contener caracteres comodín.



Las operaciones de máquina virtual solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments.

Cuando se especifica objtype=VM, no se puede utilizar la opción filelist. Especificar objtype=VM cambia el comportamiento de la opción -deltype. Cuando se especifica objtype=vm, puede utilizar -deltype=active o -deltype=inactive. No puede utilizar -deltype=all. Al especificar -deltype=inactive se muestra una lista de copias de seguridad activas e inactivas. Puede utilizar esta lista para especificar qué copias de seguridad de máquina virtual desea eliminar. Para suprimir copias de seguridad de máquinas virtuales solo activas, utilice -deltype=active.

Cuando especifica -objtype=VM, este mandato suprime únicamente las copias de seguridad de máquina virtual que se han creado con cualquiera de las siguientes modalidades: FULL, IFINCR e IFFULL. Las copias de seguridad creadas con la modalidad completa o incremental se han creado con el cliente de la versión 7.1 o anterior.

En el caso de copias de seguridad creadas con clientes de la versión 7.1 o anteriores: las copias de seguridad incrementales individuales (copias de seguridad creadas utilizando MODE=INCR) que se hayan creado después de ejecutar una copia de seguridad completa no se podrán suprimir con este mandato. Sin embargo, si suprime una copia de seguridad de imagen de máquina virtual completa (creada utilizando MODE=FULL), y si el servidor incluye alguna copia de seguridad incremental (MODE=INCR) que se creara para esta máquina virtual después de la copia de seguridad completa, al suprimir la copia de seguridad de máquina virtual completa también se suprimen los archivos que se han creado en una copia de seguridad MODE=INCR.

Si se suprime una copia de seguridad activa para una máquina virtual, la copia inactiva más reciente pasa a ser la copia de seguridad activa. Si especifica la opción -pick o -inactive, sólo se suprimirá la copia de seguridad que especifique. Si selecciona una copia de seguridad que se crea mediante MODE=IFINCR, sólo se suprimirá la copia de seguridad incremental seleccionada; no se suprimirán otras copias de seguridad incrementales para la máquina virtual.

deltype

Especifica el tipo de supresión. Especifique uno de los valores siguientes:

ACTIVE

Suprimir sólo los objetos de archivo activos. Los objetos de directorio no se suprimen. Este valor es el tipo de supresión predeterminado.

Nota: Si existe algún objeto inactivo, tras la supresión del objeto activo, el objeto inactivo más actual cambiará de inactivo a activo.

Para suprimir todas las versiones de un archivo, emita en primer lugar el mandato **delete backup** con `-deltype=inactive` y, a continuación, especifique el mandato `-deltype=active`.

INACTIVE

Suprimir sólo los objetos de archivo inactivos. Los objetos de directorios no se suprimen.

ALL

Suprimir todos los objetos activos e inactivos por debajo de un directorio determinado, incluidos todos los subdirectorios y los archivos.

Nota: No se suprime el directorio padre de los archivos y subdirectorios suprimidos. Si especifica `deltype=ALL`, no puede utilizar la opción `pick` porque `deltype=ALL` y la opción `pick` son mutuamente exclusivos.

Tabla 88. Mandato Delete Backup: opciones relacionadas

Opción	Dónde se utiliza
description "Descripción" en la página 384	Sólo línea de mandatos.
filelist "Filelist" en la página 439	Sólo línea de mandatos.
fromdate "Fromdate" en la página 446	Línea de mandatos y en la función de búsqueda de la GUI.
fromtime "Fromtime" en la página 448	Línea de mandatos y en la función de búsqueda de la GUI.
noprompt "Noprompt" en la página 503	Sólo línea de mandatos.
pick "Pick" en la página 512	Sólo línea de mandatos.
pitdate "Pitdate" en la página 512	Línea de mandatos y en la función de búsqueda de la GUI.
pittime "Pittime" en la página 513	Línea de mandatos y en la función de búsqueda de la GUI.
subdir "Subdir" en la página 581	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
tapeprompt "Tapeprompt" en la página 583	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
timeformat "Timeformat" en la página 592	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
todate "Todate" en la página 597	Línea de mandatos y en la función de búsqueda de la GUI.
totime "Totime" en la página 598	Línea de mandatos y en la función de búsqueda de la GUI.

Ejemplos

Tarea Suprimir todos los objetos de archivo activos e inactivos denominados `budget` del directorio `/data/plan/proj1`.

Mandatos:

```
delete backup /data/plan/proj1/budget.jan
-delttype=inactive
delete backup /data/plan/proj1/budget.jan
-delttype=active
```

Tarea Suprimir todos los archivos inactivos que tengan una extensión .txt y cuya copia de seguridad se ha realizado desde el directorio /data/plan/proj1 y sus subdirectorios.

Mandato: `delete backup "/data/plan/proj1/*.txt" -delttype=inactive -subdir=yes`

Tarea Suprimir los archivos activos seleccionados de los que se realiza una copia de seguridad desde el directorio /home/marymb/project. Utilice la opción -pick para que se visualice una lista de las copias de seguridad que coinciden con la especificación de archivo. En la lista, puede seleccionar qué versiones han de suprimirse.

Mandato: `delete backup "/home/marymb/project/*" -pick`

Tarea Suprimir todas las versiones activas e inactivas de los archivos y subdirectorios que se encuentran en el directorio /home/storman/myproject. A continuación, suprima todas las versiones activas e inactivas del directorio /user/myproject.

Mandato:

```
delete backup "/home/storman/myproject*"
-delttype=all
```

Referencia relacionada:

“Filelist” en la página 439

Delete Filespace

El mandato **delete filesystem** suprime espacios de archivos del almacenamiento del servidor de IBM Spectrum Protect. Un espacio de archivos es un espacio lógico del servidor que contiene archivos de los que se realizó copia de seguridad o de archivado.

Debe ser un usuario autorizado para poder utilizar este mandato.

IBM Spectrum Protect asigna un espacio de archivos por separado en el servidor para cada sistema de archivos de estación de trabajo del que ha realizado una copia de seguridad o copia archivada. El nombre del espacio de archivos es igual al nombre del sistema de archivos.

Cuando escribe el mandato **delete filesystem**, se muestra una lista de los espacios de archivos. En dicha lista, seleccione el espacio de archivos que desea suprimir.

El administrador de IBM Spectrum Protect debe otorgar autorización para suprimir un espacio de archivos. Es necesaria una autorización BACKDEL si el espacio de archivos que desea suprimir contiene versiones de copia de seguridad o la autorización ARCHDEL si el espacio de archivos contiene copias archivadas. Si el espacio de archivos contiene ambas, versiones de copia de seguridad y copias archivadas, necesita ambos tipos de autorización.

Importante: cuando se suprime un espacio de archivos, está suprimiendo todas las versiones de copia de seguridad y de copias archivadas que hay en ese espacio de

archivos. Cuando suprime un espacio de archivo, *no puede restaurar los archivos*. Verifique que los archivos están obsoletos antes de suprimirlos.

El mandato **delete filesystem** se puede utilizar para suprimir interactivamente espacios de archivos NAS del almacenamiento del servidor. Utilice la opción `nasnodename` para identificar el nodo del servidor de archivos NAS. Utilice la opción `class` para especificar la clase del espacio de archivos que se ha de suprimir.

Cientes soportados

Este mandato es válido para todos los clientes.

Sintaxis



Parámetros

Tabla 89. mandato delete filesystem: opciones relacionadas

Opción	Dónde se utiliza
class "Class" en la página 364	Sólo línea de mandatos.
detail "Detail" en la página 385	Sólo línea de mandatos.
nasnodename "Nasnodename" en la página 498	Archivo de opciones del sistema cliente o línea de mandatos.
scrolllines "Scrolllines" en la página 552	Archivo de opciones del sistema cliente o línea de mandatos.
scrollprompt "Scrollprompt" en la página 553	Archivo de opciones del sistema cliente o línea de mandatos.

Ejemplos

- Tarea** Suprimir un espacio de archivos.

Mandato: delete filesystem
- Tarea** Suprimir los espacios de archivos NAS del servidor de archivos NAS **dagordon** que hay almacenados en el servidor.

mandato: delete filesystem -nasnodename=dagordon -class=nas

Información relacionada

- "Nasnodename" en la página 498
- "Class" en la página 364

Delete Group

Utilice el mandato **delete group** para suprimir una copia de seguridad de grupo en el servidor de IBM Spectrum Protect.

Después de suprimir un grupo, el líder del grupo (`virtualfsname`) permanece en el servidor de IBM Spectrum Protect. No contiene miembros (archivos ni directorios)

pero se notifica en un mandato **query filespace** subsiguiente. No habrá archivos listados si se agrega la opción **showmembers**. Al suprimir un grupo no se suprime el espacio de archivos en el que reside porque es posible que éste contenga otros grupos. Utilice **delete filespace** si desea eliminar el espacio de archivos y todos los datos que contiene.

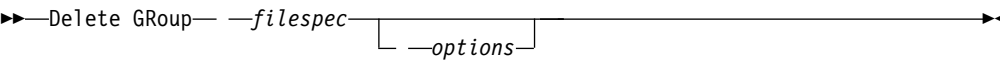
Nota:

- 1. Utilice la opción **inactive** para visualizar las versiones de copia de seguridad de grupo activas y también inactivas. De forma predeterminada, el cliente muestra las versiones activas.
- 2. Utilice la opción **pick** para seleccionar un grupo específico con el fin de suprimirlo del servidor de IBM Spectrum Protect.
- 3. Utilice la opción **noprompt** si desea eliminar la solicitud de confirmación que normalmente aparece antes de que suprima una versión de copia de seguridad de grupo. De forma predeterminada, el cliente le solicitará confirmación antes de suprimir la copia de seguridad de grupo. Al utilizar esta opción se acelera el procedimiento de supresión. Sin embargo, también aumenta el riesgo de suprimir accidentalmente una versión de copia de seguridad de grupo que desea guardar. Utilice esta opción con precaución.
- 4. Utilice el mandato **query filespace** para visualizar nombres de espacios de archivos virtuales para el nodo que se almacenan en el servidor.

Clientes soportados

Este mandato es válido para todos los clientes UNIX y Linux, a excepción de Mac OS X.

Sintaxis



Parámetros

filespec
Especifica el nombre del espacio de archivos virtual y el nombre de grupo que desea suprimir del almacenamiento del servidor.

Tabla 90. mandato delete group: opciones relacionadas

Opción	Dónde se utiliza
inactive “Inactive” en la página 456	Sólo línea de mandatos.
noprompt “Noprompt” en la página 503	Sólo línea de mandatos.
pick “Pick” en la página 512	Sólo línea de mandatos.
pitdate “Pitdate” en la página 512	Sólo línea de mandatos.
pittime “Pittime” en la página 513	Sólo línea de mandatos.

Ejemplos

Tarea Suprimir la versión activa actual del grupo /virtfs/group1.

Mandato:

```
delete group /virtfs/group1
```

Tarea Suprimir una versión de copia de seguridad del grupo /virtfs/group1 de una lista de versiones activas e inactivas.

Mandato:

```
delete group /virtfs/group1 -inactive -pick
```

Información relacionada

“Inactive” en la página 456

“Pick” en la página 512

“Noprompt” en la página 503

“Query Filespace” en la página 727

Expire

El mandato **expire** desactiva los objetos de copia de seguridad que especifica en la especificación de archivos o con la opción `filelist`. Puede especificar un archivo individual para que caduque, o un archivo que contiene una lista de archivos que caducarán. Si `OBJTYPE=VM`, este mandato desactivará la copia de seguridad actual para una máquina virtual.

Cuando se trabaja en modalidad interactiva, una solicitud le notificará si los archivos han caducado.

El mandato **expire** no suprime los archivos de estación de trabajo. Si caduca un archivo o directorio que todavía existe en la estación de trabajo, se vuelve a realizar una copia de seguridad del archivo o directorio de éste en la siguiente copia de seguridad incremental excepto en el caso de que el objeto se excluya mediante un proceso de inclusión/exclusión.

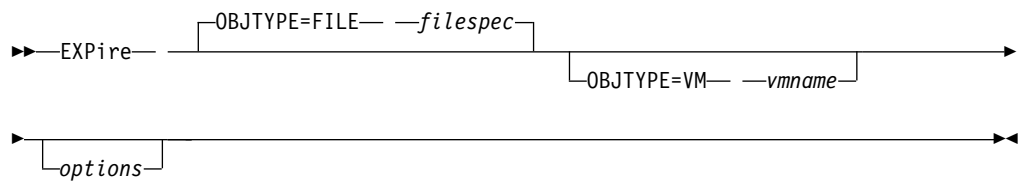
Si caduca un directorio que contiene archivos activos, estos archivos no se muestran en una consulta posterior de la GUI. Sin embargo, estos archivos se muestran en la línea de mandatos, si especifica la consulta correcta con un carácter comodín para el directorio.

Nota: Dado que el mandato **expire** cambia la imagen del servidor del sistema de archivos cliente sin cambiar el sistema de archivos cliente, el mandato **expire** no está permitido en archivos ubicados en un sistema de archivos que está supervisado por el daemon de registro por diario IBM Spectrum Protect.

Clientes soportados

Este mandato es válido para todos los clientes.

Sintaxis



Parámetros

OBJTYPE=FILE filespec

Especifica una vía de acceso y un nombre de archivo que desea que caduquen. En este mandato, sólo puede entrar una especificación de archivo. Sin embargo, puede utilizar caracteres comodín para seleccionar un grupo de archivos o todos los archivos de un directorio. Si se especifica la opción `filelist`, la designación `filespec` se ignorará.

OBJTYPE=VM vmname

`vmname` especifica el nombre de una máquina virtual. La copia de seguridad activa para la máquina virtual especificada ha caducado. El nombre de la máquina virtual no puede contener caracteres comodín.

Cuando se haya especificado `objtype=VM`, el mandato `expire` caducará sólo las copias de seguridad de la máquina virtual completas (`MODE=FULL` o `MODE=IFFULL`) para la máquina virtual que se especifica en el parámetro `vmname`. Las copias de seguridad creadas con la modalidad completa o incremental se han creado con el cliente de la versión 7.1 o anterior.



Las operaciones de máquina virtual solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments.

Tabla 91. Mandato expire: opciones relacionadas

Opción	Dónde se utiliza
<code>dateformat</code> "Dateformat" en la página 376	Archivo de opciones de usuario del cliente (<code>dsm.opt</code>) o línea de mandatos.
<code>filelist</code> "Filelist" en la página 439	Sólo línea de mandatos.
<code>noprompt</code> "Noprompt" en la página 503	Sólo línea de mandatos.
<code>numberformat</code> "Numberformat" en la página 504	Archivo de opciones de usuario del cliente (<code>dsm.opt</code>) o línea de mandatos.
<code>pick</code> "Pick" en la página 512	Sólo línea de mandatos.
<code>timeformat</code> "Timeformat" en la página 592	Archivo de opciones de usuario del cliente (<code>dsm.opt</code>) o línea de mandatos.

Ejemplos

Tarea Desactive el archivo `letter1.txt` del directorio `home`.

Mandato: `expire "/home/letter1.txt"`

Tarea Desactive todos los archivos del directorio `/admin/mydir`.

Mandato: `expire /admin/mydir/*`

Tarea Desactive todos los archivos que se denominan en el archivo /home/avi/filelist.txt.
Mandato: expire -filelist=/home/avi/filelist.txt

Help

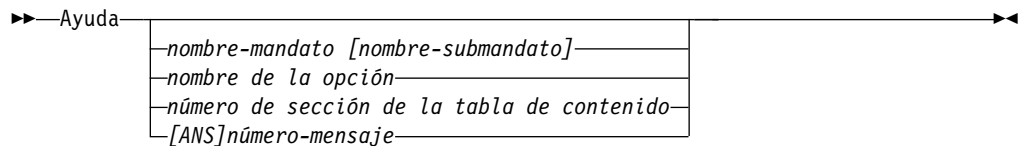
Utilice el mandato **help** para visualizar información acerca de mandatos, opciones y mensajes.

Consejo: si utiliza el mandato **help** en la línea de mandatos inicial, no se establecerá ningún contacto con el servidor y no se necesitará ninguna contraseña.

Clientes soportados

Este mandato es válido para todos los clientes.

Sintaxis



Si especifica el mandato **help** sin ningún argumento, la ayuda mostrará toda la tabla de contenido. Ya sea con el mandato inicial o cuando HELP muestre un indicador de solicitud, puede especificar los parámetros siguientes.

Parámetros

nombre-mandato [nombre-submandato]

Especifica un nombre de mandato y, opcionalmente, un nombre de submandato o su nombre abreviado, por ejemplo: **backup image**, o **b i**. En este caso, la combinación debe ser exclusiva. Los nombres abreviados no exclusivos producen la visualización de la primera sección de todo el archivo de ayuda que coincide con el nombre abreviado. Este parámetro es opcional.

nombre-opción

Especifica el nombre de la opción, por ejemplo: **domain** o **do**. Este parámetro es opcional.

número-sección-TOC

Especifica un número de sección de la tabla de contenido, por ejemplo: 1.5.3. Este parámetro es opcional.

[ANS] número-mensaje

Especifica un número de mensaje con o sin su prefijo, por ejemplo: **ans1036** o **1036**. Este parámetro es opcional. El código de gravedad no es nunca necesario. Si introduce **ans1036E** obtendrá como resultado "respuesta no encontrada".

Importante: Si especifica argumentos que no se ajusten a estas descripciones, puede provocar que se visualicen resultados no esperados (o ningún resultado). Si introduce más de dos argumentos, se rechazará su solicitud de ayuda. Cuando un nombre de mandato y un nombre de opción coinciden, por ejemplo: **incremental** (mandato) e **incremental** (opción), puede obtener ayuda sobre la opción mediante la especificación del número de sección de la tabla de contenido.

El texto de la ayuda solicitada se visualizará en una o más secciones, en función del número de líneas de visualización disponibles en la ventana del mandato. Cuando se muestran suficientes líneas para llenar el espacio de visualización, o cuando se muestre el final del texto de la ayuda solicitada, verá un indicador de solicitud junto con instrucciones sobre lo que se puede especificar en este indicador de solicitud. Para continuar visualizando el texto para la selección actual, pulse Intro o la tecla 'd' para desplazarse hacia abajo. Para desplazarse hacia arriba en la selección actual, pulse la tecla 'u' e Intro. Es posible que se presenten otras opciones, por lo que debe leer las instrucciones del indicador de solicitud.

La visualización correcta del texto de ayuda requiere un ancho de pantalla utilizable de 72 caracteres. Una anchura de visualización menor de 72 caracteres hace que las frases que tienen 72 caracteres de ancho se pasen a la línea siguiente. Esto puede hacer que el texto de ayuda desplegado comience en algún lugar dentro de la sección en lugar de al principio. Se pueden visualizar las líneas no desplegadas utilizando la función de desplazamiento del terminal para moverse hacia arriba.

Ejemplos

Tarea Visualizar la tabla de contenido de los temas de ayuda.

Mandato: dsmc help

Tarea Visualizar la información en el tema de la ayuda 2.1.2

Mandato: dsmc help 2.1.2

Tarea Visualizar información de ayuda sobre el mandato **archive**.

Mandato: dsmc help archive

Tarea Visualizar información de ayuda sobre el mensaje ANS1036.

Mandato: dsmc help 1036

Mandato: dsmc help ANS1036

Incremental

El mandato **incremental** realiza la copia de seguridad de todos los datos nuevos o modificados de las ubicaciones que especifique, a menos que los excluya de los servicios de copia de seguridad.

Puede realizar una copia de seguridad de todos los archivos o directorios nuevos o cambiados del dominio del cliente predeterminado o de los sistemas de archivos, directorios o archivos.

Para hacer copias de seguridad incrementales de archivos o directorios seleccionados, proporcione la especificación de archivo en el mandato. Si no proporciona una especificación de archivo, el valor predeterminado es realizar una copia de seguridad de los archivos o directorios del dominio predeterminado.

Sólo AIX: puede activar la copia de seguridad incremental basada en instantáneas mediante la utilización de la opción `snapshotproviderfs=JFS2`.

Los siguientes atributos de la clase de gestión asignada al archivo o directorio determinan si se va a realizar la copia de seguridad de los datos:

Frecuencia

Número de días que deben transcurrir entre las copias de seguridad sucesivas del objeto. El atributo **frequency** sólo se aplica a una copia de seguridad incremental completa.

Este atributo de clase de gestión no se tiene en cuenta durante una copia de seguridad con registro por diario.

Modalidad

Especifica si los cambios desde la última operación de copia de seguridad afectan al procesamiento. Si **mode=modified**, solo se procesan los objetos que han cambiado desde la última operación de copia de seguridad. Si **mode=absolute**, se procesan todos los objetos, independientemente de si el objeto ha cambiado desde la última operación de copia de seguridad.

Si la modalidad del grupo de copia está establecida en **modificada**, puede alterarse temporalmente mediante la opción **absolute** del cliente. Para obtener más información sobre la opción **absolute**, consulte “Absolute” en la página 345.

Serialización

Permite o deniega la copia de seguridad de archivos o directorios en función los valores siguientes:

- **estática**: para que se haga copia de seguridad de los mismos, los datos no deben haberse modificado durante la copia de seguridad o archivado.
- **Estática compartida**: si los datos del archivo o del directorio se modifican durante cada uno de los intentos permitidos de incluirlos en una operación de copia de seguridad o de archivado, no se incluyen. El valor de la opción **changingretries** determina el número de intentos realizados. El valor predeterminado es 4.
- **Dinámica**: el objeto se incluye en la operación de copia de seguridad o de archivado en el primer intento, sin tener en cuenta si los datos se modifican durante el proceso.
- **Dinámica compartida**: el objeto se incluye en la operación de copia de seguridad o de archivado en el último intento, aunque los datos se modifiquen durante el proceso.

Utilizando la opción **include** de la lista de inclusión/exclusión puede modificar la clase de gestión predeterminada para un archivo o grupo de archivos.

Puede realizar una copia de seguridad incremental completa o una copia de seguridad incremental por fecha. El valor predeterminado es una operación de copia de seguridad incremental completa.

Si está registrando por diario un sistema de archivos y el diario es válido, la copia de seguridad incremental completa realizará una copia de seguridad con registro por diario. Puede iniciarse más de una sesión de copia de seguridad con registro por diario, pero sólo puede continuar una de las sesiones. Todas las demás sesiones de copia de seguridad con registro por diario que necesiten acceso al mismo espacio de archivos deben esperar hasta que la sesión actual de copia de seguridad con registro por diario haya finalizado antes de que la siguiente sesión pueda continuar. Es posible realizar una copia de seguridad incremental completa sin diario utilizando la opción **nojournal**.

También puede utilizar el mandato **selective** para llevar a cabo una copia de seguridad que sólo realizará la copia de seguridad de los archivos, directorios o directorios vacíos especifique, con independencia de si se habían modificado.

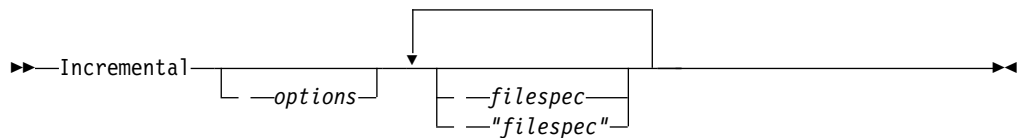
Una copia de seguridad incremental completa hace copia de seguridad de todos los archivos y directorios que sean nuevos o que hayan sido modificados desde la última copia de seguridad incremental. Durante una copia de seguridad incremental completa, el cliente consulta al servidor. IBM Spectrum Protect utiliza esta información cuando realiza las siguientes acciones:

- Hacer una copia de seguridad de archivos o directorios nuevos.
- Hacer una copia de seguridad de archivos o directorios cuyo contenido se ha modificado desde la copia de seguridad anterior.
- Marcar las versiones de copia de seguridad inactivas en el servidor para los archivos y directorios que se hayan eliminado de la estación de trabajo.
- Volver a vincular versiones de copia de seguridad con clases de gestión, si se han modificado las asignaciones de la clase de gestión.

Clientes soportados

Este mandato es válido para todos los clientes.

Sintaxis



Parámetros

filespec

Especifica la vía de acceso y el nombre del archivo del que se desea realizar la copia de seguridad. Utilice caracteres comodín para seleccionar un grupo de archivos o todos los archivos de un directorio. Si no especifica una especificación de archivo, la opción **domain** determina lo que hay que copiar.

Si especifica un sistema de archivos, se realizará la copia de seguridad de todos los archivos nuevos y cambiados. Además, la fecha de la última copia incremental del espacio de archivos se actualiza en el servidor. Si especifica un archivo o directorio, la fecha de la última copia incremental no se actualiza. Esto significa que se puede volver a hacer una copia de seguridad del archivo o directorio si se lleva a cabo una copia de seguridad posterior con la opción **incrbydate**. Si especifica un sistema de archivos, especifique el sistema de archivos sin la barra inclinada final.

Tabla 92. Mandato Incremental: opciones relacionadas

Opción	Dónde se utiliza
absolute "Absolute" en la página 345	Sólo línea de mandatos.
changingretries "Changingretries" en la página 363	Archivo dsm.sys o línea de mandatos.
compressalways "Compressalways" en la página 369	Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
compression "Compression" en la página 370	Archivo dsm.sys de una stanza del servidor o línea de mandatos.
detail "Detail" en la página 385	Sólo línea de mandatos.
diffsnapshot "Diffsnapshot" en la página 387	Sólo línea de mandatos.

Tabla 92. Mandato Incremental: opciones relacionadas (continuación)

Opción	Dónde se utiliza
dirsonly "Dirsonly" en la página 390	Sólo línea de mandatos.
dominio "Domain" en la página 394	Sólo archivo dsm.sys o archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
encryptiontype "Encryptiontype" en la página 417	Archivo de opciones del sistema (dsm.sys) dentro de una stanza de servidor.
encryptkey "Encryptkey" en la página 418	Archivo de opciones del sistema (dsm.sys) dentro de una stanza de servidor.
filelist "Filelist" en la página 439	Sólo línea de mandatos.
filesonly "Filesonly" en la página 443	Sólo línea de mandatos.
incrbydate "Incrbydate" en la página 474	Sólo línea de mandatos.
memoryefficientbackup "Memoryefficientbackup" en la página 491	Archivo de opciones del usuario cliente (dsm.opt), archivo de opciones del sistema cliente (dsm.sys), servidor o línea de mandatos.
nojournal "Nojournal" en la página 502	Sólo línea de mandatos.
preservelastaccessdate "Preservelastaccessdate" en la página 519	Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
removeoperandlimit "Removeoperandlimit" en la página 528	Sólo línea de mandatos.
snapdiff "Snapdiff" en la página 561	Sólo línea de mandatos.
snapshotcachesize "Snapshotcachesize" en la página 567	Archivo de opciones del cliente (dsm.opt) o con la opción include.fs .
snapshotproviderfs "Snapshotproviderfs" en la página 569	Archivo de opciones del sistema (dsm.sys) en una stanza del servidor o con la opción include.fs .
snapshotroot "Snapshotroot" en la página 571	Sólo línea de mandatos.
subdir "Subdir" en la página 581	Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
tapeprompt "Tapeprompt" en la página 583	Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.

Ejemplos

Tarea Ejecutar una copia de seguridad incremental del dominio de cliente que se ha especificado en el archivo de opciones de usuario del cliente (dsm.opt).
Incremental

Ejecutar una copia de seguridad incremental que haya una copia de seguridad de todos los archivos del dominio, con independencia de si éstos se han modificado desde la última copia de seguridad.

Incremental -absolute

- Tarea** Ejecutar una copia de seguridad incremental para los sistemas de archivos /home, /usr y /proj.
Incremental /home /usr /proj
- Tarea** Ejecutar una copia de seguridad incremental para el directorio /proj/test.
Incremental /proj/test/
- Tarea** Ejecutar una copia de seguridad incremental por fecha para el sistema de archivos /home.
Incremental -incrbydate /home
- Tarea** Ejecutar una copia de seguridad incremental del archivo abc en el directorio /fs/dir1.
Incremental -subdir=yes /fs/dir1/abc
- Tarea** Ejecutar una copia de seguridad incremental del objeto de directorio /fs/dir1, pero no de los archivos del directorio /fs/dir1.
Incremental /fs/dir1
- Tarea** Ejecutar una copia de seguridad incremental del objeto de directorio /fs/dir1, de todos los archivos del directorio fs/dir1 y de todos los archivos y subdirectorios de /fs/dir1.
Incremental -subdir=yes /fs/dir1/
- Tarea** Ejecutar una copia de seguridad incremental, dándose por supuesto que ha iniciado una instantánea del sistema de archivos /usr y que ha montado la instantánea como /snapshot/day1, de todos los archivos y directorios de la instantánea local y gestionar éstos en el servidor de IBM Spectrum Protect, en el nombre de espacio de archivos /usr.
dsmc inc /usr -snapshotroot=/snapshot/day1
- Tarea** Ejecutar una copia de seguridad incremental para el sistema de archivos /home utilizando la opción **snappdiff** y especificar la opción para crear la instantánea de diferencias. En el siguiente ejemplo, /home representa el punto de montaje de NFS para un volumen de archivador de NAS/N-Series.
incremental /home -snappdiff -diffsnapshot=create
- Tarea** Ejecutar una copia de seguridad incremental del sistema de archivos /proj mediante la opción **snappdiff**. Especificar la opción para utilizar la instantánea más reciente en el archivador como la instantánea de diferencia. En el siguiente ejemplo, /proj representa el punto de montaje de NFS para un volumen de archivador de NAS/N-Series.
incremental /proj -snappdiff -diffsnapshot=latest

Información relacionada

“Absolute” en la página 345

“Copia de seguridad con registro por diario” en la página 709

“Selective” en la página 775

“Opciones include” en la página 458

Copia de seguridad con registro por diario

Una copia de seguridad de un sistema de archivos concreto se basa en registro por diario cuando el daemon de registro por diario de IBM Spectrum Protect se instala y se configura para registrar por diario el sistema de archivos y se ha establecido un registro por diario válido.

La copia de seguridad basada en registro por diario se admite en clientes de copia de seguridad/archivado AIX para sistemas de archivos JFS y JFS2.

La copia de seguridad basada en el diario se admite en el cliente de archivado y copia de seguridad Linux en Ext2, Ext3, Ext4; XFS, ReiserFS, JFS, VxFS y NSS. GPFS no se admite para las copias de seguridad basadas en el diario en Linux.

Si se ha instalado y está en ejecución el daemon de registro por diario, el mandato **incremental**, de forma predeterminada, realizará una copia de seguridad con registro por diario en los sistemas de archivos que supervisa el daemon de motor de registro por diario. Se deben cumplir las condiciones siguientes para que se efectúe satisfactoriamente una copia de seguridad basada en registro por diario:

- Se debe configurar el daemon de registro por diario para que supervise el sistema de archivos que contiene los archivos y directorios de los que se hace una copia de seguridad.
- Una copia de seguridad incremental completa debe haberse ejecutado satisfactoriamente al menos una vez en el sistema de archivos del que se hace una copia de seguridad.
- Un mandato administrativo no puede haber modificado la imagen del espacio de archivos del sistema de archivos en el servidor desde la última copia de seguridad completa incremental.
- La política de gestión de almacenamiento para los archivos de los que se hace copia de seguridad no se puede haber actualizado desde la última copia de seguridad incremental completa.

El daemon de registro por diario registra en una base de datos de diario los cambios que se han producido en un objeto o en sus atributos. Durante una copia de seguridad con registro por diario, el cliente obtiene una lista de archivos que pueden utilizarse para realizar la copia de seguridad de la base de datos de diario. La copia de seguridad con registro por diario puede aumentar el rendimiento de la copia de seguridad porque el cliente no explora el sistema de archivos local ni se pone en contacto con el servidor para determinar qué archivos se deben procesar. La copia de seguridad con registro por diario también reduce el tránsito en la red entre el cliente y el servidor.

El cliente de copia de seguridad y archivado filtra la lista basándose en la lista de exclusión/inclusión actual y procesa, caduca y actualiza los archivos resultantes según las restricciones de política, como por ejemplo la serialización. Sin embargo, el cliente ignora el atributo de frecuencia del servidor durante una copia de seguridad con registro por diario. El motivo de esto es que una copia de seguridad con registro por diario elimina la consulta de la versión de la copia de seguridad al servidor; por ello, el cliente no sabe cuántos días han pasado desde la última copia de seguridad del archivo.

El daemon de registro por diario no registra los cambios en los archivos especiales de UNIX.

El daemon de registro por diario excluye archivos específicos del sistema para que los cambios no se registren en el registro por diario. Como los cambios de estos archivos no se registran por diario, el cliente no hace una copia de seguridad de estos archivos. Consulte el archivo de configuración del daemon de diario `tsmjbbd.ini` que se encuentra en el directorio de instalación del cliente decopia de seguridad y archivado para ver los archivos específicos del sistema que se excluyen.

Nota:

1. Al utilizar un programa antivirus, hay limitaciones en la copia de seguridad con registro por diario. Algunos programas antivirus pueden generar incorrectamente notificaciones de cambios en el servicio de diario de IBM Spectrum Protect, lo que hace que se produzcan anomalías en el proceso de la copia de seguridad basada en el registro por diario de los archivos que no se han modificado. Para evitar estos problemas, utilice Norton Anti-Virus Corporate Edition 8.0 y superior.
2. Es posible que una copia de seguridad con registro por diario no se realice como la copia de seguridad incremental tradicional si el dominio de políticas de su nodo se ha modificado en el servidor. Esto depende de cuándo se ha actualizado por última vez el juego de políticas de su dominio y de la fecha de la última copia de seguridad incremental. En este caso, deberá forzar una copia de seguridad incremental completa del modo tradicional para volver a vincular los archivos con el dominio nuevo. Utilice la opción `nojournal` con el mandato **incremental** para especificar que desea realizar una copia de seguridad incremental completa tradicional en lugar de la copia de seguridad con registro por diario predeterminada.

Añada una sentencia de instantánea de exclusión al archivo `tsmjbbd.ini` para AIX 6.1 (o posterior) para evitar que el daemon de copia de seguridad basada en el diario supervise los directorios de instantánea interna JFS2. Si excluye los directorios de instantáneas, los archivos en ellos serán incluidos en la copia de seguridad Copiar los directorios de instantánea es redundante y desperdicia espacio de servidor.

En las siguientes situaciones, cuando la base de datos de diario no es válida y el cliente realiza la copia de seguridad incremental completa tradicional:

- Se ha modificado el nombre del espacio de archivos registrado por diario.
- Se ha modificado el nombre del nodo cliente.
- El cliente se pone en contacto con un servidor distinto para que haga la copia de seguridad.
- Se han producido modificaciones en la política (se ha activado un nuevo juego de políticas).
- El diario está dañado (condición de falta de espacio, error de disco).
- El diario no funciona.

La copia de seguridad con registro por diario se diferencia de la copia de seguridad incremental completa tradicional en los siguientes aspectos:

- IBM Spectrum Protect no fuerza frecuencias de copia no establecidas de forma predeterminada (distintas de 0).
- Los cambios realizados en archivos especiales de UNIX no se detectan.

Puede utilizar la opción `nojournal` con el mandato **incremental** para especifica que desea realizar una copia de seguridad incremental completa tradicional en lugar de la copia de seguridad con registro por diario que se realiza de forma predeterminada.

Incremental por fecha

Una copia de seguridad incremental por fecha realiza copia de seguridad de los archivos nuevos o modificados cuya fecha de modificación sea posterior a la fecha de la última copia de seguridad incremental almacenada en el servidor, a menos que los archivos se excluyan de la copia de seguridad mediante una sentencia **exclude**.

Si se ejecuta una copia incremental por fecha sólo en parte de un sistema de archivos, no se actualizará la fecha de la última copia incremental completa, y la próxima copia incremental por fecha volverá a efectuar copia de seguridad de estos archivos. Los cambios en las listas de control de accesos (ACL) o en los atributos ampliados no hacen que se lleven a cabo copias de seguridad de los archivos durante una copia de seguridad incremental por fecha. Utilice el mandato **query fileSPACE** para determinar la fecha y la hora de la última copia de seguridad incremental de todo el sistema de archivos.

Para realizar una copia de seguridad incremental por fecha, utilice la opción **incrbydate** con el mandato **incremental**.

A diferencia de una copia de seguridad incremental completa, una copia de seguridad incremental por fecha no conserva el almacenamiento del servidor actual de *todos* los archivos de la estación de trabajo por los motivos siguientes:

- No da caducidad a las versiones de copia de seguridad de los archivos que se han suprimido de la estación de trabajo.
- No revincula versiones de copia de seguridad con una nueva clase de gestión si ésta ha cambiado.
- No efectúa copias de seguridad de archivos cuyos atributos han cambiado, a no ser que se hayan modificado también la fecha y la hora.
- No tiene en cuenta el atributo de frecuencia de grupo de copia de las clases de gestión.

Por las razones expuestas, si dispone de un tiempo limitado durante la semana para realizar las copias de seguridad, pero dispone de tiempo adicional los fines de semana, puede realizar una copia de seguridad incremental por fecha durante la semana y una copia de seguridad incremental completa los fines de semana para conservar el almacenamiento del servidor actual de los archivos de la estación de trabajo.

Si vuelve a emitirse el mandato **incremental** por haberse producido una anomalía en las comunicaciones o una pérdida de la sesión, las estadísticas de la transferencia visualizarán el número de bytes que el cliente intenta transferir durante todos los intentos de ejecución del mandato. Por ello, es posible que las estadísticas de bytes transferidos no coincidan con las estadísticas de archivos, como las relativas al tamaño de archivo.

Asociación de una instantánea local a un espacio de archivos del servidor

Utilice la opción **snapshotroot** con el mandato **incremental** junto con una aplicación suministrada por otro proveedor que proporcione una instantánea de un volumen lógico para asociar los datos de la instantánea local con los datos del espacio de archivos reales que se almacenan en el servidor de IBM Spectrum Protect.

La opción `snapshotroot` no proporciona ningún recurso para tomar una instantánea de volumen, sólo para gestionar los datos que ha creado una instantánea de volumen.

Loop

El mandato **loop** inicia una sesión de línea de mandatos interactiva que se mantiene hasta que el usuario escribe `quit`.

Si debe especificar una contraseña, se le solicitará antes de que aparezca el indicador de modalidad de bucle.

Nota: no es posible entrar en modalidad de bucle sin un contacto de servidor. Una de las consecuencias de ello es que algunos mandatos, como `restore backupset -location=file`, sólo se aceptan en la línea de mandatos inicial cuando no hay un servidor válido disponible.

En una sesión de línea de mandatos interactiva, no es necesario que cada nombre de mandato vaya precedido de **dsmc** y la contraseña, si procede.

En la modalidad interactiva, las opciones que especifique en la línea de mandatos inicial modificarán temporalmente el valor que ha especificado en el archivo de opciones de usuario del cliente (`dsm.opt`) o el archivo `dsm.sys`. Este valor seguirá aplicándose durante toda la sesión interactiva a menos que un valor distinto lo modifique en un mandato interactivo determinado. Por ejemplo, si establece la opción `subdir` en *yes* en el archivo de opciones del usuario cliente (`dsm.opt`) y especifica `-subdir=no` en la línea de mandatos inicial, el valor `-subdir=no` seguirá en vigor durante la totalidad de la sesión interactiva a menos que lo modifique temporalmente mediante el valor `-subdir=yes` en un mandato interactivo determinado. Sin embargo, el valor `subdir=yes` sólo afectará al mandato en el que se especifique éste. Cuando ese mandato se haya completado, el valor volverá a establecerse en `subdir=no`, el valor que tenía al inicio de la sesión interactiva.

En la modalidad interactiva, puede especificar todos los mandatos válidos, *excepto* los mandatos **schedule** y **loop**.

Algunas opciones no pueden utilizarse en la sesión interactiva creada por el mandato **loop** y se indican en la descripción de opciones de la siguiente forma: *Esta opción sólo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.*

Nota:

1. En la modalidad de bucle, después de una operación de restauración directamente desde cinta, el punto de montaje no se libera por si se realizan solicitudes de restauración adicionales de dicho volumen. Si solicita una operación de copia de seguridad en la misma sesión y dicho punto de montaje es el único que está disponible, la operación de copia de seguridad se interrumpirá con el mensaje siguiente:

Esperando a que se monte un medio fuera de línea.

En este caso, el punto de montaje no se libera hasta que se cumple una de las siguientes condiciones:

- Se satisface el límite `MOUNTRETENTION` de la clase de dispositivo.
- Se satisface el período de inactividad (`idletimeout`) del cliente.

- La sesión de bucle **dsmc** se cierra una vez que ha finalizado la operación de restauración, lo que permite iniciar otra sesión en modalidad de bucle para realizar la operación de copia de seguridad.
2. En la modalidad interactiva, no se puede introducir una especificación de archivo que contenga caracteres específicos del idioma nacional. Si un mandato contiene caracteres de este tipo, procese el mandato en modalidad por lotes, especificando el nombre del programa ejecutable **dsmc** antes del nombre del mandato.

Clientes soportados

Este mandato es válido para todos los clientes.

Sintaxis

►►—LOOP—◄◄

Parámetros

No hay parámetros para este mandato.

Ejemplos

Tarea Iniciar una sesión de línea de mandatos interactiva.

Mandato: **dsmc**

En el indicador de mandatos **Protect>**, especifique un mandato.

Existen dos métodos para finalizar una sesión interactiva:

- Especifique **quit**.
- Si ha establecido **editor=yes**, puede realizar lo siguiente:
 1. Pulse la tecla de escape (Esc).
 2. Escriba una Q y pulse la tecla Intro.

Nota: El valor predeterminado es **editor=yes**.

Nota: Para interrumpir un mandato **dsmc** antes de que el cliente haya terminado el proceso, especifique **QQ** en la consola de IBM Spectrum Protect. En la mayoría de los casos, no en todos, ello interrumpirá el mandato.

