

Rapid Recovery 6.0 en dispositivos DL

Guía del usuario

Notas, precauciones y avisos

 **NOTA:** Una NOTA proporciona información importante que le ayuda a utilizar mejor su equipo.

 **PRECAUCIÓN:** Una PRECAUCIÓN indica la posibilidad de daños en el hardware o la pérdida de datos, y le explica cómo evitar el problema.

 **AVISO:** Un mensaje de AVISO indica el riesgo de daños materiales, lesiones corporales o incluso la muerte.

© 2016 Dell Inc. Todos los derechos reservados. Este producto está protegido por leyes internacionales y de los Estados Unidos sobre los derechos de autor y la protección intelectual. Dell y el logotipo de Dell son marcas comerciales de Dell Inc. en los Estados Unidos y en otras jurisdicciones. El resto de marcas y nombres que se mencionan en este documento pueden ser marcas comerciales de las compañías respectivas.

Tabla de contenido

1 Introducción al dispositivo DL.....	11
Arquitectura de Implementación.....	11
Smart Agent.....	13
Dispositivo DL Core.....	13
Proceso de instantáneas.....	13
Sitio de recuperación de desastres de replicación o proveedor de servicio.....	14
Recuperación.....	14
Características del producto	14
Definición de los repositorios.....	14
Desduplicación en Rapid Recovery.....	16
Descripción de las claves de cifrado.....	16
Replicación con Rapid Recovery.....	17
Retención y archivado.....	20
Virtualización y nube.....	21
Administración de alertas y eventos.....	22
Portal de licencias.....	22
Consola web.....	22
API de administración de servicios.....	22
2 Trabajar con el Core del Dispositivo DL	23
Descripción de la Core Console de Rapid Recovery.....	23
Acceso a la Core Console de Rapid Recovery.....	23
Comprensión de la Guía de inicio rápido.....	23
Desplazarse hasta la Rapid Recovery Core Console.....	25
Visualización del menú Equipos protegidos.....	29
Visualización de equipos replicados en el menú de navegación.....	34
Visualización en el menú Solo puntos de recuperación.....	34
Visualización en el menú Grupos personalizados.....	35
Uso del cuadro de diálogo Error.....	35
Configuración del Core.....	35
Configuración del Core de Rapid Recovery.....	35
Copia de seguridad y restauración de la configuración del Core.....	65
Herramientas de nivel del Core.....	66
Planificación de la configuración del Core	69
Repositorios.....	69
Administración de un repositorio DVM.....	69
Administración de la seguridad	82
Aplicación o retirada del cifrado de un equipo protegido.....	82
Administración de las claves de cifrado.....	85
Administración de cuentas de nube.....	92
Acerca de las cuentas de servicios en la nube.....	93

Incorporación de una cuenta de nube.....	93
Modificación de una cuenta de nube.....	94
Configuración de los parámetros de cuentas de nube.....	95
Eliminación de una cuenta de nube.....	95
Archivado.....	95
Cómo funciona la archivación.....	96
Creación de una archivación.....	96
Modificación de una archivación programada.....	99
Cómo realizar una pausa o reanudar un archivo programado.....	101
Forzar un trabajo de archivación.....	101
Comprobación de una archivación.....	102
Adición de un archivo comprimido.....	103
Importación de un archivo.....	104
Eventos.....	106
Rapid Recovery de Rapid Recovery.....	106
Visualización de eventos mediante las tareas, las alertas y el diario.....	106
Información sobre las notificaciones por correo electrónico.....	110
Grupos de notificación, valores del SMTP y plantillas de notificaciones de eventos del sistema.....	113
Configuración de grupos de notificación.....	113
Acerca de la configuración de la reducción de repeticiones.....	116
Configuración de la retención de eventos.....	117
Recuperación automática rápida del dispositivo (RASR).....	117
Creación de la memoria USB de RASR.....	118
Ejecución de RASR.....	118
Local Mount Utility.....	119
Acerca de Local Mount Utility.....	119
Cómo trabajar con equipos Rapid Recovery Core en la Utilidad de montaje local.....	120
Cómo trabajar con equipos protegidos en Local Mount Utility.....	123
Uso del menú de bandeja de Local Mount Utility.....	125
3 Administración del servidor.....	127
Supervisión del estado del dispositivo.....	127
Copia de seguridad de Windows.....	127
Estado de la copia de seguridad.....	128
Política de copia de seguridad de Windows.....	129
Aprovisionamiento de almacenamiento.....	130
Eliminación de asignación de espacio para un disco virtual.....	131
Utilidad de recuperación y actualización.....	132
Actualización del dispositivo.....	132
Reparación del dispositivo.....	132
4 Protección de estaciones de trabajo y servidores.....	134
Protección de máquinas.....	134
Acerca de la protección de los equipos con Rapid Recovery	134
Acceso a los diagnósticos de equipos protegidos.....	198
Administración de equipos.....	199