Información relacionada

Capítulo 10, “Opciones de proceso”, en la página 313 para opciones que no pueden utilizarse en la modalidad interactiva.

Macro

El mandato **macro** ejecuta una serie de mandatos que se especifican en un archivo de macros.

Mediante la inclusión de los mandatos **macro** dentro de un archivo de macro, pueden anidarse hasta diez niveles de mandatos.

Las líneas de comentarios no se pueden utilizar en el archivo de macro especificado para el mandato **macro**.

Cientes soportados

Este mandato es válido para todos los clientes.

Sintaxis

►►—Macro— *—macroname—*—————►►

Parámetros

nombremacro

Especifica el nombre completo del archivo que contiene los mandatos.

Ejemplos

A continuación, se muestra un ejemplo de cómo utilizar el mandato **macro**.

Tarea Realizar una copia de seguridad selectiva de los archivos de los siguientes directorios:

- /devel/project/proja
- /devel/project/projb
- /devel/project/projc

Mandato:macro backabc.mac

Donde backabc.mac contiene las sentencias siguientes:

```
Selective /devel/project/proja/  
Selective /devel/project/projb/  
Selective /devel/project/projc/
```

Monitor Process

El mandato **monitor process** visualiza una lista de los procesos actuales de copia de seguridad de imagen y de restauración NAS (si se ha activado el soporte de NDMP) para los que el usuario de administración dispone de autorización. Se le solicitará el ID de administrador de IBM Spectrum Protect.

El usuario de administración puede seleccionar el proceso que desea supervisar. El privilegio de propietario cliente es una autorización suficiente para poder supervisar los procesos de copia de seguridad de imágenes o restauración NAS seleccionados.

Cientes soportados

Este mandato sólo es válido para los clientes AIX, Linux, y Solaris.

Sintaxis

►►—MONitor Process——————►►

Parámetros

No hay parámetros para este mandato.

Ejemplos

Tarea Supervisar los procesos de copia de seguridad de imagen o restauración NAS actuales.

Mandato: monitor process

Preview Archive

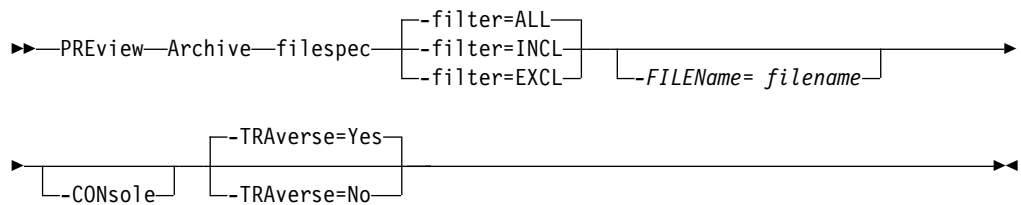
El mandato **preview archive** simula un mandato de copia de seguridad sin enviar los datos al servidor.

El mandato **preview** genera un archivo de texto delimitado por tabuladores que se puede importar a un programa de hojas de cálculo. La vista preliminar contiene información, por ejemplo, sobre si el archivo está excluido o incluido. Si el archivo está excluido, se mostrará el patrón o motivo por el que se ha excluido el archivo, junto con el origen del patrón.

Clientes soportados

Este mandato es válido para todos los clientes.

Sintaxis



Parámetros

filespec

Especifica la vía de acceso y el nombre del archivo que se desea archivar. Utilice caracteres comodín para seleccionar un grupo de archivos o todos los archivos de un directorio.

-filter Especifica la salida que se debe visualizar. Puede visualizar objetos incluidos, objetos excluidos o ambos.

ALL Muestra la salida para los objetos incluidos y excluidos. Éste es el valor predeterminado.

INCLuded

Muestra la salida sólo para los objetos incluidos.

EXCLuded

Muestra la salida sólo para los objetos excluidos.

-FILENAME=

Especifica el nombre de archivo en el que se debe grabar la salida delimitada por tabuladores. El valor predeterminado es dsmprev.txt.

-CONsole

La salida se graba en la consola y en el archivo.

-TRAverse

Previsualiza el directorio actual y sus subdirectorios.

Yes Previsualiza los directorios actuales y sus subdirectorios. Éste es el valor predeterminado.

No Sólo previsualiza el directorio actual, sin subdirectorios.

Importante: la especificación de **-traverse** no ofrece una previsualización de los directorios que se han excluido mediante la utilización de la opción `exclude.dir`.

Previsualizar copia de seguridad

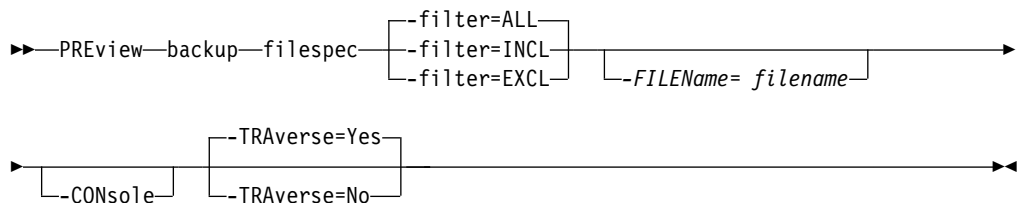
El mandato **preview** simula un mandato de copia de seguridad sin enviar los datos al servidor.

El mandato **preview** genera un archivo de texto delimitado por tabuladores que se puede importar a un programa de hojas de cálculo. La vista preliminar contiene información, por ejemplo, sobre si el archivo está excluido o incluido. Si el archivo está excluido, se mostrará el patrón o motivo por el que se ha excluido el archivo, junto con el origen del patrón.

Clientes soportados

Este mandato es válido para todos los clientes.

Sintaxis



Parámetros

filespec

Especifica la vía de acceso y el nombre del archivo del que se desea realizar la copia de seguridad. Utilice caracteres comodín para seleccionar un grupo de archivos o todos los archivos de un directorio.

-filter Especifica la salida que se debe visualizar. Puede visualizar objetos incluidos, objetos excluidos o ambos.

ALL Muestra la salida para los objetos incluidos y excluidos. Éste es el valor predeterminado.

INCLuded

Muestra la salida sólo para los objetos incluidos.

EXCLuded

Muestra la salida sólo para los objetos excluidos.

-FILENAME=

Especifica el nombre de archivo en el que se debe grabar la salida delimitada por tabuladores. El valor predeterminado es dsmprev.txt.

-CONsole

La salida se graba en la consola y en el archivo.

-TRAverse

Previsualiza el directorio actual y sus subdirectorios.

Yes Previsualiza los directorios actuales y sus subdirectorios. Éste es el valor predeterminado.

No Sólo previsualiza el directorio actual, sin subdirectorios.

Importante: la especificación de **-traverse** no ofrece una previsualización de los directorios que se han excluido mediante la utilización de la opción `exclude.dir`.

Query Access

El mandato **query access** muestra los usuarios a los que ha otorgado acceso a las versiones de copia de seguridad o copias archivadas de archivos específicos.

El cliente de copia de seguridad y archivado muestra una lista de las reglas de autorización que ha definido con el mandato **set access** o con el menú **Programas de utilidad > Lista de acceso a nodo** de la interfaz gráfica de usuario (GUI) del cliente de copia de seguridad y archivado.

A continuación se indica la información incluida:

- Autorización que ha otorgado a un usuario para restaurar versiones de copia de seguridad o para recuperar copias archivadas.
- El nombre de nodo del usuario al que se otorga autorización.
- El identificador del usuario de dicho nodo al que se ha otorgado autorización.
- Los archivos para los que el usuario dispone de acceso.

Clientes soportados

Este mandato es válido para todos los clientes.

Sintaxis

►►—Query Access—◄◄

Parámetros

No hay parámetros para este mandato.

Ejemplos

Tarea Visualizar una lista de los usuarios que tienen acceso a sus archivos.

Mandato: query access

Query Archive

El mandato **query archive** muestra una lista de las copias archivadas y la siguiente información acerca de cada archivo: tamaño de archivo, fecha de archivado, especificación de archivo, fecha de caducidad y descripción de archivado.

Si utiliza la opción **detail** con el mandato **query archive**, el cliente visualizará la información adicional siguiente:

- Fecha de última modificación
- Fecha de último acceso
- Fecha de último cambio de atributos de archivo (inode)
- Tipo de compresión
- Tipo de cifrado
- Deduplicación de datos del lado del cliente
- Iniciación de retención
- Si el archivo está en espera
- Tamaño de metadatos de ACL (IBM Spectrum Scale), para clientes AIX y Linux
- Información de almacenamiento del servidor (clase de medios, ID de volumen y orden de restauración), para clientes AIX y Linux

En el siguiente ejemplo se muestra un ejemplo de la salida del mandato **query archive** con la opción **detail**:

```
Tamaño  Fecha - Hora archivado - Caducidad archivo - Descripción
-----
219 B  08/15/2016 09:32:13 /Volumes/Data/info.txt 08/16/2016
Archive Date: 08/16/2016
RetInit:STARTED Obj
Held:NO
Modificado: 03/02/2016 19:43:00 Accedido: 03/03/2016 09:31:23 Inode cambiado: 03/02/2016 19:43:00
Tipo compresión: LZ4 Tipo cifrado: Ninguno Deduplicado por cliente: YES
ACL Size: 0 Media Class: Fixed Volume ID: 0008 Restore Order: 00000000-0000001F-00000000-00600774
```

Para obtener más información sobre el tipo de compresión, consulte el apartado “Compression” en la página 370.

Clientes soportados

Este mandato es válido para todos los clientes.

Sintaxis

```
➤➤ Query ARchive [—options] [—filespec] [—"filespec"] ➤➤
```

Parámetros

filespec

Especifica la vía de acceso y el nombre del archivo que se desea consultar. Utilice caracteres comodín para especificar un grupo de archivos o todos los archivos de un directorio. Si utiliza caracteres comodín, incluya la especificación de archivo entre comillas. Especifique un asterisco (*) para consultar todas las copias archivadas del directorio actual.

Tabla 93. Mandato *query archive*: opciones relacionadas

Opción	Dónde se utiliza
dateformat “Dateformat” en la página 376	Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.

Tabla 93. Mandato query archive: opciones relacionadas (continuación)

Opción	Dónde se utiliza
description "Descripción" en la página 384	Sólo línea de mandatos.
detail "Detail" en la página 385	Sólo línea de mandatos.
dirsonly "Dirsonly" en la página 390	Sólo línea de mandatos.
filelist "Filelist" en la página 439	Sólo línea de mandatos.
filesonly "Filesonly" en la página 443	Sólo línea de mandatos.
fromdate "Fromdate" en la página 446	Sólo línea de mandatos.
fromnode "Fromnode" en la página 447	Sólo línea de mandatos.
fromowner "Fromowner" en la página 448	Sólo línea de mandatos.
fromtime "Fromtime" en la página 448	Sólo línea de mandatos.
numberformat "Numberformat" en la página 504	Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
querysummary "Querysummary" en la página 525	Sólo línea de mandatos.
scrolllines "Scrolllines" en la página 552	Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
scrollprompt "Scrollprompt" en la página 553	Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
subdir "Subdir" en la página 581	Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
timeformat "Timeformat" en la página 592	Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
todate "Todate" en la página 597	Sólo línea de mandatos.
totime "Totime" en la página 598	Sólo línea de mandatos.

Ejemplos

Tarea Visualizar una lista de todas las copias archivadas del directorio de trabajo actual.

Mandato: q archive "*"

Tarea Visualizar una lista de todas las copias archivadas del directorio /devel y de todos sus subdirectorios.

Mandato: query archive "/devel/*" -subdir=yes

Tarea Visualizar una lista de todas las copias archivadas del directorio actual. Utilice las opciones `dateformat` y `timeformat` para volver a formatear las fechas y las horas.

Mandato: `q ar -date=5 -time=1 "*"`

Tarea Visualizar una lista de todas las copias archivadas del directorio actual. Utilice la opción `detail` para que se visualicen la última fecha de modificación y la última fecha de acceso de cada archivo.

Mandato: `q ar -detail "*"`

Tarea Visualizar una lista de todas las copias archivadas del directorio `/home/proj` cuyos cuatro primeros caracteres del nombre del archivo empecen por `proj`.

Mandato: `q ar "/home/proj/proj*"`

Query Backup

El mandato **query backup** muestra una lista de versiones de copia de seguridad de los archivos almacenadas en el servidor de IBM Spectrum Protect, o del interior de un juego de copias de seguridad del servidor cuando se especifica la opción `backupsetname`.

El mandato muestra la siguiente información adicional:

- Especificación de archivo
- Tamaño del archivo
- Fecha de la copia de seguridad
- Si el archivo está activo o inactivo
- La clase de gestión asignada al archivo. En el nombre de la clase de gestión únicamente se muestran los 10 diez caracteres.

Si utiliza la opción `detail` con el mandato **query backup**, el cliente visualizará la información adicional siguiente:

- Fecha de última modificación
- Fecha de último acceso
- Última fecha de cambio de atributos de archivo (inode)
- Tipo de compresión
- Tipo de cifrado
- Deduplicación de datos del lado del cliente
- Indica si el archivo ha migrado o premigrado. Un valor de Yes significa que el archivo ha migrado o premigrado. Un valor de No indica que el archivo no ha migrado o premigrado.
- Número de inodo de archivo (para clientes AIX y Linux)
- Tamaño de metadatos de ACL (IBM Spectrum Scale) (para clientes AIX y Linux)
- Información de almacenamiento del servidor (clase de medios, ID de volumen y orden de restauración) (para clientes AIX y Linux)

En el siguiente ejemplo se muestra un ejemplo de la salida del mandato **query backup** con la opción `detail`:

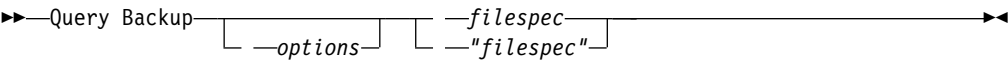
Tamaño	Fecha copia seg.	Clase gest.	Archivo A/I
----	-----	-----	-----
1,500,000 B	08/15/2016 16:01:25	DEFAULT	A /home/test/mydir/myfile1.txt

Para obtener más información sobre el tipo de compresión, consulte el apartado “Compression” en la página 370.

Cientes soportados

Este mandato es válido para todos los clientes.

Sintaxis



Parámetros

filespec
Especifica la vía de acceso y el nombre del archivo que se desea consultar. Utilice caracteres comodín para especificar un grupo de archivos o todos los archivos de un directorio. Si utiliza caracteres comodín, incluya la especificación de archivo entre comillas. Especifique un asterisco (*) para ver información acerca de las versiones de copia de seguridad de todos los archivos del directorio actual. No utilice caracteres comodín cuando consulte las imágenes del sistema de archivos NAS con la opción -class=nas.

Tabla 94. mandato query backup: opciones relacionadas

Opción	Dónde se utiliza
backupsetname "Backupsetname" en la página 360	Sólo línea de mandatos.
class "Class" en la página 364	Sólo línea de mandatos.
dateformat "Dateformat" en la página 376	En el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos.
detail "Detail" en la página 385	Sólo línea de mandatos.
dironly "Dironly" en la página 390	Sólo línea de mandatos.
filelist "Filelist" en la página 439	Sólo línea de mandatos.
filesonly "Filesonly" en la página 443	Sólo línea de mandatos.
fromdate "Fromdate" en la página 446	Sólo línea de mandatos.
fromowner "Fromnode" en la página 447	Sólo línea de mandatos.
fromowner "Fromowner" en la página 448	Sólo línea de mandatos.
fromtime "Fromtime" en la página 448	Sólo línea de mandatos.

Tabla 94. mandato query backup: opciones relacionadas (continuación)

Opción	Dónde se utiliza
inactive "Inactive" en la página 456	Sólo línea de mandatos.
nasnodename "Nasnodename" en la página 498	En el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos.
numberformat "Numberformat" en la página 504	Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
pitdate "Pitdate" en la página 512	Sólo línea de mandatos.
pittime "Pittime" en la página 513	Sólo línea de mandatos.
querysummary "Querysummary" en la página 525	Sólo línea de mandatos.
scrolllines "Scrolllines" en la página 552	Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
scrollprompt "Scrollprompt" en la página 553	Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
subdir "Subdir" en la página 581	Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
timeformat "Timeformat" en la página 592	Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
todate "Todate" en la página 597	Sólo línea de mandatos.
totime "Totime" en la página 598	Sólo línea de mandatos.

Ejemplos

Tarea Visualizar una lista de todas las versiones de copia de seguridad activas o inactivas que se realizaron de los archivos del directorio actual.

```
dsmc query backup -inactive "*"
```

Tarea Visualizar una lista de todas las copias de seguridad del directorio actual. Utilice la opción detail para que se visualicen la última fecha de modificación y la última fecha de acceso de cada archivo.

```
dsmc q backup -detail "*"
```

Tarea Visualizar una lista de los archivos cuya copia de seguridad se ha realizado desde el directorio /home/proj y cuyos nombres de archivos empiezan por proj.

```
dsmc q b "/home/proj/proj*"
```

Tarea Visualizar una lista de las versiones de archivos de copia de seguridad activos e inactivos del sistema de archivos /home.

```
dsmc q b -ina -su=yes /home/
```

Tarea Consultar imágenes de sistemas de archivos del servidor de archivos NAS nas2.

```
dsmc query backup -nasnodename=nas2 -class=nas
```

Información relacionada

“Restauración de datos desde un conjunto de copias de seguridad” en la página 240

Consultar imágenes de sistemas de archivos NAS

Puede utilizar el mandato **query backup** para mostrar información acerca de las imágenes del sistema de archivos de un servidor de archivos NAS de las que se ha hecho una copia de seguridad. El cliente le solicita un ID de administrador.

Cuando reciba soporte, utilice la opción `nasnodename` para identificar el servidor de archivos NAS que debe consultarse. Especifique la opción `nasnodename` en el archivo de opciones del sistema cliente (`dsm.sys`). El valor del archivo de opciones del cliente es el valor predeterminado, pero este valor puede modificarse temporalmente en la línea de mandatos.

Utilice la opción `class` para especificar la clase del espacio de archivos que se ha de consultar. Para que se visualice una lista de las imágenes que pertenecen a un nodo NAS, utilice la opción `-class=nas`.

Referencia relacionada:

“Class” en la página 364

“Nasnodename” en la página 498

Query Backupset

El mandato **query backupset** consulta un juego de copias de seguridad de un archivo local, de un dispositivo de cinta (si es aplicable) o del servidor de IBM Spectrum Protect.

Este mandato muestra el nombre del juego de copias de seguridad, la fecha de generación, la retención (para un juego de copias de seguridad en el servidor de IBM Spectrum Protect) y una descripción proporcionada por el usuario.

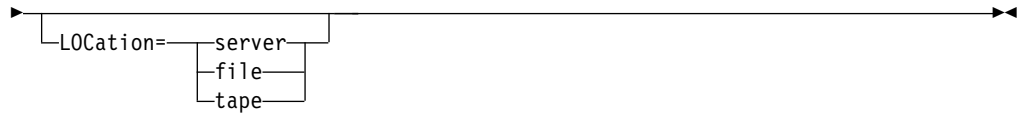
Clientes soportados

Este mandato es válido para todos los clientes.

El soporte para cintas solo está disponible en clientes de AIX y Oracle Solaris.

Sintaxis

```
➤➤ Query BACKUPSET [options] BACKUPSetName=[backupsetname  
localfilename  
tapedevice]➤➤
```



Parámetros

BACKUPSETName=

Especifica el nombre de un juego de copias de seguridad que desea consultar. Puede utilizar caracteres comodín para especificar el nombre del juego de copias de seguridad. Si utiliza caracteres comodín o no especifica ningún nombre de juego de copias de seguridad, se visualizarán todos los juegos de copias de seguridad que posea. Este parámetro es obligatorio.

Cuando se crea un juego de copias de seguridad, el servidor designa al usuario root como el propietario del juego de copias de seguridad. Al consultar un juego de copias de seguridad en el servidor, un usuario que no sea root no podrá ver el juego de copias de seguridad listado, incluso aunque conozca el nombre del juego de copias de seguridad y lo utilice en la consulta.

El valor de **backupsetname** depende de la ubicación del conjunto de copias de seguridad y se corresponde con una de estas tres opciones:

backupsetname

Especifica el nombre del juego de copias de seguridad del servidor. Si se especifica el parámetro **location**, debe establecer **-location=server**.

localfilename

Especifica el nombre de archivo del primer volumen del juego de copias de seguridad. Debe establecer **-location=file**.

tapedevice

Especifica el nombre del dispositivo de cinta que contiene el volumen del juego de copias de seguridad. Tiene que utilizar un controlador de dispositivo nativo de Windows, no el controlador de dispositivo proporcionado por IBM. Debe establecer **-location=tape**.

LOcation=

Especifica dónde ha de buscar el cliente de copia de seguridad y archivado el juego de copias de seguridad. Si no especifica el parámetro de ubicación, el cliente buscará juegos de copias de seguridad en el servidor de IBM Spectrum Protect.

server Especifica que el cliente buscará el juego de copias de seguridad del servidor. Esta ubicación es el valor predeterminado.

file Especifica que el cliente buscará el juego de copias de seguridad en un archivo local.

tape Especifica que el cliente buscará el juego de copias de seguridad en un dispositivo de cinta local.

Tabla 95. mandato query backupset: opciones relacionadas

Opción	Dónde se utiliza
description "Descripción" en la página 384	Sólo línea de mandatos.
scrolllines "Scrolllines" en la página 552	Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.

Tabla 95. mandato query backupset: opciones relacionadas (continuación)

Opción	Dónde se utiliza
scrollprompt "Scrollprompt" en la página 553	Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.

Ejemplos

Tarea Consultar todos los juegos de copias de seguridad del servidor de IBM Spectrum Protect.

Mandato: query backupset -backupsetname=*

Tarea Consultar un juego de copias de seguridad denominado monthly_financial_data desde el servidor IBM Spectrum Protect.

Mandato: query backupset
-backupsetname=monthly_financial_data.12345678

Tarea Consultar el juego de copias de seguridad en el archivo /home/budget/weekly_budget_data.ost.

mandato: dsmc query backupset -backupsetname="/home/budget/
weekly_budget_data.ost" -loc=file

Tarea Consultar el juego de copias de seguridad del dispositivo de cinta /dev/rmt0.

Mandato: dsmc query backupset -backupsetname=/dev/rmt0 -loc=tape

Información relacionada

"Restauración de datos desde un conjunto de copias de seguridad" en la página 240

query Backupset sin el parámetro backupsetname

El mandato **query backupset** se puede utilizar sin el parámetro **backupsetname**.

La sintaxis preferida para el mandato **query backupset** requiere el parámetro **backupsetname**. Antes de la especificación del parámetro **backupsetname**, el cliente de copia de seguridad y archivado ha consultado los conjuntos de copias de seguridad con una sintaxis distinta.

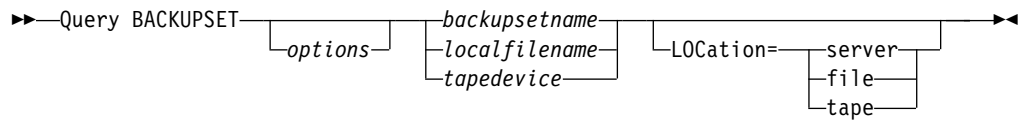
Aunque pueda utilizar la sintaxis de releases anteriores para este mandato, no lo haga a menos que tenga una necesidad específica y no pueda sustituir la sintaxis antigua por con sintaxis de Tivoli Storage Manager Versión 6.1. Para obtener los mejores resultados, utilice el parámetro **backupsetname**.

Clientes soportados

Este mandato es válido para todos los clientes.

El soporte para cintas solo está disponible en clientes de AIX y Oracle Solaris.

Sintaxis



Parámetros

backupsetname

Especifica el nombre del juego de copias de seguridad del servidor de IBM Spectrum Protect. Si se especifica el parámetro **location**, debe establecer `-location=server`.

localfilename

Especifica el nombre de archivo del primer volumen del juego de copias de seguridad. Debe establecer `-location=file`.

tapedevice

Especifica el nombre del dispositivo de cinta que contiene el volumen del juego de copias de seguridad. Tiene que utilizar un controlador de dispositivo nativo de Windows, no el controlador de dispositivo proporcionado por IBM. Debe establecer `-location=tape`.

LOCation=

Especifica dónde ha de buscar el cliente el juego de copias de seguridad. Si no especifica el parámetro de ubicación, el cliente buscará juegos de copias de seguridad en el servidor de IBM Spectrum Protect.

servidor

Especifica que el cliente buscará el juego de copias de seguridad del servidor. Éste es el valor predeterminado.

file

Especifica que el cliente buscará el juego de copias de seguridad en un archivo local.

tape

Especifica que el cliente buscará el juego de copias de seguridad en un dispositivo de cinta local.

Tabla 96. mandato query backupset: opciones relacionadas

Opción	Dónde se utiliza
description "Descripción" en la página 384	Sólo línea de mandatos.
scrolllines "Scrolllines" en la página 552	Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
scrollprompt "Scrollprompt" en la página 553	Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.

Ejemplos

Tarea Consultar todos los juegos de copias de seguridad del servidor de IBM Spectrum Protect.

Mandato: query backupset

Tarea Consultar un juego de copias de seguridad denominado `monthly_financial_data` del servidor de IBM Spectrum Protect.

Mandato: query backupset monthly_financial_data.12345678

Tarea Consultar el juego de copias de seguridad en el archivo
/home/budget/weekly_budget_data.ost.

Mandato: dsmc query backupset /home/budget/weekly_budget_data.ost
-loc=file

Tarea Consultar el juego de copias de seguridad del dispositivo de cinta
/dev/rmt0.

Mandato: dsmc query backupset /dev/rmt0 -loc=tape

Información relacionada

“Restauración de datos desde un conjunto de copias de seguridad” en la página 240

Query Filespace

El mandato **query filesystem** muestra una lista de espacios de archivos para un nodo. Los espacios de archivos se almacenan en el servidor de IBM Spectrum Protect o en el interior de un juego de copias de seguridad del servidor cuando se especifica la opción backupsetname. También puede especificar un único nombre de espacio de archivos para su consulta.

Un *espacio de archivos* es un espacio lógico del servidor que contiene archivos de los que se realizó copia de seguridad o de archivado. Se asigna un espacio de archivos por separado en el servidor para cada nodo de la estación de trabajo de la que ha realizado una copia de seguridad o ha archivado archivos.

Se asigna un espacio de archivos por separado en el servidor para cada sistema de archivos de la estación de trabajo de la que ha realizado una copia de seguridad o ha archivado archivos. El nombre del espacio de archivos es igual al nombre del sistema de archivos.

Clientes soportados

Este mandato es válido para todos los clientes.

Sintaxis

►► Query Filespace —filespace_{name} —options ►►

Parámetros

filespace_{name}

Especifica una serie de caracteres opcional que puede incluir caracteres comodín. Utilice este argumento para especificar un subconjunto de espacios de archivos. El valor predeterminado es la visualización de todos los espacios de archivos.

Tabla 97. Mandato query filespace: opciones relacionadas

Opción	Dónde se utiliza
backupsetname "Backupsetname" en la página 360	Sólo línea de mandatos.
class "Class" en la página 364	Sólo línea de mandatos.
dateformat "Dateformat" en la página 376	Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
detail "Detail" en la página 385	Sólo línea de mandatos.
fromnode "Fromnode" en la página 447	Sólo línea de mandatos.
fromowner "Fromowner" en la página 448	Sólo línea de mandatos.
nasnodename "Nasnodename" en la página 498	En el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos.
scrolllines "Scrolllines" en la página 552	Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
scrollprompt "Scrollprompt" en la página 553	Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
timeformat "Timeformat" en la página 592	Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.

Ejemplos

Visualizar los espacios de archivos. Utilice las opciones dateformat y timeformat para volver a formatear las fechas y las horas.

```
query filespace -date=5 -time=4
```

Visualizar el espacio de archivos /home.

```
query filespace /home
```

Visualizar los nombres de espacio de archivos que incluyen el patrón smith.

```
query filespace "*smith"
```

Consultar un espacio de archivos del servidor de archivos NAS nas2.

```
query filespace -nasnodename=nas2 -class=nas
```

Visualizar información detallada acerca del espacio de archivos que muestra el estado de réplica durante una migración tras error.

Mandato:

```
query filespace -detail
```

Salida:

#	Fecha último Incr	Tipo	fsID	Unicode	Réplica	Espacio archivos
1	00/00/0000 00:00:00	HFS	3	Si	Actual	/
	Fecha últ. alm.	Servidor			Local	
	Datos cop. seg.: 04/29/2013 16:49:55				04/29/2013 16:49:55	
	Datos archivado: Ninguna fecha disponible				Ninguna fecha disponible	

Conceptos relacionados:

“Restauración de datos desde un conjunto de copias de seguridad” en la página 240

“Visión general de migración tras error de cliente automatizado” en la página 94

Tareas relacionadas:

“Determinación del estado los datos replicados del cliente” en la página 100

Referencia relacionada:

“Nasnodename” en la página 498

“Class” en la página 364

“Nrtablepath” en la página 503

Consulta de espacios de archivos NAS

Utilice la opción `nasnodename` para identificar el servidor de archivos NAS que se debe consultar. Cuando se utilice una sesión de línea de mandatos interactiva con un ID que no es un ID de administración, el cliente solicitará un ID de administrador.

Especifique la opción `nasnodename` en el archivo de opciones del sistema cliente (`dsm.sys`). El valor del archivo de opciones de sistema del cliente es el valor predeterminado, pero este valor puede alterarse temporalmente en la línea de mandatos. Si no se ha especificado la opción `nasnodename` en el archivo de opciones del sistema del cliente, deberá especificarse en la línea de mandatos al procesar sistemas de archivos NAS.

Utilice la opción `class` para especificar la clase de objeto que se ha de consultar. Para que se visualice una lista de los espacios de archivos que pertenecen a un nodo NAS, utilice la opción `-class=nas`.

Query Group

Utilice el mandato **query group** para que se visualice información acerca de una copia de seguridad de grupo y sus miembros.

Nota:

1. Utilice la opción `showmembers` para visualizar y seleccionar los miembros individuales del grupo que desea consultar. La opción `showmembers` no es válida con la opción `inactive`. Si desea visualizar los miembros de un grupo que actualmente no están activos, utilice las opciones `pitdate` y `pittime` para especificar la fecha y la hora de copia de seguridad del miembro que desea consultar.
2. Utilice el mandato **query filespace** para visualizar nombres de espacios de archivos virtuales para el nodo que se almacenan en el servidor de IBM Spectrum Protect.

3. Si realiza una copia de seguridad de grupo completa y diferencial, una consulta de este grupo en la que se utilice la opción `-inactive` visualizará dos copias de seguridad activas con el mismo nombre, una de tipo FULL (completa) y otra de tipo DIFF (diferencial).

```
Protect> q group {/fs}/v1 -inactive
```

Tamaño	Fecha	copia seg.	Clase	gest	Grupo	A/I
978 B	06/02/2007 11:57:04	DEFAULT	A	FULL	/fs/v1	
32 B	06/05/2007 13:52:04	DEFAULT	A	DIFF	/fs/v1	

Si consulta una copia de seguridad de grupo sin la opción `-inactive`, la consulta sólo visualizará la última copia de seguridad de grupo, tanto si es de tipo FULL (completa) como de tipo DIFF (diferencial):

```
Protect> q group {/fs}/v1
```

Tamaño	Fecha	copia seg.	Clase	gest	Grupo	A/I
32 B	06/05/2007 13:52:04	DEFAULT	A	DIFF	/fs/v1	

Cientes soportados

Este mandato es válido para todos los clientes, a excepción de Mac OS X.

Sintaxis

►► Query GGroup — *filespec* — *options* ►►

Parámetros

filespec

Especifica el nombre del espacio de archivos virtual y el nombre del grupo que desea consultar en el servidor.

Tabla 98. Mandato `query group`: opciones relacionadas

Opción	Dónde se utiliza
fromnode "Fromnode" en la página 447	Sólo línea de mandatos.
fromowner "Fromowner" en la página 448	Sólo línea de mandatos.
inactive "Inactive" en la página 456	Sólo línea de mandatos.
pitdate "Pitdate" en la página 512	Sólo línea de mandatos.
pittime "Pittime" en la página 513	Sólo línea de mandatos.
showmembers "Showmembers" en la página 559 (no se aplica a Mac OS X)	Sólo línea de mandatos.

Ejemplos

Tarea Visualizar todos los grupos del espacio de archivos `/virtfs`.

Mandato:

```
query group /virtfs/*
```

Tarea Visualizar las versiones activas e inactivas del espacio de archivos /virtfs/group1.

Mandato:

```
query group /virtfs/group1 -inactive
```

Tarea Visualizar el espacio de archivos /virtfs/group1. Utilice la opción showmembers para que se visualice una lista de miembros de grupo a partir de los que poder seleccionar el miembro o miembros que desea consultar.

Mandato:

```
query group /virtfs/group1 -showmembers
```

Información relacionada

“Query Filespace” en la página 727

Query Image

El mandato **query image** muestra información sobre las imágenes del sistema de archivos que se almacenan en el servidor de IBM Spectrum Protect, o en el interior de un juego de copias de seguridad del servidor de IBM Spectrum Protect, cuando se especifica la opción backupsetname.

Se visualizará la siguiente información acerca de las imágenes del sistema de archivo:

- Tamaño de imagen - El tamaño del volumen del que se ha realizado la copia de seguridad.
- Tamaño almacenado - El tamaño de imagen real almacenado en el servidor. La imagen almacenada en el servidor de IBM Spectrum Protect tiene un tamaño que equivale a la capacidad del volumen. Para las copias de seguridad de imágenes en línea basadas en instantáneas, la imagen almacenada puede ser más grande que el sistema de archivos, basándose en el tamaño de los archivos de la caché. La imagen almacenada en el servidor tiene un tamaño que equivale a la capacidad del volumen.
- Tipo de sistema de archivos
- Fecha y hora de la copia de seguridad
- Clase de gestión que se asigna a la copia de seguridad de imágenes
- Si la copia de seguridad de imágenes es una copia activa o inactiva
- El nombre de la imagen

Nota: La API de IBM Spectrum Protect debe estar instalada para utilizar el mandato **query image**.

Clientes soportados

Esta opción es válida para clientes de AIX, Linux y Oracle Solaris.

Sintaxis

```

>> Query Image [—options] [—logicalvolumename] [—filespace] >>

```

Parámetros

nombrevolumenlógico

El nombre de un volumen lógico que desea consultar. Debe especificarse el nombre exacto de la imagen. No puede utilizar caracteres comodín. El valor predeterminado son todas las imágenes activas (a menos que se limiten mediante una o varias opciones).

filespace

Especifica el nombre del espacio de archivos que desea consultar.

Si omite *nombrevolumenlógico* y *nombreespacioarchivos*, se visualizarán todas las imágenes.

Tabla 99. Mandato query image: opciones relacionadas

Opción	Dónde se utiliza
backupsetname "Backupsetname" en la página 360	Sólo línea de mandatos.
dateformat "Dateformat" en la página 376	Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
fromnode "Fromnode" en la página 447	Sólo línea de mandatos.
fromowner "Fromowner" en la página 448	Sólo línea de mandatos.
inactive "Inactive" en la página 456	Sólo línea de mandatos.
numberformat "Numberformat" en la página 504	Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
pitdate "Pitdate" en la página 512	Sólo línea de mandatos.
pittime "Pittime" en la página 513	Sólo línea de mandatos.
scrolllines "Scrolllines" en la página 552	Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
scrollprompt "Scrollprompt" en la página 553	Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
timeformat "Timeformat" en la página 592	Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.

Ejemplos

Tarea Mostrar todas las imágenes de las que se ha realizado copia de seguridad.

Mandato: q image

Tarea Mostrar todas las imágenes de las que se ha realizado copia de seguridad propiedad de kutas en el nodo avalon.

Mandato: query image -fromnode=avalon -fromowner=kutas

Tarea Visualizar las versiones activas e inactivas de la imagen /usr.

Mandato: q i /usr -inactive

Tarea Mostrar todas las imágenes que están contenidas en el juego de copias de seguridad llamado `weekly_backup_data.32145678`.

Mandato: `query image -backupsetname=weekly_backup_data.32145678`

Información relacionada

“Restauración de datos desde un conjunto de copias de seguridad” en la página 240

Query Inclexcl

El mandato **query inclexcl** visualiza una lista de sentencias de inclusión/exclusión en el orden en que se procesan durante las operaciones de copia de seguridad/archivado. La lista visualiza el tipo de opción, el ámbito de la opción (archive, all, etc.), y el nombre del archivo fuente.

El cliente de archivado y copia de seguridad excluye algunos archivos de las operaciones de copia de seguridad y restauración del sistema de archivos. Puede utilizar el mandato **query inclexcl** para visualizar una lista de estos archivos. En la salida del mandato, estos archivos tienen Sistema operativo junto a la vía de acceso.

Puede comprobar la validez de los patrones que desea utilizar en la lista de inclusión/exclusión antes de insertarlos realmente en el archivo de opciones. Consulte la explicación sobre *el patrón de prueba*.

Utilice la opción `detail` para que se visualice la clase de gestión que se asocia a una sentencia de inclusión/exclusión.

Clientes soportados

Este mandato es válido para todos los clientes.

Sintaxis

```
►► Query INCLexcl — [test pattern] [-DETail] —►►
```

Parámetros

test pattern

Se utiliza para comprobar la validez de los patrones que desea utilizar en la lista de inclusión/exclusión. Cuando utilice un patrón de prueba con este mandato, ocurre lo siguiente:

- No se muestra la lista de inclusión/exclusión interna.
- El patrón se procesa como si se hubiera originado en una sentencia de inclusión/exclusión, incluyendo toda la comprobación de errores habitual
- El patrón se muestra tal y como aparecería en la lista de inclusión/exclusión

Si el patrón de prueba no contiene errores, el resultado del patrón compilado es el mismo que el del patrón de prueba.

-DETail

Visualiza la clase de gestión que se asocia a cada sentencia.

Ejemplos

Tarea Excluir un archivo de la eliminación de duplicados excluyéndolo del archivo de opciones de cliente:

```
Exclude Dedup *\...\file2
```

Tarea Visualiza una lista básica de sentencias de inclusión/exclusión. Mandato:

```
query inclexcl
```

Tarea Visualizar una lista de sentencias de inclusión/exclusión. Visualiza la clase de gestión que se asocia con cada sentencia.

```
query inclexcl -detail
```

Tarea Comprobar la validez de este patrón: `/.../?x?/*.log`

```
query inclexcl /.../?x?/*.log
```

Query Mgmtclass

El mandato **query mgmtclass** visualiza la información sobre las clases de gestión disponibles en el conjunto de políticas activo.

El administrador define clases de gestión que contienen atributos que controlan si un archivo es elegible para los servicios de copias de seguridad o archivado. Las clases de gestión también determinan el modo en que se gestionan las copias de seguridad y las copias archivadas en el servidor.

El conjunto de políticas activo contiene una clase de gestión predeterminada; puede contener cualquier número de clases de gestión adicionales. Puede asignar clases de gestión específicas a los archivos mediante la utilización de las opciones `include` que se encuentran en el archivo de opciones de usuario del cliente (`dsm.opt`). Si no asigna una clase de gestión a un archivo, se utiliza la clase de gestión predeterminada.

Si realiza una copia archivada, podrá modificar temporalmente la clase de gestión asignada utilizando la opción `archmc`.

Clientes soportados

Este mandato es válido para todos los clientes.

Sintaxis

```
►►—Query Mgmtclass—┐
                    └─options─┘►►
```

Parámetros

Tabla 100. Mandato query mgmtclass: opciones relacionadas

Opción	Dónde se utiliza
<code>detail</code> “Detail” en la página 385	Sólo línea de mandatos.
<code>fromnode</code> “Fromnode” en la página 447	Sólo línea de mandatos.

Ejemplos

Tarea Mostrar las clases de gestión predeterminadas y disponibles.

Mandato: query mgmtclass

Query Node

El mandato **query node** muestra todos los nodos en los que un identificador de usuario de administración dispone de autorización para realizar operaciones. Se le solicitará el ID de administrador de IBM Spectrum Protect.

Idealmente, el ID de usuario de administración tiene como mínimo autorización de propietario de cliente sobre el nodo de estación de trabajo de cliente que utiliza desde la línea de mandatos o desde la Web.

Utilice la opción `type` para especificar el tipo de nodo que se ha de filtrar. Los valores válidos son los siguientes:

- nas
- client
- servidor
- any

El valor predeterminado es **any**.

Nota: Cuando se instala el archivo de licencia de IBM Spectrum Protect for Virtual Environments: Data Protection for VMware en un servidor de copia de seguridad vStorage, la serie de la plataforma almacenada en el servidor IBM Spectrum Protect se establece en "TDP VMware" para todos los nombres de nodo utilizados en esa máquina. La serie de la plataforma puede utilizarse en el contexto de los cálculos de PVU. Si un nodo se está utilizando para realizar una copia de seguridad de la máquina con funciones de cliente con copia de seguridad-archivado estándar (por ejemplo, a nivel de archivo o copia de seguridad de imágenes), esta serie de plataforma debe interpretarse como un "cliente" para los cálculos de PVU.

Para obtener más información sobre unidades de valor del procesador, consulte *Estimación de unidades de valor de procesador (PVU)* en la documentación del servidor de IBM Spectrum Protect.

Clientes soportados

Este mandato es válido para todos los clientes.

Sintaxis

►► Query Node —options— ►►

Parámetros

Tabla 101. Mandato query node: opciones relacionadas

Opción	Dónde se utiliza
type "Type" en la página 600	Sólo línea de mandatos.

Tabla 101. Mandato query node: opciones relacionadas (continuación)

Opción	Dónde se utiliza
scrolllines "Scrolllines" en la página 552	Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
scrollprompt "Scrollprompt" en la página 553	Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.

Ejemplos

Tarea Mostrar todos los nodos NAS.

Mandato: query node -type=nas

Tarea Visualizar todos los nodos cliente que son clientes de copia de seguridad/archivado.

Mandato: query node -type=client

Información relacionada

"Type" en la página 600

Query Options

Utilice el mandato **query options** para que se visualicen todas o parte de las opciones y sus valores actuales relacionados con el cliente de línea de mandatos.

Clientes soportados

Este mandato es válido para todos los clientes.

Sintaxis

```

▶▶ Query Options [—options—] —pattern—▶▶

```

Parámetros

patrón

Serie de caracteres opcional que puede incluir comodines. Utilice este argumento para especificar un subconjunto de opciones. El valor predeterminado consiste en visualizar todas las opciones.

Tabla 102. Mandato query options: opciones relacionadas

Opción	Dónde se utiliza
scrolllines "Scrolllines" en la página 552	Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
scrollprompt "Scrollprompt" en la página 553	Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.

Ejemplos

Tarea Visualizar todas las opciones y sus valores.
`query options`

Tarea Visualizar sólo las opciones que empiezan por *comm*.
`query options comm*`

Tarea Visualiza el valor de la opción **sustituir**.
`query options replace`

Tarea Emita el mandato para visualizar todas las opciones y sus valores. Se visualizará la información de estado de migración tras error.
`query options`

Salida:

```
MYPRIMARYSERVERNAME: SERVER1
MYREPLICATIONSERVER: TARGET
  REPLSERVERNAME: TARGET
    Address: 192.0.2.9
      Port: 1501
    SSLPort: 1502
    GUID: 39.5a.da.d1.ae.92.11.e2.82.d3.00.0c.29.2f.07.d3
    Used: yes
```

Conceptos relacionados:

“Configuración y uso de la migración tras error automática del cliente” en la página 94

Tareas relacionadas:

“Determinación del estado los datos replicados del cliente” en la página 100

Query Restore

El mandato **query restore** visualiza una lista de las sesiones de restauración reiniciables de la base de datos del servidor. La lista contiene los siguientes campos: owner, replace, subdir, preservepath, source y destination.

Se crea una sesión de restauración reinicialable cuando un mandato restore no se ejecuta correctamente debido a una anomalía en la red, en el cliente, en el servidor o cualquier otro problema parecido. Cuando se produce una anomalía, se bloquea el espacio de archivos del servidor por lo que no se pueden traspasar los archivos fuera de los volúmenes secuenciales. Para desbloquear el espacio de archivos, reinicie la restauración hasta que finalice (mandato **query restore**), o cancele la restauración (mandato **cancel restore**). Utilice **query restore** para determinar si hay sesiones de restauración reiniciables y qué espacios de archivos se ven afectados.

Clientes soportados

Este mandato es válido para todos los clientes.

Sintaxis

►►—Query Restore—◄◄

Parámetros

No hay parámetros para este mandato.

Ejemplos

Tarea Mostrar la sesión de restauración reinicial en la base de datos del servidor.

Mandato: query restore

Query Schedule

El mandato **query schedule** visualiza los eventos planificados de su nodo. El administrador puede establecer planificaciones para realizar operaciones de copia de seguridad/archivado de forma automática. A fin de planificar el trabajo, utilice este mandato para determinar cuándo van a ocurrir los siguientes eventos planificados.

Clientes soportados

Este mandato es válido para todos los clientes.

Sintaxis

►►—Query SChedule—◄◄

Parámetros

No hay parámetros para este mandato.

Ejemplos

Tarea Mostrar los eventos planificados.

Mandato: query schedule

Query Session

El mandato **query session** muestra información acerca de la sesión como, por ejemplo, el nombre de nodo actual, cuándo se ha establecido la sesión, información del servidor e información de conexión del servidor.

Clientes soportados

Este mandato es válido para todos los clientes.

Sintaxis

►►—Query SSession—◄◄

Parámetros

No hay parámetros para este mandato.

Ejemplos

Tarea Mostrar información acerca de la sesión.

Mandato: query session

A continuación, se muestra una pantalla **query session** de ejemplo:

```
Nombre de servidor.....: HALLEY_SERVER1
Tipo de servidor.....: Windows
Protección de archivo de retención..: "No"
Versión de servidor.....: Ver. 6, Rel. 2, Niv. 0.0
Fecha último acceso.....: 09/03/2009 09:08:13
Suprimir archivos copia seg.....: "No"
Suprimir copias archivadas.....: "Sí"
Deduplicación.....: "Sólo servidor"

Nombre de nodo.....: HALLEY
Nombre de usuario.....:
```

Valores posibles de eliminación de duplicados de parte del cliente:

- Ninguna
 - Se visualizará al conectarse a un servidor IBM Spectrum Protect anterior a V6.1
- Sólo servidor
- Cliente o Servidor

Tarea

A continuación, se muestra una pantalla **query session** con Activar sin LAN activado de ejemplo:

Información de conexión de IBM Spectrum Protect Server

```
Nombre de servidor.....: TEMPLAR
Tipo de servidor.....: AIX
Protección de archivo de retención..: "No"
Versión de servidor.....: Ver. 6, Rel. 1, Niv. 4.0
Fecha último acceso.....: 08/12/10 22:10:15
Suprimir archivos copia seg.....: "No"
Suprimir copias archivadas.....: "Sí"
```

```
Nombre de nodo.....: LAN2
Nombre de usuario.....: root
```

```
Nombre agente almacenamiento...: TEMPLAR_STA
Tipo agente almacenamiento.....: AIX
Versión agente almacenamiento..: Ver. 6, Rel. 1, Niv. 3.3
```

Query Systeminfo

Utilice el mandato **query systeminfo** para recopilar información y enviar esta información a un archivo o a la consola.

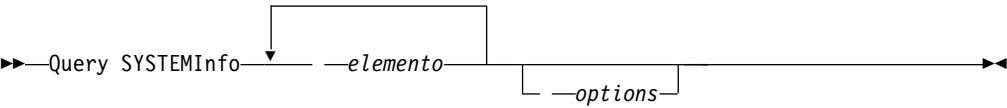
La finalidad principal de este mandato es ayudar al soporte de IBM en el diagnóstico de problemas. Sin embargo, los usuarios que estén familiarizados con los conceptos relacionados con esta información también podrían encontrarlo de utilidad.

Si utiliza la opción `console`, no se realiza ningún formato especial de la salida para ajustarla a la altura o anchura de la pantalla. Por consiguiente, es posible que la salida de la consola sea difícil de leer debido a la longitud y a la acomodación de líneas. Si la salida de la consola es difícil de leer, utilizar la opción `filename` con el mandato **query systeminfo**. Esta combinación permite que la salida se grabe en un archivo que puede enviarse al soporte de IBM.

Clientes soportados

Este mandato es válido para todos los clientes.

Sintaxis



Parámetros

elemento

Especifica el elemento o elementos de los que desea recopilar información y que la información debe enviarse al nombre de archivo que ha especificado con la opción *filename* o a la consola. El valor predeterminado consiste en reunir todos los elementos.

Puede recopilar información acerca de uno o varios de los elementos siguientes:

- DSMOPTFILE - El contenido del archivo *dsm.opt*.
- DSMSYSFILE - El contenido del archivo *dsm.sys*.
- ENV - Variables de entorno.
- ERRORLOG - El archivo de anotaciones de errores del cliente.
- FILE - Atributos para el nombre de archivo que especifique.
- INCLEXCL - Compila una lista de sentencias de inclusión/exclusión en el orden en el que se procesan durante las operaciones de copia de seguridad y archivado.
- OPTIONS - Opciones compiladas.
- OSINFO - Nombre y versión del sistema operativo cliente (incluye la información *ULIMIT* para UNIX).
- POLICY - Volcado de conjunto de políticas.
- SCHEDLOG - Contenido del registro de planificación (por lo general, *dsmsched.log*).
- CLUSTER - Información de clústeres de AIX.
- ENCRYPT - Métodos de cifrado disponibles.

Nota:

1. Utilice la opción *filename* para especificar un nombre de archivo en el que almacenar la información que se ha recopilado a partir de los elementos que ha especificado. Si no especifica un nombre de archivo, la información se almacenará, de forma predeterminada, en el archivo */Library/Application Support/tivoli/tsm/client/ba/bin/dsminfo.txt* (para Mac OS X) o en el archivo *dsminfo.txt* (para otros sistemas UNIX y Linux).
2. Utilice la opción *console* si desea que la información se muestre en la consola.

Tabla 103. mandato *query systeminfo*: opciones relacionadas

Opción	Dónde se utiliza
<i>console</i> "Console" en la página 372	Sólo línea de mandatos.
<i>filename</i> "Filename" en la página 442	Sólo línea de mandatos.

Ejemplos

Tarea Recopilar y almacenar el contenido del archivo dsm.opt y del archivo de anotaciones de error de IBM Spectrum Protect en el archivo tsminfo.txt.

Mandato: query systeminfo dsmoptfile errorlog -filename=tsminfo.txt

Información relacionada

“Filename” en la página 442

“Console” en la página 372

Query VM

Utilice el mandato **query VM** para ver una lista y verificar las copias de seguridad correctas de las máquinas virtuales.

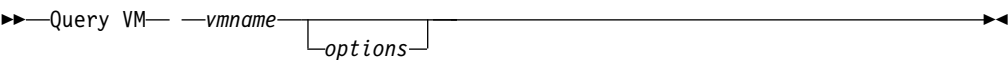
Query VM para máquinas virtuales VMware

Utilice el mandato **query vm** para determinar de qué máquinas virtuales VMware se ha realizado una copia de seguridad.

Clientes soportados

Este mandato es válido en clientes Linux instalados en un servidor de copia de seguridad vStorage.

Sintaxis



Parámetros

vmname

Especifica el nombre de host de máquina virtual que desea consultar. Si omite el nombre de la máquina virtual, el mandato muestra todas las copias de seguridad de máquina virtual en el servidor IBM Spectrum Protect.

Tabla 104. Mandato Query VM: opciones relacionadas para consultas de la máquina virtual VMwar.

Opción	Dónde se utiliza
detail “Detail” en la página 385 Válido para vmbackuptype=fullvm	Línea de mandatos.
inactive “Inactive” en la página 456 Válido para vmbackuptype=fullvm	Línea de mandatos.
pitdate “Pitdate” en la página 512 Válido para vmbackuptype=fullvm	Línea de mandatos.
pittime “Pittime” en la página 513 Válido para vmbackuptype=fullvm	Línea de mandatos.

Tabla 104. Mandato Query VM: opciones relacionadas para consultas de la máquina virtual VMwar. (continuación)

Opción	Dónde se utiliza
vmbackuptype "Vmbackuptype" en la página 611	Línea de mandatos o archivo de opciones del cliente.
vmchost "Vmchost" en la página 612	Línea de mandatos o archivo de opciones del cliente.
vmcpw "Vmcpw" en la página 613	Línea de mandatos o archivo de opciones del cliente.
vmcuser "Vmcuser" en la página 615	Línea de mandatos o archivo de opciones del cliente.

Ejemplos de Query VM (VMware)

A continuación, se muestran ejemplos del uso del mandato **query VM** con una máquina virtual completa, y con una máquina virtual completa y la opción **-detail**.

Máquina virtual completa

```

QUERY
VM -INA -vmbackuptype=FULLVM

```

Núm	Fecha	copia	seg	Clase	gest	Tipo	A/I	Máquina virtual
1	09/26/2010 11:34:14			DEFAULT		VMFULL	A	vm1
2	09/26/2010 11:34:37			DEFAULT		VMFULL	A	vm2
3	09/26/2010 11:34:49			DEFAULT		VMFULL	A	vm3
4	09/26/2010 12:35:08			DEFAULT		VMFULL	I	vm2
5	09/26/2010 12:35:18			DEFAULT		VMFULL	I	vm3

VM completa con opción **-detail**

```

q vm Small-SQL -detail
IBM Spectrum Protect
Interfaz de línea de mandatos del cliente de copia de
seguridad/archivado
Versión de cliente 8, release 1, nivel 0.0
Fecha/hora del cliente: 12/09/2016 12:05:35
(c) Copyright by IBM Corporation y otros 1990, 2016. Reservados todos los derechos.

Nombre de nodo: BAClient-DM
Sesión establecida con el servidor TSM_SERVER1: Windows
Versión de servidor 8, release 1, nivel 0.0
Fecha/hora del servidor: 12/09/2016 12:05:35 Último acceso: 12/08/2016 14:22:55

Consultar máquina virtual para copia completa de máquina
virtual

# Fecha copia seg. Clase gest Tamaño Tipo A/I Máquina
virtual
- - - - -
1 06/26/2012 14:07:13 STANDARD 19.53 GB FULL A Small-SQL
Tamaño de la copia de seguridad incremental: n/d
Número de copias de seguridad incrementales desde la última completa: n/d
Cantidad de datos adicionales: n/d
Fragmentación de objetos: n/d
Copia de seguridad representada por: n/d
Tipo de protección de aplicaciones: TSM VSS
Aplicaciones protegidas: MS SQL 2008
DISK[1]Etiqueta: Disco duro 1
DISK[1]Nombre: [datastore1] Cloned-Small-SQL/Cloned-Small-SQL-000001.vmdk
DISK[1]Estado: Protegido

```

Consultar todas las máquinas virtuales VMware de las que se hizo copia de seguridad utilizando `-vmbacktype=fullvm`:

```
q vm * -vmbackuptype=fullvm
```

Tareas relacionadas:

“Preparación del entorno para copias de seguridad paralelas de máquinas virtuales VMware” en la página 220

Restart Restore

El mandato **restart restore** visualiza una lista de las sesiones de restauración reiniciables en la base de datos del servidor.

Sólo puede reiniciar una única sesión de restauración reinicialable al mismo tiempo. Vuelva a ejecutar el mandato **restart restore** para reiniciar más restauraciones.

La restauración reiniciada utiliza las mismas opciones que se usaron en la restauración que no se pudo ejecutar. La restauración reiniciada continúa a partir del punto en que se detuvo la restauración anterior.

Para cancelar sesiones de restauración reiniciables, utilice el mandato **cancel restore**. Utilice el mandato **restart restore** cuando:

- Las sesiones de restauración reiniciables bloquean el espacio de archivos del servidor, por lo que los archivos no se pueden traspasar fuera de los volúmenes secuenciales del servidor.
- No se puede hacer una copia de seguridad de archivos afectados por una restauración reinicialable.

Las opciones de la sesión que no se pudo ejecutar sustituyen a las opciones nuevas o modificadas de la sesión reiniciada.

Clientes soportados

Este mandato es válido para todos los clientes.

Sintaxis

►—REStArt Restore—◄◄

Parámetros

No hay parámetros para este mandato.

Ejemplos

Tarea Reiniciar una restauración.

Mandato: restart restore

Restore

El mandato **restore** obtiene copias de versiones de las copias de seguridad de los archivos del servidor de IBM Spectrum Protect o en el interior de un conjunto de copias de seguridad.

Para restaurar los archivos, especifique los directorios o los archivos seleccionados o seleccione los archivos en una lista. Puede restaurar los archivos en el directorio desde donde se realizó la copia de seguridad o en otro directorio. El cliente de copia de seguridad y archivado utiliza la opción **preservepath** con el valor subtree como valor predeterminado para restaurar los archivos.

Nota:

1. En los sistemas UNIX y Linux, cuando se ha creado un enlace simbólico, la hora de modificación de éste se establece en la hora actual del sistema y no puede cambiarse. De esta manera, cuando se restaura un vínculo simbólico, su fecha y hora de modificación se establecen en la fecha y la hora de la restauración y no en la fecha y la hora en que se hizo copia de seguridad del vínculo. Como resultado, el cliente hará copia de seguridad del vínculo simbólico durante la siguiente copia de seguridad incremental, puesto que su hora de modificación ha cambiado desde la última copia de seguridad.

Si establece la opción **subdir** en yes al restaurar una vía de acceso y un archivo específicos, el cliente restaura de forma recursiva todos los subdirectorios bajo esa vía de acceso y las instancias del archivo especificado que existan en los subdirectorios.

Si restaura un directorio o un árbol de directorios completo y no especifica las opciones inactive, latest, pick, todote y fromdate en el mandato **restore**, el cliente hace un seguimiento de los objetos que se restauran. Si, por alguna razón, el proceso de restauración se interrumpe, puede reiniciar la restauración en el punto de interrupción emitiendo el mandato **restart restore**. Se pueden crear varias sesiones de restauración reiniciables. Las restauraciones sólo son reiniciables si la especificación de archivo consta sólo de caracteres comodín. Por ejemplo, para una restauración reinicialable, emita:

```
dsmc rest /home/* -sub=yes
```

Para una restauración que no sea reinicialable, emita:

```
dsmc rest "/Users/user1/file?.c" -sub=yes
```

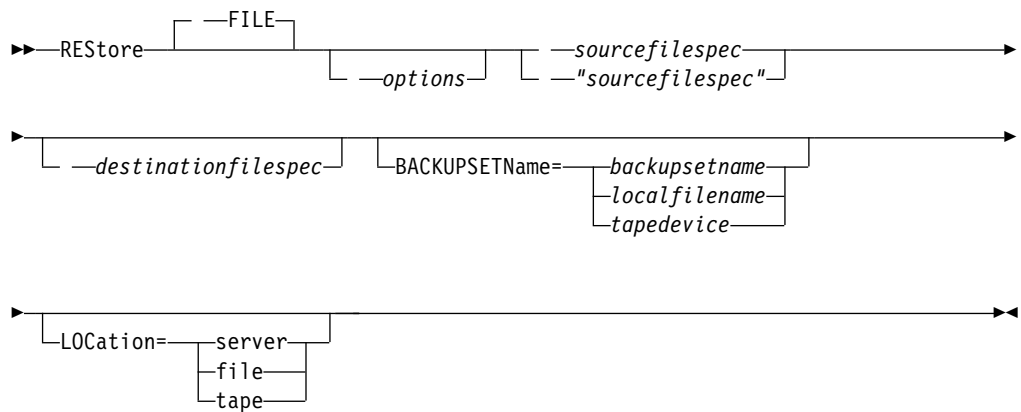
Utilice el mandato **query restore** para visualizar una lista de las sesiones de restauración reinicialables en la base de datos del servidor. No podrán realizarse copias de seguridad del sistema de archivos adicionales, a menos que la restauración reinicialable se complete mediante la utilización del mandato **restart restore** o se cancele mediante la utilización del mandato **cancel restore**.

```
dsmc rest "/Users/user1/file?.c" -sub=yes
```

Clientes soportados

Este mandato es válido para todos los clientes.

Sintaxis



Parámetros

file

Este parámetro especifica que el nombre del archivo origen es un nombre de archivo explícito. Este parámetro es necesario cuando se restaura un nombre de archivo desde la vía de acceso actual, cuando no se especifica una vía de acceso relativa o absoluta y cuando el nombre de archivo entra en conflicto con una de las palabras clave reservadas del mandato **restore**, como **restore backupset**.

sourcefilespec

Especifica la ruta y el nombre del archivo del almacenamiento que desea restaurar. Utilice caracteres comodín para especificar un grupo de archivos o todos los archivos de un directorio.

{filespace}

Nombra el espacio de archivos (incluido entre llaves) del servidor que contiene los archivos que quiere restaurar. Éste es el nombre de la unidad de la estación de trabajo desde la que realizó la copia de seguridad de los archivos.

Especifique el nombre del espacio de archivos si el nombre de etiqueta de unidad ha sido modificado o si está restaurando archivos cuyas copias de seguridad se realizaron desde otro nodo con nombres de etiqueta de unidad diferentes de los suyos.

destinationfilespec

Indica la ruta y el nombre de archivo donde desea colocar los archivos restaurados. Si no especifica un destino, el cliente restaura los archivos en la ruta de origen inicial.

- Si *sourcefilespec* especifica un único archivo, *destinationfilespec* puede ser un archivo o un directorio. Si está restaurando un único archivo, tiene la opción de terminar la especificación con un nombre de archivo si desea cambiar el nombre del archivo restaurado por uno nuevo.
- Si *sourcefilespec* contiene caracteres comodín o se especifica *subdir=yes*, *destinationfilespec* debe ser un directorio y debe terminar con un delimitador de directorio (\).

Nota: Si la vía de acceso de destino o cualquier parte de ella no existe, el cliente creará una vía de acceso.

Nota: si no especifica un destino, el cliente determina si puede accederse al sistema de archivos original. Si no es posible acceder al sistema de archivos original, el cliente no restaurará el archivo. En este caso, puede especificar un destino distinto y volver a intentar el mandato.

BACKUPSETName=

Especifica el nombre de un juego de copias de seguridad. Este parámetro es opcional. Si especifica el parámetro **backupsetname** con el mandato **restore**, no puede utilizar la opción **pick**.

El valor de **backupsetname** depende de la ubicación del conjunto de copias de seguridad y se corresponde con una de las opciones siguientes:

backupsetname

Especifica el nombre del juego de copias de seguridad del servidor de IBM Spectrum Protect. Si se especifica el parámetro **location**, debe establecer **-location=server**. Si el conjunto de copias de seguridad está ubicado en el almacenamiento del servidor de IBM Spectrum Protect, el juego de copias de seguridad debe tener una tabla de contenido.

localfilename

Especifica el nombre de archivo del primer volumen del juego de copias de seguridad. Debe establecer **-location=file**.

tapedevice

Especifica el nombre del dispositivo de cinta que contiene el volumen del juego de copias de seguridad. Tiene que utilizar un controlador de dispositivo proporcionado por Windows, no el controlador de dispositivo que proporciona IBM. Debe establecer **-location=tape**.

LOCation=

Especifica dónde ha de buscar el cliente el juego de copias de seguridad. Si no especifica el parámetro de ubicación, el cliente buscará juegos de copias de seguridad en el servidor de IBM Spectrum Protect.

servidor

Especifica que el cliente buscará el juego de copias de seguridad del servidor. Se trata de la ubicación predeterminada.

file Especifica que el cliente buscará el juego de copias de seguridad en un archivo local.

tape Especifica que el cliente buscará el juego de copias de seguridad en un dispositivo de cinta local.

Tabla 105. mandato Restore: opciones relacionadas

Opción	Dónde se utiliza
dateformat "Dateformat" en la página 376	Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
dirsonly "Dirsonly" en la página 390	Sólo línea de mandatos.
filelist "Filelist" en la página 439	Sólo línea de mandatos.
filesonly "Filesonly" en la página 443	Sólo línea de mandatos.
followsymbolic "Followsymbolic" en la página 444	Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
fromdate "Fromdate" en la página 446	Sólo línea de mandatos.
fromnode "Fromnode" en la página 447	Sólo línea de mandatos.
fromowner "Fromowner" en la página 448	Sólo línea de mandatos.
fromtime "Fromtime" en la página 448	Sólo línea de mandatos.
ifnewer "Ifnewer" en la página 453	Sólo línea de mandatos.
inactive "Inactive" en la página 456	Sólo línea de mandatos.
latest "Latest" en la página 483	Sólo línea de mandatos.
numberformat "Numberformat" en la página 504	Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
pick Nota: Si especifica el parámetro backupsetname con el mandato restore , no puede utilizar la opción pick. "Pick" en la página 512	Sólo línea de mandatos.
pitdate "Pitdate" en la página 512	Sólo línea de mandatos.
pittime "Pittime" en la página 513	Sólo línea de mandatos.
preservepath "Preservepath" en la página 520	Sólo línea de mandatos.
replace "Replace" en la página 529	Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
subdir "Subdir" en la página 581	Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
tapeprompt "Tapeprompt" en la página 583	Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.

Tabla 105. mandato Restore: opciones relacionadas (continuación)

Opción	Dónde se utiliza
timeformat "Timeformat" en la página 592	Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
todate "Todate" en la página 597	Sólo línea de mandatos.
totime "Totime" en la página 598	Sólo línea de mandatos.

Ejemplos

- Tarea** Restaurar un único archivo denominado budget en el directorio /Users/user1/Documents.
- ```
restore /home/devel/projecta/budget
```
- Tarea** Restaurar un único archivo denominado budget que existe en el directorio actual.
- ```
restore file budget
```
- Tarea** Restaurar todos los archivos que tienen la extensión de archivo .c del directorio /home/devel/projecta.
- ```
restore "/home/devel/projecta/*.c"
```
- Tarea** Restaurar archivos en el directorio /user/project. Utilice las opciones pick e inactive para seleccionar las versiones de copia de seguridad activas e inactivas.
- ```
restore "/user/project/*" -pick -inactive
```
- Tarea** Restaurar todos los archivos del directorio /home/devel/projecta que finalizan con el carácter .c en el directorio /home/newdevel/projectn/projecta. Si el directorio projectn o projectn/projecta no existe, se creará.
- ```
restore "/home/devel/projecta/*.c" /home/newdevel/projectn/
```
- Tarea** Restaurar todos los archivos del directorio /home/mydir en el estado que éstos tenían a las 13:00 horas del día 17 de agosto de 2002.
- ```
restore -pitd=8/17/2002 -pitt=13:00:00 /home/mydir/
```
- Tarea** Restaurar todos los objetos en el directorio /home/myid/. Puesto que esta operación de restauración se especifica sólo con caracteres comodín, si el proceso se interrumpiera, se crearía una sesión de restauración reinicializable.
- ```
res "/home/myid/*"
```
- Tarea** Restaurar todos los archivos del directorio /home/mydir en el estado que éstos tenían a las 13:00 horas del día 17 de agosto de 2002.
- ```
restore -pitd=8/17/2002 -pitt=13:00:00 /home/mydir/
```

Información relacionada

"Restauración de datos desde un conjunto de copias de seguridad" en la página 240

"Preservepath" en la página 520

Restauración desde espacios de archivos que no están activados para Unicode

Si desea realizar una restauración desde espacios de archivos que no están activados para Unicode, debe especificar el origen en el servidor y un destino en el cliente, antes de instalar el cliente activado para Unicode.

Nota: Esta sección acerca de Unicode sólo se aplica a Mac OS X.

Por ejemplo, imaginemos que Jaguar es el nombre del disco de arranque y que ha realizado la copia de seguridad de todos los archivos `.log` en el directorio `/Users/user5/Documents`. Antes de que se produzca la operación de copia de seguridad, el servidor cambia el nombre del espacio de archivos por `Jaguar_OLD`. La operación de copia de seguridad coloca los datos especificados en la operación actual en el espacio de archivos activado para Unicode denominado `/`. Ahora, el nuevo espacio de archivos activado para Unicode sólo contiene el directorio `/Users/user5/Documents` y los archivos `*.log` especificados en la operación.

Si desea restaurar un archivo del espacio de archivos *nombre cambiado* (old) en su ubicación original, deberá especificar el origen y el destino de la forma siguiente:

```
restore Jaguar_OLD/Users/user5/Documents  
/mylog.log /Users/user5/Documents/
```

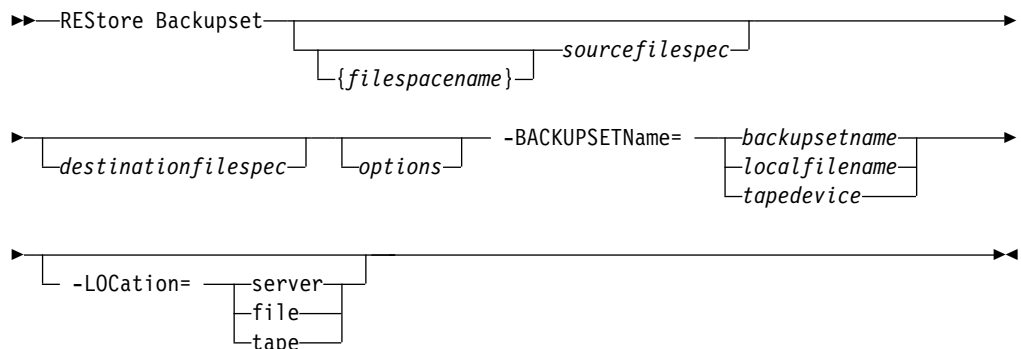
Restore Backupset

El mandato **restore backupset** restaura un juego de copias de seguridad del servidor de IBM Spectrum Protect, de un archivo local o de un dispositivo de cinta local. Puede restaurar todo el juego de copias de seguridad o, en algunos casos, archivos específicos del juego de copias de seguridad.

Clientes soportados

Este mandato es válido para todos los clientes.

Sintaxis



Parámetros

`{filespace name}`

Nombra el espacio de archivos (incluido entre llaves) del servidor que contiene los archivos que quiere restaurar. Éste es el nombre de la unidad de la estación

de trabajo de cuyos archivos se realizó copia de seguridad o el nombre de espacio de archivos virtual para el grupo.

Especifique un nombre de espacio de archivos cuando restaure un conjunto de copias de seguridad que contenga un grupo.

Especifique un nombre de espacio de archivos cuando el parámetro *sourcefilespec* no exista en el sistema de destino. Esto puede suceder si el nombre de la etiqueta de unidad ha sido modificado o si está restaurando archivos de los que ha realizado copia de seguridad desde otro nodo con etiquetas de unidad distintas de las suyas.

sourcefilespec

Especifica la vía de acceso de origen de una parte del conjunto de copias de seguridad. El valor predeterminado es restaurar todo el conjunto de copias de seguridad.

destinationfilespec

Especifica la vía de acceso de destino para los archivos restaurados. Si no especifica *sourcefilespec*, no puede especificar *destinationfilespec*. Si no especifica un destino, el cliente de copia de seguridad y archivado restaura los archivos en la ruta de origen inicial. Si está restaurando más de un archivo, debe terminar la especificación de archivo con un delimitador de directorio (/); de lo contrario, el cliente presupone que el último nombre es un nombre de archivo e indica que se ha producido un error. Si está restaurando un único archivo, tiene la opción de terminar la especificación de archivo con un nombre de archivo si desea cambiar el nombre del archivo restaurado por uno nuevo. Cuando *sourcefilespec* no existe en la estación de trabajo de destino, debe especificar *destinationfilespec*.

-BACKUPSETName=

Especifica el nombre del conjunto de copias de seguridad desde el que se realiza una operación de restauración. No puede utilizar caracteres comodín para especificar el nombre del juego de copias de seguridad. El valor de *backupsetname* depende de la ubicación del conjunto de copias de seguridad y se corresponde con una de las opciones siguientes:

backupsetname

Especifica el nombre del conjunto de copias de seguridad del servidor desde el que se realiza la operación de restauración. Si se especifica **location**, debe establecer **-location=server**.

localfilename

Especifica el nombre de archivo del primer volumen del juego de copias de seguridad. Debe establecer **-location=file**.

tapedevice

Especifica el nombre del dispositivo de cinta que contiene el volumen del juego de copias de seguridad. Tiene que utilizar un controlador de dispositivo proporcionado por Windows, no el controlador de dispositivo que proporciona IBM. Debe establecer **-location=tape**.

-LOCation=

Especifica la ubicación del conjunto de copias de seguridad. Si no especifica el parámetro de ubicación, el cliente buscará juegos de copias de seguridad en el servidor de IBM Spectrum Protect. Si especifica el parámetro de ubicación, el valor debe corresponder a una de las tres opciones siguientes:

server Especifica que el juego de copias de seguridad se encuentra en el servidor de IBM Spectrum Protect. Server es la ubicación predeterminada.

- file** Especifica que el conjunto de copias de seguridad se encuentra en un sistema de archivos disponible.
- tape** Especifica que el conjunto de copias de seguridad se encuentra en un dispositivo de cinta disponible.

Tabla 106. mandato Restore Backupset: opciones relacionadas

Opción	Dónde se utiliza
dirsonly "Dirsonly" en la página 390	Sólo línea de mandatos.
filesonly "Filesonly" en la página 443	Sólo línea de mandatos.
ifnewer "Ifnewer" en la página 453	Sólo línea de mandatos.
preservepath "Preservepath" en la página 520	Sólo línea de mandatos.
quiet "Quiet" en la página 526	Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
replace "Replace" en la página 529	Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
subdir "Subdir" en la página 581	Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.

Ejemplos

Tarea Restaurar el conjunto de copias de seguridad denominado `monthly_financial_data.87654321` del servidor.

```
dsmc restore backupset
-backupsetname=monthly_financial_data.87654321
-loc=server
```

Tarea Restaurar todo el conjunto de copias de seguridad contenido en el archivo: `/home/budget/weekly_budget_data.ost`.

```
dsmc restore backupset
-backupsetname="/home/budget/weekly_budget_data.ost"
-loc=file
```

Tarea Restaurar todo el conjunto de copias de seguridad del dispositivo `/dev/rmt0`.

```
dsmc restore backupset
-backupsetname="/dev/rmt0" -loc=tape
```

Tarea Restaurar un único archivo denominado `/home/jones/budget.dev` del dispositivo de cinta `/dev/rmt0` en la vía de acceso de origen original.

```
dsmc restore backupset
-backupsetname="/dev/rmt0 "/home/jones/budget.dev"
-loc=tape
```

Tarea Restaurar todos los archivos del directorio `budget` que tienen la extensión `.txt` desde cintas del dispositivo `/dev/rmt0` en la ruta original.

```
dsmc restore backupset "/home/budget/*.txt"  
-backupsetname=/dev/rmt0 -loc=tape
```

Tarea Restaurar todo el conjunto de copias de seguridad en un archivo local llamado "/home/jones/bset01.file"

```
dsmc restore backupset  
-backupsetname="/home/jones/bset01.file"  
-loc=file
```

Tarea Restaurar grupos del conjunto de copias de seguridad mybackupset.12345678 en el servidor de IBM Spectrum Protect en el directorio /home/devel/projectb. El espacio de archivos virtual de los grupos es accounting.

```
dsmc restore backupset {/accounting}/*  
/home/devel/projectb/  
-backupsetname=mybackupset.12345678 -loc=server  
-subdir=yes
```

Tarea Restaurar grupos del conjunto de copias de seguridad local mybackupset.ost en el directorio /home/devel/projectb/. El espacio de archivos virtual de los grupos es accounting.

```
dsmc restore backupset {/accounting}/*  
/home/devel/projectb/  
-backupsetname=mybackupset.ost  
-loc=server -subdir=yes
```

Información relacionada

"Restauración de datos desde un conjunto de copias de seguridad" en la página 240

Restauración de conjuntos de copias de seguridad: consideraciones y restricciones

Existen algunas consideraciones y restricciones que debe tener en cuenta cuando restaure conjuntos de copias de seguridad.

Consideraciones de restauración del conjunto de copias de seguridad

Al restaurar conjuntos de copias de seguridad, tenga en cuenta lo siguiente:

- Si el objeto que desea restaurar se ha generado desde un nodo cliente cuyo nombre es distinto del nodo actual, especifique el nombre del nodo original con el parámetro **filespace**name en cualquiera de los mandatos restore.
- Si no puede restaurar un conjunto de copias de seguridad desde el medio portable, póngase en contacto con el administrador de IBM Spectrum Protect para asegurarse de que el medio portable se creó en un dispositivo con un formato compatible con el suyo.
- Si utiliza el mandato **restore backupset** en la línea de mandatos inicial con el parámetro -location=tape o -location=file, el cliente no intenta ponerse en contacto con el servidor de IBM Spectrum Protect.
- Cuando restaure un grupo a partir de un conjunto de copias de seguridad:

- Se restaurará todo el grupo, o todos los grupos, del espacio de archivos virtual. Si hay varios grupos en el mismo espacio de archivos virtual, no podrá restaurar un solo grupo especificando el nombre de grupo. No puede restaurar una parte de un grupo especificando una vía de acceso de archivo.
- Especifique un grupo utilizando los valores siguientes:
 - Especifique el nombre de espacio de archivos individual con el parámetro **filespace**name.
 - Utilice la opción `subdir` para incluir subdirectorios.
- Se proporciona soporte limitado para la restauración de conjuntos de copias de seguridad desde dispositivos de cinta conectados al sistema cliente. Se debe utilizar siempre un controlador de dispositivo nativo proporcionado por el fabricante del dispositivo. El controlador de dispositivo proporcionado por IBM para que lo utilice el servidor de IBM Spectrum Protect no se puede utilizar en el sistema cliente para restaurar juegos de copias de seguridad locales.
- Si un conjunto de copias de seguridad contiene archivos de distintos propietarios, el propio conjunto de copias de seguridad será propiedad del ID de usuario root y los ID de usuarios que no sean root no verán el conjunto de copias de seguridad. En tal caso, los ID de usuario que no son root pueden restaurar sus archivos si el administrador de IBM Spectrum Protect `rd>` les proporciona el nombre del juego de copias de seguridad. Los usuarios que no sean root sólo podrán restaurar sus propios archivos.
- Para permitir que la GUI del cliente restaure un conjunto de copias de seguridad de un dispositivo local, sin que sea necesaria una conexión al servidor, utilice la opción `localbackupset`.

Consideraciones de restauración del conjunto de copias de seguridad

Al restaurar conjuntos de copias de seguridad, tenga en cuenta las siguientes restricciones:

- No es posible restaurar ni utilizar los datos de los conjuntos de copias de seguridad de los que se ha hecho una copia de seguridad mediante la API.
- No puede restaurar datos de imagen de un conjunto de copias de seguridad mediante la utilización del mandato **restore backupset**. Sólo puede restaurar datos de imagen de un conjunto de copias de seguridad con el mandato **restore image**.
- No puede restaurar datos de imagen de un conjunto de copias de seguridad local (`location=tape` o `location=file`). Sólo puede restaurar datos de imagen de un juego de copias de seguridad del servidor de IBM Spectrum Protect.

Referencia relacionada:

“Localbackupset” en la página 484

“Restore” en la página 744

“Restore Image” en la página 758

“Restore Backupset” en la página 749

Restauración de conjuntos de copias de seguridad en un entorno SAN

Puede restaurar conjuntos de copias de seguridad en una red de área de almacenamiento (SAN) de una de las siguientes maneras:

- Si el conjunto de copias de seguridad se encuentra en un dispositivo de almacenamiento conectado con la SAN, especifique el dispositivo mediante la

utilización del parámetro *filename* y utilice la opción *location=tape* donde se aplique. El cliente de copia de seguridad y archivado restaura el conjunto de copias de seguridad directamente del dispositivo de almacenamiento conectado a SAN, consiguiendo un rendimiento de restauración de alta velocidad.

Nota: es preciso asegurarse de que la cinta adecuada está montada en la unidad de cintas conectada a SAN antes de emitir el mandato **restore**. El cliente de copia de seguridad/archivado no iniciará un autocambiador SCSI para montar la cinta de forma automática.

- Si el conjunto de copias de seguridad no está en medios locales o en un dispositivo de almacenamiento conectado a SAN, puede especificar el conjunto de copias de seguridad utilizando la opción **backupsetname**. Utilice la opción *location=server* para restaurar el conjunto de copias de seguridad directamente desde el servidor mediante la utilización de Lan.

restore Backupset sin el parámetro backupsetname

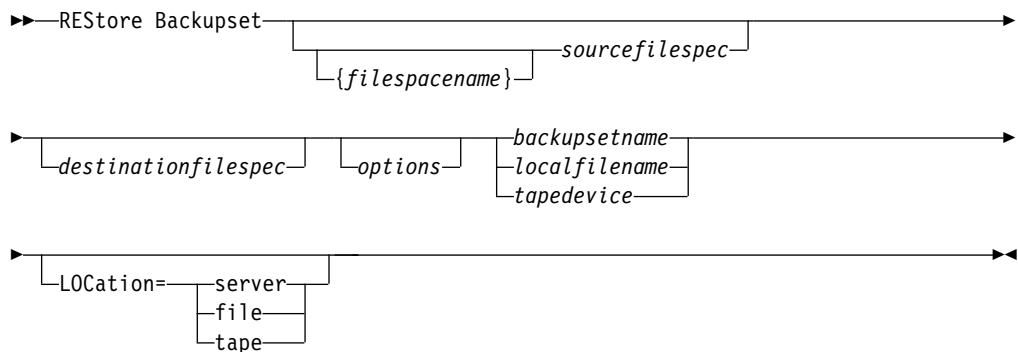
El mandato **restore backupset** se puede utilizar sin el parámetro **backupsetname**.

La sintaxis preferida para el mandato **restore backupset** requiere el parámetro **backupsetname**. Antes de la especificación del parámetro **backupsetname**, el cliente de copia de seguridad y archivado ha restaurado los conjuntos de copias de seguridad con una sintaxis distinta. Se admite la sintaxis anterior, pero se recomienda, siempre que sea posible, que siga la sintaxis que requiere el parámetro **backupsetname**. La sintaxis anterior está documentada para aquellos casos en los que no se puede sustituir por la sintaxis preferida.

Clientes soportados

Este mandato es válido para todos los clientes.

Sintaxis



Parámetros

opciones

Todas las opciones que son válidas con la sintaxis preferida de **restore backupset** son válidas con la sintaxis anterior de **restore backupset**.

{filespace name}

Nombra el espacio de archivos (incluido entre llaves) del servidor que contiene los archivos que quiere restaurar. Éste es el nombre de la unidad de la estación de trabajo de cuyos archivos se realizó copia de seguridad o el nombre de espacio de archivos virtual para el grupo.

Especifique un nombre de espacio de archivos cuando restaure un conjunto de copias de seguridad que contenga un grupo.