Retirada de un equipo.....	200
Cancelación de operaciones en un equipo.....	200
Visualización de la información de licencia en un equipo.....	200
Exportación de VM.....	201
Información sobre la exportación a máquinas virtuales con Rapid Recovery.....	201
Administración de exportaciones.....	213
Administración de datos anteriores.....	227
Acerca de la retención y el archivado de datos de Rapid Recovery.....	227
Administración de políticas de retención.....	227
Replicación.....	233
Replicación con Rapid Recovery.....	233
Cadenas del punto de recuperación y huérfanos.....	236
Cuando comienza una replicación.....	236
Determinación de la estrategia y necesidades de inicialización.....	237
Consideraciones de rendimiento para la transferencia de datos replicados.....	239
Replicación a un Core de destino administrado automáticamente.....	240
Visualización de la replicación entrante y saliente.....	243
Configuración de la replicación.....	245
Replicación en un Core de destino externo.....	246
Cómo agregar un equipo a una replicación existente.....	250
Consumo de la unidad de inicialización en un Core de destino.....	252
Administración de configuraciones de replicación.....	254
Eliminación de replicación.....	261
Recuperación de datos replicados.....	263
5 Datos de recuperación.....	264
Administración de la recuperación	264
Instantáneas y puntos de recuperación.....	264
Administración de instantáneas y puntos de recuperación.....	264
Visualización de la página de puntos de recuperación de un equipo protegido.....	264
Montaje de un punto de recuperación.....	267
Desmontaje de puntos de recuperación.....	268
Trabajo con puntos de recuperación de Linux.....	268
Cómo forzar una instantánea.....	270
Eliminación de puntos de recuperación.....	271
Eliminación de una cadena de puntos de recuperación huérfanos.....	272
Migración de puntos de recuperación manual a un repositorio diferente.....	272
Restauración de datos.....	273
Acerca de la restauración de datos con Rapid Recovery.....	273
Descripción de Live Recovery.....	273
Restauración de datos desde puntos de recuperación.....	274
Restauración de volúmenes desde un punto de recuperación.....	275
Restauración de clústeres y nodos de clúster.....	278
Restauración a partir de un archivo conectado.....	279
Comprensión de la restauración Bare Metal Restore para equipos Windows.....	280
Restauración Bare Metal Restore para equipos con Windows.....	280

Descripción de la creación del CD de inicio para equipos Windows.....	285
Uso de la Universal Recovery Console para una BMR.....	288
Realización de una restauración Bare Metal Restore para Linux.....	296
Comprobación de una restauración Bare Metal Restore.....	305
6 Creación y visualización de informes.....	309
Acerca de los informes de Rapid Recovery.....	309
Generación de un informe desde la Core Console.....	310
Administración de informes programados desde la Core Console.....	313
Uso del menú de informes.....	318
Uso de la barra de herramientas de informes.....	318
Descripción del informe de trabajo.....	320
Comprensión del informe de resumen de trabajos.....	320
Comprensión del informe de error.....	321
Comprensión del informe de resumen.....	322
Descripción del informe del repositorio.....	323
Central Management Console.....	323
Descripción de la Consola de administración central de Rapid Recovery.....	324
Configuración de la Consola de administración central Rapid Recovery.....	325
Información de los informes de la administración central de Cores de la consola.....	329
7 Comprensión de la utilidad Administración de línea de comandos de Rapid Recovery.....	331
Comandos.....	332
Archivado.....	333
CancelActiveJobs (Cancelar trabajos activos).....	334
CheckRepository.....	335
CreateArchiveRepository.....	336
CreateBootCD.....	338
CreateRepository (Crear repositorio).....	339
DeleteRepository.....	340
Dismount (Desmontar).....	341
DismountArchiveRepository.....	342
EditEsxServer.....	343
Forzar.....	344
ForceAttach (Forzar conexión).....	345
ForceChecksum (Forzar suma de comprobación).....	346
ForceLogTruncation (Forzar truncamiento del registro).....	347
ForceMount (Forzar montaje).....	348
ForceReplication (Forzar replicación).....	349
ForceRollup (Forzar consolidación).....	349
ForceVirtualStandby.....	350
Ayuda.....	351
List (Enumerar).....	352
Montar.....	354
MountArchiveRepository.....	355
NewCloudAccount.....	356

OpenDvmRepository.....	357
Pausar.....	358
Proteger.....	360
Proteger clúster.....	361
ProtectEsxServer.....	362
RemoveAgent.....	363
RemoveArchiveRepository.....	364
RemovePoints (Eliminar puntos).....	365
RemoveScheduledArchive.....	366
RemoveVirtualStandby.....	367
Replicación.....	367
Replicación.....	369
RestoreAgent.....	371
RestoreArchive (Restaurar archivo).....	372
RestoreUrc.....	373
Reanudar.....	375
SeedDrive.....	376
StartExport (Iniciar exportación).....	377
UpdateRepository (Actualizar repositorio).....	380
Versión.....	381
VirtualStandby.....	382
Traducción.....	384
Apéndice A: Referencias de la Core Console.....	385
Visualización de la interfaz para el usuario de la Core Console.....	385
Barra de botones.....	386
Barra de iconos.....	387
Menú de navegación izquierdo.....	389
Visualización del panel de máquinas protegidas.....	392
Visualización de eventos de un equipo protegido.....	395
Visualización del menú Más para máquinas protegidas.....	396
Apéndice B: Descripción del módulo PowerShell de Rapid Recovery.....	398
Requisitos previos para utilizar PowerShell.....	399
powershell.exe.config.....	399
Inicio de PowerShell e importación del módulo.....	399
Trabajo con comandos y cmdlets.....	399
Cómo obtener ayuda y ejemplos de cmdlets.....	400
Cmdlets del módulo Rapid Recovery PowerShell.....	400
Edit-EsxVirtualStandby.....	403
Edit-Hyper VVirtualStandby.....	404
Edit-ScheduledArchive.....	406
Edit-VBVirtualStandby.....	407
Edit-VMVirtualStandby.....	409
Get-ActiveJobs.....	410
Get-Clusters.....	412
Get-CompletedJobs.....	412

Get-ExchangeMailStores.....	414
Get-Failed.....	414
Get-FailedJobs.....	415
Get-Mounts.....	417
Get-Passed.....	418
Get-ProtectedServers.....	419
Get-ProtectionGroups.....	419
Get-QueuedJobs.....	420
Get-RecoveryPoints.....	422
Get-ReplicatedServers.....	422
Get-Repositories.....	423
Get-ScheduledArchives.....	424
Get-SqlDatabases.....	425
Get-UnprotectedVolumes.....	426
Get-VirtualizedServers.....	427
Get-Volumes.....	427
New-Base.....	428
New-CloudAccount.....	429
New-EncryptionKey.....	431
New-EsxiVirtualStandby.....	431
New-HyperVVirtualStandby.....	433
New-Mount.....	435
Resume-Replication.....	436
New-Repository.....	437
New-ScheduledArchive.....	438
New-Snapshot.....	440
New-VBVirtualStandby.....	441
New-VMVirtualStandby.....	443
Push-Replication.....	444
Push-Rollup.....	445
Remove-Agent.....	446
Remove-Mount.....	447
Remove-Mounts.....	448
Remove-RecoveryPoints.....	448
Eliminación del repositorio.....	450
Remove-ScheduledArchive.....	451
Remove-VirtualStandby.....	451
Resume-Replication.....	452
Resume-Snapshot.....	454
Resume-VirtualStandby.....	454
Resume-VMExport.....	455
Start-Archive.....	456
Start-AttachabilityCheck.....	457
Start-ChecksumCheck.....	458
Start-EsxiExport.....	459