Especifique un nombre de espacio de archivos cuando el parámetro *sourcefilespec* no exista en el sistema de destino. Esto puede suceder si el nombre de la etiqueta de unidad ha sido modificado o si está restaurando archivos de los que ha realizado copia de seguridad desde otro nodo con etiquetas de unidad distintas de las suyas.

sourcefilespec

Especifica la vía de acceso de origen de una parte del conjunto de copias de seguridad. El valor predeterminado es restaurar todo el conjunto de copias de seguridad.

destinationfilespec

Especifica la vía de acceso de destino para los archivos restaurados. Si no especifica *sourcefilespec*, no puede especificar *destinationfilespec*. Si no especifica un destino, el cliente restaura los archivos en la ruta de origen inicial. Si está restaurando más de un archivo, debe terminar la especificación de archivo con un delimitador de directorio (/); de lo contrario, el cliente presupone que el último nombre es un nombre de archivo e indica que se ha producido un error. Si está restaurando un único archivo, tiene la opción de terminar la especificación de archivo con un nombre de archivo si desea cambiar el nombre del archivo restaurado por uno nuevo. Si *sourcefilespec* no existe en la estación de trabajo de destino, debe especificar *destinationfilespec*.

backupsetname

Especifica el nombre del juego de copias de seguridad del servidor de IBM Spectrum Protect. Si se especifica el parámetro **location**, debe establecer **-location=server**.

localfilename

Especifica el nombre de archivo del primer volumen del juego de copias de seguridad. Debe establecer **-location=file**.

tapedevice

Especifica el nombre del dispositivo de cinta que contiene el volumen del juego de copias de seguridad. Tiene que utilizar un controlador de dispositivo proporcionado por Windows, no el controlador de dispositivo que proporciona IBM. Debe establecer **-location=tape**.

LOCation=

Especifica la ubicación del conjunto de copias de seguridad. Si no especifica el parámetro de ubicación, el cliente buscará juegos de copias de seguridad en el servidor de IBM Spectrum Protect. Si especifica el parámetro de ubicación, el valor debe corresponder a una de las tres opciones siguientes:

server Especifica que el juego de copias de seguridad se encuentra en el servidor. Server es la ubicación predeterminada.

file Especifica que el conjunto de copias de seguridad se encuentra en un sistema de archivos disponible.

tape Especifica que el conjunto de copias de seguridad se encuentra en un dispositivo de cinta disponible.

Ejemplos

Tarea Restaurar el juego de copias de seguridad denominado `monthly_financial_data.87654321` del servidor.

```
dsmc restore backupset monthly_financial_data.87654321 -loc=server
```

- Tarea** Restaurar todo el conjunto de copias de seguridad contenido en el archivo:/home/budget/weekly_budget_data.ost.
- ```
dsmc restore backupset "/home/budget/weekly_budget_data.ost"
-loc=file
```
- Tarea** Restaurar todo el juego de copias de seguridad del dispositivo /dev/rmt0.
- ```
dsmc restore backupset "/dev/rmt0" -loc=tape
```
- Tarea** Restaurar un único archivo denominado /home/jones/budget.dev del dispositivo de cinta /dev/rmt0 en la vía de acceso de origen original.
- ```
dsmc restore backupset /dev/rmt0 "/home/jones/budget.dev" -loc=tape
```
- Tarea** Restaurar todos los archivos del directorio budget que tienen la extensión .txt desde una o más cintas del dispositivo /dev/rmt0 en la vía de acceso original.
- ```
dsmc restore backupset /dev/rmt0 "/home/budget/*.txt" -loc=tape
```
- Tarea** Restaurar todo el juego de copias de seguridad contenido en el archivo local "/home/jones/bset01.file"
- ```
dsmc restore backupset "/home/jones/bset01.file" -loc=file
```
- Tarea** Restaurar grupos del juego de copias de seguridad mybackupset.12345678 en el servidor de IBM Spectrum Protect en el directorio /home/devel/projectb. El espacio de archivos virtual de los grupos es accounting.
- ```
dsmc restore backupset mybackupset.12345678 {/accounting}/*
/home/devel/projectb/ -loc=server -subdir=yes
```
- Tarea** Restaurar grupos del juego de copias de seguridad local mybackupset.ost en el directorio /home/devel/projectb/. El espacio de archivos virtual de los grupos es accounting.
- ```
dsmc restore backupset mybackupset.ost {/accounting}/*
/home/devel/projectb/ -loc=server -subdir=yes
```

#### Información relacionada

“Restauración de datos desde un conjunto de copias de seguridad” en la página 240

---

## Restore Group

Utilice el mandato **restore group** para restaurar miembros específicos o todos los miembros de una copia de seguridad de grupo.

#### Nota:

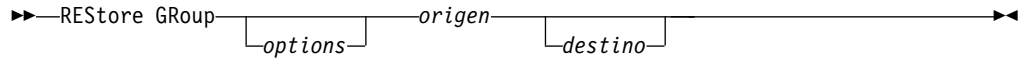
1. Utilice la opción **pick** para que se visualice una lista de grupos a partir de los que poder seleccionar el grupo que desea restaurar.
2. Utilice la opción **showmembers** con la opción **pick** para visualizar y restaurar uno o más miembros de un grupo. En este caso, primero debe seleccionar el grupo del que desea restaurar miembros específicos y, a continuación, debe seleccionar el miembro o miembros del grupo que desea restaurar.
3. Puede restaurar un grupo de un juego de copias de seguridad.



## Clientes soportados

Este mandato es válido para todos los clientes, excepto Mac OS X.

## Sintaxis



## Parámetros

### *origen*

Especifica el nombre del espacio de archivos virtual y el nombre del grupo que desea restaurar en el servidor.

### *destino*

Especifica la vía de acceso en la que desea colocar el grupo o uno o más miembros del grupo. Si no especifica un destino, el cliente restaurará los archivos en su ubicación original.

Tabla 107. Mandato restore Group: opciones relacionadas

| Opción                                                 | Dónde se utiliza                                                  |
|--------------------------------------------------------|-------------------------------------------------------------------|
| backupsetname<br>“Backupsetname” en la<br>página 360   | Sólo línea de mandatos.                                           |
| followsymbolic<br>“Followsymbolic” en la<br>página 444 | Archivo de opciones del cliente (dsm.opt) o línea de<br>mandatos. |
| fromdate “Fromdate” en la<br>página 446                | Sólo línea de mandatos.                                           |
| fromnode “Fromnode” en la<br>página 447                | Sólo línea de mandatos.                                           |
| fromowner “Fromowner” en la<br>página 448              | Sólo línea de mandatos.                                           |
| fromtime “Fromtime” en la<br>página 448                | Sólo línea de mandatos.                                           |
| ifnewer “Ifnewer” en la<br>página 453                  | Sólo línea de mandatos.                                           |
| inactive “Inactive” en la<br>página 456                | Sólo línea de mandatos.                                           |
| latest “Latest” en la página<br>483                    | Sólo línea de mandatos.                                           |
| pick “Pick” en la página 512                           | Sólo línea de mandatos.                                           |
| pitdate “Pitdate” en la<br>página 512                  | Sólo línea de mandatos.                                           |
| pittime “Pittime” en la<br>página 513                  | Sólo línea de mandatos.                                           |
| preservepath<br>“Preservepath” en la página<br>520     | Sólo línea de mandatos.                                           |
| replace “Replace” en la<br>página 529                  | Archivo de opciones del cliente (dsm.opt) o línea de<br>mandatos. |

Tabla 107. Mandato restore Group: opciones relacionadas (continuación)

| Opción                                                                      | Dónde se utiliza                                                       |
|-----------------------------------------------------------------------------|------------------------------------------------------------------------|
| showmembers “Showmembers” en la página 559<br><br>(no se aplica a Mac OS X) | Sólo línea de mandatos.                                                |
| subdir “Subdir” en la página 581                                            | Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos. |
| tapeprompt “Tapeprompt” en la página 583                                    | Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos. |
| todate “Todate” en la página 597                                            | Sólo línea de mandatos.                                                |
| totime “Totime” en la página 598                                            | Sólo línea de mandatos.                                                |

## Ejemplos

**Tarea** Restaurar todos los miembros de la copia de seguridad de grupo /virtfs/group1 en su ubicación original en el sistema cliente.

**Mandato:**

```
restore group /virtfs/group1
```

**Tarea** Visualizar todos los grupos del espacio de archivos virtual /virtfs. Utilice la opción showmembers para visualizar una lista de miembros de grupo a partir de los que poder seleccionar el miembro o miembros que desea restaurar.

**Mandato:**

```
restore group /virtfs/
* -pick -showmembers
```

**Tarea** Visualizar una lista de los grupos del espacio de archivos virtual /virtfs desde la que podrá seleccionar uno o varios grupos para su restauración.

**Mandato:**

```
restore group /virtfs/* -pick
```

## Información relacionada

“Restore Backupset” en la página 749

## Restore Image

El mandato **restore image** restaura un sistema de archivos o una imagen de volumen RAW cuya copia de seguridad se ha realizado con el mandato **backup image**.

El mandato restore obtiene la imagen de copia de seguridad del servidor de IBM Spectrum Protect, o del interior de un conjunto de copias de seguridad del servidor de IBM Spectrum Protect, cuando se especifica la opción **backupsetname**. Este mandato puede restaurar una imagen base activa o una imagen base a un instante específico con sus actualizaciones incrementales asociadas.

**Nota:**

1. La utilización de la opción **incremental** con el mandato **restore image** para realizar una copia de seguridad de imágenes dinámica no recibe soporte.
2. Si utiliza IBM Spectrum Protect HSM for Windows o IBM Spectrum Protect for Space Management, y restaura una copia de seguridad de imagen del sistema de archivos y planifica ejecutar la reconciliación, deberá restaurar los archivos cuya copia de seguridad se ha efectuado tras la copia de seguridad de imágenes. De lo contrario, los archivos migrados que se crearon tras la copia de seguridad de la imagen caducarán del almacenamiento del archivado de HSM en el servidor de IBM Spectrum Protect.

Puede utilizar la opción **verifyimage** con el mandato **restore image** para especificar que desea activar la detección de sectores defectuosos en el volumen de destino. Si se detectan sectores defectuosos en el volumen de destino, el cliente emite un mensaje de aviso en la consola y en el registro de errores.

Si existen sectores defectuosos en el volumen de destino, puede utilizar la opción **imagnetofile** con el mandato **restore image** para especificar que desea restaurar la imagen de origen en un archivo. Más tarde, puede utilizar el programa de utilidad de copia de datos que elija para transferir la imagen del archivo a un volumen de disco.

Consideraciones:

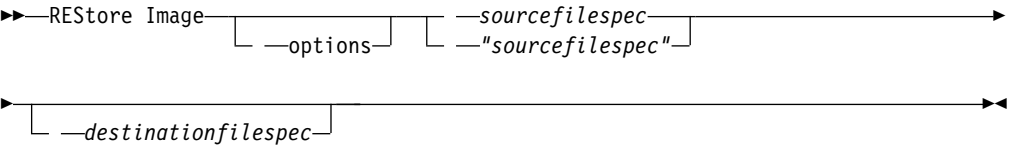
- La API debe estar instalada para utilizar el mandato **restore image**.
- La restauración de imagen no está soportada para el sistema de archivos QFS de Sun.
- La restauración de imagen no está admitida en los sistemas de archivos GPFS en Linux x86\_64, Linux on POWER y Linux para System.
- En sistemas Linux, algunos sistemas de archivos como ext2, ext3, ext4, btrfs y xfs utilizan un UUID (universally unique identifier) para que se identifiquen con el sistema operativo. Si crea una copia de seguridad de imagen de tal volumen y la restaura en una ubicación distinta, es posible que tenga dos volúmenes con el mismo UUID. Si utiliza UUID para definir los sistemas de archivos en `/etc/fstab`, tenga en cuenta que es posible que el cliente de copia de seguridad y archivado no pueda montar correctamente el sistema de archivos restaurado debido al conflicto de UUID. Para evitar esta situación, restaure la imagen a su ubicación original. Si debe restaurarla a una ubicación distinta, cambie el UUID de cualquier volumen original o restaurado antes de montar el sistema de archivos restaurado. Consulte la documentación de Linux para obtener instrucciones sobre cómo cambiar un UUID. También es posible que deba editar manualmente el archivo `/etc/fstab` para que se pueda montar el volumen original, el volumen restaurado, o ambos volúmenes.
- Si utiliza la opción **pick**, se visualizará la siguiente información para las imágenes del sistema de archivos de las que el cliente ha realizado copia de seguridad:
  - Tamaño de imagen
  - Tamaño almacenado - Este valor es el tamaño de la imagen real que se almacena en el servidor de IBM Spectrum Protect. La imagen almacenada en el servidor tiene un tamaño que equivale a la capacidad del volumen.
  - Tipo de sistema de archivos
  - Fecha y hora de la copia de seguridad
  - La clase de gestión que está asignada a las copias de seguridad de imágenes
  - Si la copia de seguridad de imágenes es una copia activa o inactiva
  - El nombre de la imagen

- Si por algún motivo se daña una imagen restaurada, puede utilizar la herramienta **fsck** para intentar repararla.

## Cientes soportados

Esta opción es válida para clientes de AIX, Linux y Oracle Solaris.

# Sintaxis



## Parámetros

*sourcefilespec*

Especifica el nombre de un sistema de archivos imagen de origen para restaurar. Sólo puede especificarse una imagen origen; no pueden utilizarse caracteres comodín.

*destinationfilespec*

Especifica el nombre de un sistema de archivos montado existente o la vía de acceso y el nombre de archivo en el que se restaurará el sistema de archivos de origen. El valor predeterminado es la ubicación original del sistema de archivos.

*Tabla 108. Comando restore image: opciones relacionadas*

| Opción                                                   | Dónde se utiliza                                                       |
|----------------------------------------------------------|------------------------------------------------------------------------|
| <b>backupsetname</b><br>“Backupsetname” en la página 360 | Sólo línea de mandatos.                                                |
| <b>dateformat</b> “Dateformat” en la página 376          | Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos. |
| <b>deletefiles</b><br>“Deletefiles” en la página 383     | Sólo línea de mandatos.                                                |
| <b>fromnode</b> “Fromnode” en la página 447              | Sólo línea de mandatos.                                                |
| <b>fromowner</b> “Fromowner” en la página 448            | Sólo línea de mandatos.                                                |
| <b>imagetofile</b><br>“Imagetofile” en la página 455     | Sólo línea de mandatos.                                                |
| <b>inactive</b> “Inactive” en la página 456              | Sólo línea de mandatos.                                                |
| <b>incremental</b><br>“Incremental” en la página 475     | Sólo línea de mandatos.                                                |
| <b>noprompt</b> “Noprompt” en la página 503              | Sólo línea de mandatos.                                                |
| <b>pick</b> “Pick” en la página 512                      | Sólo línea de mandatos.                                                |

Tabla 108. Comando `restore image`: opciones relacionadas (continuación)

| Opción                                               | Dónde se utiliza                                                       |
|------------------------------------------------------|------------------------------------------------------------------------|
| <b>pitdate</b> "Pitdate" en la página 512            | Sólo línea de mandatos.                                                |
| <b>pittime</b> "Pittime" en la página 513            | Sólo línea de mandatos.                                                |
| <b>timeformat</b> "Timeformat" en la página 592      | Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos. |
| <b>verifyimage</b><br>"Verifyimage" en la página 605 | Sólo línea de mandatos.                                                |

El mandato **restore image** no define ni monta el espacio de archivos de destino. El volumen de destino debe existir, ser lo suficientemente grande para contener el origen y, si contiene un sistema de archivos, deberá tratarse de un volumen montado. Si una copia de seguridad de imagen contiene un sistema de archivos y los restaura en otra ubicación, tenga en cuenta lo siguiente:

- Si el volumen de destino es más pequeño que el volumen de origen, la operación fallará.
- Si el volumen de destino es más grande que el volumen de origen, tras la operación de restauración perderá la diferencia entre los tamaños. El espacio perdido puede recuperarse incrementando el tamaño del volumen, que también aumentará el tamaño del volumen restaurado.

## Ejemplos

**Tarea** Restaurar el directorio `/home/test` en el que se ha montado el volumen lógico en su ubicación original.

Mandato: `dsmc rest image /home/test`

**Tarea** Restaure el directorio `/home/proj` sobre el que está montado el volumen lógico en su ubicación original y aplique los cambios de la última copia de seguridad incremental de la imagen original que está registrada en el servidor. Entre los cambios se incluye la supresión de archivos.

Mandato: `dsmc restore image /home/proj -incremental -deletefiles`

**Tarea** Restaurar el sistema de archivos `/usr` en su ubicación original. Utilice la opción **verifyimage** para activar la detección de sectores defectuosos en el volumen de destino.

Mandato: `dsmc restore image /usr -verifyimage`

**Tarea** Si existen sectores defectuosos en el volumen de destino, utilice la opción **imagetofile** para restaurar el sistema de archivos `/usr` en el archivo `/home/usr.img` para evitar que se dañen los datos.

Mandato: `dsmc restore image /usr /home/usr.img -imagetofile`

Información relacionada

"Verifyimage" en la página 605

"Imagetofile" en la página 455

---

## Restore NAS

El mandato **restore nas** restaura la imagen de un sistema de archivos perteneciente a un servidor de archivos NAS (almacenamiento conectado a red). Cuando se utilice una sesión de línea de mandatos interactiva con un ID que no es un ID de administración, se le solicitará un ID de administrador.

El servidor de archivos NAS realiza el proceso de traspaso de datos externos. Un proceso del servidor realiza la restauración.

Si ha utilizado la opción **toc** con el mandato **backup nas** o la opción **include.fs.nas** para guardar la información de la Tabla de contenido (TOC) para cada copia de seguridad del sistema de archivos, puede utilizar el mandato de servidor **QUERY TOC** para determinar el contenido de una copia de seguridad del sistema de archivos con el mandato de servidor **RESTORE NODE** para restaurar archivos individuales o árboles de directorios. También puede utilizar el cliente web para examinar todo el árbol del sistema de archivos y seleccionar los archivos y directorios que han de restaurarse. Si no guarda la información de las TOC, podrá restaurar archivos individuales o árboles de directorios con el mandato de servidor **RESTORE NODE**, si conoce el nombre calificado al completo de cada archivo o directorio y sepa en qué imagen se ha realizado la copia de seguridad de ese objeto.

Utilice la opción **nasnodename** para especificar el nombre de nodo del servidor de archivos NAS. El nombre de nodo NAS identifica el servidor de archivos NAS en el servidor de IBM Spectrum Protect. Debe inscribir el nombre de nodo NAS en el servidor. Especifique la opción **nasnodename** en el archivo de opciones del sistema cliente (**dsm.sys**). El valor del archivo de opciones del cliente es el valor predeterminado, pero este valor puede modificarse temporalmente en la línea de mandatos.

Puede utilizar la opción **pick** para visualizar una lista de imágenes de NAS que sean propiedad del nodo NAS que especifique. En esta lista puede seleccionar una o varias imágenes para restaurarlas. Si selecciona varias imágenes para restaurarlas con la opción **pick**, no utilice la opción **monitor** o las restauraciones se realizarán en serie. Para iniciar varios procesos de restauración simultáneamente al realizar la restauración de varias imágenes, no especifique **monitor=yes**.

Utilice la opción **monitor** para especificar si desea supervisar una imagen del sistema de archivos NAS y visualizar información sobre el proceso en la pantalla.

Utilice el mandato **monitor process** para visualizar una lista de los procesos de restauración actuales de todos los nodos NAS para los que el ID de usuario de administración está autorizado. El ID de usuario de administración debe tener como mínimo autorización de propietario de cliente sobre el nodo NAS y sobre el nodo de la estación de trabajo cliente que están utilizando desde la línea de mandatos o desde la Web.

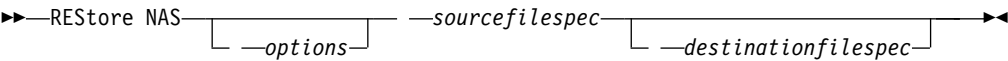
Utilice el mandato **cancel process** para detener el proceso de restauración de NAS.

Con independencia de la plataforma del cliente utilizada, las especificaciones del sistema de archivos NAS utilizan como separador la barra inclinada (/), como en el ejemplo siguiente: **/vol/vol0**.

## Clientes soportados

Este mandato sólo es válido para los clientes AIX y Solaris.

## Sintaxis



## Parámetros

### *sourcefilespec*

Especifica el nombre de la imagen del sistema de archivos NAS que desea restaurar. Este parámetro es necesario a menos que utilice la opción `pick` para mostrar una lista de las imágenes de NAS en la que puede realizar una selección. No se pueden utilizar caracteres comodín cuando se especifica *sourcefilespec*.

### *destinationfilespec*

Especifica el nombre de un sistema de archivos montado existente en el dispositivo NAS en el que desea restaurar la imagen. Este parámetro es opcional. El valor predeterminado es la ubicación original del sistema de archivos en el dispositivo NAS.

Tabla 109. Mandato restore NAS: opciones relacionadas

| Opción                                                    | Dónde se utiliza                                                                                  |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| <code>dateformat "Dateformat"</code> en la página 376     | Archivo de opciones del usuario cliente ( <code>dsm.opt</code> ) o línea de mandatos.             |
| <code>inactive "Inactive"</code> en la página 456         | Sólo línea de mandatos.                                                                           |
| <code>mode "Mode"</code> en la página 492                 | Sólo línea de mandatos.                                                                           |
| <code>monitor "Monitor"</code> en la página 496           | Sólo línea de mandatos.                                                                           |
| <code>nasnodename "Nasnodename"</code> en la página 498   | En el archivo de opciones del sistema cliente ( <code>dsm.sys</code> ) o en la línea de mandatos. |
| <code>numberformat "Numberformat"</code> en la página 504 | Archivo de opciones del usuario cliente ( <code>dsm.opt</code> ) o línea de mandatos.             |
| <code>pick "Pick"</code> en la página 512                 | Sólo línea de mandatos.                                                                           |
| <code>pitdate "Pitdate"</code> en la página 512           | Sólo línea de mandatos.                                                                           |
| <code>pittime "Pittime"</code> en la página 513           | Sólo línea de mandatos.                                                                           |
| <code>timeformat "Timeformat"</code> en la página 592     | Archivo de opciones del usuario cliente ( <code>dsm.opt</code> ) o línea de mandatos.             |

## Ejemplos

**Tarea** Restaurar la imagen del sistema de archivos NAS `/vol/vol1` en el sistema de archivos `/vol/vol2` del servidor de archivos NAS denominado `nas1`.

**Mandato:** restore nas -nasnodename=nas1 /vol/vol1 /vol/vol2

**Tarea** Restaurar imágenes NAS inactivas.

**Mandato:** restore nas -nasnodename=nas2 -pick -inactive

#### Información relacionada

“Nasnodename” en la página 498

“Monitor” en la página 496

“Cancel Process” en la página 691

---

## Restore VM

Utilice el mandato **restore vm** para restaurar una máquina virtual de la que se había realizado previamente una copia de seguridad.



Las operaciones de máquina virtual solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments.

### Restauración VM para máquinas virtuales VMware

El mandato **Restore VM** se puede utilizar para restaurar tanto máquinas virtuales VMware como plantillas de máquina virtual VMware.

Si tiene el cliente de archivado de copia de seguridad instalado en un sistema distinto configurado como un servidor de copia de seguridad vStorage, puede restaurar las copias de seguridad de la máquina virtual completas en el servidor ESX o ESXi de las que proceden, o a un servidor distinto. Para restaurar las copias de seguridad de máquina virtual completas en un servidor diferente, utilice la opción **-host**. El cliente de copia de seguridad histórica copia los datos del servidor de IBM Spectrum Protect a través de la LAN o SAN. A continuación, el cliente graba los datos directamente en el servidor ESX, utilizando el método de transporte que se ha especificado en el archivo de opciones del cliente.

Restaurar una copia de seguridad de máquina virtual completa crea una nueva máquina virtual; la información sobre configuración y contenido de la nueva máquina es idéntico a la que existía al crear la copia de seguridad. Todos los discos de máquinas virtuales se restauran en un punto específico en el tiempo como discos virtuales en la máquina virtual recién creada.

Al restaurar un disco específico, utilizando la sintaxis **:vmdk=**, se actualiza una máquina virtual existente con los datos del disco virtual especificado. Solo los discos especificados se restauran en la máquina virtual existente; otros discos de la máquina virtual no se modifican. La máquina virtual existente en la que está restaurando el disco debe apagarse antes de iniciar la operación de restauración.

Para crear una nueva máquina virtual, especifique el parámetro **-vmname** e indique el nombre de la nueva máquina virtual. El parámetro **-vmname** crea una nueva máquina virtual con una configuración que es idéntica a la que existía cuando la copia de seguridad se produjo. Si también especifica la sintaxis **:vmdk=**, los datos se



restauran en cualquier disco que se incluya en los parámetros **:vmdk=**; los discos que no se incluyan se restaurarán, pero sólo como discos no formateados que no contengan datos.

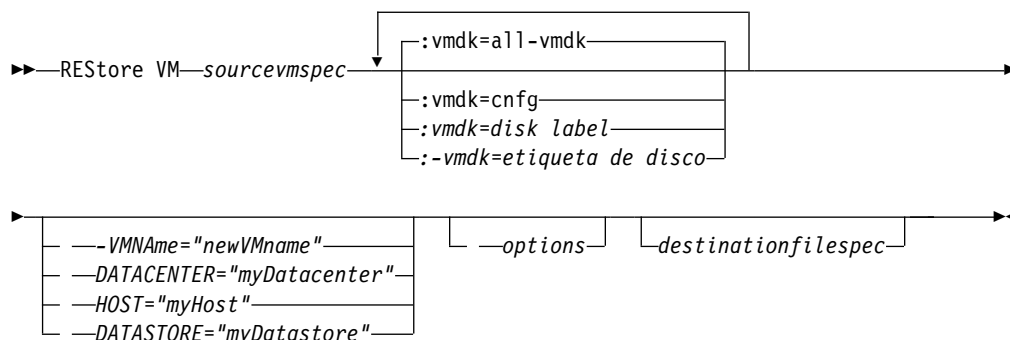
Las máquinas virtuales se restauran en su agrupación de recursos, clúster o carpeta originales si existen los contenedores. Durante una operación de restauración, si el destino (un vCenter o un host ESXi) no tiene los contenedores necesarios, la máquina virtual se restaurará en la ubicación predeterminada de nivel superior en el host ESXi de destino. Si utiliza el cliente de línea de mandatos para restaurar una máquina virtual y si la máquina virtual no se puede restaurar en su ubicación de inventario original, se visualiza un mensaje informativo (ANS2091I). Si utiliza la GUI Java para restaurar una máquina virtual y si la máquina virtual no puede restaurarse en su ubicación de inventario original, el mensaje informativo no se visualiza, pero la máquina virtual se restaura de todas formas en la ubicación predeterminada de nivel superior.

Los códigos de protección de datos de los cuales se han ejecutado copias de seguridad al ejecutar el mandato **backup vm** se restauran con la máquina virtual. Los códigos de protección de datos se utilizan para excluir máquinas virtuales de copias de seguridad y especificar la política de retención de copias de seguridad.

## Clientes soportados

Este mandato solo es válido en clientes de Linux instalados en un servidor de copias de seguridad vStorage para una máquina virtual VMware.

## Sintaxis



## Parámetros

Cualquier parámetro que contenga espacios debe estar entre comillas (" ").

### sourcevmspec

Especifique el nombre de la máquina virtual (o plantilla de la máquina virtual) de la que se realizó una copia de seguridad.

### VMName

Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se ha efectuado una copia de seguridad utilizando VCB.

Especifica el nombre nuevo para la máquina virtual después de que se restaure (si no desea utilizar el nombre especificado por *sourcevmspec*). No puede utilizar caracteres comodín en el nombre de la máquina virtual.

#### DATACENTER

Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB.

Especifica el nombre del centro de datos para restaurar la máquina virtual como se define en el vSphere vCenter. Si el centro de datos se encuentra en una carpeta, debe especificar la opción `-datacenter` al restaurar la máquina virtual e incluir la estructura de la carpeta del centro de datos en el nombre del centro de datos. Por ejemplo, la siguiente sintaxis es válida:

`-datacenter=nombre_carpeta/nombre_centrodatos`

Cuando restaure una máquina virtual mediante la GUI, debe restaurar la máquina virtual en una ubicación diferente. Si restaura en la ubicación original, no puede especificar el nombre de la carpeta del centro de datos. Sin un nombre de carpeta para ayudar a localizar el centro de datos originales, la operación de restauración fallará.

#### HOST

Especifica el nombre de dominio del servidor del host ESX donde se realizará la restauración, como se ha definido en vSphere vCenter.

Este parámetro distingue entre mayúsculas y minúsculas y debe ser el mismo valor que el nombre de host mostrado en el cliente web de VMware vSphere. Para confirmar el nombre de host en el cliente web de vSphere, seleccione un host y pulse **Gestionar > Redes > Configuración de TCP/IP > DNS**.

Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB.

#### DATASTORE

Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB.

Especifica el almacén de datos de VMware en el que restaurar la máquina virtual. El almacén de datos solo puede estar en SAN, NAS, un dispositivo iSCSI o un volumen virtual VMware (vVol). Solo puede especificar un almacén de datos al restaurar una máquina virtual. Si no especifica un parámetro **datastore**, el archivo VMDK de la máquina virtual se restaura en el almacén de datos que estaba activo al crear la copia de seguridad.

#### **:vmdk=all-vmdk**

Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB.

Esta opción especifica que todos los discos virtuales (archivos \*.vmdk) se incluyen cuando la máquina virtual se restaura. Éste es el valor predeterminado.

#### **:vmdk=cnfg**

Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB.

Esta opción especifica que se restaure la información de configuración de máquina virtual. La información de configuración siempre se restaura cuando se crea una máquina virtual nueva. Sin embargo, de forma predeterminada la configuración no se restaura cuando se actualiza una máquina virtual existente con discos virtuales seleccionados.

Normalmente, la restauración de información de configuración en una máquina virtual existente falla porque la información de configuración restaurada está en conflicto con la información de configuración de máquina virtual existente. Utilice esta opción si se ha suprimido el archivo de configuración existente para una máquina virtual en el servidor ESX y quiere utilizar la configuración de la copia de seguridad para restaurarlo.

**:vmdk=etiqueta de disco**

Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB.

Esta opción se utiliza para especificar la etiqueta de disco de los discos virtuales que desea incluir en la operación de restauración. Especifique esta opción únicamente si desea restaurar datos de forma selectiva de discos específicos.

**Nota:** En el mandato **Restore VM**, los nombres de etiqueta de los archivos vmdk que desea incluir (:vmdk= parámetro) en una operación **Restore VM** debe especificarse con el nombre de etiqueta English-language, ya que se muestra en la salida del mandato Backup VM *vmname* -preview. Ejemplos de las etiquetas vmdk English son "Hard Disk 1", "Hard Disk 2", etc.

**:-vmdk=etiqueta de disco**

Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB.

Esta opción se utiliza para especificar la etiqueta de disco de uno o más discos virtuales que desea excluir en la operación de restauración.

**Nota:** En el mandato **Restore VM**, los nombres de etiqueta de los archivos vmdk que desea excluir (:vmdk= parameter) de una operación **Restore VM** deben especificarse con el nombre de etiqueta English-language, ya que se muestra en la salida del mandato Backup VM *vmname* -preview. Ejemplos de las etiquetas vmdk English son "Hard Disk 1", "Hard Disk 2", etc.

*Tabla 110. Mandato Restore VM: opciones relacionadas cuando se restauran máquinas virtuales VMware*

| Opción     | Dónde se utiliza                                                                                                                                                       |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| datacenter | Línea de mandatos o archivo de opciones. Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB. |
| datastore  | Línea de mandatos o archivo de opciones. Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB. |
| host       | Línea de mandatos o archivo de opciones. Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB. |
| inactive   | Línea de mandatos.                                                                                                                                                     |
| pick       | Línea de mandatos. Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB.                       |

Tabla 110. Mandato Restore VM: opciones relacionadas cuando se restauran máquinas virtuales VMware (continuación)

| Opción               | Dónde se utiliza                                                                                                                                                                   |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| pitdate              | Línea de mandatos. Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB.                                   |
| pittime              | Línea de mandatos. Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB.                                   |
| vmbackdir            | Línea de mandatos o archivo de opciones del cliente.                                                                                                                               |
| vmbackuptype         | Línea de mandatos o archivo de opciones del cliente.                                                                                                                               |
| vmmaxrestoresessions | Línea de mandatos o archivo de opciones del cliente.                                                                                                                               |
| vmvstortransport     | Línea de mandatos o archivo de opciones del cliente. Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB. |

## Ejemplos

**Tarea** Restaure la versión más reciente de la copia de seguridad de *myVM* con su nombre original. Utilice la interfaz de gestión VMware para suprimir la máquina virtual inicial, antes de restaurarla con esta sintaxis.

```
dsmc restore vm myvm
```

**Tarea** Restaure la versión de copia de seguridad más reciente de *myvm* a una máquina nueva que se crea con el nombre “Test Machine”, y con el destino de restauración del centro de datos, host de ESX y almacén de datos todos especificados en el mandato.

```
dsmc restore vm myvm -vmname="Test Machine"
 -datacenter="myDatacenter" -host="myHostName"
 -datastore="myDatastore"
```

**Tarea** Restaurar la versión más reciente de la copia de seguridad de *myvm*. Restaurar el centro de datos denominado *mydatacenter*. El centro de datos está dentro de vCenter; la vía de acceso relativa dentro de vCenter es *dirA/datacenters/*.

```
dsmc restore vm myvm -vmname="Test Machine"
 -datacenter="dirA/datacenters/myDatacenter"
 -host="myHostName" -datastore="myDatastore"
```

**Tarea** Restaurar una plantilla de máquina virtual en la misma ubicación y con el mismo nombre.

```
dsmc restore vm nombrePlantillaVm
```

**Tarea** Restaurar una plantilla de máquina virtual en una ubicación nueva.

```
dsmc restore vm nombrePlantillaVm -vmname=nombreNuevo
 -datastore=almacénDatosNuevo -host=hostNuevo
 -datacenter=centroDatosNuevo
```

**Tarea** Restaurar únicamente Hard Disk 2 y Hard Disk 3 en la máquina virtual existente denominada vm1.

```
dsmc restore vm "vm1:vmdk=Hard Disk 2:vmdk=Hard Disk 3"
```

**Tarea** Restaurar todos los discos de la máquina virtual existente denominada vm1, pero no restaurar los datos del Hard Disk 4.

```
dsmc restore vm "vm1:-vmdk=Hard Disk 4"
```

**Tarea** Restaura solo los datos del Hard Disk 1 a la vm1 máquina virtual existente; no actualiza ninguna información de configuración.

**Nota:** Cuando restaura una máquina virtual existente, el comportamiento predeterminado es no actualizar la información de configuración.

```
dsmc restore vm "vm1:vmdk=Hard Disk 1:-vmdk=cnfg"
```

**Tarea** Restaurar todos los discos de la máquina virtual existente denominada vm1.

```
dsmc restore vm "vm1:vmdk=all-vmdk"
```

Este mandato actualiza todos los discos virtuales en una máquina virtual existente, denominada vm1. Tenga en cuenta que esta acción es distinta a la acción que se realiza mediante `dsmc restore vm vm1`, que crea una nueva máquina virtual denominada vm1 (vm1 no debe existir para que `dsmc restore vm vm1` sea satisfactorio).

**Tarea** Definir un máximo de tres sesiones para utilizarlas en operaciones de restauración de discos virtuales en la máquina virtual vm1:

```
dsmc restore vm vm1 -vmmaxrestoresessions=3
```

**Importante:** Para máquinas virtuales de Windows: Si intenta ejecutar una restauración de máquina virtual completa de una copia de seguridad de protección de aplicaciones creada con 2 o más intentos de instantánea, la instantánea del proveedor de sistema estará presente en la máquina virtual restaurada. A medida que la aplicación escriba en el disco, el espacio de almacenamiento de instantáneas crecerá hasta que se quede sin espacio en disco.

En general, si se ha utilizado la protección de aplicaciones durante una copia de seguridad, utilice solo la restauración de la protección de aplicaciones. Al restaurar la aplicación, el volumen se revierte automáticamente. Sin embargo, si tiene que restaurar la máquina virtual completa, debe revertir o suprimir la instantánea.

Una vez restaurada la máquina virtual completa, asegúrese de que la restauración se haya realizado correctamente y de que los datos no estén dañados. Si los datos no están dañados, suprima la instantánea. Si los datos están dañados, revierta la instantánea para restaurar la integridad de los datos.

Puede determinar qué instantánea suprimir o revertir buscando el archivo `dsmShadowCopyID.txt` en el directorio raíz de cada volumen restaurado. Este archivo contiene los ID de las instantáneas creadas durante los intentos de instantánea. Puede utilizar el mandato de **diskshadow delete shadows** para suprimir estos ID, o bien el mandato **revert** para revertir la instantánea. Una vez completadas la supresión o la reversión, también puede suprimir el archivo `dsmShadowCopyID.txt`.

Para obtener más información, consulte el apartado “INCLUDE.VMSNAPSHOTATTEMPTS” en la página 469.

**Conceptos relacionados:**

“Opciones exclude de la máquina virtual” en la página 429

“Opciones include de la máquina virtual” en la página 465

#### Tareas relacionadas:

“Preparación del entorno para copias de seguridad paralelas de máquinas virtuales VMware” en la página 220

---

## Retrieve

El mandato **retrieve** obtiene copias de archivos archivados del servidor de IBM Spectrum Protect. Puede recuperar archivos específicos o directorios completos.

Utilice la opción **description** para especificar las descripciones asignadas a los archivos que desea recuperar.

Utilice la opción **pick** para mostrar una lista de los archivos en la que puede seleccionar el archivo que desea recuperar.

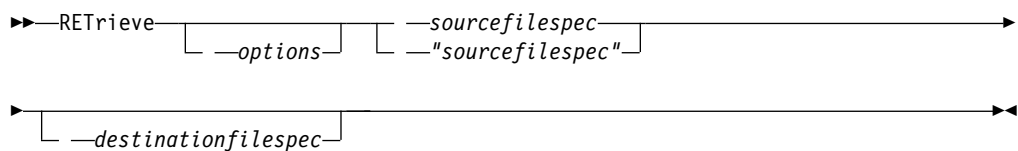
Recupere los archivos en el mismo directorio desde donde se archivaron o en un directorio distinto. El cliente de copia de seguridad y archivado utiliza la opción **preservepath** con el valor subtree como valor predeterminado para restaurar los archivos.

**Nota:** Cuando se recupera un directorio, la fecha y la hora de modificación de éste se establecen en la fecha y la hora de la recuperación, no en la fecha y la hora que tenía el directorio cuando se realizó la copia archivada de éste. Esto se debe a que el cliente de copia de seguridad y archivado recupera primero los directorios y luego añade los archivos a los directorios.

### Clientes soportados

Este mandato es válido para todos los clientes.

### Sintaxis



### Parámetros

#### *sourcefilespec*

Especifica la vía de acceso y el nombre del archivo que se desea recuperar. Utilice caracteres comodín para especificar un grupo de archivos o todos los archivos de un directorio.

#### *destinationfilespec*

Especifica la vía de acceso y el nombre de archivo en el que desea grabar los archivos. Si no especifica un destino, el cliente restaura los archivos en la ruta de origen inicial.

**Nota:** si no especifica un destino, el cliente de copia de seguridad y archivado determina si puede accederse al sistema de archivos original. Si no es posible acceder al sistema de archivos original, el cliente no restaura el archivo.

Este problema también puede darse si elimina la opción **virtualmountpoint** del archivo **dsm.sys**. En este caso, puede especificar otro destino o restaurar la opción **virtualmountpoint** original en el archivo **dsm.sys**, reiniciar el cliente y volver a intentar el mandato.

*Tabla 111. mandato Retrieve: opciones relacionadas*

| Opción                                                  | Dónde se utiliza                                                          |
|---------------------------------------------------------|---------------------------------------------------------------------------|
| <b>dateformat</b> "Dateformat" en la página 376         | Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos. |
| <b>description</b> "Descripción" en la página 384       | Sólo línea de mandatos.                                                   |
| <b>dirsonly</b> "Dirsonly" en la página 390             | Sólo línea de mandatos.                                                   |
| <b>filelist</b> "Filelist" en la página 439             | Sólo línea de mandatos.                                                   |
| <b>filesonly</b> "Filesonly" en la página 443           | Sólo línea de mandatos.                                                   |
| <b>followsymbolic</b> "Followsymbolic" en la página 444 | Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos. |
| <b>fromdate</b> "Fromdate" en la página 446             | Sólo línea de mandatos.                                                   |
| <b>fromnode</b> "Fromnode" en la página 447             | Sólo línea de mandatos.                                                   |
| <b>fromowner</b> "Fromowner" en la página 448           | Sólo línea de mandatos.                                                   |
| <b>fromtime</b> "Fromtime" en la página 448             | Sólo línea de mandatos.                                                   |
| <b>ifnewer</b> "Ifnewer" en la página 453               | Sólo línea de mandatos.                                                   |
| <b>pick</b> "Pick" en la página 512                     | Sólo línea de mandatos.                                                   |
| <b>preservepath</b> "Preservepath" en la página 520     | Sólo línea de mandatos.                                                   |
| <b>replace</b> "Replace" en la página 529               | Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos. |
| <b>subdir</b> "Subdir" en la página 581                 | Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos. |
| <b>tapeprompt</b> "Tapeprompt" en la página 583         | Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos. |
| <b>timeformat</b> "Timeformat" en la página 592         | Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos. |
| <b>todate</b> "Todate" en la página 597                 | Sólo línea de mandatos.                                                   |
| <b>totime</b> "Totime" en la página 598                 | Sólo línea de mandatos.                                                   |

## Ejemplos

**Tarea** Recuperar un único archivo denominado budget.

```
retrieve /home/devel/projecta/budget
```

**Tarea** Recuperar todos los archivos que tienen la extensión .c del directorio /home/devel/projecta.

```
retrieve "/home/devel/projecta/*.c"
```

**Tarea** Recuperar todos los archivos en el directorio /home.

```
retrieve /home/
```

**Tarea** Recuperar todos los archivos que tienen la extensión de archivo .c desde el directorio /home/devel/projecta hasta el directorio /home/newdevel/projectn/projecta. Si el directorio /projectn o /projectn/projecta no existe, se creará.

```
retrieve "/home/devel/projecta/*.c" /home/newdevel/projectn/
```

**Tarea** Recuperar archivos en el directorio /user/project. Utilizar la opción **pick**.

```
ret "/user/project/*" -pick
```

**Tarea** Recuperar todos los archivos que se han archivado del directorio /proj con la descripción "2012 survey results".

```
retrieve "/proj/*" -desc="2012 survey results"
```

**Tarea** Recuperar la copia archivada /home/devel/budget que tiene la descripción "mi presupuesto" en la unidad de cintas /dev/rmt1.

```
mkfifo fifo
dd if=fifo of=/dev/rmt1&
dsmc retrieve -replace=yes -description="mi presupuesto"
/home/devel/budget fifo
```

**Tarea** Recuperar un archivo del espacio de archivos renombrado Jaguar\_OLD en su ubicación original. Especifique el origen y el destino como se indica a continuación:

```
ret Jaguar_OLD/user5/Documents/myresume.doc /Users/user5/Documents/
```

### Información relacionada

"Consulta de opciones del cliente" en la página 345

## Recuperación de archivos desde espacios de archivos que no están activados para Unicode

Si desea recuperar archivos de espacios de archivos cuyos nombres ha cambiado el cliente activado para Unicode, deberá especificar el origen en el servidor y el destino en el cliente.

Esta sección sólo se aplica a Mac OS X. Por ejemplo, imaginemos que Jaguar es el nombre del disco de arranque y que desea realizar el archivado de todos los archivos .log del directorio /Users/user5/Documents. Antes de que se produzca la operación de archivado, el servidor cambia el nombre del espacio de archivos por Jaguar\_OLD. La operación de archivado coloca los datos especificados en la operación actual en el espacio de archivos activado para Unicode denominado /. El nuevo espacio de archivos activado para Unicode sólo contiene el directorio Users/user5/Documents y los archivos \*.log especificados en la operación.



Si desea recuperar un archivo del espacio de archivos *nombre cambiado* (old) en su ubicación original, deberá especificar el origen y el destino de la forma siguiente:

```
retrieve Jaguar_OLD/Users/user5/Documents/mylog.log /Users/user5/Documents/
```

---

## Schedule

El mandato **schedule** inicia el planificador cliente en la estación de trabajo. El planificador cliente debe estar en ejecución para que se pueda iniciar el trabajo planificado.

**Usuario autorizado:** el mandato **schedule** inicia el planificador cliente en la estación de trabajo. El planificador cliente debe estar en ejecución para que se pueda iniciar el trabajo planificado.

### Nota:

1. El mandato **schedule** no se puede utilizar si la opción **managedservices** se ha establecido en **schedule**.
2. Sólo para Mac OS X: para utilizar el mandato **schedule**, especifique **managedservices none** en el archivo **dsm.sys**.
3. Este mandato sólo es válido en la línea de mandatos inicial. No es válido en la modalidad interactiva ni en un archivo de macro.

Si la opción **schedmode** se establece para el sondeo, el planificador cliente establecerá contacto con el servidor para gestionar los eventos planificados en función del intervalo de hora que ha especificado con la opción **querschedperiod** en el archivo de opciones de usuario cliente (**dsm.opt**). Si el administrador indica un valor en la opción **querschedperiod** para todos los nodos, dicho valor modifica el valor indicado en el cliente.

Si se están utilizando comunicaciones TCP/IP, el servidor puede solicitar a la estación de trabajo que inicie un evento planificado cuando sea la hora de ejecutarlo. Para ello, establezca la opción **schedmode** en *prompted* en el archivo de opciones del cliente (**dsm.opt**) o en el mandato **schedule**.

Puede utilizar la opción **sessioninitiation** con el mandato **schedule** para controlar si el servidor o el cliente ha de iniciar las sesiones por medio de un cortafuegos.

Después de haber iniciado el planificador cliente, éste seguirá ejecutando e iniciando los eventos planificados hasta que se pulse **Ctrl+C**, se detenga el proceso del planificador con el mandato de UNIX **kill**, vuelva a iniciarse la estación de trabajo o se apague ésta para finalizarlo.

En vez de que se inicia el planificador del cliente, éste sigue ejecutando e iniciando eventos planificados hasta que se pulsa **Ctrl+C**, se efectúa una doble pulsación en la tecla **Q**, se inicia de nuevo la estación de trabajo o se apaga la misma para finalizarlo.

**Nota:** *no se puede* entrar este mandato en modalidad interactiva.

## Clientes soportados

Este mandato es válido para todos los clientes.

## Sintaxis



## Parámetros

Tabla 112. mandato Schedule: opciones relacionadas

| Opción                                                    | Dónde se utiliza                                                                   |
|-----------------------------------------------------------|------------------------------------------------------------------------------------|
| maxcmdretries<br>"Maxcmdretries" en la página 488         | En el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos. |
| password "Contraseña" en la página 507                    | Archivo de opciones del usuario cliente (dsm.opt)                                  |
| querschedperiod<br>"Querschedperiod" en la página 524     | En el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos. |
| retryperiod<br>"Retryperiod" en la página 542             | En el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos. |
| schedlogname<br>"Schedlogname" en la página 547           | En el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos. |
| schedmode "Schedmode" en la página 550                    | En el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos. |
| sessioninitiation<br>"Sessioninitiation" en la página 556 | En el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos. |
| tcpclientport<br>"Tcpclientport" en la página 588         | En el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos. |

## Ejemplos

**Tarea** Arrancar el planificador cliente.

**Mandato:** dsmc sch -password=notell

**Tarea** Para AIX: iniciar el planificador durante el arranque del sistema especificando este mandato en el archivo /etc/inittab. Asegúrese de que la opción *passwordaccess* esté establecida en *generate*.

**mandato:** tsm::once:/usr/bin/dsmc sched > /dev/null 2>&1 #TSM

**Tarea** Iniciar de forma interactiva el planificador y mantenerlo en funcionamiento como proceso de fondo.

**Mandato:** nohup dsmc sched 2> /dev/null &

Cuando ejecute el mandato **schedule**, todos los mensajes relacionados con el trabajo planificado se enviarán al archivo dsm Sched.log o al archivo que ha especificado con la opción schedlogname en el archivo de opciones del sistema del cliente (dsm.sys). Si no especifica una vía de acceso de directorio con el nombre del archivo en la opción schedlogname, dsm Sched.log residirá en el directorio de trabajo actual, a excepción de cuando se utilice Mac OS X. Para Mac OS X, dsm Sched.log residirá en el directorio /Library/Logs/tivoli/tsm/.

**Importante:** Establezca la variable de entorno DSM\_LOG para asignar un nombre a un directorio donde los permisos predeterminados permitan el acceso necesario para evitar que se produzcan anomalías en la grabación de las anotaciones y la finalización de procesos en determinados casos.

### Información relacionada

“Sessioninitiation” en la página 556

---

## Selective

El mandato **selective** realiza copias de seguridad de los archivos que especifique. Si estos archivos se dañan o se pierden, podrá sustituirlos por las versiones de copia de seguridad del servidor.

Al ejecutar una copia de seguridad selectiva, todos los archivos son aptos para la copia de seguridad, salvo que se excluyan de la misma, o no satisfagan los requisitos de clase de gestión para la serialización.

Durante una copia de seguridad selectiva, se envían copias de los archivos al servidor, incluso si no se han modificado desde la última copia de seguridad, lo que puede generar más de una copia del mismo archivo en el servidor. Si ocurre esto, puede que no se tengan en el servidor tantas versiones distintas de nivel inferior del archivo como se pretendía. El límite de versiones podría consistir únicamente en archivos idénticos. Para evitarlo, utilice el mandato **incremental** para realizar copias de seguridad sólo cuando los archivos se modifiquen o sean nuevos.

Puede realizar copias de seguridad selectivas de archivos únicos o directorios. También puede utilizar caracteres comodín para realizar copia de seguridad de grupos de archivos relacionados.

Si establece la opción `subdir` en `yes` al realizar una copia de seguridad de una vía de acceso y un archivo específicos, el cliente hace una copia de seguridad de forma recursiva todos los subdirectorios bajo esa vía de acceso y las instancias del archivo especificado que existan en los subdirectorios.

Durante una copia de seguridad selectiva, se puede hacer una copia de seguridad de una vía de acceso de directorio, incluso en el caso de que el archivo específico del que se tiene que hacer una copia de seguridad no se encuentra. Por ejemplo, el siguiente mandato sigue realizando la copia de seguridad de `dir1` y `dir2`, aunque el archivo `bogus.txt` no exista.

```
selective /Users/user1/Documents/dir1/bogus.txt
selective "/dir1/dir2/bogus.txt"
```

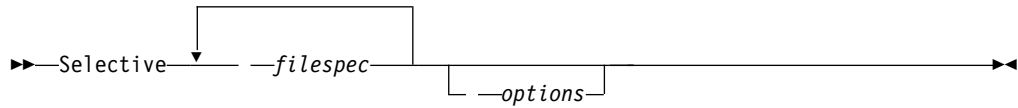
Si vuelve a emitirse el mandato **selective** por haberse producido una anomalía en las comunicaciones o una pérdida de la sesión, las estadísticas de la transferencia visualizarán el número de bytes que el cliente intenta transferir durante *todos* los intentos de ejecución del mandato. Por ello, es posible que las estadísticas de bytes transferidos no coincidan con las estadísticas de archivos, como las relativas al tamaño de archivo.

Puede utilizar la opción `removeoperandlimit` para especificar que se elimina el límite de 20 operandos. Si especifica la opción `removeoperandlimit` con el mandato **selective**, no se aplicará el límite de 20 operandos, y las únicas restricciones serán los recursos disponibles u otros límites del sistema operativo.

## Clientes soportados

Este mandato es válido para todos los clientes.

## Sintaxis



## Parámetros

### *filespec*

Especifique la vía de acceso y el nombre del archivo del que desea realizar la copia de seguridad. Utilice caracteres comodín para incluir un grupo de archivos o todos los archivos de un directorio.

Para incluir varias especificaciones de archivo, separe cada especificación de archivo con un carácter de espacio. Si se incluyen varias especificaciones de archivo, y dos o más de las especificaciones tienen directorios padre comunes, entonces es posible hacer una copia de seguridad para los objetos de directorio comunes más de una vez. Las condiciones bajo las que este comportamiento ocurre son dependientes del tiempo de ejecución, pero el comportamiento por sí mismo no tiene efectos adversos.

Por ejemplo, si la especificación de archivo es `/home/amr/ice.doc` `/home/amr/fire.doc`, entonces se pueden hacer copia de seguridad de `/home` y `/home/amr` dos veces. La copia de seguridad de los objetos de archivo, `ice.doc` y `fire.doc`, se hace solo una vez.

Si desea evitar incluir el directorio padre compartido más de una vez, utilice separar, no superponer mandatos **selective** para realizar copias de seguridad de cada especificación de archivo.

Si hace una copia de seguridad de un sistema de archivos, incluya una barra inclinada final (`/home/`).

Existe un límite de 20 operandos. Este límite previene un número excesivo de sesiones cuando el procesador de mandatos de shell de UNIX expande los caracteres comodín. Puede impedir que la expansión del shell supere el límite de 20 operandos colocando entre comillas las especificaciones de archivo que contienen caracteres comodín ("`home/docs/*`").

Puede utilizar la opción **removeoperandlimit** para especificar que se elimina el límite de 20 operandos. Si especifica la opción **removeoperandlimit**, el límite de 20 operandos no se aplica y queda restringido únicamente a los recursos disponibles u otros límites del sistema operativo. Por ejemplo, elimine el límite de 20 operandos para realizar una copia de seguridad de 21 especificaciones de archivo:

```
selective -removeoperandlimit filespec1 filespec2 ... filespec21
```

Puede utilizar la opción **filelist**, en lugar de las especificaciones de archivo, para identificar qué archivos se han de incluir en esta operación. Sin embargo, estos dos métodos se excluyen mutuamente. No puede incluir parámetros de especificación de archivo y utilizar la opción **filelist**. Si se especifica la opción **filelist**, cualquiera de las especificaciones de archivo que se incluyen se ignoran.

Tabla 113. Mandato selective: opciones relacionadas

| Opción                                                              | Dónde se utiliza                                                                                 |
|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| changingretries<br>"Changingretries" en la página 363               | En el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos.               |
| compressalways<br>"Compressalways" en la página 369                 | Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.                           |
| compression<br>"Compression" en la página 370                       | Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.                           |
| dironly "Dironly" en la página 390                                  | Sólo línea de mandatos.                                                                          |
| filelist "Filelist" en la página 439                                | Sólo línea de mandatos.                                                                          |
| filesonly "Filesonly" en la página 443                              | Sólo línea de mandatos.                                                                          |
| preservelastaccessdate<br>"Preservelastaccessdate" en la página 519 | Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.                           |
| removeoperandlimit<br>"Removeoperandlimit" en la página 528         | Sólo línea de mandatos.                                                                          |
| snapshotcachesize<br>"Snapshotcachesize" en la página 567           | Archivo de opciones del cliente (dsm.opt) o con la opción include.fs.                            |
| snapshotproviderfs<br>"Snapshotproviderfs" en la página 569         | Archivo de opciones del sistema (dsm.sys) en una stanza del servidor o con la opción include.fs. |
| snapshotroot<br>"Snapshotroot" en la página 571                     | Sólo línea de mandatos.                                                                          |
| subdir "Subdir" en la página 581                                    | Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.                           |
| tapeprompt "Tapeprompt" en la página 583                            | Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.                           |

## Ejemplos

**Tarea** Realizar la copia de seguridad del archivo proja en el directorio /home/devel.

**Mandato:** selective /home/devel/proja

**Tarea** Realizar la copia de seguridad de todos los archivos del directorio /home/devel cuyos nombres de archivo empieza por proj.

**Mandato:** selective "/home/devel/proj\*"

**Tarea** Realizar la copia de seguridad de todos los archivos del directorio /home/devel cuyos nombres de archivo empieza por proj. Realizar copia de seguridad de un único archivo denominado budget en el directorio /user/home.

**Mandato:** selective "/home/devel/proj\*" /user/home/budget

**Tarea** Realizar la copia de seguridad del sistema de archivos /home.

**Mandato:** selective /home/ -subdir=yes

**Tarea** Suponiendo que ha iniciado una instantánea del sistema de archivos /usr y ha montado la instantánea como /snapshot/day1, ejecute una copia de seguridad selectiva del árbol de directorios /usr/dir1/sub1 desde la instantánea local y gestiónelo en el servidor de IBM Spectrum Protect debajo del nombre de espacio de archivos /usr.

**Mandato:** dsmc sel "/usr/dir1/sub1/\*" -subdir=yes -snapshotroot=/snapshot/day1

## Asociación de una instantánea local a un espacio de archivos del servidor

Utilice la opción snapshotroot con el mandato **selective** junto con una aplicación de otro proveedor de software independiente que proporcione una instantánea de un volumen lógico para asociar los datos de la instantánea local con los datos del espacio de archivos reales que se almacenan en el servidor de IBM Spectrum Protect. La opción snapshotroot no proporciona ningún recurso para tomar una instantánea de volumen, sólo para gestionar los datos que ha creado una instantánea de volumen.

Sólo AIX: puede realizar una copia de seguridad selectiva basada en instantáneas mediante la especificación de la opción snapshotproviderfs=JFS2.

---

## Set Access

El mandato **set access** otorga a usuarios determinados de otros nodos acceso a las versiones de copia de seguridad o copias archivadas.

También puede utilizar el mandato **set access** para otorgar a usuarios de otros nodos acceso a las imágenes de copia de seguridad.

Puede otorgar a un usuario determinado acceso a un archivo o imagen específicos, a varios archivos o imágenes o a todos los archivos de un directorio. Cuando da acceso a otro usuario, éste puede restaurar o recuperar sus objetos. Especifique en el mandato si se otorga acceso a las copias archivadas o las copias de seguridad.

Para máquinas virtuales de VMware, puede ofrecer a un usuario de otro nodo acceso a las copias de seguridad de una máquina virtual específica.

Cuando se exporta un nodo a otro servidor IBM Spectrum Protect, las reglas de acceso se pueden cambiar en el servidor de importación. Si se aplica una regla de acceso a todos los espacios de archivos en el servidor de exportación, la regla de acceso del servidor de exportación está restringida únicamente a aquellos espacios de archivos que se importan. Los espacios de archivos están restringidos en la regla de acceso en el servidor de importación por razones de seguridad. Así mismo, las reglas de acceso no reconocen la primera aparición de un carácter comodín en la especificación de archivo cuando restaura o recupera. Esto significa que si restaura o recupera con un carácter comodín en una especificación de archivo, los subdirectorios se ignoran.

**Consejo:** Si exporta un nodo a otro servidor de IBM Spectrum Protect, no utilice un único carácter comodín como especificación de archivo en la regla de acceso. En lugar de eso, cree una regla de acceso para cada uno de los espacios de archivos.

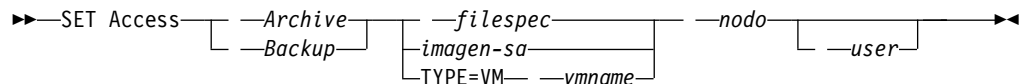
**Nota:** no puede otorgar acceso a copias de seguridad y copias archivadas con un único mandato.

Cuando se cambia el nombre de un espacio de archivos existente durante la conversión de Unicode, las reglas de acceso que se han definido para el espacio de archivos siguen aplicándose al espacio de archivos original. Sin embargo, deberán definirse las nuevas reglas de acceso que han de aplicarse al nuevo espacio de archivos Unicode.

## Clientes soportados

Este mandato es válido para todos los clientes.

## Sintaxis



## Parámetros

### *Archive*

Permite acceder a copias archivadas o imágenes.

### *Backup*

Permite acceder a las versiones de copia de seguridad de los archivos o imágenes.

### *filespec*

Especifica la vía de acceso, el archivo, la imagen o el directorio para el que otorga acceso al otro nodo o usuario. Utilice caracteres comodín para especificar un grupo de archivos o de imágenes o bien todos los archivos de un directorio, todos los objetos de una rama de directorios o todos los objetos de un sistema de archivos. Utilice un único asterisco "\*" en la especificación de archivo para otorgar acceso a todos los archivos o todas las imágenes de los que el usuario es propietario y de los que se ha realizado copia de seguridad en el servidor. Cuando se especifica el mandato set access backup "\*" node, no se realiza ninguna comprobación con el servidor; se da por supuesto que, como mínimo, dispone de un objeto cuya copia de seguridad ha realizado.

Si se otorga acceso a una rama del directorio de trabajo actual, especifique sólo la rama. Si se otorga acceso a objetos que no se encuentren en una rama del directorio de trabajo actual, deberá especificarse la vía de acceso completa. La especificación de archivo a la que se otorga acceso debe tener al menos un objeto de versión de copia de seguridad o de copia archivada (archivo o directorio) en el servidor.

Para especificar todos los archivos de un directorio determinado, especifique /home/mine/proj1/\* en la línea de mandatos.

Para otorgar acceso a todos los objetos bajo un determinado nivel, utilice un asterisco, un delimitador de directorio y un asterisco al final de la especificación de archivo. Por ejemplo, para otorgar acceso a todos los objetos de home/test, utilice la especificación de archivo home/test/\*/\*.

**Importante:** La utilización del formato /\*/\* sin ninguna indicación adicional no otorgará acceso a los objetos del directorio especificado; solo podrá accederse a los directorios incluidos en el directorio especificado.

Las reglas son básicamente las mismas si se trata del directorio raíz. Escriba `/*` en un mandato de acceso establecido, y `/*/*` en otro, si desea que otro usuario disponga de acceso a todos los archivos y directorios que se encuentran en el directorio raíz, o debajo de él. La primera indicación `/*` otorga acceso a todos los directorios y a todos los archivos del directorio raíz. La segunda indicación `/*` permite acceder a todos los directorios y archivos que se encuentran debajo del directorio raíz.

Por ejemplo:

- La estructura de directorios consta de varios niveles: `/home/sub1/subsub1`.
- El directorio `/home` contiene los archivos `h1.txt` y `h2.txt`.
- El directorio `/home/sub1` contiene el archivo `s1.htm`.
- El directorio `/home/sub1/sub2` contiene el archivo `ss1.cpp`.

Para que pueda accederse a todos los archivos del directorio `/home/sub1/sub2`, especifique:

```
set access backup /home/sub1/sub2/* * *
```

Para que solo pueda accederse a los archivos del directorio `/home`, especifique:

```
set access backup /home/* * *
```

Para que pueda accederse a todos los archivos de todos los directorios que se encuentran en el directorio `/home`, o debajo de él, escriba:

```
set access backup /home/* * *
set access backup /home/*/* * *
```

#### *image-fs*

Es el nombre del sistema de archivos de imagen a compartir. Puede especificarse con un asterisco (\*) para permitir el acceso a todas las imágenes cuyo propietario es el usuario que otorga el acceso.

#### **-TYPE=VM *vmname***

Este parámetro es necesario si está utilizando este mandato para proporcionar otro usuario con acceso a las copias de seguridad de la máquina virtual VMware. La opción *vmname* solo se especifica si se indica `-TYPE=VM`; *vmname* es el nombre de la máquina virtual VMware a la que está permitiendo el acceso.

#### *nodo*

Especifica el nodo cliente del usuario al que se está otorgando acceso. Utilice caracteres comodín para otorgar acceso a más de un nodo con nombres de nodo similares. Utilice un asterisco (\*) para otorgar acceso a todos los nodos.

#### *user*

Se trata de un parámetro opcional que restringe el acceso al usuario indicado del nodo especificado. Para permitir que cualquier usuario autorizado acceda a la copia de seguridad de los datos o a los datos archivados, especifique **root** como usuario.

## **Ejemplos**

**Tarea** Otorgar al usuario del nodo\_2 autorización para restaurar el archivo budget del directorio `/home/user`.

```
set access backup /home/user/budget node_2
```

**Tarea** Otorgar a nodo\_3 autorización para recuperar todos los archivos del directorio `/home/devel/proja`.

```
set ac archive /home/devel/proja/ node_3
```



**Tarea** Otorgar a todos los nodos cuyos nombres terminen por bldgb autorización para restaurar todas las versiones de copia de seguridad de los directorios que tienen el nombre de espacio de archivos project.

```
set ac b "{project}/*" "*bldgb"
```

**Tarea** Otorgar a cualquier usuario autorizado en node1 la autorización para recuperar todos los archivos del directorio /home/devel/projb.

```
set access archive /home/devel/projb/ node1 root
```

**Tarea** Otorgar al usuario elena del nodo \_5 autorización para restaurar todas las imágenes del espacio de archivos montado en el directorio /home/devel/proja.

```
set acc backup "home/devel/proja/*/*" node_5 elena
```

**Tarea** Otorgar al nodo denominado **myOtherNode** autorización para restaurar archivos de copias de seguridad de la máquina virtual VMware denominada **myTestVM**.

```
set access backup -TYPE=VM myTestVM myOtherNode
```

---

## Set Event

Con el mandato **set event** puede especificar las circunstancias que se deben dar cuando se suprimen datos archivados.

Puede utilizar el mandato **set event** de las siguientes maneras:

- Impedir la supresión de datos al final de su período de retención asignado
- Permitir que caduquen los datos, según define el grupo de copia de archivado (liberar una espera de suspensión)
- Iniciar la ejecución del reloj de caducidad cuando tenga lugar un evento concreto (notificar al servidor que se ha producido un evento).

Los objetos afectados pueden especificarse con una especificación de archivo estándar (incluidos los caracteres comodín), una lista de archivos cuyos nombres se encuentren en el archivo que se ha especificado mediante la utilización de la opción **filelist** o un grupo de copias archivadas cuya descripción se ha especificado con la opción **description**.

**Nota:** Cuando sólo se utiliza una especificación de archivo, <filespec>, se verán afectadas todas las copias archivadas de los archivos o carpetas que coincidan con la especificación de archivo. Si desea que se vean afectadas ciertas versiones de un archivo, utilice la opción **-pick** y seleccione uno de los elementos que aparecen en la lista.

### Interacción con servidores de nivel inferior

Si el mandato **set event** se emite cuando el cliente está conectado con un servidor que no admite la política basada en eventos (anterior a IBM Spectrum Protect 5.2.2), el mandato se rechazará y se generará un mensaje de error en el que se indicará que el servidor actual no admite la política basada en eventos.

### Clientes soportados

Este mandato es válido para todos los clientes.

## Sintaxis

```
►--SET Event--TYPE= Hold-----<filespec>-----►
 Release-----
 Activateretention-----
►--filelist=<filespec>--description=--pick-----►
```

## Parámetros

*TYPE=*

Especifica el valor del tipo de evento. Este parámetro debe especificarse.

*hold*

Impide que se suprima el objeto, independientemente de la política de caducidad.

*release*

Permite que tenga lugar la caducidad controlada por eventos habitual.

*activateretention*

Indica al servidor que se ha producido el evento de control e inicia la ejecución del reloj de caducidad.

*-pick*

Proporciona una lista de objetos que el usuario puede seleccionar para aplicar el evento.

Las opciones siguientes también se pueden utilizar y tienen la misma finalidad que habitualmente:

- Dateformat
- Numberformat
- Noprompt
- Subdir
- Timeformat

## Ejemplos

**Tarea** En el ejemplo siguiente se muestran la salida detallada y la información de las estadísticas del mandato **set event** `set event type=hold /home/accounting/ledgers/*05.books`, con objetos revinculados (frente a la notación de objetos de copia archivada o cualquier otra notación).

```
Rebinding--> 274 /home/accounting/ledgers/
 jan05.books
Rebinding--> 290 /home/accounting/ledgers/
 feb05.books
```

```
Número total de objetos archivados: 0
Número total de objetos con errores: 0
Número total de objetos revinculados: 2
Número total de bytes transferidos: 0 B
Tiempo de transferencia de datos: 0,00 s
Velocidad de transferencia de datos de red: 0,00 KB/s
Velocidad de transferencia de datos compuesta: 0,00 KB/s
Objetos comprimidos al: 0%
Tiempo transcurrido en el proceso: 00:00:02
```

**Tarea** La opción `-pick` cuando se utiliza con el mandato `set event set event type=activate /user/tsm521/common/unix` muestra el tipo de evento en lugar del nombre de mandato:

Scrollable PICK Window - Retention Event : ACTIVATE

| Núm. | Fecha/hora archivado | Tamaño   | Archivo                      |
|------|----------------------|----------|------------------------------|
| 1.   | 08/05/2003 08:47:46  | 766 B    | /user/tsm521<br>/common/unix |
| 2.   | 08/01/2003 10:38:11  | 766 B    | /user/tsm521<br>/common/unix |
| 3.   | 08/05/2003 08:47:46  | 5.79 KB  | /user/tsm521<br>/common/unix |
| 4.   | 08/01/2003 10:38:11  | 5.79 KB  | /user/tsm521<br>/common/unix |
| 5.   | 08/05/2003 08:47:46  | 10.18 KB | /user/tsm521<br>/common/unix |

### Información relacionada

“Dateformat” en la página 376

“Numberformat” en la página 504

“Noprompt” en la página 503

“Subdir” en la página 581

“Timeformat” en la página 592

## Establecer Netappsvm

El mandato **set netappsvm** asocia las credenciales de inicio de sesión para un servidor de gestión de clústeres, que se especifican en el mandato **set password**, con una máquina virtual de almacenamiento NetApp y el nombre de máquina virtual de almacenamiento (SVM) de datos (Vserver de datos). Debe especificar este mandato antes de crear una copia de seguridad incremental por diferencia de instantánea de un volumen de NetApp en clúster.

Este mandato normalmente sólo se especifica una vez. Los parámetros se almacenan y se reutilizan la próxima vez que realiza una copia de seguridad de un volumen en clúster que esté gestionado por la máquina virtual de almacenamiento. Si traslada una máquina virtual de almacenamiento a otro servidor de gestión de clústeres, deberá volver a especificar este mandato y especificar el nuevo servidor de gestión de clúster. Si fuera necesario, cambie las credenciales de inicio de sesión utilizando el mandato **set password**.

### Clientes soportados

Este mandato es válido para los clientes de archivado y copia de seguridad de Linux que completan copias de seguridad de diferencia de instantáneas de volúmenes de servidor de archivo ONTAP-c-mode de datos en clúster.

### Sintaxis

```

►► SET NETAPPSVM [svm_hostname—cms_hostname— svm_name]
 [—remove—svm_hostname]

```

## Parámetros

### ***svm\_hostname***

Especifica el nombre de host o la dirección IP de la máquina virtual de almacenamiento que gestiona los volúmenes e interfaces lógicas (LIFs), para los volúmenes que quiera proteger.

### ***cms\_hostname***

Especifica el nombre de host o la dirección IP del servidor de gestión de clústeres. Especifique el mismo nombre de host que haya especificado para este servidor de gestión de clústeres cuando utilizó el mandato **setpassword** para establecer las credenciales de inicio de sesión.

### ***svm\_name***

Especifica el nombre de los datos de SVM que gestionan los volúmenes montados. Póngase en contacto con el administrador de SVM de NetApp para obtener el nombre de SVM de datos asignado a la máquina virtual.

### ***-remove svm\_hostname***

Desasocia la SVM del servidor de gestión de clústeres con el que previamente estaba asociada. Especifique un nombre de host de SVM.

Puede especificar este parámetro si ha asociado de forma accidental una máquina virtual de almacenamiento con un servidor de archivos 7-mode. Si elimina un servidor de archivos 7-mode y asocia un servidor de gestión de clústeres, establezca las credenciales de inicio de sesión para el servidor de gestión de clústeres utilizando el mandato **set password**.

## Ejemplos

Configurar las credenciales y el acceso a una máquina virtual de almacenamiento:

```
set netappsvm svm_example.com cms_filer1.example.com svm_2
dsmc set password cms_filer1.example.com user_name password
```

Eliminar las asociaciones que se crearon para la máquina virtual de almacenamiento:

```
set netappsvm -remove svm_example.com
```

### **Tareas relacionadas:**

“Protección de volúmenes de servidor de archivos ONTAP NetApp de datos en clúster” en la página 116

---

## Establecer contraseña

El mandato **set password** cambiará la contraseña de IBM Spectrum Protect para la estación de trabajo, o establece las credenciales que se utilizan para acceder a otro servidor.

Si omite las contraseñas antigua y nueva cuando escribe el mandato **set password**, se le solicitará que escriba una vez la contraseña antigua y dos veces la contraseña nueva.

Las contraseñas pueden tener una longitud máxima de 63 caracteres. Las restricciones de contraseña varían, dependiendo del lugar donde se almacenan y gestionan las contraseñas y en función de la versión del servidor IBM Spectrum Protect al que se conecta el cliente.

**Si el servidor de IBM Spectrum Protect tiene la versión 6.3.3 o posterior y si usa un servidor de directorios LDAP para autenticar contraseñas:**

Utilice cualquiera de los siguientes caracteres para crear una contraseña:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ()
| { } [] : ; < > , ? / ~
```

Las contraseñas son sensibles a las mayúsculas y minúsculas, y están sujetas a restricciones adicionales que puedan imponer las políticas de LDAP.

**Si el servidor IBM Spectrum Protect está en la versión 6.3.3 o posterior, y si no utiliza un servidor LDAP para gestionar contraseñas**

Utilice cualquiera de los siguientes caracteres para crear una contraseña:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ()
| { } [] : ; < > , ? / ~
```

Las contraseñas se almacenan en la base de datos del servidor IBM Spectrum Protect y no distinguen entre mayúsculas y minúsculas.

**Si el servidor IBM Spectrum Protect es anterior a la versión 6.3.3**

Utilice cualquiera de los siguientes caracteres para crear una contraseña:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9
_ - & + .
```

Las contraseñas se almacenan en la base de datos del servidor IBM Spectrum Protect y no distinguen entre mayúsculas y minúsculas.

### **Recuerde:**

En la línea de mandatos, escriba entre comillas todos los parámetros que contengan uno o varios caracteres especiales. Sin las comillas, los caracteres especiales se pueden interpretar como caracteres de escape, caracteres de redirección de archivos u otros caracteres que tienen importancia para el sistema operativo.

### **En sistemas AIX, Linux y Solaris:**

Escriba los parámetros de mandato entre comillas simples (').

#### **Ejemplo de línea de mandatos:**

```
dsmc set password -type=vmguest 'Win 2012 SQL'
'tsml2dag\administrator' '7@#$$^&7'
```

Las comillas no son necesarias cuando escribe una contraseña con caracteres especiales en el archivo de opciones.

## **Clientes soportados**

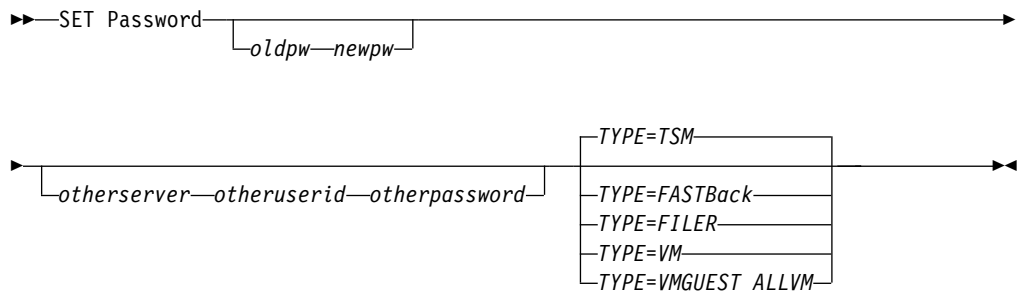
Este mandato es válido para todos los clientes.

Los parámetros siguientes se aplican a las operaciones de VMware, que solo están disponibles si se utiliza el cliente como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

- TYPE=DOMAIN

- TYPE=VM
- TYPE=VMGUEST

## Sintaxis



## Parámetros

### *contraseñaantigua*

Especifica la contraseña actual para la estación de trabajo.

### *contraseñanueva*

Especifica la contraseña nueva para la estación de trabajo.

### *other\_server other\_user\_id other\_password*

Estos tres parámetros especifican los atributos que utiliza el cliente para acceder a otro servidor, como un archivador o un host ESXi.

#### *other\_server*

Especifica el nombre de host o la dirección IP del servidor al que puede acceder el cliente para proteger los archivos.

#### *other\_user\_id*

El ID de usuario de una cuenta en el servidor que utiliza el cliente para iniciar una sesión en el otro servidor. La cuenta debe tener los privilegios necesarios para realizar las operaciones que se ejecutan una vez que el usuario inicie la sesión en el otro servidor.

#### *other\_password*

La contraseña asociada con el ID de usuario en el otro servidor.

### *TYPE*

Especifica si la contraseña es para el cliente de copia de seguridad y archivado o para otro tipo de servidor.

Utilice TYPE=TSM para especificar la contraseña del cliente de copia de seguridad y archivado. El tipo predeterminado es TYPE=TSM.

Utilice TYPE=FastBack, en clientes Linux y Windows, para almacenar las credenciales de Tivoli Storage Manager FastBack necesarias para montar y desmontar los volúmenes de FastBack en el servidor FastBack Disaster Recovery Hub de Windows.

El archivo de contraseñas en el servidor de copia de seguridad vStorage debe tener el ID de administrador de Windows del sistema de centro virtual de VMware o el ID de usuario de UNIX de un servidor ESX específico. Para una copia de seguridad de proxy FastBack, el archivo de contraseñas tiene que contener el ID de administrador y la contraseña de FastBack. A continuación, se muestran algunos ejemplos:

```
dsmc set password 192.0.2.24 admin admin 123 -type=fastback
```

```
dsmc set password 192.0.2.24 WORKGROUP:admin admin 123 -type=fastback
```

```
dsmc set password windserv administrator windpass4 -type=fastback
```

**Importante:** Tiene que definir las credenciales de usuario necesarias para montar y desmontar los volúmenes de FastBack desde un repositorio en un cliente de archivado y copia de seguridad antes de especificar el submandato de FastBack de copia de seguridad y archivado. Utilice la opción `fbserver` para definir las credenciales.

Aquí tiene una breve descripción de las distintas configuraciones y credenciales que necesita:

- El cliente de copia de seguridad y archivado se instala en un servidor de copia de seguridad vStorage. El cliente del servidor de copia de seguridad vStorage debe conectarse a varios repositorios de unidades compartidas de red.

Siga estos pasos para cada uno de los repositorios de compartimiento de red en los que esté conectado el cliente:

1. Configure el repositorio para un acceso de red remoto desde FastBack Manager. Consulte la documentación del producto Tivoli Storage Manager FastBack en el IBM Knowledge Center, en <http://www.ibm.com/support/knowledgecenter/SS9NU9/welcome>.

Este paso establece un nombre de dominio, un ID de usuario de red compartida, y una contraseña de red compartida para conectarse remotamente al repositorio.

2. En la estación de trabajo del cliente de copia de seguridad y archivado, entre manualmente el siguiente mandato:

```
dsmc set password type=fastback FBServer domain:networkaccessuserid
networkaccesspassword
```

La opción `fbserver` especifica el nombre de host abreviado de la estación de trabajo del servidor FastBack. Para el FastBack DR Hub, la opción `fbserver` especifica el nombre abreviado de la estación de trabajo donde se ha instalado DR Hub.

*Networkaccessuserid* es el ID de administrador de Windows o la contraseña de administración de FastBack.

*Domain* es el nombre de dominio del ID de usuario.

*Networkaccesspassword* es el ID de administrador de Windows o la contraseña de administración de FastBack.

3. Estas credenciales se recuperan en base al nombre corto de host que especifica con la opción `fbserver`.

Utilice `TYPE=FILER`, en sistemas Linux y Windows, para especificar que esta contraseña es para operaciones de diferencia de instantánea en un servidor de archivos.

Para `TYPE=FILER`, debe especificar un nombre de servidor de archivos, y el ID de usuario y la contraseña que se utilizan para acceder al servidor de archivos. Por ejemplo: `dsmc set password -type=filer myfiler filerid filerpasswd`. Al especificar `TYPE=FILER`, la contraseña se almacena en el archivo `TSM.PWD` sin validar que la contraseña sea correcta. Las contraseñas almacenadas con `TYPE=FILER` se pueden compartir entre nodos cliente. Por ejemplo, una contraseña almacenada por `NODE_A` puede utilizarla `NODE_B`. Sólo se almacena un conjunto de credenciales por servidor de archivos.

Utilice `TYPE=VM` para establecer la contraseña que se utiliza para iniciar sesión en un servidor vCenter o ESX.

```
dsmc SET PASSWORD -type=VM hostname administrator password
```

donde:

***nombre\_host***

Especifica el servidor de VMware VirtualCenter o ESX que desea restaurar, consultar o del que desea hacer una copia de seguridad. Este nombre de host debe coincidir con la sintaxis del nombre de host que se utiliza en la opción **vmchost**. Es decir, si **vmchost** utiliza una dirección IP en lugar de un nombre de host, este mandato debe proporcionar la dirección IP, y no un nombre de host corto o un nombre de host completo.

***administrator***

Especifica la cuenta necesaria para iniciar sesión en el host de vCenter o ESXi.

***password***

Especifica la contraseña asociada con la cuenta de inicio de sesión que ha especificado para el administrador de vCenter o ESXi.

Utilice el Editor de preferencias para establecer las opciones **vmchost**, **vmcuser** y **vmcpw**.

También puede establecer la opción **vmchost** en el archivo de opciones del cliente y luego utilizar el mandato **set password** para asociar el nombre de host con la cuenta del administrador y la contraseña de la cuenta del administrador utilizada para iniciar la sesión en dicho host. Por ejemplo, `set password TYPE=VM myvmchost.example.com administrator_name administrator_password`.

Utilice **TYPE=VMGUEST**, en clientes Linux y Windows, si utiliza la opción **INCLUDE.VMTSMVSS** para proteger una máquina virtual. Utilice el formato siguiente para el mandato **set password**:

```
set password -type=vmguest guest_VM_name administrator password
```

donde:

***nombre\_máquina\_virtual\_invitado***

Especifica el nombre del invitado de máquina virtual que desea proteger.

***administrator***

Especifica la cuenta necesaria para iniciar sesión en la máquina virtual huésped.

***password***

Especifica la contraseña asociada con la cuenta de inicio de sesión.

Si utiliza las mismas credenciales para iniciar sesión en varias máquinas virtuales protegidos por la opción **INCLUDE.VMTSMVSS**, puede establecer la contraseña para todas las máquinas virtuales especificando el parámetro **ALLVM**. El parámetro **ALLVM** hace que se utilicen las mismas credenciales cuando el cliente inicia sesión en cualquier invitado incluido en una opción **INCLUDE.VMTSMVSS**. El mandato **TYPE=TSM** es un ejemplo de cómo utilizar **ALLVM**. En este ejemplo, el nombre de usuario "Administrator" y la contraseña "Password" se utilizan para iniciar la sesión en cualquier máquina virtual que ha incluido en un **INCLUDE.VMTSMVSS** opción:

```
set password -type=vmguest ALLVM Administrator Password
```

También puede establecer una combinación de credenciales compartidas e individuales. Por ejemplo, si la mayoría de las máquinas virtuales en su entorno utilizan las mismas credenciales, pero hay algunas máquinas virtuales



que utilizan credenciales diferentes, puede utilizar varios mandatos **set password** para especificar las credenciales. Por ejemplo, suponga que la mayoría de las máquinas virtuales utilizan “Administrator1” como el nombre de usuario y “Password1” como contraseña. Supongamos también que una máquina virtual, llamada VM2, utiliza “Administrator2” como nombre de usuario y “Password2” como contraseña. Los siguientes mandatos se utilizan para establecer las credenciales para esta situación:

```
set password -type=vmguest ALLVM Administrator1 Password1 (establece las credenciales para la mayoría de las máquinas virtuales).
```

```
set password -type=vmguest VM2 Administrator2 Password2 (establece credenciales exclusivas para VM2).
```

## Ejemplos

A continuación, se muestran ejemplos que utilizan el mandato **set password**.

**Tarea** Cambiar la contraseña osecret por nsecret.

```
set password osecret nsecret
```

**Tarea** Configurar un ID de usuario y una contraseña para el usuario root en el servidor de archivos myFiler.example.com.