Start-HypervExport.....	461
Start-LogTruncation.....	463
Start-MountabilityCheck.....	464
Start-Protect.....	465
Start-ProtectCluster.....	466
Start-RepositoryCheck.....	467
Start-RestoreArchive.....	468
Start-ScheduledArchive.....	469
Start-VBExport.....	470
Start-VirtualStandby.....	472
Start-VMExport.....	473
Stop-ActiveJobs.....	474
Suspend-Replication.....	475
Suspend-RepositoryActivity.....	477
Suspend-ScheduledArchive.....	478
Suspend-Snapshot.....	478
Suspend-VirtualStandby.....	479
Suspend-VMExport.....	480
Update-Repository.....	481
Localización.....	482
Calificadores.....	482
Apéndice C: Extensión de trabajos de Rapid Recovery mediante secuencias de comandos.....	484
Uso de secuencias de comandos PowerShell en Rapid Recovery.....	484
Requisitos previos para las secuencias de comandos de PowerShell.....	485
powershell.exe.config.....	485
Prueba de las secuencias de comandos de PowerShell.....	485
Localización.....	485
Calificadores.....	486
Parámetros de entrada para las secuencias de comandos de PowerShell.....	486
AgentProtectionStorageConfiguration (espacio de nombres Replay.Common.Contracts.Agents).....	486
AgentTransferConfiguration (espacio de nombres Replay.Common.Contracts.Transfer).....	487
BackgroundJobRequest (espacio de nombres Replay.Core.Contracts.BackgroundJobs).....	488
ChecksumCheckJobRequest (espacio de nombres Replay.Core.Contracts.Exchange.ChecksumChecks).....	489
DatabaseCheckJobRequestBase (espacio de nombres Replay.Core.Contracts.Exchange).....	489
ExportJobRequest (espacio de nombres Replay.Core.Contracts.Export).....	489
NightlyAttachabilityJobRequest (espacio de nombres Replay.Core.Contracts.Sql).....	490
RollupJobRequest (espacio de nombres Replay.Core.Contracts.Rollup).....	490
TakeSnapshotResponse (espacio de nombres Replay.Agent.Contracts.Transfer).....	490
TransferJobRequest (espacio de nombres Replay.Core.Contracts.Transfer).....	490
TransferPrescriptParameter (espacio de nombres Replay.Common.Contracts.PowerShellExecution).....	492
TransferPostscriptParameter (espacio de nombres Replay.Common.Contracts.PowerShellExecution)...	492
TransferScriptParameterBase (namespace Replay.Common.Contracts.PowerShellExecution).....	494
VirtualMachineLocation (espacio de nombres Replay.Common.Contracts.Virtualization).....	494
VolumemageldsCollection (espacio de nombres Replay.Core.Contracts.RecoveryPoints).....	495

VolumeName (espacio de nombres Replay.Common.Contracts.Metadata.Storage).....	495
VolumeNameCollection (espacio de nombres Replay.Common.Contracts.Metadata.Storage).....	495
VolumeSnapshotInfo (namesapce Replay.Common.Contracts.Transfer).....	496
VolumeSnapshotInfoDictionary (espacio de nombres Replay.Common.Contracts.Transfer).....	496
Secuencias de comandos de PowerShell de prueba.....	496
PreTransferScript.ps1.....	496
PostTransferScript.ps1.....	497
PreExportScript.ps1.....	497
PostExportScript.ps1.....	498
PreNightlyJobScript.ps1.....	498
PostNightlyJobScript.ps1.....	500
Uso de las secuencias de comandos de Bourne Shell en Rapid Recovery.....	501
Requisitos previos para las secuencias de comandos de Bourne Shell.....	502
Parámetros compatibles de secuencias de comandos de transferencia y transferencia posterior.....	502
Prueba de secuencias de comandos de Bourne Shell.....	503
Parámetros de entrada para las secuencias de comandos de Bourne Shell.....	503
TransferPrescriptParameters_VolumeNames.....	503
TransferPostscriptParameter.....	504
Secuencias de comandos de muestra de Bourne Shell.....	504
PreTransferScript.sh.....	505
PostTransferScript.sh.....	505
PostExportScript.sh.....	506
Apéndice D: API de Rapid Recovery.....	507
Público al que va dirigido.....	507
Trabajar con las API de REST de Rapid Recovery.....	507
Descargar y ver las API de Core y Agent.....	507
Lectura adicional recomendada.....	509
Acerca de Dell.....	510
Cómo ponerse en contacto con Dell.....	510
Recursos de asistencia técnica.....	510
Glosario.....	511

Introducción al dispositivo DL

El dispositivo DL con software Rapid Recovery es una solución de copia de seguridad, replicación y recuperación con objetivos de tiempo de recuperación casi nulos y objetivos de punto de recuperación. Rapid Recovery ofrece protección de datos, recuperación frente a desastres, migración de datos y administración de datos. Le ofrece la flexibilidad de realizar una realización completa (a hardware similar o diferente), y puede restaurar copias de seguridad en máquinas físicas o virtuales, independientemente del origen. Con Rapid Recovery puede replicar en uno o más destinos para obtener mayor redundancia y seguridad.

El dispositivo establece un nuevo estándar para la protección unificada de datos mediante la combinación de copia de seguridad, replicación y recuperación en una única solución que se ha diseñado para ser la copia de seguridad más rápida y fiable de protección de máquinas virtuales (MV), máquinas físicas y entornos en la nube. El servidor permite gestionar petabytes de datos con deduplicación global integrada, compresión, cifrado y replicación en cualquier infraestructura de nube privada o pública. Los datos y las aplicaciones de servidor pueden recuperarse en cuestión de minutos con fines de retención de datos y cumplimiento de normas.

El servidor admite entornos de varios hipervisores en VMware vSphere y Microsoft Hyper-V y nubes públicas y privadas.

Características de Rapid Recovery:

- **Flexibilidad.** Puede realizar una recuperación universal para varias plataformas, incluida la restauración desde máquina física a virtual, virtual a física, virtual a virtual, y física a física.
- **Integración en la nube.** Puede archivar y replicar la nube a través de proveedores de almacenamiento en la nube que admiten plataformas patentadas y de código abierto.
- **Desduplicación inteligente.** Puede reducir los requisitos de almacenamiento mediante el almacenamiento único de los datos y haciendo referencia a ellos posteriormente (una vez por repositorio o dominio de cifrado).
- **Recuperación instantánea.** Nuestra función de Recuperación directa le permite acceder a los datos críticos en primer lugar, mientras que las operaciones de restauración restantes se completan en paralelo.
- **Recuperación de nivel de archivo.** Puede recuperar los datos a nivel de archivo en su propia ubicación, desde una ubicación remota o desde la nube.
- **Soporte Virtual.** El soporte optimizado para la virtualización incluye protección sin agente y descubrimiento automático para VMware® ESXi™ 5 y posterior y exportación a volúmenes de clúster compartido Microsoft® Hyper-V®.

Consulte los recursos siguientes para obtener más información sobre Rapid Recovery.

- La página web de asistencia al producto Rapid Recovery de Dell en <https://support.software.dell.com/rapid-recovery/>
- La página web de documentación de Dell en <https://support.software.dell.com/rapid-recovery/release-notes-guides/> y <http://www.dell.com/support/home/>.

Temas:

- [Arquitectura de Implementación](#)
- [Características del producto](#)

Arquitectura de Implementación

El servidor es un producto de copia de seguridad y recuperación escalable que se implementa de forma flexible dentro de la empresa o como servicio ofrecido por un proveedor de servicio administrado. El tipo de implementación depende del tamaño y los requisitos del cliente. Preparar la implementación del servidor implica planificar la topología de almacenamiento de red, la infraestructura de hardware del Core y de recuperación de desastres y la seguridad.

La arquitectura de implementación se compone de componentes locales y remotos. Los componentes remotos pueden ser opcionales para los entornos que no necesitan usar un sitio de recuperación de desastres o un proveedor de servicio administrado para recuperación

externa. Una implementación local básica se compone de un servidor de copia de seguridad denominado Core y una o más máquinas protegidas. El componente externo se habilita mediante la replicación que ofrece capacidades de recuperación completas en el sitio de DR. El Core utiliza imágenes base e instantáneas incrementales para compilar los puntos de recuperación de las máquinas protegidas.

Además, el servidor reconoce aplicaciones porque detecta la presencia de Microsoft Exchange y SQL y de sus respectivas bases de datos y archivos de registro y, a continuación, agrupa automáticamente estos volúmenes con dependencia para una protección global y una recuperación efectiva. Esto le garantiza que jamás tendrá copias de seguridad incompletas cuando esté realizando recuperaciones. Las copias de seguridad se realizan mediante instantáneas de nivel de bloque que reconocen aplicaciones. El servidor también puede realizar truncamientos de registro de los servidores de Microsoft Exchange y SQL protegidos.

En el siguiente diagrama se representa una implementación sencilla. En este diagrama, el software del Agent de AppSure se instala en máquinas como un servidor de archivos, de correo electrónico, de bases de datos o en máquinas virtuales y se conectan y se protegen mediante un solo Core, que también incluye el repositorio central. El Portal de licencias administra las suscripciones de licencias, grupos y usuarios de las máquinas protegidas y de los Cores de un entorno. El Portal de licencias permite a los usuarios iniciar sesión, activar cuentas, descargar software e implementar máquinas y Cores en el entorno en función de su licencia.

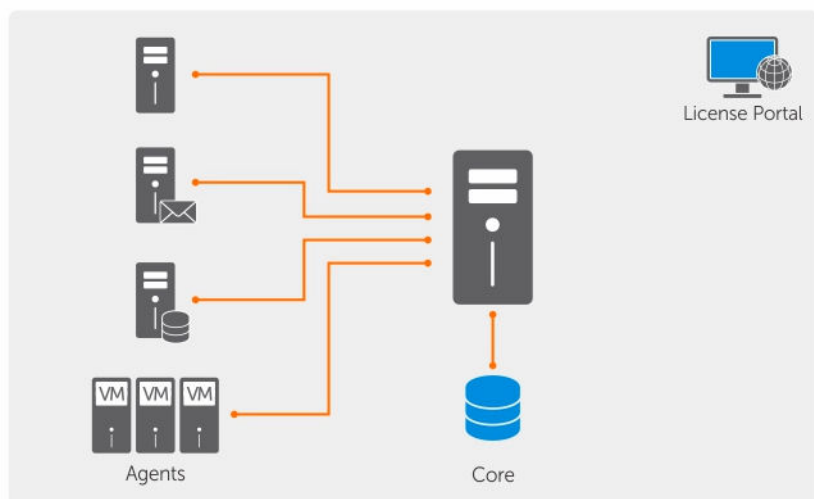


Ilustración 1. Arquitectura de implementación básica

También puede implementar varios Cores según se muestra en el siguiente diagrama. Una consola central administra varios Cores.