```
dsmc set password -type=filer myFiler.example.com root
Please enter password for user id "root@myFiler.example.com":
***** Re-enter the password for verification:***** ANS0302I
Successfully done.
```

**Tarea** Configurar un ID de usuario y una contraseña para el usuario root en el servidor de archivos myFiler.example.com.

```
dsmc set password -type=filer myFiler.example.com root secret
```

**Tarea** Configurar un ID de usuario y una contraseña para el servidor de FastBack myFastBackServer. Utilice la opción -fbserver de los mandatos **archive fastback** y **backup fastback** para el nombre del servidor.

```
dsmc set password -type=FASTBack myFastBackServer myUserId
'pa$sword'
```

### Importante:

1. El mandato `dsmc set password -type=fastback` tiene que repetirse en una estación de trabajo de proxy de cliente dedicado una vez para cada repositorio de FastBack donde se espera que se conecte el cliente de copia de seguridad y archivado.
2. Para los repositorios de recursos compartidos de red, emita el mandato `dsmc set password -type=fastback` con este formato: `dsmc set password -type=fastback myFBServer domainName:userId password`. El nombre de servidor especificado, que es myFBServer en este ejemplo, debe coincidir con el nombre especificado en la opción **-fbserver** en un mandato **backup fastback** o **archive fastback**.
3. Para el servidor de FastBack o el FastBack Disaster Recovery Hub, el ID de usuario y la contraseña especificados tienen que tener privilegios de administrador de FastBack. Tiene que emitir el mandato `dsmc set password -type=fastback` una vez para cada repositorio de ramificaciones del servidor de FastBack en el FastBack DR Hub al que está previsto que se conecte el cliente de archivado y copia de seguridad.

**Tarea** El cliente de archivado y copia de seguridad está conectado al repositorio de servidor de FastBack cuyo nombre de host abreviado es myFbServer. user ID es el ID de usuario de red de FastBack con acceso de lectura/escritura al repositorio compartido. DOMAIN es el dominio al que pertenece el ID de usuario. myNetworkPass es la contraseña correspondiente para el ID de usuario.

```
dsmc set password -type=fastback myFbServer DOMAIN:USERID
myNetworkPass
```

**Tarea** El cliente de copia de seguridad y archivado está conectado a un repositorio en una máquina DR Hub cuyo nombre de host abreviado es myFbDrHub. El ID de usuario es el ID del administrador de Windows . DOMAIN es el dominio al que pertenece la máquina DR Hub. myNetworkPass es la contraseña correspondiente para el ID de administrador.

```
dsmc set password -type=fastback myFbDrHub DOMAIN:administrator
adminPasswd
```

**Referencia relacionada:**

“Snapdiff” en la página 561

---

## Set Vmtags

El mandato **set vmtags** crea categorías y códigos de protección de datos que se pueden añadir a los objetos de inventario de VMware. Puede gestionar las copias de seguridad de IBM Spectrum Protect de máquinas virtuales de estos objetos de VMware especificando los códigos con herramientas como VMware vSphere PowerCLI versión 5.5 R2 o posterior.



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Si utiliza la Extensión de IBM Spectrum Protect para gestionar copias de seguridad, no es necesario para ejecute antes el mandato **set vmtags**. Los códigos y las categorías se crean automáticamente.

Si va a escribir scripts para aplicar estos códigos a objetos de inventario de VMware, solo necesita emitir el mandato **set vmtags** una vez para que se creen los códigos de protección de datos antes de que se añadan al inventario de VMware.

Puede gestionar las copias de seguridad de máquinas virtuales en los siguientes niveles de objeto de inventario de VMware:

- Centro de datos
- Carpeta (carpetas de clúster y host y carpetas de plantilla y máquina virtual)
- Host
- Clúster de host
- Agrupación de recursos
- Máquina virtual

Si desea la lista de códigos admitidos, consulte el apartado “Códigos de protección de datos admitidos” en la página 793.

En el caso de los códigos relacionados con las planificaciones, las máquinas virtuales tienen que estar en un conjunto de protección protegido por una

planificación. Un conjunto de protección consta de las máquinas virtuales de un contenedor al que se ha asignado el código Schedule (IBM Spectrum Protect).

Tras ejecutar el mandato **set vmtags**, puede asignar los códigos a objetos de VMware para gestionar la protección de las máquinas virtuales. Por ejemplo, puede excluir máquinas virtuales de, o incluirlas en, servicios de copia de seguridad planificada, especificar la política de retención para las copias de seguridad, configurar la coherencia de datos de las instantáneas o seleccionar los discos de la máquina virtual que se van a proteger.

Si los códigos de protección de datos ya existen, cuando se ejecuta el mandato **set vmtags** no se vuelven a crear los códigos.

Si está actualizando desde una versión anterior del transportador de datos, al volver a ejecutar el mandato **set vmtags** se crearán nuevos códigos que están disponibles en la nueva versión del transportador de datos.

**Requisitos:** Antes de ejecutar el mandato **set vmtags**, asegúrese de que se cumplan los siguientes requisitos:

- VMware vCenter Server debe estar en la Versión 6.0 Actualización 1 o posterior.
- La opción vmchost debe estar configurada en el archivo dsm.opt en los transportadores de datos de Windows o el archivo dsm.sys en los transportadores de datos de Linux. El nombre de usuario y la contraseña asociados al valor vmchost también se deben establecer. Si aún no lo están, puede utilizar el mandato **dsmc set password** para establecer el nombre de usuario y la contraseña.

## Clientes admitidos

Este mandato solo es válido en clientes admitidos de Linux x86\_64 instalados en un servidor de seguridad de vStorage que protege los activos de VMware.

## Sintaxis

►►—SET VMTAGS—◄◄

## Parámetros

No se necesita ningún parámetro para este mandato.

## Ejemplos

**Tarea** Cree categorías y códigos de protección de datos que se puedan añadir a los objetos de inventario de VMware:

```
dsmc set vmtags
```

**Conceptos relacionados:**

“Clases de gestión y grupos de copia” en la página 300

**Referencia relacionada:**

“Vmchost” en la página 612

“Vmtagdatamover” en la página 641

“Establecer contraseña” en la página 784

## Visión general de los códigos de protección de datos

Para gestionar la protección de datos de máquinas virtuales, puede asignar códigos de IBM Spectrum Protect a objetos de inventario de VMware. Puede asignar códigos a objetos VMware especificando los valores de protección de datos de Extensión de IBM Spectrum Protect del cliente web de vSphere. Si no utiliza Extensión de IBM Spectrum Protect, puede asignar códigos utilizando herramientas de script como VMware Power CLI.

Si habilita el soporte de códigos para gestionar las copias de seguridad, puede gestionar la protección de máquinas virtuales, como la exclusión o la inclusión de máquinas virtuales en servicios de copia de seguridad planificada, o la asignación de una planificación para proteger máquinas virtuales en un contenedor. En el caso de los códigos relacionados con las planificaciones, las máquinas virtuales tienen que estar en un conjunto de protección protegido por una planificación. Un conjunto de protección consta de las máquinas virtuales de un contenedor al que se ha asignado el código Schedule (IBM Spectrum Protect).

También puede especificar la política de retención para copias de seguridad, definir la coherencia de datos de las instantáneas, especificar los discos de la máquina virtual que se van a proteger o habilitar la protección de aplicaciones con la Extensión de IBM Spectrum Protect.

Los siguientes objetos de inventario de VMware son los contenedores que se pueden utilizar para gestionar las copias de seguridad de la máquina virtual:

- Centro de datos
- Carpeta (carpetas de clúster y host y carpetas de plantilla y máquina virtual)
- Host
- Clúster de host
- Agrupación de recursos
- Máquina virtual

Si se habilita el soporte a la codificación, puede asignar códigos de protección de datos a contenedores de VMware. Si no utiliza Extensión de IBM Spectrum Protect, tiene que ejecutar el mandato **set vmtags** para crear categorías y códigos de protección de datos en el inventario de VMware. Para obtener información sobre cómo crear códigos, consulte la publicación Creación de códigos en el inventario de VMware. Para obtener la lista de códigos admitidos, consulte el apartado “Códigos de protección de datos admitidos” en la página 793.

Cuando la opción **vmtagdatamover** se establece en *yes*, se realiza una copia de seguridad de todos los códigos que se asignan a una máquina virtual durante las operaciones **backup vm**. Los códigos se restauran cuando se ejecuta el mandato **restore vm**. No se efectúan copias de seguridad de los códigos que se asignan a otros objetos de inventario, por lo que no se pueden restaurar.

### Representación de códigos en Extensión de IBM Spectrum Protect

Al especificar valores de protección de datos en la ventana de IBM Spectrum Protect de Extensión de IBM Spectrum Protect, se asignan códigos de protección de datos al objeto de inventario.

Por ejemplo, si ha seleccionado **Sí** en el campo **Excluir de copia de seguridad**, la categoría Backup Management (IBM Spectrum Protect) y el código Excluded se

asignan al objeto de inventario. El código y la categoría asignados se muestran en el portlet **Códigos** del separador Resumen del objeto de inventario.

## Códigos de protección de datos admitidos

Se pueden asignar códigos de protección de datos de IBM Spectrum Protect a los objetos de inventario de VMware para controlar cómo se gestionan las copias de seguridad de máquina virtual.



Las operaciones de VMware solo están disponibles si el cliente funciona como transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Si utiliza Extensión de IBM Spectrum Protect para configurar la política de copia de seguridad, no tiene que asignar manualmente los códigos y categorías a los objetos de inventario. Puede utilizar la ventana de IBM Spectrum Protect para especificar los valores de protección de datos de los objetos de inventario en el cliente web de vSphere. Esta acción es equivalente a la asignación de códigos a un objeto de inventario.

Si utiliza las herramientas de script para la codificación, puede utilizar el mandato **set vmtags** de la línea de mandatos del transportador de datos para crear los códigos y las categorías del inventario de vSphere.

A menos que se indique lo contrario, puede asignar códigos de protección de datos a los siguientes tipos de objetos de inventario:

- Centro de datos
- Carpeta (carpetas de clúster y host y carpetas de plantilla y máquina virtual)
- Host
- Clúster de host
- Agrupación de recursos
- Máquina virtual

Se admiten los siguientes códigos de protección de datos.

| Categoría                                | Código                                                | Descripción del código                                                                          |
|------------------------------------------|-------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| Backup Management (IBM Spectrum Protect) | Excluded                                              | IBM Spectrum Protect siempre excluye el objeto de las copias de seguridad                       |
| Backup Management (IBM Spectrum Protect) | Included                                              | IBM Spectrum Protect siempre incluye el objeto en las copias de seguridad                       |
| Data Mover (IBM Spectrum Protect)        | <i>Datamover_name</i>                                 | Transportador de datos utilizado para las copias de seguridad en IBM Spectrum Protect           |
| Disk Backup List (IBM Spectrum Protect)  | Include   Exclude: <i>disk number,disk number,...</i> | Lista de discos virtuales que IBM Spectrum Protect incluye o excluye de las copias de seguridad |
| Management Class (IBM Spectrum Protect)  | <i>Management_class_name</i>                          | La política utilizada para valores de retención en IBM Spectrum Protect                         |

| Categoría                                     | Código                    | Descripción del código                                                                                                      |
|-----------------------------------------------|---------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Schedule (IBM Spectrum Protect)               | <i>Schedule_name</i>      | La planificación que se utilizará para las copias de seguridad de IBM Spectrum Protect                                      |
| Snapshot Attempts (IBM Spectrum Protect)      | <i>quiesce,nonquiesce</i> | Número de instantáneas detenidas o no detenidas que probará IBM Spectrum Protect antes de la copia de seguridad dé un error |
| Application Protection (IBM Spectrum Protect) | Enabled                   | IBM Spectrum Protect proporciona protección de aplicaciones                                                                 |
| Application Protection (IBM Spectrum Protect) | EnabledKeepSqlLog         | Proteja Microsoft SQL Server y conserve los archivos de registro para la gestión de archivos de registro en invitado        |

Los nombres de código y categoría de IBM Spectrum Protect distinguen entre mayúsculas y minúsculas. Las combinaciones de código y categoría se definen de la manera siguiente:

#### **Backup Management (IBM Spectrum Protect)**

##### **Excluded**

Excluye las máquinas virtuales de un objeto de inventario de los servicios de copia de seguridad planificada.

##### **Included**

Incluye las máquinas virtuales de un objeto de inventario en los servicios de copia de seguridad planificada. Este código es el predeterminado para la categoría Backup Management (IBM Spectrum Protect) y normalmente no es necesario definirlo.

Utilice este código cuando se asigne a un objeto padre el código Excluded, o si quiere asegurarse de que las máquinas virtuales de un objeto siempre se incluyan en copias de seguridad planificada, independientemente de los valores heredados.

Si no asigna estos códigos, y no existe ningún valor heredado, las máquinas virtuales se incluirán en las copias de seguridad planificadas.

Estos códigos sustituyen a la opción del transportador de datos domain.vmfull.

#### **Data Mover (IBM Spectrum Protect)**

##### ***Datamover\_name***

Asigna un transportador de datos para ejecutar copias de seguridad de máquinas virtuales.

Si utiliza Extensión de IBM Spectrum Protect, los transportadores de datos se asignarán automáticamente a máquinas virtuales si se aplican la categoría y el código de Schedule a un contenedor. Sin embargo, también puede actualizar manualmente los transportadores de datos de máquinas virtuales individuales.

Si no utiliza Extensión de IBM Spectrum Protect para aplicar el código de Schedule a un contenedor, tiene que asignar a mano

transportadores de datos a las máquinas virtuales, o sus contenedores padre, que se encuentren en la planificación.

Si no asigna un transportador de datos a una máquina virtual, el transportador de datos se hereda del objeto padre. Si no existe ningún valor heredado, la copia de seguridad de las máquinas virtuales la ejecutará el transportador de datos predeterminado, en caso de haberlo. De lo contrario, no se ejecutará la copia de seguridad de las máquinas virtuales y se identificará en la tabla Supervisor de Extensión de IBM Spectrum Protect con el estado **En riesgo** hasta que se asigna un transportador de datos a las máquinas virtuales.

Este código sustituye la opción del transportador de datos `nodename`.

### **Disk Backup List (IBM Spectrum Protect)**

#### **Include | Exclude:***disk number,disk number,...*

Incluye o excluye un conjunto de discos duros de máquinas virtuales en operaciones de seguridad. Los discos duros de la máquina virtual se identifican por el número de disco de la máquina virtual. Por ejemplo, en la mayoría de los casos, el disco 1 es el disco del sistema. Si no asigna este código a una máquina virtual, se hace una copia de seguridad de todos los discos duros de la máquina virtual.

Por una cuestión de facilidad de uso, la categoría Disk Backup List (IBM Spectrum Protect) se rellena con varios códigos utilizados habitualmente:

#### **Include:all**

Incluye todos los discos en una copia de seguridad.

#### **Include:1**

Incluye solo el disco 1 en una copia de seguridad y excluye explícitamente todos los discos restantes.

#### **Exclude:1**

Incluye todos los discos, excepto el disco 1 de una copia de seguridad.

Puede modificar el número de discos para que se ajuste a sus necesidades. Puede especificar un número de disco que se encuentre en el intervalo 1 - 999. Los números de disco deben aparecer como valores separados por comas, sin espacios entre las comas y los números.

Por ejemplo, para incluir solo los discos 1, 3 y 5 en las copias de seguridad, asigne la categoría Disk Backup List (IBM Spectrum Protect) y el código `Include:1,3,5` a una máquina virtual.

Para realizar una copia de seguridad de todos los discos, excepto del 1, el 2 y el 4, asigne la categoría Disk Backup List (IBM Spectrum Protect) y el código `Exclude:1,2,4` a una máquina virtual.

Si no especifica los discos que se van a incluir o excluir y no existe ningún valor heredado, se efectúa una copia de seguridad de todos los discos de la máquina virtual.

Estos códigos sustituyen a las opciones del transportador de datos `include.vmdisk` y `exclude.vmdisk`.

### **Management Class (IBM Spectrum Protect)**

#### *Management\_class\_name*

Especifica el nombre de la política de retención que define el tiempo durante el cual se conservan las versiones de copia de seguridad en el servidor de IBM Spectrum Protect o cuántas versiones de la copia de seguridad pueden existir en el servidor antes de que caduquen.

Si no se especifica la clase de gestión, la política de retención se hereda del objeto padre. Si no existe ningún valor heredado, se utiliza la clase de gestión especificada en la opción `vmmc`. Si no se ha definido la opción `vmmc`, se utiliza la política de retención predeterminada del nodo del centro de datos.

Este código sustituye a las opciones `include.vm`, `vmmc` o `vmctlmc`.

### **Schedule (IBM Spectrum Protect)**

#### *Schedule\_name*

Especifica el nombre de la planificación que se utiliza para las copias de seguridad de la máquina virtual en el servidor de IBM Spectrum Protect. El nombre de la planificación tiene que ser exclusivo.

El administrador de VMware o el administrador del servidor de IBM Spectrum Protect son quienes configuran las planificaciones para realizar automáticamente copias de seguridad de las máquinas virtuales en el inventario de vSphere. Por una cuestión de facilidad de uso, los administradores pueden utilizar IBM Spectrum Protect Operations Center Versión 8.1 para crear planificaciones compatibles con la codificación.

Al asignar esta categoría y este código a un objeto de inventario, se realiza una copia de seguridad, de acuerdo a la planificación, de todas las máquinas virtuales a nivel de objeto de inventario y a nivel de objeto hijo.

Sólo las planificaciones con la opción `-domain.vmfull="Schedule-Tag"` (y ningún otro parámetro a nivel de dominio) en las definiciones de planificación son compatibles con el soporte de codificación. En caso contrario, se omite el código `Schedule` y no se realizan copias de seguridad de las máquinas virtuales en objetos de inventario codificados con planificaciones no compatibles.

Para lograr la compatibilidad con la codificación, deben incluirse los criterios siguientes en la definición de planificación:

- Se debe especificar la opción `-domain.vmfull="Schedule-Tag"` (y ningún otro parámetro a nivel de dominio) en la serie de opciones. La opción no distingue entre mayúsculas y minúsculas y no puede contener espacios. El entrecomillado del parámetro `Schedule-Tag` es opcional.
- La planificación tiene que contener los parámetros `ACTION=BACKUP` y `SUBACTION=VM`.
- La serie de opciones tiene que contener la opción `-asnodename=centro_datos`, donde el valor del parámetro



*centro\_datos* tiene que corresponderse con el centro de datos que está gestionando Extensión de IBM Spectrum Protect.

- Si se especifica la opción *-vmbackuptype=backuptype* en la serie de opciones, el valor del parámetro *backuptype* tiene que ser FULLVM (no distingue entre mayúsculas y minúsculas).

El siguiente mandato del servidor de muestra define una planificación compatible con la codificación:

```
define schedule nombre_dominio nombre_planificación
description=descripción_planificación action=backup subaction=VM
starttime=NOW+00:10 schedstyle=Classic period=1 perunits=Weeks
durunits=minutes duration=10 options='-vmbackuptype=fullvm
-asnodename=nombre_nodo_centro_datos -mode=IFIncremental
-domain.vmfull="Schedule-Tag"'
```

El administrador del servidor tiene que asociar también un transportador de datos a la planificación utilizando el siguiente mandato de servidor:

```
define association nombre_dominio nombre_planificación nombre_nodo_transportador_a
```

Esta categoría y este código se pueden asignar a centros de datos, carpetas, hosts, clústeres de host y agrupaciones de recursos. No puede asignar una planificación a máquinas virtuales individualmente.

**Consejo:** Si asigna el código Schedule a un contenedor sin utilizar Extensión de IBM Spectrum Protect, la categoría y el código del Data Mover no se asignarán automáticamente a las máquinas virtuales del contenedor. Tiene que asignar manualmente el código del Data Mover a cada máquina virtual. Otra opción es que, si la planificación está asociada a solo un transportador de datos, se asigne el transportador de datos directamente al contenedor protegido por la planificación.

Si no establece este código en un objeto, se hereda el código Schedule del objeto padre. Si no existe ningún valor heredado, las máquinas virtuales no se incluyen en las copias de seguridad planificadas.

Todos los parámetros a nivel de dominio de la opción del transportador de datos *domain.vmfull* se omiten en una planificación compatible con la codificación.

## Snapshot Attempts (IBM Spectrum Protect)

### *quiesce,nonquiesce*

Esta combinación de categoría y código especifica el número total de intentos de instantánea para una operación de copia de seguridad de máquina virtual que no se ejecuta correctamente debido a un error de instantánea. El valor del código consta de un par de parámetros de posición, que describen el número de veces que se intenta realizar una instantánea y la coherencia de datos que se busca conseguir durante el intento.

### *quiesce*

Un parámetro de posición que especifica el número de veces que se intenta realizar la instantánea con detención, lo que crea una instantánea coherente con la aplicación.

- En el caso de las máquinas virtuales de Windows a las que se haya asignado el código Application Protection,

el parámetro *detención* especifica el número de veces que se intentará realizar la instantánea con detención de VSS de IBM Spectrum Protect y detención de VSS del proveedor de sistema Microsoft Windows.

Según el número especificado, el primer intento de instantánea se realiza siempre con detención de VSS de IBM Spectrum Protect. Los siguientes intentos de instantánea se realizan con detención de VSS del proveedor de sistema Windows.

- En el caso de máquinas virtuales de Windows sin código Application Protection o en el caso de máquinas virtuales de Linux, el parámetro *detención* especifica el número de veces que es necesario intentar realizar la instantánea con detención del sistema de archivos de herramientas de VMware.

Puede especificar un valor comprendido entre 0 y 10. El valor predeterminado es 2.

#### *nonquiesce*

Parámetro de posición que especifica el número de veces que se debe intentar realizar una instantánea sin detención, una vez completados los intentos de instantánea con detención (tal y como especifica el parámetro *quiesce*). Sin detención de instantánea, se crean instantáneas que no resultan afectadas en caso de bloqueo. Con las instantáneas que no resultan afectadas en caso de bloqueo, no se garantiza la coherencia de aplicación, del sistema operativo o del sistema de archivos.

Puede especificar un valor comprendido entre 0 y 10. El valor predeterminado es 0.

**Restricción:** La entrada 0,0 no es válida. Las operaciones de copia de seguridad requieren como mínimo una instantánea.

Los siguientes intentos de instantánea son opciones comunes que se utilizan para mantener la coherencia de datos:

#### **2,0 - siempre coherente con la aplicación**

Se intentan dos instantáneas con detención antes de que la copia de seguridad falle. Esta es la combinación predeterminada.

#### **2,1 - intento de coherencia con la aplicación**

Se intentan dos instantáneas con detención y, como intento final, una instantánea sin detención que no resulta afectada en caso de bloqueo.

#### **0,1 - solo coherencia con la máquina**

Se intenta solo una instantánea sin detención para máquinas virtuales que no pueden completar una instantánea con detención.

Si no se especifican los intentos de instantánea y no existe ningún valor heredado, se utilizan los intentos de instantánea especificados en la opción `include.vmsnapshotattempts`.

Este código sustituye a la opción `include.vmsnapshotattempts`.

## Application Protection (IBM Spectrum Protect)

### Enabled

Notifica a las aplicaciones de máquina virtual que está a punto de ejecutarse una copia de seguridad. Esta combinación de categoría y código permite a la aplicación truncar registros y confirmar transacciones, de manera que la aplicación pueda reanudarse desde un estado coherente cuando finaliza la copia de seguridad.

Cuando a una máquina virtual se le asignan esta categoría y esta etiqueta, IBM Spectrum Protect proporciona la protección de aplicaciones. El transportador de datos se bloquea, desbloquea los grabadores VSS y trunca los registros de aplicación. Si no se asigna este código a una máquina virtual, la protección de aplicaciones la proporciona VMware, que se bloquea y desbloquea los grabadores VSS, pero no trunca los registros de aplicación.

Puede asignar este código y esta categoría solo a máquinas virtuales.

Si asigna esta categoría y este código a una máquina virtual, tiene que completar un paso de configuración adicional. En cada transportador de datos que esté utilizando para realizar una copia de seguridad de las máquinas virtuales, almacene las credenciales de la máquina virtual huésped en Data Protection for VMware ejecutando el siguiente mandato desde la línea de mandatos del transportador de datos:

```
dsmc set password -type=vmquest nombre_visualización_huésped_mv ID_admin_huésped
contraseña_admin_huésped
```

Donde *nombre\_visualización\_huésped\_mv* especifica el nombre de la máquina virtual huésped como se ve en el cliente web de VMware vSphere.

Este mandato almacena las credenciales de la máquina virtual huésped, cifradas en el sistema que aloja el transportador de datos. Se necesitan los siguientes permisos mínimos para *ID\_admin\_huésped* *contraseña\_admin\_huésped*:

Derechos de copia de seguridad: Microsoft Exchange Server 2013 y 2016: permisos de gestión de organización (pertenencia al grupo de roles de gestión, gestión de organización)

Derechos de copia de seguridad: Microsoft SQL Server 2014 y 2016: permisos de gestión de organización (pertenencia al grupo de roles de gestión, gestión de organización)

Si utiliza las mismas credenciales para iniciar sesión en varias máquinas virtuales habilitadas para la protección de aplicaciones, puede definir la contraseña de todas las máquinas virtuales especificando el parámetro **allvm** en el mandato siguiente:

```
dsmc set password -type=vmquest allvm ID_admin_huésped contraseña_admin_huésped
```

Para obtener más información, consulte el apartado Configuración de Data Protection for VMware.

Si no habilita la protección de aplicación, se utiliza el valor de la opción `include.vmtsmvss`. Este valor no se puede heredar.

Este código sustituye a la opción `include.vmtsmvss`.

### **EnabledKeepSqlLog**

Proporciona protección de aplicaciones y evita que los registros de Microsoft SQL Server se trunquen si un transportador de datos realiza una copia de seguridad de una máquina virtual que está ejecutando Microsoft SQL Server. Al especificar este código, el administrador del servidor SQL puede gestionar a mano los registros del servidor SQL, de manera que se puedan conservar y utilizar para restaurar las transacciones de SQL a un determinado punto de comprobación, una vez restaurada la máquina virtual. El administrador del servidor SQL tiene que realizar la copia de seguridad a mano y, posiblemente, truncar los registros del servidor SQL en la máquina virtual huésped.

Puede asignar este código y esta categoría solo a máquinas virtuales. Además de este código, tiene que asignar este código de Enabled a las máquinas virtuales.

Si se especifica este código, el registro de servidor SQL no se trunca y el mensaje siguiente se visualiza y se registra en el servidor de IBM Spectrum Protect:

```
ANS4179I IBM Spectrum Protect application protection
no ha truncado los registros de Microsoft SQL Server en la máquina virtual 'VM'.
```

Si tiene que habilitar el recorte de registros del servidor SQL una vez completada una copia de seguridad, elimine el código EnabledKeepSqlLog y asigne la categoría y el código Application Protection (IBM Spectrum Protect) Enabled a la máquina virtual. En este caso, el transportador de datos no efectúa una copia de seguridad de los archivos de registro SQL.

Si no establece este código, los registros de Microsoft SQL Server no se conservan durante la copia de seguridad habilitada para la protección de aplicaciones. Este código no se puede heredar.

Este código sustituye al parámetro keepsqllog en la opción include.vmtsmvss.

**Consejo:** Los códigos de protección de datos se pueden heredar de objetos de alto nivel. Para obtener más información, consulte el apartado “Herencia de valores de protección de datos”.

#### **Referencia relacionada:**

“Vmtagdatamover” en la página 641

“Vmtagdefaultdatamover” en la página 639

“Domain.vmfull” en la página 401

“Include.vmdisk” en la página 467

“INCLUDE.VMSNAPSHOTATTEMPTS” en la página 469

“INCLUDE.VMTSMVSS” en la página 472

### **Herencia de valores de protección de datos**

Los valores de protección de datos, o códigos, de IBM Spectrum Protect se pueden heredar, o transmitir, desde un objeto de inventario padre de alto nivel en el navegador del cliente web de vSphere.

Al asignar un código de protección de datos a un objeto de inventario en el cliente web de vSphere, los objetos hijo heredan el mismo código de protección de datos que el objeto de inventario padre al que se asignó el código.

En la lista siguiente, se muestran los tipos de objetos de inventario de vSphere que se pueden codificar y que pueden heredar códigos de protección de datos:

- Centro de datos
- Carpeta (carpetas de clúster y host y carpetas de plantilla y máquina virtual)
- Host
- Clúster de host
- Agrupación de recursos
- Máquina virtual

Por ejemplo, si se asigna el código `Excluded` a un clúster de host, todos los objetos hijos del objeto del clúster de host (host, carpeta de host y máquina virtual) heredarán el código `Excluded`. En este ejemplo, todas las máquinas virtuales que se encuentran en el clúster de host quedan excluidas de las copias de seguridad planificadas.

Si a un objeto hijo se le asigna un código y hereda códigos en la misma categoría, el código asignado al objeto hijo sustituirá al código heredado. Si un objeto hijo hereda códigos en la misma categoría de varios objetos ancestro, el código heredado del ancestro más próximo sustituirá a los códigos de otros ancestros.

Si no se asignan códigos de protección de datos en la jerarquía de inventario de vSphere, se aplicarán los valores de codificación predeterminados del sistema. Para obtener información sobre los códigos compatibles y los valores de codificación predeterminados, consulte el apartado “Códigos de protección de datos admitidos” en la página 793.

## Orden de prelación en las herencias

Según el objeto (objeto de destino) al que esté intentando asignar un código de protección de datos, existe una prioridad para determinar la distancia del objeto de destino a sus ancestros durante el procesamiento de herencia de códigos de varios ancestros. La tabla siguiente contiene objetos de destino y los posibles ancestros de cada tipo de objeto de destino, basándose en la jerarquía de objetos que se presenta en el navegador de cliente web de vSphere.

*Tabla 114. Orden de prelación de los objetos de inventario de vSphere*

| Objeto de destino          | Orden de prelación de códigos procesado                                                                                                                                                |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Máquina virtual            | Máquina virtual de destino → Carpetas anidadas de máquina virtual → Agrupaciones de recursos anidados → Host → Clúster de host → Carpetas de host anidadas → Centro de datos           |
| Carpeta de máquina virtual | Carpeta de máquina virtual de destino → Otras carpetas de máquina virtual anidadas → Centro de datos                                                                                   |
| Carpeta de host            | Carpeta de host de destino → Otras carpetas de host anidadas → Centro de datos                                                                                                         |
| Agrupación de recursos     | Agrupación de recursos de destino → Otra agrupación de recursos anidados → Carpetas de máquina virtual anidadas → Host → Clúster de host → Carpetas de host anidadas → Centro de datos |
| Host                       | Host de destino → Carpetas de host anidadas → Clúster → Centro de datos                                                                                                                |
| Clúster                    | Clúster de destino → Carpetas de host anidadas → Centro de datos                                                                                                                       |
| Centro de datos            | Centro de datos de destino                                                                                                                                                             |

Si el objeto de destino es una máquina virtual, se pueden asignar códigos de la misma categoría a la propia máquina virtual y a cualquier combinación de sus ancestros (incluidas carpetas de máquina virtual, agrupaciones de recursos, host, clúster de host, carpetas de host, centro de datos). Durante el proceso, cada tipo de objeto se incorpora en orden de prelación y el procesamiento se detiene cuando se encuentra un código de la misma categoría o cuando se llega al final de la lista.

Por ejemplo, para determinar si se aplica a las máquinas virtuales el código Excluded o Included de la categoría Backup Management (IBM Spectrum Protect), IBM Spectrum Protect busca los códigos Excluded e Included en el inventario de un centro de datos. Según el orden de prelación del objeto de destino de la máquina virtual, la búsqueda de los códigos Excluded e Included empieza en el propio objeto de destino (máquina virtual), seguido de la lista de posibles ancestros. Si se encuentra un código antes de llegar al final de la lista, este se aplica al objeto de destino. De lo contrario, no se aplica ningún código de la categoría Backup Management (IBM Spectrum Protect) a la máquina virtual de destino.

#### **Conceptos relacionados:**

“Consejos para la codificación de la protección de datos”

### **Consejos para la codificación de la protección de datos**

Las políticas de copia de seguridad las determinan las asignaciones de códigos de protección de datos en objetos de inventario de vSphere. El rendimiento del procesamiento de códigos de protección de datos también se puede ver afectado por la cantidad de códigos aplicados al inventario de vSphere y por el lugar de aplicación de dichos códigos.

Considere efectuar las acciones siguientes cuando defina la política de copia de seguridad de objetos en el inventario de vSphere:

- Beneficiarse del orden de prelación para codificar objetos de inventario. Cree una configuración de política general para una empresa a través de la definición de políticas de copia de seguridad (o códigos) en el contenedor superior de la jerarquía de inventarios de vSphere. Las políticas son heredadas por contenedores hijo y sus máquinas virtuales. En general, no es necesario que defina políticas en máquinas virtuales individuales.

A continuación, cree excepciones cambiando la política de un contenedor hijo o de máquinas virtuales individuales para alterar temporalmente el valor de política heredado.

Otra opción es que, si no quiere configurar una política de copia de seguridad general, no asigne códigos de protección de datos a los objetos de alto nivel. Asigne los códigos de protección de datos a objetos de un nivel más bajo.

- Por cuestiones de rendimiento y de facilidad de mantenimiento y uso, evite asignar códigos a demasiados objetos de inventario.
- Para facilitar el mantenimiento y reducir la complejidad, evite asignar códigos a distintos tipos de objeto. Por ejemplo, asigne códigos solo a clústeres, hosts, carpetas de host y máquinas virtuales, o bien solo a carpetas de máquina virtual y máquinas virtuales, pero no ambas opciones al mismo tiempo.
- Con el soporte a la codificación, puede asignar varias planificaciones a distintos transportadores de datos. No debe solapar las planificaciones de un transportador de datos. De lo contrario, algunas planificaciones se pasarán por alto.

- Por una cuestión de facilidad de uso, los administradores pueden utilizar IBM Spectrum Protect Operations Center Versión 8.1 para crear planificaciones compatibles con la codificación.

**Conceptos relacionados:**

“Herencia de valores de protección de datos” en la página 800





---

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

Las funciones de accesibilidad ayudan a los usuarios con discapacidades, como movilidad restringida o visión limitada, para que puedan utilizar el contenido de las tecnologías de la información satisfactoriamente.

### Visión general

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

- Operaciones solo con teclado
- Operaciones que utilizan un lector de pantalla

La familia de productos de IBM Spectrum Protect utiliza el último estándar de W3C, WAI-ARIA 1.0 ([www.w3.org/TR/wai-aria/](http://www.w3.org/TR/wai-aria/)), para garantizar la conformidad con US Section 508 ([www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards](http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards)) y Web Content Accessibility Guidelines (WCAG) 2.0 ([www.w3.org/TR/WCAG20/](http://www.w3.org/TR/WCAG20/)). Para sacar partido de las funciones de accesibilidad, utilice la última versión del lector de pantalla y el último navegador web admitido por el producto.

Se ha añadido accesibilidad a la documentación del producto disponible en IBM Knowledge Center. Las funciones de accesibilidad de IBM Knowledge Center están descritas en la sección de accesibilidad de la ayuda de IBM Knowledge Center ([www.ibm.com/support/knowledgecenter/about/releasesnotes.html?view=kc#accessibility](http://www.ibm.com/support/knowledgecenter/about/releasesnotes.html?view=kc#accessibility)).

### Navegación mediante teclado

Este producto utiliza teclas de navegación estándar.

### Información sobre la interfaz

Las interfaces de usuario no tienen contenido que se actualice entre 2 y 55 veces por segundo.

Las interfaces de usuario web se basan en hojas de estilo en cascada para representar adecuadamente el contenido y proporcionar una experiencia fácil de utilizar. La aplicación proporciona un método equivalente para que los usuarios con problemas de visión utilicen los valores de visualización del sistema, incluida la modalidad de contraste alto. Puede controlar el tamaño de fuente utilizando la configuración del dispositivo o del navegador web.

Entre las interfaces web, se incluyen puntos de referencia de navegación WAI-ARIA que se pueden utilizar para ir rápidamente a las áreas funcionales de la aplicación.

### Software del proveedor

La familia de productos de IBM Spectrum Protect incluye determinado software de proveedor que no está incluido en el acuerdo de licencia de IBM. IBM no es

responsable de las funciones de accesibilidad de estos productos. Póngase en contacto con el proveedor para ver la información de accesibilidad de sus productos.

### **Información de accesibilidad relacionada**

Además del centro de atención al cliente de IBM y los sitios web de soporte, IBM tiene un servicio telefónico TTY que pueden utilizar los clientes sordos o con dificultades auditivas para acceder a los servicios de soporte y ventas:

Servicio TTY  
800-IBM-3383 (800-426-3383)  
(en Norteamérica)

Para obtener más información sobre el compromiso de IBM con la accesibilidad, consulte el apartado Accesibilidad de IBM ([www.ibm.com/able](http://www.ibm.com/able)).

---

## Avisos

Esta información se ha desarrollado para productos y servicios que se ofrecen en Estados Unidos. Este material puede estar disponible en IBM en otros idiomas. Sin embargo, es posible que tenga obligación de tener una copia del producto o de la versión del producto en dicho idioma para poder acceder.

IBM no proporcionará los productos, servicios o funciones que se tratan en este documento en otros países. Póngase en contacto con su representante local de IBM para obtener más información acerca de los productos y servicios que actualmente están disponibles en su país. Cualquier referencia a un producto, programa o servicio de IBM no significa ni implica que sólo pueda utilizar este determinado producto, programa o servicio de IBM. En su lugar, puede utilizarse cualquier producto, programa o servicio equivalente funcionalmente que no infrinja los derechos de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patente pendientes que cubran el tema central tratado en este documento. El presente documento no le confiere ningún derecho sobre estas patentes. Si lo desea, puede realizar consultas sobre licencias, por escrito, dirigiéndose a:

*IBM Director of Licensing  
IBM Corporation  
North Castle Drive, MD-NC119  
Armonk, NY 10504-1785  
EE.UU.*

Para consultas sobre licencias relativas a información del juego de caracteres de doble byte (DBCS), póngase en contacto con el departamento de propiedad intelectual de IBM en su país o envíe las consultas, por escrito, a:

*Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan Ltd.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokio 103-8510, Japón*

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍA DE NINGUNA CLASE, NI EXPRESA NI IMPLÍCITA, INCLUIDAS, PERO NO LIMITADAS A LAS GARANTÍAS IMPLÍCITAS DE NO CUMPLIMIENTO, COMERCIALIZACIÓN O IDONEIDAD PARA UNA FINALIDAD DETERMINADA. Algunos países no permiten la renuncia de garantías expresas ni implícitas en determinadas transacciones, por lo que esta declaración puede no ser aplicable a su caso.

Esta información puede contener imprecisiones técnicas o errores tipográficos. Periódicamente se efectúan cambios en la información aquí contenida; estos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede realizar mejoras y/o cambios en los productos o programas descritos en esta publicación sin previo aviso.

Cualquier referencia a esta información en sitios web que no son de IBM se proporciona solamente para su comodidad y no equivale de ninguna manera a una aprobación de dichos sitios web. El material de esos sitios web no forma parte del material correspondiente a este producto IBM y el uso de esos sitios web se realiza por cuenta y riesgo del usuario.

IBM puede utilizar o distribuir cualquier información que usted proporcione de la forma que considere apropiada sin incurrir en ninguna obligación con usted.

Los poseedores de licencias de este programa que deseen obtener información sobre éste a efectos de permitir: (i) el intercambio de información entre programas creados de forma independiente y otros programas (incluido éste) y (ii) el uso mutuo de la información intercambiada, deben ponerse en contacto con:

*IBM Director of Licensing  
IBM Corporation  
North Castle Drive, MD-NC119  
Armonk, NY 10504-1785  
EE.UU.*

Esta información puede estar disponible, sujeta a los términos y condiciones adecuados, incluyendo en algunos casos el pago de una tarifa.

El programa bajo licencia que se describe en este documento y todo el material bajo licencia disponible los proporciona IBM bajo los términos de las Condiciones Generales de IBM, Acuerdo Internacional de Programas Bajo Licencia de IBM o cualquier acuerdo equivalente entre las partes.

Los datos de rendimiento que se mencionan aquí se presentan tal como se han obtenido en determinadas condiciones operativas. Los resultados reales pueden variar.

La información acerca de productos ajenos a IBM se ha obtenido de los proveedores de dichos productos, sus anuncios publicados u otras fuentes de disponibilidad pública. IBM no ha probado dichos productos y no puede confirmar la precisión del rendimiento, la compatibilidad ni otras afirmaciones relacionadas con productos que no son de IBM. Las preguntas relacionadas con las prestaciones de los productos que no son de IBM deberían dirigirse a los proveedores de dichos productos.

Esta información contiene ejemplos de datos e informes utilizados en operaciones comerciales cotidianas. Para ilustrarlos de la forma más completa posible, se han utilizado nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier parecido con nombres y direcciones de una empresa real es pura coincidencia.

#### LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de ejemplo en código fuente, que ilustran técnicas de programación en diferentes plataformas operativas. Debe copiar, modificar y distribuir estos programas de muestra en cualquiera de las formas sin pago para IBM, para el desarrollo, utilización, marketing o distribución de los programas de aplicación conforme a la interfaz de programación de la aplicación para la plataforma operativa para la que están escritos los programas de muestra. Estos ejemplos no se han probado exhaustivamente bajo todas las condiciones. Por tanto, IBM no puede garantizar ni implicar la fiabilidad, utilidad

o función de estos programas. Los programas de ejemplo se proporcionan "TAL CUAL" y sin garantía de ninguna clase. IBM no será responsable de ningún daño que surja del uso de los programas de muestra.

Cada copia o fragmento de estos programas de ejemplo o cualquier trabajo derivado deben incluir un aviso de copyright como el siguiente: © (nombre de su empresa) (año). Partes de este código derivan de programas de ejemplo de IBM Corp. © Copyright IBM Corp. \_escriba el año o años\_.

## **Marcas registradas**

el logotipo de IBM, el logotipo de IBM, e ibm.com son marcas o marcas registradas de International Business Machines Corp., registradas en muchas jurisdicciones de todo el mundo. Otros nombres de servicios y productos pueden ser marcas registradas de IBM o de otras compañías. Hay disponible una lista actual de marcas registradas de IBM en la web, en sección "Copyright and trademark information" de [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Adobe es una marca comercial registrada de Adobe Systems Incorporated en los Estados Unidos y/o en otros países.

Linear Tape-Open, LTO y Ultrium son marcas registradas de HP, IBM Corp. y Quantum en EE.UU. y en otros países.

Intel y Itanium son marcas registradas de Intel Corporation o sus filiales en Estados Unidos y/o en otros países.

Linux es una marca registrada de Linus Torvalds en Estados Unidos y/o en otros países.

Microsoft, Windows y Windows NT son marcas registradas de Microsoft Corporation en Estados Unidos y/o en otros países.

Java y todas las marcas y logotipos basados en Java son marcas comerciales o marcas registradas de Oracle y de sus filiales.

SoftLayer es una marca registrada de SoftLayer, Inc., empresa de IBM.

UNIX es una marca registrada de The Open Group en Estados Unidos y en otros países.

## **Términos y condiciones de la documentación del producto**

Los permisos para la utilización de estas publicaciones se otorgan sujetos a los siguientes términos y condiciones.

### **Validez**

Estos términos y condiciones se añaden a los términos de utilización del sitio web de IBM.

### **Uso personal**

Puede reproducir estas publicaciones para su uso personal, no comercial, siempre que se conserven todos los avisos sobre derechos de propiedad. No podrá distribuir, visualizar ni crear trabajo derivado de estas publicaciones, o cualquier parte de éstas, sin el consentimiento expreso de IBM.

### **Uso comercial**

Puede reproducir, distribuir y mostrar estas publicaciones solamente dentro de su empresa, siempre y cuando se conserven todos los avisos de propiedad. No puede realizar trabajos derivados de estas publicaciones ni reproducir, distribuir o visualizar estas publicaciones ni parte de las mismas fuera de la empresa sin el consentimiento expreso de IBM.

### **Derechos**

Si no se indica lo contrario en este permiso, no se otorgan otros permisos, licencias o derechos, ya sea de forma expresa o implícita, a las publicaciones u otra información, datos, software u otra propiedad intelectual que contenga este documento.

IBM se reserva el derecho de retirar los permisos que se hayan proporcionado siempre que, bajo su discreción, el uso de las publicaciones sea perjudicial para sus intereses o, según determine IBM, no se estén siguiendo adecuadamente las instrucciones detalladas anteriormente.

Queda prohibido descargar, exportar o reexportar esta información si no se cumplen íntegramente todas las leyes aplicables y regulaciones, incluyendo las leyes y regulaciones de exportación de los Estados Unidos.

IBM NO PROPORCIONA NINGUNA GARANTÍA RELACIONADA CON EL CONTENIDO DE ESTAS PUBLICACIONES. LAS PUBLICACIONES SE PROPORCIONAN "TAL CUAL" Y SIN GARANTÍAS DE NINGÚN TIPO, YA SEA DE FORMA EXPRESA O IMPLÍCITA, INCLUYENDO PERO SIN LIMITARSE A ELLAS GARANTÍAS IMPLÍCITAS DE NO INFRACCIÓN, COMERCIALIZACIÓN Y ADECUACIÓN PARA UN PROPÓSITO CONCRETO.

## **Consideraciones sobre la política de privacidad**

Los productos de IBM Software, incluido el software como soluciones de servicio, ("Ofertas de software") pueden utilizar cookies u otras tecnologías para recopilar información del uso del producto, ayudar a mejorar la experiencia del usuario final, adaptar las interacciones con el usuario final o para otros fines. En muchos casos, las Ofertas de software no recopilan información de identificación personal. Algunas de nuestras ofertas de software pueden ayudarle a recopilar información de identificación personal. Si esta oferta de software utiliza cookies para recopilar información de identificación personal, la información específica sobre la utilización de cookies de esta oferta se expone más adelante.

Esta oferta de software no utiliza cookies u otras tecnologías para recopilar información de identificación personal.

Si las configuraciones desplegadas para esta Oferta de software le ofrecen como cliente la posibilidad de recopilar información de identificación personal de los usuarios finales mediante cookies y otras tecnologías, debe buscar asesoramiento legal sobre las leyes aplicables a dicha recopilación de datos, incluidos los requisitos de aviso y consentimiento.

Para obtener más información sobre el uso de distintas tecnologías, incluidas las cookies, para estos fines, consulte la Política de privacidad de IBM en <http://www.ibm.com/privacy> y la Declaración de privacidad en línea de IBM en <http://www.ibm.com/privacy/details>, en la sección "Cookies, Web Beacons and Other Technologies", e "IBM Software Products and Software-as-a-Service Privacy Statement" en <http://www.ibm.com/software/info/product-privacy>.

---

## Glosario

Hay un glosario disponible con términos y definiciones para la familia de productos de IBM Spectrum Protect.

Consulte el apartado Glosario de IBM Spectrum Protect.

Para ver glosarios de otros productos de IBM, consulte Terminología de IBM.





---

# Índice

## Caracteres Especiales

\* ? 235

### A

acceso

    permisos, archivar 275

ACL

    sistemas de archivos admitidos 162

actualización automática 355

actualización automática del cliente 2

actualización del cliente de archivado y copia de seguridad  
    desde versiones anteriores del producto 1

Actualizaciones de software 47

afmskipuncachedfiles 346

Agente de almacenamiento

    para el traspaso de datos fuera de la LAN 158

    utilizar para el traspaso de datos sin LAN 416

agrupaciones de almacenamiento

    GPFS 249

AIX

    configurar para instantáneas 114

    partición de carga de trabajo (WPAR)

        copia de seguridad 215

        restaurar 253

almacenamiento

    visualizar sesiones de restauración reiniciables 737

almacenamiento conectado a red (NAS)

    cancelar procesos de copia de seguridad y

        restauración 691, 714

    consultar imágenes de sistemas de archivos que pertenecen  
        a 720

    especificar nombre de nodo para operaciones 498

    especificar para consulta 600

    especificar si guardar la tabla de contenido para cada copia  
        de seguridad de sistema de archivos 596

    excluir archivos de la copia de seguridad 425

    restaurar sistemas de archivos 254, 762

    sistemas de archivos de copia de seguridad 208, 680

    supervisar operaciones de copia de seguridad o  
        restauración 496

    supresión de espacios de archivos 698

    visualizar espacios de archivos en el servidor 727

    visualizar nodos para los que el ID de administrador tiene  
        autorización 735

anotación de eventos

    planificador 291

anotaciones

*Véase también* anotaciones de planificación

    anotaciones de errores, eliminar 420

    cliente Web 545

    controlar el tamaño 476

    DSM\_LOG, variable de entorno 422, 477, 547

    errorlogretention, opción 422

    especificar vía de acceso y nombre de archivo 422, 477,  
        547, 773

    opción errorlogname 422

    opción instrlogmax 476

    opción intrlogname 477

    schedlogname, opción 547, 773

anotaciones (*continuación*)

    schedlogretention, opción 547, 773

anotaciones de planificación

    controlar el tamaño 545

    especificar número de días para mantener entradas y si se  
        guardan entradas eliminadas 549

    especificar vía de acceso y nombre de archivo para  
        almacenar información de registro de planificación 547

API de HP-UX Itanium 2

    desinstalación 18

    instalación 16

    métodos de comunicación 6

API de Linux on Power Systems

    desinstalación 27

API de Linux on Power Systems (Big Endian)

    instalación 25

API de Ubuntu Linux on Power Systems (Little Endian)

    instalación 22

archivado

    asignación de descripciones en la línea de mandatos 272

    asignar descripción 384

    asociación de una instantánea local al espacio de archivos  
        del servidor 272, 571

    btrfs 205

    cómo se gestionan 278, 299

    comprimir archivos 370

    configurar soporte de proxy del nodo cliente 272

    consultar acceso de usuarios 717

    copia, atributos de grupo 301

    datos compartidos en varios clientes bajo un único nombre  
        de nodo 272, 349

    ejecutar 269

    eliminar indicador de confirmación antes de suprimir 503

    enlaces simbólicos 275

    incluir archivos 458

    información, consultar 718

    inicio de una sesión del cliente web 147

    lista de archivos 272, 439

    mandato 664

    más de una especificación de archivo 272

    mejorar la velocidad mediante memoria compartida 315

    modalidad de copia 304

    número de intentos para realizar una copia archivada de  
        archivos abiertos 363

    período de gracia de retención 300

    procesar sólo directorios (no archivos) 390

    recuperar mediante la línea de mandatos 277

    removeoperandlimit 528

    resumen de opciones 316

    sólo archivos 603

    sólo archivos, no directorios 272

    subdirectorios 272

    suprimir archivos después 383

    suprimir archivos individuales del espacio de archivos de  
        servidor 274, 693

    suprimir espacios de archivos 186, 267

    sustitución de la clase de gestión durante 307

    tareas primarias 269

    utilización de mandatos 270, 274

    vinculación de clases de gestión a archivos 272

    vincular clase de gestión 347

- archivado (*continuación*)
  - vínculos fijos 276
  - visualizar fecha de última modificación y fecha de último acceso o fecha de creación 718
- archive fastback
  - mandato 667
- archivo de configuración de diario
  - cómo configurar 78
- archivo de opciones de inclusión/exclusión
  - espacios de archivos activados para Unicode 456
  - especificación de la vía de acceso y el nombre de archivo de 456
  - gestionar archivos 278
  - proceso ascendente 136
  - visión general 161
- archivo de opciones de usuario de cliente
  - modificación temporal mediante los mandatos 336
- archivo de opciones de usuario de cliente predeterminado
  - crear y modificar 58
  - ejemplo de 58
- archivo de opciones del cliente
  - crear y modificar 56
  - opciones necesarias de 56
  - visión general 54
- archivo de opciones del sistema cliente
  - copiar y modificar 56
  - especificar opciones de inclusión/exclusión 125
- archivo dsm.opt
  - crear 58
  - crear y modificar 56
  - ejemplo de 58
  - especificar una especificación de unidad con caracteres comodín 131
  - opciones necesarias de 56
  - personalizar 60
- archivo dsm.opt.smp 58
- archivo dsm.smp
  - copiar en dsm.opt 56
  - location 56
- Archivo dsm.sys
  - crear 56
  - ejemplo de 56
- archivo dsm.sys.smp 56
- archivo dsmerlog.pru 420
- archivo dsmerror.log 420
- archivo ejecutable
  - códigos de retorno de 297
- archivo TSM.PWD 418
- archivos
  - archivado 269, 664
  - archivado mediante mandatos 274
  - archivar lista 272, 439
  - archivar más de una especificación de archivo 272
  - archivos, cómo se gestionan 278
  - asignar clases de gestión 229
  - autorizar a otro usuario para restaurar o recuperar 264
  - cambiar el nombre de los espacios de archivos que no son Unicode al formato Unicode 356, 775
  - cifrado 161
  - clasificar lista de 150
  - comprimir durante archivado o copia de seguridad 370
  - consultar acceso de usuarios 717
  - consultar información de copias archivadas 718
  - consultar información sobre copia de seguridad 720
  - copia archivada, sustitución de clase de gestión 307
  - copia de seguridad con enlaces fijos 232
  - copia de seguridad de abiertos 234
- archivos (*continuación*)
  - definición de modificado 170
  - excluir grupos 131, 132
  - gestionar crecimiento durante compresión 369
  - incluir grupos 131, 132
  - inclusión/exclusión
    - crear en formato Unicode 457
  - procesar inclusión/exclusión 136
  - realización de grandes operaciones de restauración 260
  - recuperación de archivos que pertenecen a otro nodo 265
  - recuperar copias archivadas 277
  - recuperar mediante mandatos 277
  - restauración 258
  - restauración de archivos que pertenecen a otro nodo 265
  - restaurar, mediante mandatos 264
  - restaurar con enlaces fijos 232
  - restaurar dispersos 232
  - restaurar o recuperar en otra estación de trabajo 266
  - suprimir archivos individuales del espacio de archivos de servidor 274, 693
  - suprimir copias de seguridad individuales del espacio de archivos de servidor 695
  - suprimir después de archivar 383
  - tamaño máximo de archivo para operaciones 166
  - vinculación de clases de gestión 308
- archivos de base de datos de diario
  - errorlog 80
  - journaldir 80
- archivos de control 609
- archivos de copia de seguridad
  - asignar clase de gestión 306
- archivos del sistema
  - excluir 129
- archivos esparcidos
  - copia de seguridad 232
  - especificar cómo restaurar o recuperar 485
  - restaurar 232
- archivos para la eliminación de duplicados
  - exclude 93
- archmc, opción 347
- archsymbkfile, opción 348
- asnodename, opción 349
- asnodename, valores de sesión 350
- atributo Destino de copia 305
- atributo Frecuencia de copia 302
- atributo Nombre de grupo de copia 302
- atributo Retener única versión 303
- atributo Retener versión 305
- atributo Retener versiones adicionales 303
- atributo Serialización de copia 303
- atributo Tipo de copia 302
- autenticación
  - cliente de IBM Spectrum Protect 141
- automatización de servicios de copia de seguridad
  - iniciar el planificador cliente 69
  - opciones 292
  - procesar mandatos antes de la copia de seguridad 517
  - procesar mandatos después de la copia de seguridad 514
  - visualizar trabajos planificados 289, 291
- automount, opción 358
- autorización
  - opciones 333
  - usuario para restaurar o recuperar los archivos 264
- ayuda en línea
  - foro en línea 152
  - servicio de soporte técnico 152
  - visualizar 152

## B

- backup group, mandato 672
- backup image
  - btrfs 205
  - utilizar DSM\_DIR para hacer referencia a una biblioteca de complementos 62
- backup image, mandato 674
  - dispositivos admitidos 197
- backup nas, mandato 680
- backup vm, mandato 683
- biblioteca de complementos
  - para imagen o copia de seguridad o restauración NAS 62
- btrfs 237, 758

## C

- cadenas de entrada
  - con espacios en blanco 145
- campo Nombre de nodo 265
- cancel process, mandato 691
- cancel restore, mandato 692
- caracteres comodín
  - directrices 663
  - especificar una especificación de unidad en dsm.opt 131
  - incluir o excluir archivos 130
  - incluir o excluir grupos de archivos 131
  - para incluir o excluir grupos de archivos 132
  - utilizar con especificaciones de archivo 235
  - utilizar con mandatos 235
- características de accesibilidad 805
- carpetas
  - visión general del proceso de copia de seguridad incremental 170
- changingretries, opción 363
- cifrado
  - datos de archivos 161
  - guardar contraseña de clave de cifrado 418
  - varios clientes bajo un único nombre de nodo 349
- cifrado de datos durante el archivado 161
- cifrado de datos durante la copia de seguridad 161
- CIFS
  - copia de seguridad de sistemas de archivos 213
- clase de gestión
  - asignar 229
- clase de gestión estándar
  - atributo Eliminar duplicados de datos 305
  - Destino de copia 305
  - Frecuencia de copia 302
  - modalidad de copia
    - absoluta 304
    - Modificados 304
  - Nombre de grupo de copias 302
  - Retener única versión 303
  - Retener versión 305
  - Retener versiones adicionales 303
  - Serialización de copia 303
  - Tipo de copia 302
  - valores predeterminados 301
  - Versiones si datos existen 302
  - Versiones si datos suprimidos
    - versiones activas 303
    - versiones inactivas 303
- clase de gestión predeterminada 299
- clases de gestión
  - asignación a directorios 307, 308, 389
  - asignar a archivos 306

- clases de gestión (*continuación*)
  - aspectos a tener en cuenta 305
  - cómo las utiliza IBM Spectrum Protect 161
  - especificación con la opción include 306
  - predeterminado 300
  - procesar 306
  - selección para archivos 305
  - sustitución del valor predeterminado 306
  - sustitución durante el proceso de copia archivada 307
  - utilización de clase de gestión, ejemplo 306
  - vinculación a archivos 308
  - vincular copias archivadas a 272
  - visualizar 301
  - visualizar información sobre 734
- client
  - actualización automática 2
  - dirección TCP/IP del cliente distinta de la utilizada para el primer contacto del servidor 587
  - establecer contraseña 124
  - inscripción con servidor 123
  - número de puerto TCP/IP del cliente distinto del utilizado para el primer contacto del servidor 588
  - tamaño de la ventana deslizante de TCP/IP para el nodo cliente 591
- cliente, opciones
  - exclude
    - exclude.archive 126
    - exclude.attribute.symlink 126
    - exclude.backup 126
    - exclude.compression 126
    - exclude.dir 126
    - exclude.file 126
    - exclude.file.backup 126
    - exclude.fs 126
    - exclude.image 126
  - modificación temporal utilizando la línea de mandatos 336
  - orden de proceso (precedencia) 336
  - utilizar con mandatos 336
  - visión general 660
  - visualización de los valores actuales 736
- cliente AIX
  - componentes del cliente 5
  - desinstalación 15
  - instalación 12
  - métodos de comunicación 5
- cliente de administración
  - permitir sesiones seguras dentro de una red privada 585
- cliente de archivado y copia de seguridad
  - instalación 12
  - visión general 1
- cliente de IBM Spectrum Protect
  - autenticación 141
- cliente de Ubuntu Linux on Power Systems (Little Endian)
  - desinstalación 24
  - instalación 22
- cliente HP-UX Itanium 2
  - aumento del límite predeterminado del tamaño de segmento de datos 18
- cliente IBM Spectrum Protect en Mac OS X
  - desinstalación 43
- cliente Linux on System z
  - componentes del cliente 8
  - desinstalación 41
  - instalación 37
  - métodos de comunicación 9

- cliente Linux x86\_64
  - componentes del cliente 8
  - desinstalación 31, 36
  - instalación 28
  - métodos de comunicación 8
- cliente Mac OS X
  - componentes del cliente 9
  - instalación 42
  - métodos de comunicación 10
  - pasos para la instalación 42
- cliente Macintosh
  - requisitos de instalación 9
  - requisitos previos de entorno 9
- cliente Oracle Solaris
  - componentes del cliente 10
  - métodos de comunicación 10
- cliente Solaris
  - instalación 44
  - instalación en zonas Solaris 44
- cliente Ubuntu x86\_64
  - instalación 33
- cliente Web
  - configurar 66
  - descripción general de la configuración 65
  - especificar direcciones de los puertos TCP/IP para 450
  - establecer comunicaciones a través de un cortafuegos 72, 450
  - funciones no admitidas 155
  - GUI 209
  - iniciar 147
  - limitar el acceso del administrador al cliente que ejecuta el cliente web 543
  - NAS
    - copia de seguridad de sistemas de archivos 209
    - navegadores admitidos 147
    - permitir ejecutar en un navegador activado para Swing 147
    - restricciones para sistemas de archivos NAS 208
    - resumen de opciones 335
    - utilizar a través de un cortafuegos 650
- clientes de archivado y copia de seguridad 1
- clúster IBM PowerHA SystemMirror
  - planificar 191
- codificación de protección de datos
  - herencia de códigos 800
  - lista soportada 793
  - visión general 792
- codificación de VMware
  - códigos de protección de datos compatibles 793
  - herencia 800
  - se representa en forma de valores de protección de datos 792
  - sugerencias para configurar políticas de copia de seguridad 802
  - visión general 792
- códigos de retorno para operaciones 297
- colocatebyfilespec, opción 365
- commmethod, opción 366
- Common Internet File System (CIFS)
  - copia de seguridad de sistemas de archivos 213
- commrestartduration, opción 368
- commrestartinterval, opción 368
- cómo empezar
  - cambio de la contraseña 141
  - clasificación de las listas de archivos 141
  - fin de una sesión 141
  - planificador cliente 141
  - cómo empezar (*continuación*)
    - sesión de línea de mandatos 141
    - sesión del cliente web 141
    - sesión GUI 141
    - visualizar ayuda en línea 141
- comparación de copias de seguridad: incremental, incremental por fecha 176
- comparación de planificador
  - aceptador de cliente frente a planificador tradicional 67
- compartida, serialización dinámica 303
- componentes de AIX
  - instalables 5
- componentes de HP-UX
  - instalables 6
- componentes de Linux on System z
  - instalables 8
- componentes de Linux x86\_64
  - instalables 8
- componentes del cliente
  - cliente AIX 5
  - cliente Linux on System z 8
  - cliente Linux x86\_64 8
  - cliente Mac OS X 9
  - cliente Oracle Solaris 10
  - Linux en el cliente Power Systems 7
- componentes Mac OS X
  - instalables 9
- compressalways, opción 369
- compression
  - activar proceso 464
  - desactivar proceso 464
  - sentencias de inclusión y exclusión 464
- compression, opción 370
- comprobaciones de integridad de cadena de copia de seguridad 644, 646
- comunicación cliente-servidor
  - dirección de puerto TCP/IP del servidor de IBM Spectrum Protect 590
  - dirección de puerto TCP/IP en el que establecer una conexión de memoria compartida 558
  - dirección TCP/IP del cliente distinta de la utilizada para el primer contacto del servidor 587
  - dirección TCP/IP del servidor de IBM Spectrum Protect 590
  - dirección TCP/IP para dsmcad 587
  - especificar nombre del servidor que debe contactarse para los servicios 555
  - especificar número de kilobytes que el cliente almacena en el almacenamiento intermedio antes de enviar la transacción al servidor 599
  - especificar servidor predeterminado 383
  - establecer 56
  - identificar la estación de trabajo ante el servidor 501
  - intentos de reconexión tras error 368
  - intervalo de reconexión tras error 368
  - método 366
  - número de puerto TCP/IP del cliente distinto del utilizado para el primer contacto del servidor 588
  - si deben enviarse transacciones pequeñas al servidor sin almacenarlas primero en el almacenamiento intermedio 589
  - tamaño de la ventana deslizante de TCP/IP para el nodo cliente 591
  - tamaño del almacenamiento intermedio de comunicaciones TCP/IP interno 586
  - tamaño máximo del almacenamiento intermedio de E/S de disco que utiliza el cliente al leer o escribir archivos 392

- comunicaciones
  - establecer a través de un cortafuegos 72
  - establecimiento con Secure Sockets Layer (SSL) 74
- con comillas 145
- Configuración de Tivoli Storage Manager FastBack 102
- configuración del cliente para eliminación de duplicados de datos 90
- configuración del cliente web 66
- configurar
  - planificador cliente 67
  - planificador gestionado por el aceptador de clientes 68
  - tareas necesarias 49
  - tareas obligatorias de usuario root 56
  - tareas opcionales 49
- configurar el cliente para la eliminación de duplicados de datos 90
- configurar soporte a las copias de seguridad del proxy de nodo cliente 188
- conjunto de copias de seguridad
  - activación de la GUI para la restauración local 240
  - activación de la GUI para la restauración local de 484
  - restaurar 237, 240
  - restaurar en un entorno de SAN 753
- conjunto de copias de seguridad locales
  - activación de la GUI para la restauración local 240
- conjuntos de copias de seguridad
  - consideraciones sobre la restauración 243, 752
- consideraciones acerca del mandato de restauración de conjuntos de copias de seguridad 243, 752
- consideraciones de copia de seguridad 227
- consideraciones sobre el cifrado 53
- console, opción 372
- consulta
  - archivos para otro nodo 447
  - cantidad de información que aparece en pantalla 552
  - copias de seguridad, establecer instante específico 513
  - descripción de 384
  - en función de fecha y la hora de la copia de seguridad, archivado 446, 449
- grupo
  - mandato 729
  - visualizar miembros de 559
- información del sistema 739
- lista de inclusión/exclusión 733
- NAS u objetos de cliente 364
- nodos para los que el cliente tiene autorización de nodo proxy 188
- nodos para los que el cliente tiene autorización de proxy 272
- preferencias de desplazamiento tras mostrar información en pantalla 553
- procesar sólo directorios (no archivos) 390
- visualizar objetos activos e inactivos 456
- consulta de opciones del cliente 345
- consulta de planificación ampliada 289
- contraseña
  - cambiar 148
  - caracteres válidos 148
  - establecer para cliente 124
  - número de caracteres 148
  - utilizar 144
- contraseña de IBM Spectrum Protect
  - utilizar 143
- copia de seguridad 180
  - almacenamiento conectado a red (NAS) 680
  - archivos nuevos o modificados 170
  - btfrs 205
  - copia de seguridad (*continuación*)
    - consultar acceso de usuarios 717
    - copia de seguridad selectiva mediante la línea de mandatos del cliente 182
    - datos compartidos en varios clientes bajo un único nombre de nodo 349
    - en paralelo 622, 623, 625, 627
    - en sesiones paralelas 223
    - enlaces simbólicos 229
    - imagen 194
      - con copia de seguridad incremental 679
      - dominio de cliente 399
    - imagen: instantánea, dinámica, estática 194
    - incremental
      - asociación de una instantánea local al espacio de archivos del servidor 712
    - incremental por fecha
      - línea de mandatos del cliente 182
    - inicio de una sesión del cliente web 147
    - mejorar la velocidad mediante memoria compartida 315
    - modalidad de copia 304
    - multisesión, enviar archivos contiguamente al servidor 365
    - número de intentos para realizar una copia de seguridad de archivos abiertos 363
    - omitir proceso de acl 559
    - período de gracia de retención 300
    - plantillas de máquina virtual 620
    - procesar sólo directorios (no archivos) 390
    - resumen de opciones 316
    - selectiva
      - asociación de una instantánea local al espacio de archivos del servidor 778
    - Sistemas de archivos de cifrado (EFS) 217
    - tareas primarias 155
    - una sesión de servidor por especificación de archivo 365
    - visión general 155
    - visualizar estado del proceso 224
  - copia de seguridad basada en el registro por diario
    - restauración 174
  - copia de seguridad con proxy de nodo cliente
    - Nodo agente 188
    - Nodo de destino 188
    - visión general 188
  - copia de seguridad con registro por diario 172, 709
    - comparar con copia de seguridad incremental, incremental por fecha 176
    - cuándo se debe utilizar 176
    - especificar valores de configuración 78
    - excluir archivos 127
    - exclusión de directorios 127
    - opciones de inclusión/exclusión
      - copia de seguridad con registro por diario 127
    - realizar incremental completa tradicional en lugar de 502, 709
  - copia de seguridad de archivos abiertos 234
  - copia de seguridad de archivos dispersos 232
  - copia de seguridad de datos 221
  - copia de seguridad de enlaces fijos 232
  - copia de seguridad de grupo
    - especificar completa o diferencial 492
    - especificar nombre de espacio de archivos virtual 606
    - especificar nombre de grupo 449
    - visión general 187
    - visualizar objetos activos e inactivos 456
    - visualizar todos los miembros 559

- copia de seguridad de imagen
  - con copia de seguridad incremental 199, 679
  - consideraciones 196
  - copia de seguridad de imagen incremental por fecha 201
  - especificar selectiva o incremental 492
  - excluir archivos 425
  - include.dedup 458
  - incluir archivos; asignar clase de gestión 458
  - instantánea dinámica, estática 194
  - mediante la GUI 201
  - mediante la línea de mandatos 203
  - realizar 194
  - restauración a un instante específico 679
  - revocar acceso 692
  - soporte de tipo de dispositivo de volumen 197
  - suprimir 695
  - utilización con copia de seguridad incremental por fecha 200
  - utilizar con sistema de archivos, incremental 201
- copia de seguridad de imagen basada en LAN
  - copia de seguridad de instantánea 674
- copia de seguridad de imágenes, consideraciones 196
- copia de seguridad de los datos de Tivoli Storage Manager FastBack 224
- copia de seguridad de NAS
  - utilizar DSM\_DIR para hacer referencia a una biblioteca de complementos 62
- copia de seguridad de sistemas de archivos NAS
  - cliente Web
    - GUI 209
  - línea de mandatos 211
- copia de seguridad de volumen 167
- copia de seguridad diferencial de instantánea
  - con HTTPS 178
- copia de seguridad diferencial de instantáneas con conexión HTTPS 566
- copia de seguridad difusa 303
- copia de seguridad incremental
  - algoritmo de reserva de memoria 491
  - directorios, visión general del proceso 170
  - por fecha 182
- copia de seguridad incremental completa tradicional 172
- copia de seguridad incremental diferencial de instantáneas 561
- copia de seguridad selectiva 571
- copias de seguridad basadas en el diario
  - restauración 174
- copias de seguridad completas, creación 222
- copias de seguridad en paralelo 622, 623, 627
- copias de seguridad paralelas 223, 625
- copias de seguridad planificadas (automatizadas)
  - cerrar archivos después de la copia de seguridad 234
  - iniciar 69
  - opciones 292
  - procesar mandatos antes de la copia de seguridad 517
  - procesar mandatos después de la copia de seguridad 514
  - reiniciar aplicaciones después de la copia de seguridad 234
  - visualizar trabajos planificados 289, 291
- copias de seguridad simultáneas 223
- cortafuegos
  - especificar puertos TCP/IP para el cliente web 650
  - establecer comunicaciones a través de 72, 450, 590
  - si el servidor o el cliente inician sesiones a través de 556
  - utilizar cliente web a través de 650
- createnewbase 373

## D

- daemon de aceptación de clientes
  - configurar para gestionar planificador 68
  - gestionar planificador, cliente web o ambos 486
- daemon de registro por diario
  - valores del archivo de configuración de diario 78
- datacenter, opción 375
- datastore, opción 376
- dateformat, opción 376
- datos
  - restauración 259
- defaultserver, opción 383
- definición de variables de entorno
  - API, UNIX y Linux
    - DSMI\_CONFIG 65
    - DSMI\_DIR 65
    - DSMI\_LOG 65
- definir entorno regional de idioma 61
- delete access, mandato 692
- delete archive, mandato 693
- delete backup, mandato 695
- delete group, mandato 699
- deletefiles, opción 383
- descargar actualizaciones de mantenimiento 47
- descripción general de la configuración del cliente web 65
- description, opción 384
- desinstalación
  - API de HP-UX Itanium 2 18
  - API de Linux on Power Systems 27
  - API de Ubuntu Linux on Power Systems (Little Endian) 24
  - cliente AIX 15
  - cliente de Ubuntu Linux on Power Systems (Little Endian) 24
  - cliente IBM Spectrum Protect en Mac OS X 43
  - cliente Linux on System z 41
  - cliente Linux x86\_64 31, 36
  - IBM Spectrum Protect en clientes Oracle Solaris 47
  - Linux on Power Systems (Little Endian), cliente 21
- detail, opción 301, 385
- detener aplicaciones 472
- diagnóstico
  - opciones 335
- diagrama de sintaxis
  - leer xiv
  - opciones obligatorias xiv
  - repetición de valores xiv
- diferencia de instantánea 114, 561
  - con HTTPS 178
- diffsnapshot, opción 387
- directorios
  - asignar clases de gestión para 389
  - especificar en la línea de mandatos 662
  - excluir 126
  - excluir de proceso de copia de seguridad 425
  - proceso durante la copia de seguridad incremental por fecha 175
  - visión general del proceso de copia de seguridad incremental 170
- dirmc, opción 389
- dirsonly, opción 390
- discapacidad 805
- diskbuffsize, opción 392
- diskcachelocation, opción 393