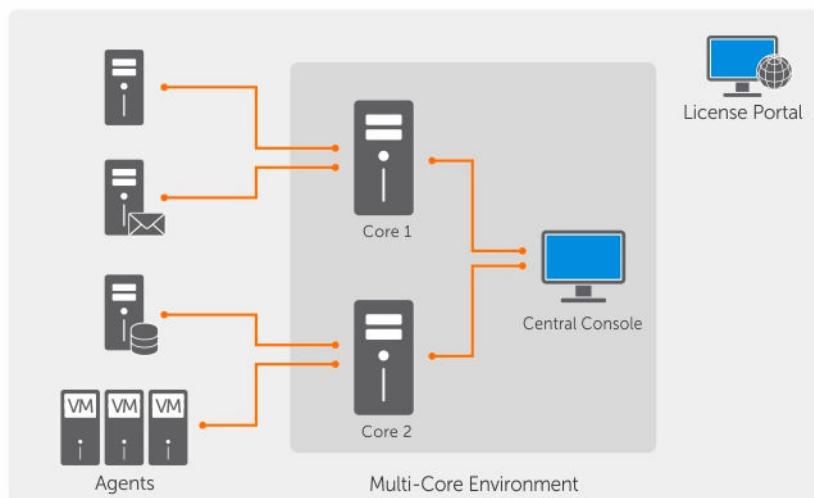


Ilustración 2. Arquitectura de implementación de varios Cores

Smart Agent

Smart Agent supervisa los bloques modificados en el volumen de disco y, a continuación, toma una imagen de los bloques modificados a un intervalo de protección predefinido. El método de instantáneas de nivel de bloque incremental permanente evita que se repita la copia de los mismos datos desde la máquina protegida al Core. Rapid Recovery Smart Agent se instala en las máquinas que están protegidas por Rapid Recovery Core.

Smart Agent reconoce las aplicaciones y detecta el tipo de aplicación que está instalada y también la ubicación de los datos. Automáticamente agrupa los volúmenes de datos con dependencia, como las bases de datos, y luego los registra juntos para una protección eficaz y una recuperación rápida. Una vez configurado el software Rapid Recovery Agent, utiliza tecnología inteligente para realizar un seguimiento de los bloques modificados de los volúmenes de disco protegidos. Cuando la instantánea está lista, se transfiere rápidamente al Core usando conexiones basadas en sockets o multiproceso. Para conservar la memoria y el ancho de banda de la CPU en las máquinas protegidas, el Smart Agent no cifra ni deduplica los datos en el origen y las máquinas protegidas se emparejan con un Core para su protección.

Dispositivo DL Core

El Core es el componente central de la arquitectura de implementación. El Core almacena y administra todas las copias de seguridad de las máquinas y proporciona servicios de Core para copias de seguridad, recuperación y retención; replicación, archivado y administración. El Core es un equipo de red direccionable autocontenido que ejecuta una de 64 bits del sistema operativo Microsoft Windows. El dispositivo realiza una compresión en línea basada en el objetivo, cifrado y deduplicación de los datos recibidos desde la máquina protegida. El Core almacena a continuación las copias de seguridad de las instantáneas en repositorios, como por ejemplo, red de área de almacenamiento (SAN) o de almacenamiento adjunto directo (DAS).

El repositorio también puede residir en almacenamiento interno del Core. El Core se administra accediendo a la siguiente URL desde un explorador de web: **<https://CORENAME:8006/apprecovery/admin>**. Internamente, se puede acceder a todos los servicios de Core a través de las API de REST. A los servicios de Core se puede acceder desde dentro del Core o directamente a través de Internet desde cualquier aplicación que pueda enviar una solicitud HTTP/HTTPS y recibir una respuesta HTTP/HTTPS. Todas las operaciones de API se realizan sobre SSL y se autentican mutuamente mediante certificados X.509 v3.

Los Cores se emparejan con otros Cores para la replicación.

Proceso de instantáneas

Una instantánea tiene lugar cuando una imagen base se transfiere desde una máquina protegida al Core. Las instantáneas capturan y almacenan el estado de un volumen de disco en un momento específico mientras las aplicaciones que generan los datos aún están en uso. En Rapid Recovery puede forzar una instantánea, pausar instantáneas de manera temporal o ver listas de los puntos de recuperación actuales en el repositorio, así como eliminarlos si es necesario. Los puntos de recuperación se usan para restaurar máquinas protegidas o para montar en un sistema de archivos local. Las instantáneas capturadas por Rapid Recovery se realizan a nivel de bloque y son sensibles a las aplicaciones. Esto implica la realización de todas las transacciones abiertas y los registros de transacción agregados, y que las cachés se vacían al disco antes de crear la instantánea.

Rapid Recovery utiliza una controladora de filtro de volumen de bajo nivel que se conecta a los volúmenes montados. Posteriormente realiza el seguimiento de todos los cambios a nivel de bloque para la siguiente instantánea inminente. Se utiliza Microsoft Volume Shadow Services (VSS) para facilitar las instantáneas consistentes con bloqueos de aplicación.

Sitio de recuperación de desastres de replicación o proveedor de servicio

El proceso de replicación requiere una relación de emparejamiento de origen-destino entre dos Cores. El Core de origen copia los puntos de recuperación de las máquinas protegidas y, a continuación, los transmite de forma continua y asíncrona hasta el Core de destino en un sitio de recuperación de desastres remoto. La ubicación externa puede ser un centro de datos propiedad de la empresa (Core administrado automáticamente) o una ubicación o entorno de nube del proveedor de servicio (MSP) administrado por un tercero. Cuando replique a un MSP, puede usar flujos de trabajo integrados que le permiten solicitar conexiones y recibir notificaciones de comentarios automáticas. Para la transferencia de datos inicial, puede realizar la inicialización de datos mediante el uso de medios externos; esto es útil para conjuntos de datos o sitios grandes con enlaces lentos.

Si se produce una interrupción grave, el servidor admite conmutación por error y conmutación por recuperación en entornos replicados. Si se produce una interrupción completa, el Core de destino en el sitio secundario puede recuperar instancias desde máquinas protegidas replicadas e iniciar inmediatamente la protección en las máquinas conmutadas por error. Después de restaurar el sitio primario, el Core replicado puede conmutar por recuperación los datos desde las instancias recuperadas de vuelta a las máquinas protegidas en el sitio primario.

Recuperación

La recuperación se puede realizar en el sitio local o en el sitio remoto replicado. Cuando la implementación esté en estado estable con protección local y replicación opcional, Core le permitirá realizar la recuperación mediante Verified Recovery, Universal Recovery, o Live Recovery.

Características del producto

Puede administrar la protección y recuperación de datos críticos mediante las siguientes características y funcionalidad:

- [Repository \(Repositorio\)](#)
- [Desduplicación en Rapid Recovery](#)
- [Cifrado](#)
- [Replicación](#)
- [Retención y archivado](#)
- [Virtualización y nube](#)
- [Administración de alertas y eventos](#)
- [Portal de licencias](#)
- [Consola web](#)
- [API de administración de servicios](#)

Definición de los repositorios

Un repositorio es una ubicación central en la que se almacenan y gestionan los datos de instantáneas de copia de seguridad capturados de sus estaciones de trabajo y servidores protegidos. Los datos se guardan en un repositorio en forma de puntos de recuperación.

Un repositorio puede residir en diferentes tecnologías de almacenamiento, que incluyen Storage Area Network (Red de área de almacenamiento - SAN), Direct Attached Storage (Almacenamiento conectado directamente - DAS) o Network Attached Storage (Almacenamiento conectado a la red - NAS).

NOTA: Almacene repositorios para Rapid Recovery Core en dispositivos de almacenamiento principales. La velocidad del volumen de almacenamiento es el factor más crítico. No se admiten dispositivos de archivado tales como Data Domain (Dominio de datos), debido a limitaciones de rendimiento. De forma similar, no almacene los repositorios en repositorios en filtros NAS que estén conectados a la nube, ya que estos dispositivos suelen tener limitaciones de rendimiento cuando se utilizan como almacenamiento principal.

DAS ofrece el más alto ancho de banda de datos y la velocidad de acceso más rápida, y es fácil de implementar. Para obtener resultados óptimos, utilice DAS con almacenamiento 6 mediante matriz redundante de discos independientes (RAID). Para obtener más información, consulte la [Base de conocimientos de Dell, artículo 118153](#), "Opciones de repositorio: Almacenamiento adjunto directo, Red de área de almacenamiento o Almacenamiento conectado a la red."

La ubicación de almacenamiento para cualquier repositorio debe estar siempre en un subdirectorio que haya especificado (por ejemplo, `E:\Repository`), no en la raíz de un volumen (por ejemplo, `E:\`).

El formato del repositorio de Rapid Recovery (Recuperación rápida) utiliza el Administrador de volúmenes de deduplicación (DVM). Los repositorios de DVM admiten varios volúmenes, hasta 255 repositorios en un único Core, y el uso de extensiones. Puede crear repositorios de DVM en equipos que sólo ejecuten sistemas operativos Windows. Es posible utilizar este tipo de repositorio cuando utilice las nuevas instalaciones de Rapid Recovery. El tamaño de un repositorio de DVM puede especificarse después de crearlo, y las extensiones pueden agregarse más tarde.

Funciones y atributos del repositorio de DVM:

- Admite la recuperación a partir de archivos Rapid Recovery 6.x y puntos de recuperación
- Es compatible con las ubicaciones de almacenamiento sólo en sistemas operativos Windows. El volumen de repositorio pueden local (en un almacenamiento conectado al servidor Core), o en una ubicación de almacenamiento en una ubicación compartida de Common Internet File System (Sistema de archivos de Internet común - CIFS).
- Los tipos de almacenamiento admitidos incluyen el Storage Area Network (Red de área de almacenamiento - SAN), Direct Attached Storage (Almacenamiento de conexión directa - DAS), o Network Attached Storage (Almacenamiento conectado a la red - NAS)
- Requiere 8 GB de RAM, preferiblemente memoria con verificación y corrección de errores (ECC)
- Requiere un procesador de cuatro núcleos en máquina (este requisito permanente es ahora obligatorio)
- Admite varios repositorios de DVM por host
- Servicios adicionales innecesarios: los repositorios de DVM utilizan servicios Core para la comunicación con Core y para eventos de seguimiento
- Cada repositorio de DVM admite hasta 4 096 extensiones de repositorio (también denominadas ubicaciones de almacenamiento)
- Tamaño fijo; el repositorio de DVM exige que especifique el tamaño del repositorio en un volumen. El tamaño que especifique no puede superar el tamaño del volumen. Cada volumen que defina como una ubicación de almacenamiento debe tener un mínimo de 1 GB de espacio libre disponible.
- La ubicación de almacenamiento puede ser un repositorio simple o un disco dinámico, con la velocidad como el factor más importante
- Puede utilizar claves de cifrado estándar creadas y administradas en la Consola de Core (cifrado basado en Core)
- Realiza la deduplicación de los datos en todo el repositorio (o entre dominios de cifrado dentro de cada repositorio, si se utilizan claves de cifrado)
- Utiliza una caché de deduplicación de DVM dedicado y redimensionable, con una ubicación de almacenamiento configurable en los ajustes del Core
- Optimizado para escribir datos, almacenar los datos de instantáneas en un repositorio local para el Core, con todos los datos procesados a través del Core
- El nombre no puede cambiarse después de crear el repositorio
- Es posible crear nueve repositorios de este tipo utilizando las API de REST, la utilidad de administración de línea de comandos de Rapid Recovery (`cmdutil.exe`), o Windows PowerShell `@ cmdlet`

Cuando se crea un repositorio de DVM, el Rapid Recovery Core preasigna el espacio de almacenamiento necesario para los datos y metadatos en la ubicación especificada. El tamaño mínimo del repositorio de DVM es de 1 GB, que por razones prácticas es generalmente demasiado pequeño, excepto para la realización de pruebas.