- domain, opción 394
- domain.image, opción 399

- dominio
    - copia de seguridad mediante la GUI 181
    - incluir para copia de seguridad de imagen de NAS 400
    - incluir para copia de seguridad de imágenes 399
    - incluir para copia de seguridad incremental 394
    - incluir para copias de seguridad de máquina virtual completas 401
    - incremental, copia de seguridad 231
    - predeterminado, definición de unidades 181
  - dominio de políticas estándar 299
  - dominio de políticas predeterminado 299
  - dominio predeterminado
    - excluir dominios de la copia de seguridad 182, 394
  - dominios de políticas
    - dominio de políticas estándar 299
    - dominio de políticas predeterminado 299
  - DSM\_CONFIG 62
    - agregar al archivo .cshrc 64
    - hacer referencia a un archivo de opciones del usuario cliente 58, 62
    - utilizar en Solaris 62
  - DSM\_DIR
    - agregar al archivo .cshrc 64
    - establecer para imagen o copia de seguridad o restauración NAS 62
    - hacer referencia a archivos de recursos 62
    - hacer referencia a archivos ejecutables 62
    - hacer referencia al archivo dsm.sys 62
  - DSM\_LOG
    - agregar al archivo .cshrc 64
    - establecer para hacer referencia a dsmerror.log, dsmwebcl.log, dsm Sched.log 62
  - dsmerror.log
    - establecer DSM\_LOG para hacer referencia 62
  - DSMI\_CONFIG, variable de entorno
    - API, UNIX y Linux 65
  - DSMI\_DIR, variable de entorno
    - API, UNIX y Linux 65
  - DSMI\_LOG, variable de entorno
    - API, UNIX y Linux 65
  - dsm Sched.log 545, 549
  - dsm tca, archivo ejecutable
    - establecer DSM\_DIR para hacer referencia a 62
  - dsmwebcl.log 545, 549
- ## E
- Editor de preferencias
    - excluir dominios de la copia de seguridad 181
  - ejecutar una copia de seguridad diferencial de la instantánea con HTTPS 179
  - ejecutar una instantánea de la copia de seguridad diferencial con HTTPS 179
  - eliminación de datos duplicados 86
  - enablearchiveretentionprotection, opción 412
  - encryptkey, opción
    - encryptkey=generate 418
    - encryptkey=prompt
    - encryptkey=save 418
  - enlaces simbólicos
    - archivar y recuperar 275
    - copia de seguridad 229, 464
    - excluir de copia de seguridad 464
    - opciones exclude 464
    - procesar 464
    - restauración 444
    - restricciones Linux y UNIX 744
  - enlaces simbólicos y alias
    - copia de seguridad 428, 464
    - excluir de copia de seguridad 428, 464
    - opciones exclude 428, 464
    - procesar 428, 464
  - Entidades emisoras de certificados
    - certificados raíz 77
    - Entidades emisoras de certificados 77
  - entorno en clúster
    - instalar IBM Spectrum Protect 103
  - entornos regionales de idioma
    - admitidos 61
  - entornos regionales de idioma admitidos 61
  - errorlogretention, opción 420, 423
  - espacio de archivos
    - determinación de fsID 385
    - excluir 126
    - NAS u objetos de cliente 364
    - realizar una copia de seguridad de imagen 674
    - suprimir 186, 267, 698
  - espacio de disco, AIX 5
  - espacio de disco, HP-UX Itanium 2 6
  - espacio de disco, Linux on Power Systems 7
  - espacio de disco, Linux System z 9
  - espacio de disco, Linux x86\_64 8
  - espacio de disco, Mac OS X 9
  - espacio de disco, Solaris 10
  - espacio de disco de AIX 5
  - espacio de disco de HP-UX Itanium 2 6
  - espacio de disco de Linux System z 9
  - espacio de disco de Linux x86\_64 8
  - espacio de disco de Mac OS X 9
  - espacio de disco de Solaris 10
  - espacios de archivos 167
  - especificación de archivo
    - máximo permitido en mandatos 662
  - especificar si actualizar fecha de último acceso 519
  - establecer
    - privilegios de usuario 148
  - establecer netappsvm 116
  - estado del sistema
    - visualizar objetos activos e inactivos 456
  - etiqueta de volumen
    - nombres duplicados 167
  - eventos planificados, visualizar 738
  - exclude
    - EXCLUDE.VMDISK 430
  - exclude.image, opción 126
  - EXCLUDE.VMDISK 430
  - excluir archivos
    - archivos del sistema 129
    - caracteres comodín 131
    - utilización de caracteres comodín 132
  - excluir archivos de la eliminación de duplicados 93
  - excluir archivos de los servicios de copia de seguridad 161
  - expire, mandato 701
- ## F
- fecha de último acceso
    - especificar si actualizar durante copia de seguridad o archivado 170, 519
  - filename, opción 442
  - filesonly, opción 443
  - followsymbolic, opción 444
  - formato
    - resumen de opciones 332

- formato de fecha
  - especificación 376
- formato de hora
  - especificación 592
- formato e idioma
  - resumen de opciones 332
- fromdate, opción 446
- fromowner, opción 448
- fromtime, opción 449
- función de estimación 181

## G

- groupname, opción 449
- grupo de copia archivada 300
- grupo de copias de seguridad 156, 300
  - atributos 301
- grupos de copia 300
  - archivado 300
  - copia de seguridad 300
- GUI
  - fin de una sesión 152
  - iniciar una sesión 142
  - realización de restauración a un instante específico 251
  - sustitución de la clase de gestión durante la copia
    - archivada 307
- GUI Java
  - restricciones de configuración 144

## H

- habilitar el cifrado para usuarios autorizados 53
- help
  - foro en línea 152
  - recursos de Internet 152
  - servicio de soporte técnico 152
  - visualizar en línea 152
- help, mandato 703
- host, opción 450
- httpport, opción 450

## I

- IBM Knowledge Center xiv
- IBM Spectrum Protect
  - actualización desde versiones anteriores del producto 1
  - componentes del cliente
    - cliente AIX 5
    - cliente Linux on System z 8
    - cliente Linux x86\_64 8
    - cliente Mac OS X 9
    - cliente Oracle Solaris 10
    - Linux en el cliente Power Systems 7
  - contraseña 144
  - foro en línea 152
  - métodos de comunicación
    - API de HP-UX Itanium 2 6
    - cliente AIX 5
    - cliente Linux on System z 9
    - cliente Linux x86\_64 8
    - cliente Mac OS X 10
    - cliente Oracle Solaris 10
    - Linux en el cliente Power Systems 7
  - requisitos de instalación 9
- IBM Spectrum Protect en clientes Oracle Solaris
  - desinstalación 47

- IBM Spectrum Protect en clientes Oracle Solaris *(continuación)*
  - pasos para la instalación 44
- ifnewer, opción 453
- imagegapsize, opción 454
- imagen
  - restaurar 237
  - utilizar chkdsk para reparar 237
  - utilizar fsck para reparar 237, 758
  - utilizar la herramienta chkdsk para reparar 758
- imagen de copia de seguridad, soporte de tipo de dispositivo
  - de volumen 197
- imagen en archivo
  - restauración 248
- imagnetofile, opción 455
- imponer copia de seguridad incremental 345
- inactive, opción 456
- inexcl, opción 456
- include, opción
  - caracteres comodín 131, 132
  - clase de gestión 306
  - proceso 136
- include.vmtsmvss option 472
- incluir plantillas de máquina virtual en copia de
  - seguridad 620
- inclusión/exclusión, proceso
  - opciones 126
  - visión general 126
- incrbydate, opción 474
- incremental, asociación de una instantánea local con un
  - espacio de archivos del servidor 194
- incremental, copia de seguridad
  - archivos nuevos y con cambios con fecha de modificación
    - posterior a la de la última copia de seguridad 474
  - archivos nuevos y modificados 170
  - asociación de una instantánea local al espacio de archivos
    - del servidor 571
  - carpetas, visión general 170
  - con copia de seguridad de imágenes 199, 679
  - de carpetas
    - visión general del proceso 170
  - de directorios
    - visión general del proceso 170
  - description 170
  - dominio de cliente 394
  - enlaces simbólicos 229
  - GPFS, entorno de clúster de varios nodos 162, 394
  - línea de mandatos 182
  - línea de mandatos del cliente 182
  - omitir comprobación de actualización de ACL 560
  - optimizar la memoria durante 161
  - procesar una lista de archivos 439
  - realizar una copia de seguridad de archivos nuevos y con
    - cambios con fecha de modificación posterior a la de la
      - última copia de seguridad 474
  - utilizar la GUI Java del cliente 181
  - visión general 170
- incremental, mandato 704
  - copia de seguridad con registro por diario 709
- incremental, opción 475
- incremental completa
  - comparación con incremental por fecha 176
  - comparar con incremental por fecha y con diario 176
  - cuándo se debe utilizar 176
  - definición 170
  - description 170
- incremental parcial
  - definición 170



- incremental parcial (*continuación*)
  - incremental por fecha
    - ejecutar 182
- incremental por fecha
  - comparación con incremental 176
  - comparar con incremental y con diario 176
  - cuándo se debe utilizar 176
  - de directorios
    - visión general del proceso 175
  - description 175
  - línea de mandatos 182
  - línea de mandatos del cliente 182
  - visión general 170
- incremental por fecha, copia de seguridad 175
  - utilizar con copia de seguridad de imagen 200
  - utilizar la GUI Java del cliente 181
- información de la sesión, visualizar 738
- información del sistema
  - recopilación 372, 442
- iniciar
  - automático 148
  - visión general 1
- iniciar el planificador cliente al inicio 287
- iniciar una sesión
  - modalidad interactiva 145
  - modalidad por lotes 144
- inscripción abierta
  - permisos 124
  - utilizar 124
- inscripción cerrada
  - permisos 124
  - utilizar 124
- instalación
  - API de HP-UX Itanium 2 16
  - API de Linux on Power Systems (Big Endian) 25
  - API de Ubuntu Linux on Power Systems (Little Endian) 22
  - cliente AIX 12
  - cliente de archivado y copia de seguridad 12
  - cliente de Ubuntu Linux on Power Systems (Little Endian) 22
  - cliente Linux on System z 37
  - cliente Linux x86\_64 28
  - cliente Mac OS X 42
  - cliente Solaris 44
  - cliente Ubuntu x86\_64 33
  - Linux on Power Systems (Little Endian), cliente 19
  - visión general 1
- instalación del servicio de gestión de cliente 48
- instalar IBM Spectrum Protect
  - entorno en clúster 103
- instantánea local
  - asociación de una instantánea local con un espacio de archivos del servidor 194
- instantáneas
  - configurar 114
- interfaz de programas de aplicación (API)
  - establecer 65
- interfaz gráfica de usuario (GUI)
  - fin de una sesión 152
  - habilitación para la restauración del conjunto de copias local 484
  - habilitar el conjunto de copias de seguridad locales 240
  - iniciar una sesión 142
  - modificar contraseña 148
  - realizar una copia de seguridad de imágenes 201

- interfaz gráfica de usuario (GUI) (*continuación*)
  - suprimir archivos o imágenes individuales del espacio de archivos de servidor 695
  - utilizar para hacer copias de seguridad de objetos 181
  - visualizar ayuda en línea 152
  - visualizar estado del proceso 224
  - visualizar versiones de copia de seguridad activas e inactivas 150, 257

## J

- juegos de políticas
  - juego de políticas activo 299

## K

- Knowledge Center xiv

## L

- lanfreecommmethod, opción 478
- lanfreetcpserveraddress, opción 482
- latest, opción 483
- línea de mandatos
  - archivar copias 274
  - asignación de descripciones para archivado 272
  - códigos de retorno para operaciones 297
  - copia de seguridad de sistemas de archivos NAS 211
  - entrar especificación de archivo 662
  - entrar mandatos 660
  - especificar archivo de opciones durante la sesión 506
  - fin de una sesión 152
  - iniciar una sesión 144
  - realización de grandes operaciones de restauración 260
  - realización de restauración a un instante específico 251
  - realizar una copia de seguridad de imágenes 203
  - recuperar archivos archivados 277
  - reglas generales para especificar opciones con mandatos 336
  - restricciones para sistemas de archivos NAS 208
  - sustitución de la clase de gestión durante la copia archivada 307
  - utilización de caracteres comodín 663
  - visión general de parámetros 661
  - visualización de los valores actuales para las opciones del cliente 736
  - visualizar
    - estado del proceso 224
- Linux, gestor de volúmenes lógicos
  - copia de seguridad de instantánea de volúmenes 194
- Linux en el cliente Power Systems
  - componentes del cliente 7
  - métodos de comunicación 7
- Linux on Power Systems, componentes
  - instalables 7
- Linux on Power Systems, espacio de disco 7
- Linux on Power Systems (Little Endian), cliente
  - desinstalación 21
  - instalación 19
- Linux on Power Systems, requisitos de hardware 7
- Linux on Power Systems, requisitos de sistema 7
- Linux on Power Systems, requisitos de software 7
- lista de inclusión/exclusión 161
  - consultar orden de proceso 733
  - crear 125
  - previsualización 135

lista de inclusión/exclusión (*continuación*)

restricción de tamaño 136

listas de control de accesos

permisos, copia de seguridad 180

permisos ampliados, copia de seguridad 180

loop, mandato 712

LVM

detener una aplicación antes de iniciar LVM 523

iniciar una aplicación después de iniciar LVM 516

## M

macro, mandato 713

mandato backup fastback 669

mandato mejorado enhanced query 738

mandato query VM 741

mandato restore vm 764

mandato set vmtags 790

mandatos

archivado 664

archive fastback 667

backup fastback 669

backup group 672

backup image 674

backup nas 680

backup vm 683

cancel process 691

cancel restore 692

consideraciones acerca de la restauración de conjuntos de

copias de seguridad 243, 752

delete access 692

delete archive 693

delete backup 695

delete filespace 698

delete group 699

entrar 660

entrar en la línea de mandatos 660

entrar especificación de archivo 662

especificaciones de archivo máximas permitidas 662

establecer netappsvm 783

expire 701

help 703

incremental 704

loop 712

macro 713

modalidad interactiva (loop) 659

modalidad por lotes 658

monitor process 714

planificados, activación o desactivación 292

preview archive 715

previsualizar copia de seguridad 716

query access 717

query archive 718

query backup 720

query backupset 723, 725

query filespace 727

query group 729

query image 731

query inclexcl 733

query mgmtclass 734

query node 735

query options 736

query restore 737

query schedule 738

query session 738

query systeminfo 739

query VM 741

mandatos (*continuación*)

reglas generales para especificar opciones 336

restart restore 743

restaurar 744

restore backupset 749, 754

restore group 756

restore image 758

restore NAS 762

restore vm 764

retrieve 770

schedule 773

selectiva, copia de seguridad 775

set access 778

set event 781

set password 784

set vmtags 790

utilización de caracteres comodín 663

utilizar 655

utilizar en ejecutables 297

utilizar en scripts de shell 297

utilizar opciones 336

visión general de parámetros 661

mandatos planificados

activación/desactivación 292

mantenimiento 355

actualización automática 2

máquina virtual

opciones de inclusión 466

opciones exclude 430

maxcmdretries, opción 488

mbobjrefreshtresh 489

mbpctrefreshtresh 490

medios portables

restauración de conjuntos de copias de seguridad 240

memoria

optimizar con restricciones 161

memoryefficientbackup, opción 491

mensajes

dejar de visualizar 526

visualizar en pantalla 604

método de comunicación de memoria compartida

opciones 315

métodos de comunicación

Memoria compartida

API de HP-UX Itanium 2 6

cliente AIX 5

cliente Linux on System z 9

cliente Linux x86\_64 8

cliente Oracle Solaris 10

resumen 314

software instalable 6, 7, 8, 9, 10

TCP/IP

API de HP-UX Itanium 2 6

cliente AIX 5

cliente Linux on System z 9

cliente Linux x86\_64 8

cliente Mac OS X 10

cliente Oracle Solaris 10

Linux en el cliente Power Systems 7

migración

archivos de idioma del cliente web 1

cliente Web 1

migración de espacios de archivos a Unicode 169

migración de los clientes de archivado y copia de seguridad 1

migración tras error

client 94

- migración tras error (*continuación*)
  - configuración del cliente 98
  - configuración y uso 94
  - determinar el estado de réplica 100
  - inhabilitar 101
  - otros componentes 97
  - requisitos 95
  - restaurar 247
  - restricciones 96
  - retrieve 247
- migración tras error automática del cliente
  - configuración y uso 94
  - configurar 98
  - determinar el estado de réplica 100
  - forzar una migración tras error 101
  - impedir 101
  - otros componentes 97
  - prueba de la conexión 101
  - recuperación de datos 247
  - requisitos 95
  - restauración de datos 247
  - restricciones 96
  - visión general 94
- modalidad Absoluta 304
- modalidad-c 116
- modalidad interactiva 659
- modalidad Modificados 302
- modalidad por lotes 658
  - iniciar una sesión 144
- modalidades
  - interactiva (loop) 659
  - por lotes 658
- mode, opción 492
- monitor, opción 496
- monitor process, mandato 714
- montajes por hardware, NFS 233
- montajes por software, NFS 233
- movimiento de datos sin LAN
  - activación de comunicaciones 478
  - puerto de memoria compartida para 480

## N

- NAS
  - asignar clase de gestión a sistemas de archivos 458
  - copia de seguridad de sistemas de archivos 208
  - especificar copia de seguridad completa o diferencial 492
  - query node, mandato 735
  - restaurar sistemas de archivos 254, 762
  - restore NAS, mandato 762
  - supresión de espacios de archivos 186, 267, 698
- navegador activado para Swing
  - necesario para ejecutar el cliente web 147
- netapp, servidor de archivos 116
- Network Data Management Protocol (NDMP) 11
- NFS
  - copia de seguridad de sistemas de archivos 213
  - montajes por hardware 233
  - montajes por software 233
  - puntos de montaje virtual 229
- nfstimeout, opción 233, 500
- NLSPATH, variable de entorno
  - para visualizar el menú del navegador de ayuda en el entorno regional de idioma 61
  - visualizar el menú del navegador de ayuda en su entorno regional 61
- nodename, opción 501

- nodo
  - especificar tipo de consulta 600
- nombre de nodo 56
- nombre de volumen 167
- noprompt, opción 503
- novedades del cliente de copia de seguridad y archivado V8.1.0 xvii
- numberformat
  - especificación 504
- numberformat, opción 504

## O

- ONTAP de datos en clúster 116
- opción absolute 345
- opción auditlogging 351
- opción auditlogname 353
- opción autodeploy 355
- opción autofsrrename 356
- opción backmc 359
- opción backupsetname 360
- opción basesnapshotname 361
- opción cadlistenonport 362
- opción class 364
- opción createnewbase 373
- opción dedupcachepath 380
- opción dedupcachesize 381
- opción diffsnapshotname 388
- opción disablelqr 391
- opción domain.nas 400
- opción domain.vmfull 401
- opción dontload 408
- opción dynamicimage 410
- opción efsdecrypt 411
- opción eliminación de duplicados 381
- opción enablededupcache 413
- opción enableinstrumentation 414
- opción enablelanfree 416
- opción encryptiontype 161, 417
- opción errorlogmax 420
- opción errorlogname 422
- opción fbbranch 432
- opción fbclient 432
- opción fbpolycname 434
- opción fbreposlocation 435
- opción fbserver 436
- opción fbvolumename 438
- opción filelist 439
- opción forcefailover 445
- opción fromnode 447
- opción ieobjtype 452
- opción include.vm 466
- opción include.vmsnapshotattempts 469
- opción instrlogmax 476
- opción instrlogname 477
- opción lanfreshmport 480
- opción lanfreessl 481
- opción lanfreetcpport 481
- opción localbackupset 484
- opción makesparsefile 485
- opción managedservices 486
- opción myreplicationserver 497
- opción nasnodename 498
- opción nojournal 502
- opción nrtablepath 503
- opción preservelastaccessdate 519
- opción quotesareliteral 527

- opción replserverguid 531
- opción replservername 532
- opción replsslport 534
- opción repltcpport 536
- opción repltcpserveraddress 538
- opción schedcmddisabled 544, 545
- opción schedcmduser (sólo servidor definido) 292
- opción schedlogmax 545
- opción schedrestretretrdisabled 552
- opción sessioninitiation 556
- opción skipacl 559
- opción skipaclupdatecheck 560
- opción snapdiffhttps 566
- opción snapshotproviderfs 569
- opción snapshotproviderimage 570
- opción srprepостscheddisabled 574
- opción srprepостsnapdisabled 575
- opción ssl 576
- Opción Sslfipsmode 577
- opción sslrequired 578
- opción stagingdirectory 581
- opción subdir 581
- opción updatectime 601
- opción useexistingbase 601
- opción usereplicationfailover 602
- opción v2archive 603
- opción vmbackuptype 631
- opción vmchost 612
- opción vmcpw 613
- opción vmctlmc
  - opciones
    - vmctlmc 614
- opción vmcuser 615
- opción vmdefaultdvportgroup 618
- opción vmdefaultnetwork 620
- opción vmenabletemplatebackups 620
- opción vmlimitperdatastore 622
- opción vmlimitperhost 623
- opción vmmaxbackupsessions 625
- opción vmmaxparallel 627
- opción vmmaxrestoresessions 629
- opción vmpreferdagpassive 634
- opción vmskipctlcompression 637
- opción vmtimeout 649
- opción wildcardsareliteral 651
- opciones 580
  - absolute 345
  - afmskipuncachedfiles 346
  - archivado, resumen 316
  - archmc 347
  - archsymbinkasfile 348
  - asnodename 349
  - auditlogging 351
  - auditlogname 353
  - autodeploy 355
  - autofsrename 356
  - automount 358
  - backmc 359
  - backupsetname 360
  - basesnapshotname 361
  - cadlistenonport 362
  - changingretries 363
  - class 364
  - cliente web, resumen 335
  - collocatebyfilespec 365
  - commmethod 366
  - commrestartduration 368
  - opciones (continuación)
    - commrestartinterval 368
    - compressalways 369
    - compression 370
    - comunicación, resumen 314
    - console 372
    - copia de seguridad
      - excluir estado del sistema 425
    - copia de seguridad, resumen 316
    - createnewbase 373
    - datacenter 375
    - datastore 376
    - dateformat 376
    - dedupcachepath 380
    - dedupcachesize 381
    - deduplication 381
    - defaultserver 383
    - deletefiles 383
    - description 384
    - detail 385
    - diagnóstico 335
    - diffsnapshot 387
    - diffsnapshotname 388
    - dirmc 389
    - dironly 390
    - disablenqr 391
    - diskbuffsize 392
    - diskcachelocation 393
    - domain.image 399
    - domain.nas 400
    - domain.vmfull 401
    - dominio 394
    - dontload 408
    - dynamicimage 410
    - efsdecrypt 411
    - enablearchiveretentionprotection 412
    - enablededupcache 413
    - enableinstrumentation 414
    - enablelanfree 416
    - encryptiontype 161, 417
    - encryptkey
      - encryptkey=generate 418
      - encryptkey=prompt 418
      - encryptkey=save 418
    - errorlogmax 420
    - errorlogname 422
    - errorlogretention 423
    - especificación en mandatos 336
    - estado del sistema
      - excluir del proceso de copia de seguridad 425
    - exclude
      - caracteres comodín 131, 132
      - exclude.archive 126, 425
      - exclude.attribute.symink 126, 425
      - exclude.backup 126, 425
      - exclude.compression 126, 425
      - exclude.dir 126, 425
      - exclude.encrypt 425
      - exclude.file 126, 425
      - exclude.file.backup 126, 425
      - exclude.fs 126, 425
      - exclude.fs.nas 425
      - exclude.image 126, 425
    - exclude.dedup 425
    - EXCLUDE.VMDISK 430
    - fbbranch 432
    - fbclient 432

opciones (*continuación*)

- fbpolicyname 434
- fbreposlocation 435
- fbserver 436
- fbvolumename 438
- filelist 439
- filesonly 443
- followsymbolic 444
- forcefailover 445
- formato, resumen 332
- formato e idioma, resumen 332
- fromdate 446
- fromnode 447
- fromowner 448
- fromtime 449
- groupname 449
- host 450
- httpport 450
- ieobjtype 452
- ifnewer 453
- imagegapsize 454
- imagetofile 455
- inactive 456
- inlexcl 456
- include
  - caracteres comodín 131, 132
- include.archive 458
- include.attribute.symmlink 458
- include.backup 458
- include.compression 458
- include.encrypt 458
- include.file 458
- include.fs.nas 458
- include.image 458
- include.vm 466
- include.vmsnapshotattempts 469
- include.vmtsmvss 472
- incrbydate 474
- incremental 475
- instrlogmax 476
- instrlogname 477
- lanfreecommmethod 478
- lanfreeshmport 315, 480
- lanfreessl 481
- lanfreetcpport 481
- lanfreetcpserveraddress 482
- latest 483
- localbackupset 484
- makesparsefile 485
- managedservices 486
- maxcmdretries 488
- mbobjrefreshtresh 489
- mbpctrefreshtresh 490
- memoryefficientbackup 491
- mode 492
- monitor 496
- myreplicationserver 497
- nasnodename 498
- nfstimeout 500
- nodename 501
- nojournall 502
- nombreadchivo 442
- noprompt 503
- nrtablepath 503
- numberformat 504
- opciones de autorización 333
- opciones exclude de máquina virtual 430

opciones (*continuación*)

- opciones include de máquina virtual 466
- optfile 506
- orden de proceso (precedencia) 336
- password 507
- passwordaccess 509
- passworddir 511
- pick 512
- pitdate 513
- pittime 513
- planificación central, resumen 330
- postnschedulecmd 514
- postschedulecmd 514
- postsnapshotcmd 516
- prenschedulecmd 517
- preschedulecmd 517
- preservelastaccessdate 519
- preservepath 520
- presnapshotcmd 523
- proceso de mandatos, resumen 332
- proceso de transacciones, resumen 334
- querschedperiod 524
- quersummary 525
- quiet 526
- quotesareliteral 527
- reglas generales para especificar con mandatos 336
- removeoperandlimit 528
- replace 529
- replserverguid 531
- replservername 532
- replsslport 534
- repltcpport 536
- repltcpserveraddress 538
- resourceutilization 539
- restauración y recuperación, resumen 327
- retryperiod 542
- revokeremoteaccess 543
- schedcmddisabled 544, 545
- schedcmduser (sólo servidor definido) 292
- schedlogmax 545
- schedlogname 547
- schedlogretention 549
- schedmode 550
- schedrestretredisabled 552
- scrolllines 552
- scrollprompt 553
- servername 555
- sessioninitiation 556
- shmport 558
- showmembers 559
- skipacl 559
- skipaclupdatecheck 560
- snapdiff 114, 561
- snapdiffhttps 566
- snapshotcachesize 568
- snapshotproviderfs 569
- snapshotproviderimage 570
- snapshotroot 571
- srvoptsetencryptiondisabled 573
- srprepstscheddisabled 574
- srprepstsnapdisabled 575
- ssl 576
- sslrequired 578
- stagingdirectory 581
- subdir 581
- tapeprompt 584
- tcpadminport 585

## opciones (continuación)

- tcpbuffsize 586
- tcpcadaddress 587
- tcpclientaddress 587
- tcpclientport 588
- tcpnodelay 589
- tcpport 590
- tcpserveraddress 590
- tcpwindowsize 591
- timeformat 592
- toc 596
- todate 597
- totime 598
- txnbytelimit 599
- type 600
- updatectime 601
- useexistingbase 601
- usereplicationfailover 602
- v2archive 603
- verbose 604
- verifyimage 605
- virtualfsname 606
- virtualmountpoint 606
- virtualnodename 608
- vmbackdir 609
- vmbackupmailboxhistory 610
- vmbackuptype 611
- vmchost 612
- vmcpw 613
- vmcuser 615
- vmdatastorethreshold 616
- vmdefaultdvportgroup 618
- vmdefaultdvswitch 619
- vmdefaultnetwork 620
- vmenabletemplatebackups 620
- vmlimitperdatastore 622
- vmlimitperhost 623
- vmmaxbackupsessions 625
- vmmaxparallel 627
- vmmaxrestoresessions 629
- vmmaxvirtualdisks 629
- vmmc 631
- vmnoprmdisks 632
- vmnovrmdisks 633
- vmpreferdagpassive 634
- vmprocessvmwithprdm 636
- vmprocesswithindependent 634
- mskipctlcompression 637
- mskipmaxvirtualdisks 638
- mskipmaxvmdks 639
- vmtagdatamover 642
- vmtagdefaultdatamover 639
- vmtimeout 649
- vmverifyifaction 644
- vmverifyiflatest 646
- vmvstortransport 648
- webports 650
- wildcardsareliteral 651

opciones de mandatos de cliente

- visión general 660

opciones de proceso

- autorización 333
- cliente Web 335
- comunicación 314
- copia de seguridad/archivado 316
- diagnóstico 335
- especificación en mandatos 336

## opciones de proceso (continuación)

- formato 332
- formato e idioma 332
- planificación central 330
- proceso de errores 333
- proceso de transacciones 334
- restaurar y recuperar 327
- utilizar 313
- visión general 313

opciones de servidor

- Sslfipsmode 577

opciones de usuario del cliente

- personalizar 60

opciones del sistema cliente

- exclude
  - exclude.archive 126
  - exclude.attribute.symmlink 126
  - exclude.backup 126
  - exclude.compression 126
  - exclude.dir 126
  - exclude.file 126
  - exclude.file.backup 126
  - exclude.fs 126

opciones exclude 425

- caracteres comodín 131, 132
- exclude.archive 126
- exclude.attribute.symmlink 126
- exclude.backup 126
- exclude.compression 126
- exclude.dir 126
- exclude.file 126
- exclude.file.backup 126
- exclude.fs 126
- exclude.image 126
- previsualización 135
- proceso 136

optfile, opción 506

Oracle Solaris, componentes

- instalables 10

## P

### parámetro de modalidad de copia

- absoluta 304
- Modificados 304

parámetro mode 302

parámetros

- yes y no, alternativas 345

### parámetros de mandatos

- visión general 661

pasos para la instalación

- cliente Mac OS X 42
- IBM Spectrum Protect en clientes Oracle Solaris 44

### password

- cambiar 784
- especificar si debe generarse automáticamente establecerse en el indicador de usuario 509
- especificar ubicación del directorio para almacenar archivo de contraseñas cifrado 511
- establecer 507

password, opción 507

passwordaccess, opción 509

passworddir, opción 511

período de gracia de retención

- archivado 300, 309
- copia de seguridad 300, 309

- permisos
  - acceso, guardar estándar y ampliado 275
- permisos ampliados
  - archivado 275
- pick, opción 512
- pitdate 513
- pittime, opción 513
- planificación central
  - resumen de opciones 330
- planificación de copia de seguridad 155
- planificador
  - anotación de eventos 291
  - configurar 67
  - gestionados por el daemon de aceptación de clientes 486
  - iniciar 69
  - modalidad de sondeo o modalidad de petición 550
  - número de horas entre contactos con el servidor para trabajo planificado 524
  - número de minutos entre intentos de procesar mandatos planificados 542
  - opciones 292
  - resolver retención de memoria después de las copias de seguridad planificadas 486
  - si el servidor o el cliente inician sesiones a través del cortafuegos 556
  - si ha de desactivarse la ejecución de operaciones de restauración o de recuperación 552
  - visualizar trabajos planificados 289, 291
- planificador cliente
  - ejecutar al inicio 287
  - iniciar 69, 773
  - iniciar automáticamente 148
  - opciones 292
  - visualizar trabajos planificados 289, 291
- planificar
  - clúster IBM PowerHA SystemMirror 191
  - copia de seguridad del proxy de nodo cliente 188
  - proxy del nodo de cliente 190
  - sistema de archivos GPFS 193
- plug-in PIHDW 408
- políticas, gestión de almacenamiento 299
- políticas de gestión de almacenamiento 299
  - asignar clases de gestión a archivos 229
  - clase de gestión predeterminada 299
  - clases de gestión 300
  - dominios de políticas
    - estándar 299
    - predeterminado 299
  - grupos de copia 300
  - juegos de políticas
    - juego de políticas activo 299
  - lista de inclusión/exclusión 300
  - visualizar en GUI del cliente web o del cliente de copia de seguridad/archivado 229
- postnschedulecmd, opción 514
- postsnapshotcmd, opción 516
- precauciones respecto a la asignación de nombres de volumen
  - punto de montaje UNIX 167
  - sistemas de arranque dual 168
- prenschedulecmd, opción 517
- preschedulecmd, opción 517
- preservepath, opción 520
- Presnapshotcmd, opción 523
- preview archive, mandato 715
- preview backup, mandato 716
- previsualización
  - lista de inclusión/exclusión 135
- privilegios de usuario
  - establecer 148
- procesar enlaces simbólicos 464
- procesar enlaces simbólicos y alias 428
- procesar seudónimos 464
- proceso ascendente
  - archivo de opciones de inclusión/exclusión 136
  - lista de inclusión/exclusión 136
- proceso de cifrado
  - excluir archivos 425
  - incluir archivos 458
  - métodos de cifrado disponibles 161
  - query systeminfo, mandato 739
- proceso de compresión
  - excluir de copia de seguridad 464
  - incluir archivos 458
  - opciones exclude 464
- proceso de compresión y cifrado
  - copia de seguridad 464
  - excluir de copia de seguridad 464
  - opciones exclude 464
- proceso de errores, resumen de opciones 333
- proceso de mandatos, resumen de opciones 332
- proceso de transacciones
  - resumen de opciones 334
  - txnbytelimit, opción 599
- protección de aplicaciones autocontenida 472
- protección de la retención de política basada en eventos
  - archivado 310
  - copia de seguridad 310
- protección de los subvolúmenes de Btrfs 207
- protección del sistema de archivos Btrfs 205
- proxy del nodo de cliente
  - copia de seguridad 190
  - planificar 190
  - soporte 272
  - visión general del archivado 272
- publicaciones xiv
- punto de montaje virtual, establecer 181

## Q

- query access, mandato 717
- query archive, mandato 718
- query backup, mandato 720
- query backupset, mandato 723, 725
- query filespace, mandato 727
- query group, mandato 729
- query image, mandato 731
- query inclexcl, mandato 733
- query mgmtclass, mandato 301, 734
- query node, mandato 735
- query options, mandato 736
- query restore, mandato 737
- query schedule
  - ampliada 289
- query schedule, mandato 738
- query schedule, mandato mejorado 738
- query session, mandato 738
- query systeminfo, mandato 739
- proceso de cifrado 739
- querschedperiod, opción 524
- querysummary, opción 525
- quiet, opción 526

## R

- Realización de copias de seguridad de máquina virtual
  - VMware 222
  - tipos 219
- realizar copia de seguridad incremental completa
  - tradicional 709
- recopilación de información de diagnóstico 48
- recuperación de disco 266
- recuperación tras un siniestro 266
- recuperar
  - archivos archivados mediante mandatos 277
  - archivos en otra estación de trabajo 266
  - archivos que pertenecen a otro nodo 265
  - autorización a otro usuario 264
  - btrfs 205
  - clasificar lista de archivos 150
  - copias archivadas 276
  - durante la migración tras error 247
  - ejecutar 277
  - enlaces simbólicos 275
  - inicio de una sesión del cliente web 147
  - mejorar la velocidad mediante memoria compartida 315
  - resumen de opciones 327
  - tareas primarias 269
  - vínculos fijos 276
- red de área de almacenamiento
  - para el traspaso de datos fuera de la LAN 158
  - utilizar para el traspaso de datos sin LAN 416
  - utilizar para restaurar conjuntos de copias de seguridad 416, 753
- registrar
  - cliente con servidor 123
  - utilizar la inscripción abierta 124
  - utilizar la inscripción cerrada 124
- registro de errores 62
  - eliminar 423
  - especificar vía de acceso y nombre de archivo 422
- registro de instrumentación
  - controlar el tamaño 476
  - especificar ruta y nombre de archivo para almacenar información de rendimiento 477
  - recopilación de información de rendimiento 414
- registros
  - dsmsched.log 549
  - dsmsched.pru 549
  - dsmwebcl.log 549
  - dsmwebcl.pru 549
  - truncar registros de aplicaciones 472
- removeoperandlimit, opción 528
- rendimiento
  - mejorar la velocidad de operaciones de copia de seguridad, restauración, archivo, recuperación 315
  - opciones de transacciones 334
  - proceso de transacciones 599
- replace, opción 529
- requisitos de espacio de disco
  - client 4
- requisitos de hardware, AIX 5
- requisitos de hardware, HP-UX Itanium 2 6
- requisitos de hardware, Linux on Power Systems 7
- requisitos de hardware, Linux System z 9
- requisitos de hardware, Linux x86\_64 8
- requisitos de hardware, Mac OS X 9
- requisitos de hardware, Solaris 10
- requisitos de hardware de AIX 5
- requisitos de hardware de HP-UX Itanium 2 6
- requisitos de hardware de Linux System z 9
- requisitos de hardware de Linux x86\_64 8
- requisitos de hardware de Mac OS X 9
- requisitos de hardware de Solaris 10
- requisitos de instalación
  - API de HP-UX Itanium 2 6
  - client 4
  - cliente AIX 5
  - cliente Linux para zSeries 8
  - cliente Linux x86\_64 7
  - cliente Solaris 10
  - Linux on Power Systems 7
- Requisitos de instalación de Tivoli Storage Manager
  - FastBack 11
- requisitos de sistema, AIX 5
- requisitos de sistema, HP-UX Itanium 2 6
- requisitos de sistema, Linux on Power Systems 7
- requisitos de sistema, Linux System z 9
- requisitos de sistema, Linux x86\_64 8
- requisitos de sistema, Mac OS X 9
- requisitos de sistema, Solaris 10
- requisitos de sistema de AIX 5
- requisitos de sistema de HP-UX Itanium 2 6
- requisitos de sistema de Linux System z 9
- requisitos de sistema de Linux x86\_64 8
- requisitos de sistema de Mac OS X 9
- requisitos de sistema de Solaris 10
- requisitos de sistema operativo
  - clientes 4
- requisitos de software, AIX 5
- requisitos de software, HP-UX Itanium 2 6
- requisitos de software, Linux on Power Systems 7
- requisitos de software, Linux System z 9
- requisitos de software, Linux x86/x86\_64 8
- requisitos de software, Mac OS X 9
- requisitos de software, Solaris 10
- requisitos de software de AIX 5
- requisitos de software de HP-UX Itanium 2 6
- requisitos de software de Linux System z 9
- requisitos de software de Linux x86\_64 8
- requisitos de software de Mac OS X 9
- requisitos de software de Solaris 10
- requisitos previos de entorno
  - API de HP-UX Itanium 2 6
  - cliente AIX 5
  - cliente Linux para zSeries 8
  - cliente Linux x86\_64 7
  - cliente Solaris 10
  - Linux on Power Systems 7
- resourceutilization, opción 539
- restart restore, mandato 743
  - restaurar restauración interrumpida 264
- restauración a un instante específico
  - copia de seguridad de imagen 679
- restauración clásica (estándar) 261
- restauración de los datos de Tivoli Storage Manager
  - FastBack 224
- restauración de un instante específico 251
  - mediante la GUI 251
  - mediante la línea de mandatos 251
- restauración estándar (clásica) 261
- restauración reinicializable 261
- restauración sin consulta 261
- restaurar 758
  - activar SELinux 268
  - archivos en otra estación de trabajo 266
  - archivos para otro nodo 447
  - archivos para otro usuario 448



## restaurar (continuación)

- archivos que pertenecen a otro nodo 265
- archivos y directorios 258
- autorización a otro usuario 264
- btrfs 205
- clásica (también conocida como estándar) 261
- clasificar lista de archivos 150
- conjunto de copias de seguridad
  - dispositivos de cintas admitidos 749, 754
- conjunto de copias de seguridad locales mediante la GUI 240
- conjuntos de copias de seguridad
  - visión general 240
- copias de seguridad, establecer instante específico 513
- crear lista de versiones de copia de seguridad 512
- datos utilizando la línea de mandatos 259
- de espacios de archivos que no están activados para Unicode 749
- desde medios portables
  - visión general 240
- disco 266
- durante la migración tras error 247
- en estación de trabajo distinta 608
- en función de fecha y la hora de la copia de seguridad 446, 449
- enlaces simbólicos
  - restricciones Linux y UNIX 744
- estándar (también conocida como clásica) 261
- grupo
  - mandato 756
- GUI, visualizar versiones activas e inactivas 150
- imagen 237
  - activar detección de sectores defectuosos en el volumen de destino 605
  - consideraciones 758
  - en un archivo 455
  - utilizar DSM\_DIR para hacer referencia a una biblioteca de complementos 62
  - utilizar la herramienta chkdsk para reparar 237
  - utilizar la herramienta fsck para reparar 237
- imagen, eliminar indicador de confirmación 503
- imagen en archivo 248
- inicio de una sesión del cliente web 147
- lista de archivos 439
- mejorar la velocidad mediante memoria compartida 315
- NAS
  - utilizar DSM\_DIR para hacer referencia a una biblioteca de complementos 62
- procesar sólo directorios (no archivos) 390
- proceso de la ventana de estado 258
- realización de grandes operaciones 260
- reinicializable 261
- resumen de opciones 327
- si debe preguntarse antes de sobrescribir archivos existentes 529
- sin consulta 261
- Sistemas de archivos de cifrado (EFS) 253
- sistemas de archivos NAS 254
  - cliente Web 255
  - línea de mandatos 256
- sustituir archivo existente por copia de seguridad más reciente 453
- tareas primarias 237
- usuarios no raíz en RHEL 5 268
- utilización de mandatos 264
- utilizar la herramienta fsck para reparar 758
- versión activa 257

## restaurar (continuación)

- versión de copia de seguridad más reciente 483
- versión inactiva 257
- visión general 237
- visualizar objetos activos e inactivos 456
- volumen lógico 237, 248
  - Volumen lógico raw 237
- restaurar archivos dispersos 232
- restaurar enlaces fijos 232
- restore, mandato 744
  - realización de grandes operaciones 260
- restore backupset, mandato 749, 754
- restore group, mandato 756
- restore image
  - btrfs 205
- restore image, mandato 758
- restore NAS, mandato 762
- Restricción de IBM Spectrum Protect a un grupo de usuarios IBM Spectrum Protect
  - Restricción del acceso a un grupo de usuarios 52
- restricciones
  - asnodename, opción 349
  - asnodename, valores de sesión 350
  - en una sesión de proxy 189, 272
  - especificar vía de acceso completa con el daemon de aceptación de clientes 506
- restricciones de una sesión de proxy 189, 272
- retrieve
  - archivos para otro nodo 447
  - descripción de 384
  - en estación de trabajo distinta 608
  - en función de fecha y la hora del archivado 446, 449
  - lista de archivos 439
  - procesar sólo directorios (no archivos) 390
  - si debe preguntarse antes de sobrescribir archivos existentes 529
  - sustituir archivo existente por copia archivada más reciente si el archivo existente es más nuevo 453
- retrieve, mandato 770
- retryperiod, opción 542
- revinculación de archivos a otra clase de gestión 309
- revokeremoteaccess, opción 543

## S

### SAN

- utilizar para restaurar conjuntos de copias de seguridad 753
- schedlogname, opción 547
- schedlogretention, opción 549
- schedmode, opción 550
- schedule, mandato 773
- scripts de shell
  - códigos de retorno de 297
  - utilizar mandatos en 297
- scrolllines, opción 552
- scrollprompt, opción 553
- Sección JournalSettings 80
- Secure Sockets Layer (SSL)
  - establecer comunicaciones con 74
- selectiva, copia de seguridad 775
  - asociación de una instantánea local al espacio de archivos del servidor 194
- enlaces simbólicos 229
- línea de mandatos 182
- línea de mandatos del cliente 182
- mediante la GUI Java del cliente 181

- selectiva, copia de seguridad *(continuación)*
  - visión general 170, 179, 182
- selective, mandato 775
- serialización
  - Serialización de copia
    - dinámica 303
    - estática 303
    - estática compartida 303
  - serialización dinámica compartida 303, 363
  - serialización estática 303
  - serialización estática compartida 303, 363
  - servername, opción 555
  - servicio de gestión de cliente 48
  - servicio de soporte técnico 152
  - servicios planificados
    - definición de planificaciones para identificador de usuario que no sea cero 292
    - desactivar mandatos planificados 544, 545
    - restricciones para sistemas de archivos NAS 208
- servidor
  - comunicar con 56
  - dirección TCP/IP del servidor de IBM Spectrum Protect 590
  - direcciones de los puertos TCP/IP para 590
  - especificar nombre del servidor que debe contactarse para los servicios 555
  - establecer comunicaciones a través de un cortafuegos 72
  - establecer comunicaciones con 56
  - establecimiento de comunicaciones con Secure Sockets Layer (SSL) 74
  - identificar el inicio de una sección que contenga opciones 555
- servidor de archivos NAS (Almacenamiento conectado a red)
  - supresión de espacios de archivos 186, 267
- servidor de copias de seguridad de vStorage
  - copias de seguridad fuera de host 221
- sesión de mandatos
  - finalizar 658
  - iniciar 658
- sesión interactiva
  - finalizar 712
  - iniciar 145, 712
  - utilizar 712
- sesiones de restauración reiniciables, visualizar 737
- set access, mandato 778
  - autorización de restauración/recuperación 264
- set event command 781
- set password, mandato 784
- Shell Bourne y Korn
  - hacer referencia a un archivo de opciones del usuario cliente 58
- shimport, opción 558
- showmembers, opción 559
- sistema de archivos btrfs
  - archivado 205
  - backup image 205
  - copia de seguridad 205
  - protección de los subvolúmenes 207
  - proteger 205
  - recuperación 205
  - restaurar 205
  - restore image 205
- sistema de archivos de red (NFS)
  - sistemas de archivos de copia de seguridad 213
- sistema de archivos GPFS
  - agrupaciones de almacenamiento 249
  - entorno de clúster de varios nodos 162, 394
- sistema de archivos GPFS *(continuación)*
  - planificar 193
- sistema de archivos QFS
  - restricciones 162
- sistemas de archivos
  - admitidos 162
  - Btrfs 162
  - copia de seguridad de imagen 194
  - definir punto de montaje virtual 606
  - excluir de proceso de copia de seguridad 425
  - GPFS, entorno de clúster de varios nodos 162, 394
  - QFS, restricciones 162
  - soporte de ACL para 162
  - suprimidos 234
- Sistemas de archivos de cifrado (EFS)
  - restaurar sistemas de archivos 253
  - sistemas de archivos de copia de seguridad 217
- sistemas de archivos especiales 162, 228
- sistemas de archivos suprimidos 234
- sistemas de arranque dual
  - nombres duplicados 168
- snapdiff, opción 114, 561
- snapshotcachesize, opción 568
- snapshotroot, opción 571
- soporte
  - recopilación de información del sistema para 372, 442, 739
- soporte a la codificación de VMware
  - habilitar 642
- soporte al cifrado AES de 128 bits 161
- soporte de cifrado AES de 256 bits 161
- soporte de proxy de nodo cliente 188
- srvtptsetencryptiondisabled, opción 573
- SSL (Secure Socket Layer)
  - establecer comunicaciones con 74
- subdirectorios
  - archivado 272
  - incluir en copia de seguridad 182
- suprimir
  - archivos individuales del espacio de archivos de servidor 274, 693
  - copias de seguridad individuales del espacio de archivos de servidor 695
  - espacio de archivos 186, 267
  - NAS u objetos de cliente 364
- suprimir copias de seguridad individuales del espacio de archivos de servidor 185

## T

- tamaño máximo de archivo de archivado 166
- tamaño máximo de archivo de copia de seguridad 166
- tamaño máximo de archivo de recuperación 166
- tamaño máximo de archivo de restauración 166
- tapeprompt, opción 584
- tareas
  - asignación de clases de gestión a directorios 308
  - contraseña, cambiar 148
  - GUI, sustituir clase de gestión 307
  - inscripción abierta 123
  - inscripción cerrada 123
  - sesiones, finalizar 148
  - usuario root 49
  - visualizar clases de gestión 301
- tareas de usuario root
  - configurar 56
  - crear archivo de opciones del usuario cliente predeterminado 58

- TCP/IP, método de comunicación
  - opciones 314
- tcpadminport, opción 585
- tcpbuffsize, opción 586
- tcpcadaddress, opción 587
- tcpclientaddress, opción 588
- tcpclientport, opción 588
- tcpnodelay, opción 589
- tcpserveraddress, opción 590
- tcpwindowsize, opción 591
- teclado 805
- tiempo de proceso
  - estimación 181
- timeformat, opción 592
- toc, opción 596
- today, opción 597
- totime, opción 598
- transportador de datos predeterminado 639
- traspaso de datos sin LAN 416
  - activación de comunicaciones 158, 481
  - condiciones previas 158
- Traspaso de datos sin LAN
  - opciones 158
- tsmjbdd.ini
  - configurar 78
- txnbytelimit, opción 599
- type, opción 600

## U

- Ubuntu Linux on Power Systems (Little Endian) API
  - desinstalación 24
- Unicode
  - cambiar el nombre de los espacios de archivos que no son Unicode al formato Unicode 356, 775
  - migrar espacios de archivos a 169
  - restaurar de espacios de archivos que no están activados para Unicode 749
- UNIX
  - guardar permisos de acceso estándar 275
  - sistemas de archivos, soporte de ACL 162
- UNIX y Linux
  - entorno en clúster 103
    - instalar IBM Spectrum Protect 103
  - restricciones
    - restaurar vínculos simbólicos 744
- usuario autorizado
  - definición 49
  - tareas 49
- usuario root
  - obtener acceso de usuario root 49
- usuarios autorizados
  - habilitar el cifrado 53
- utilizar varias sesiones 224

## V

- valores de protección de datos
  - herencia 800
    - se representan en forma de códigos 792
  - sugerencias para configurar políticas de copia de seguridad 802
- variable de entorno LANG
  - definir entorno regional de idioma 61
- variables de entorno
  - de shell Bourne y Korn, establecer 64

- variables de entorno (*continuación*)
  - de shell C, establecer 64
    - DSM\_CONFIG 62
    - DSM\_DIR 62
    - DSM\_LOG 62
    - establecer API 65
    - LANG 62
  - variables de shell Bourne y Korn, establecer 64
  - variables de shell C
    - establecer 64
  - verbose, opción 604
  - verifyimage, opción 605
  - versiones de copia de seguridad activas
    - restauración 257
    - visualizar 150, 257, 720
  - versiones de copia de seguridad inactivas
    - restauración 257
    - visualizar 150, 257, 720
  - versiones si datos
    - existen, atributo 302
    - existen, parámetro 303
    - suprimidos, atributo 303
    - suprimidos, parámetro 303
  - vínculos fijos
    - archivar y recuperar 276
    - copia de seguridad 232
    - restaurar 232
  - virtualfsname, opción 606
  - virtualmountpoint, opción 606
  - virtualnodename, opción 608
    - restaurar o recuperar en otra estación de trabajo 266
  - visualizar
    - ayuda en línea 152
    - eventos planificados 738
    - información de copias archivadas 718
    - información de política 301
    - información de sesión 738
    - sesiones de restauración reiniciables 737
- VM 219
  - vmbackdir, opción 609
  - vmbackupmailboxhistory 610
  - vmbackuptype, opción 611
  - vmdatastorethreshold
    - opción 616
  - vmdefaultdvswitch opción 619
  - vmmaxvirtualdisks 629
  - vmnoprdmdisks 632
  - vmnovrdmdisks 633
  - vmprocessvmwithprdm 636
  - vmprocesswithindependent 634
  - vmskipmaxvirtualdisks 638
  - vmskipmaxvmdks 639
  - vmtagdatamover
    - opción 642
  - vmtagdefaultdatamover
    - opción 639
  - vmverifyifaction 644
  - vmverifyiflatest 646
  - vmvstortransport, opción 648
  - volumen lógico
    - copia de seguridad de imagen 194
    - restauración 248
    - restaurar 237
- Volumen lógico raw
  - copia de seguridad de imagen 194
  - restaurar 237

## W

webports, opción 650

## Z

ZFS (Zettabyte File Systems) 216

    sistemas de archivos de copia de seguridad 216

zonas de Solaris 180





Número de Programa: 5725-W98  
5725-W99  
5725-X15

Impreso en España