Debido a que la deduplicación de DVM exigen una caché primaria y secundaria, asegúrese de que el espacio de almacenamiento que reserve sea tenga el doble del tamaño de la caché de deduplicación. Por ejemplo, si tiene 1,5 GB reservados en la configuración del caché

de deduplicación de DVM en el Core, reserve 3 GB en el volumen de la caché. La ruta de instalación predeterminada para la caché se encuentra en la unidad C. Para obtener más información, consulte [Funcionamiento de la caché de deduplicación y las ubicaciones de almacenamiento](#).

Puede crear varios repositorios independientes asociados con un solo Core, hasta un número máximo de 255 repositorios de DVM. Los repositorios pueden abarcar diferentes tecnologías de almacenamiento.

Puede aumentar el tamaño de un repositorio de DVM agregando nuevas extensiones de archivo o especificaciones. Un repositorio ampliado puede contener hasta 4 096 extensiones que abarcan diferentes tecnologías de almacenamiento.

Para obtener más información sobre cómo trabajar con repositorios de DVM, consulte [Administración de un repositorio DVM](#).

Desduplicación en Rapid Recovery

La deduplicación es una técnica de compresión de datos que reduce tanto los requisitos de almacenamiento como los de carga de la red. El proceso implica almacenar físicamente bloques exclusivos de datos solo una vez en el disco. En Rapid Recovery, cuando cualquier bloque de datos exclusivo se produce por segunda vez en un repositorio, en lugar de almacenar los datos de nuevo, se almacena una referencia virtual de los datos.

La deduplicación se produce en las instantáneas de copia de seguridad capturadas por el Core de Rapid Recovery. La información de las copias de seguridad se deduplica en un repositorio único. No se puede deduplicar en varios repositorios.

La Rapid Recovery de Versión 6.0.2 utiliza la deduplicación basada en el destino en todos los repositorios DVM. En este modelo, la información se transfiere al repositorio DVM (el destino), y, a continuación, se deduplica desde el repositorio.

En su mayor parte, la deduplicación se lleva a cabo en línea (durante la transferencia de información de la copia de seguridad).

Para obtener las máximas ganancias, Rapid Recovery ahora también ofrece la deduplicación que se produce durante el postprocesamiento. El postprocesamiento se denomina a veces deduplicación de paso a través. Con este modelo, los datos en el repositorio se comparan con las referencias en la caché de datos DVM. Si un bloque de datos en el repositorio ya se ha guardado, cada incidencia adicional de datos se reemplaza por un puntero o una referencia a los datos.

Este postprocesamiento puede ahorrar espacio en el volumen de almacenamiento del repositorio, en particular si la caché de deduplicación estaba llena y, por tanto, la caché se incrementó para sacar partido de la deduplicación adicional. Este tipo de deduplicación se lleva a cabo al realizar un trabajo de optimización de repositorio. Esta función es exclusiva para los repositorios DVM, y también se denomina reclamación del bloque duplicado.

Para obtener más información sobre el trabajo de optimización de repositorio, consulte [Acerca de del trabajo de optimización de repositorio](#). Para obtener más información para realizar esta acción, consulte [Optimización de un repositorio DVM](#).

Por lo tanto, Rapid Recovery se puede beneficiar de todos los tipos de deduplicación que se describen aquí: la deduplicación basada en el destino, la deduplicación en línea y la deduplicación de postprocesamiento.

Para obtener más información acerca de dónde se almacenan las referencias a bloques exclusivos en repositorios DVM, consulte [Funcionamiento de la caché de deduplicación y las ubicaciones de almacenamiento](#).

Descripción de las claves de cifrado

Rapid Recovery Core puede cifrar los datos de instantáneas para todos los volúmenes dentro de un repositorio mediante claves de cifrado definidas y administradas desde la Core Console.

En lugar de cifrar todo el repositorio, Rapid Recovery le permite especificar una clave de cifrado para una o más máquinas protegidas en un único Rapid Recovery Core. Cada clave de cifrado activa crea un dominio de cifrado. No hay límite en el número de claves de cifrado que pueden crearse en el Core.

En un entorno de varios usuarios (cuando un solo Core aloja múltiples dominios de cifrado), los datos se particionan y deduplican en cada dominio de cifrado. Como resultado, Dell recomienda el uso de una sola clave de cifrado para varias máquinas protegidas si desea maximizar los beneficios de la deduplicación entre un conjunto de sistemas protegidas.

También puede compartir las claves de cifrado entre los Cores por medio de uno de estos tres métodos. El primer método es exportar una clave de cifrado como un archivo de un Rapid Recovery Core e importarlo a otro Core. El segundo método es archivar los datos protegidos con una clave de cifrado, y, a continuación, importar los datos archivados en otro Rapid Recovery Core. El tercer método es replicar los puntos de recuperación desde una máquina protegida mediante una clave de cifrado. Una vez que se han replicado las máquinas protegidas, las claves de cifrado que se utilizan en el Core de origen aparecen claves de cifrado replicadas en el Core de destino.

En todos los casos, las claves de cifrado aparecen en el Core con un estado Locked (Bloqueado) una vez que se han importado. Para acceder a los datos desde una clave de cifrado bloqueada, primero debe desbloquearla. Para obtener más información sobre la importación, exportación, bloqueo o desbloqueo de las claves de cifrado, consulte el tema [Administración de las claves de cifrado](#).

Los conceptos y consideraciones clave de la seguridad incluyen:

- El cifrado se realiza mediante el Estandar de cifrado avanzado (AES) de 256 bits en el modo Encadenamiento de bloques de cifrado (CBC) que cumple SHA-3.
- La deduplicación se ejecuta en el dominio de cifrado para garantizar la privacidad.
- El cifrado se realiza sin afectar al rendimiento.
- Puede aplicar una única clave de cifrado al número de máquinas protegidas que desee, pero una máquina protegida solo puede tener una clave de cifrado aplicada al mismo tiempo.
- Puede agregar, quitar, importar, exportar, modificar y eliminar las claves de cifrado que se han configurado en el Rapid Recovery Core.

⚠ PRECAUCIÓN: Rapid Recovery realiza una nueva instantánea siempre que aplique una clave de cifrado para una máquina protegida. También se activa una nueva instantánea después de desvincular una clave de cifrado para una máquina protegida.

Las claves de cifrado generadas desde la Rapid Recovery Core son archivos de texto que contienen cuatro parámetros, tal y como se describe en la tabla siguiente:

Tabla 1. Componentes de una clave de cifrado

Componente	Descripción
Name (Nombre)	Este valor es equivalente al nombre de clave establecidos cuando se agrega una clave en la Rapid Recovery Core Console.
Key (Clave)	Este parámetro se compone de 107 caracteres ingleses alfabéticos, numéricos y de operadores matemáticos generados aleatoriamente.
ID (Identificador)	El Identificador de clave se compone de 26 caracteres ingleses en mayúsculas y minúsculas generados aleatoriamente.
Comment (Comentario)	El comentario contiene el texto de la descripción de clave introducida cuando se creó la clave.

Replicación con Rapid Recovery

En esta sección se proporciona información de conceptos y procedimientos que le ayudará a entender y configurar la replicación en Rapid Recovery.

La replicación es el proceso de copia de puntos de recuperación del Core de Rapid Recovery y su transferencia a otro Core de Rapid Recovery con fines de recuperación tras desastres. El proceso requiere la existencia de una relación de emparejamiento origen-destino entre dos o más Cores.

El Core de origen copia los puntos de recuperación de los equipos protegidos seleccionados y, a continuación, transmite de forma asíncrona y continua los datos de la instantánea al Core de destino.

A menos que haya cambiado el comportamiento predeterminado al establecer un calendario de programación de replicación, el Core inicia un trabajo de replicación inmediatamente después de completar las instantáneas de las copias de seguridad, la comprobación de suma de comprobación, la comprobación de conectabilidad y los trabajos nocturnos. Para obtener más información, consulte [Programación de la replicación](#).

Para lograr una seguridad de los datos óptima, los administradores por lo general utilizan un Core de destino en un sitio de recuperación tras desastres remoto. Puede configurar la replicación de salida en un centro de datos de propiedad de la empresa o en un sitio de recuperación tras desastres remoto (es decir, un Core de destino administrado automáticamente). Otra opción es configurar la replicación de salida en un proveedor de servicio gestionado por terceros (MSP) o proveedor de Nube que aloja copias de seguridad y servicios de recuperación de desastres en una ubicación externa. Al replicar en un Core de destino de terceros, puede utilizar flujos de trabajo integrados que le permiten solicitar conexiones y recibir notificaciones de comentarios automáticas.

La replicación está gestionada por equipos protegidos. Se puede configurar cualquier equipo (o todos los equipos) protegido o replicado en un Core de origen para replicar en un Core de destino.

Estos son algunos de los posibles escenarios para replicación:

- **Replicación a una ubicación local.** El Core de destino está en un centro de datos local o una ubicación in situ, y la replicación se mantiene en todo momento. En esta configuración, la pérdida del Core no impediría una recuperación.
- **Replicación a una ubicación externa.** El Core de destino se ubica en un lugar externo de recuperación tras desastres remoto, en caso de pérdida.
- **Replicación mutua.** Dos centros de datos en dos ubicaciones distintas, cada una de ellas con un Core, y que son equipos de protección y sirven como copia de seguridad de recuperación externa entre sí, en caso de desastre. En este caso, cada Core replica los equipos protegidos en el Core que se encuentra en el otro centro de datos.
- **Replicación alojada y en nube.** Los socios de MSP de Rapid Recovery mantienen varios Cores de destino en un centro de datos o en una nube pública. En cada uno de estos Cores, el socio MSP permite a uno o más de sus clientes replicar puntos de recuperación desde un Core de origen del sitio del cliente en el Core del destino del MSP, siendo un servicio de pago.

① | NOTA: En esta situación, los clientes solo tienen acceso a sus propios datos.

Estas son algunas de las configuraciones posibles de replicación:

- **Replicación de punto a punto.** Replica uno o más equipos protegidos desde un Core de origen único a un Core de destino único.

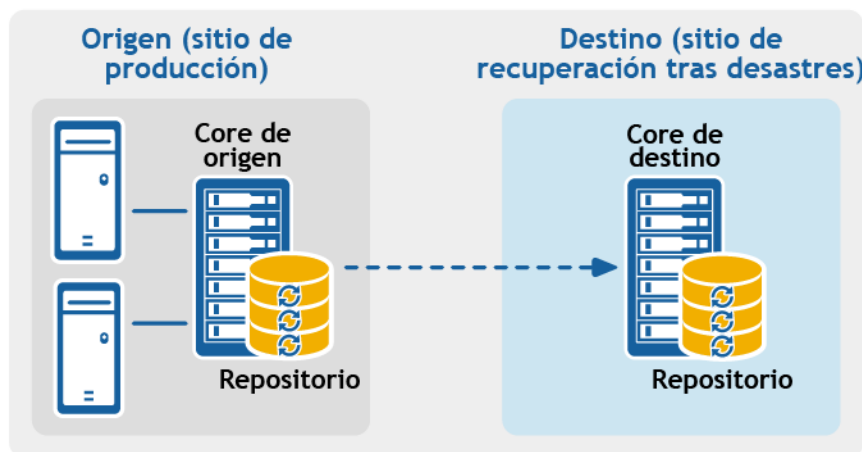


Ilustración 3. Configuración de la replicación de punto a punto

- **Replicación de multipunto a punto.** Replica los equipos protegidos de varios Cores de origen en un único Core de destino.

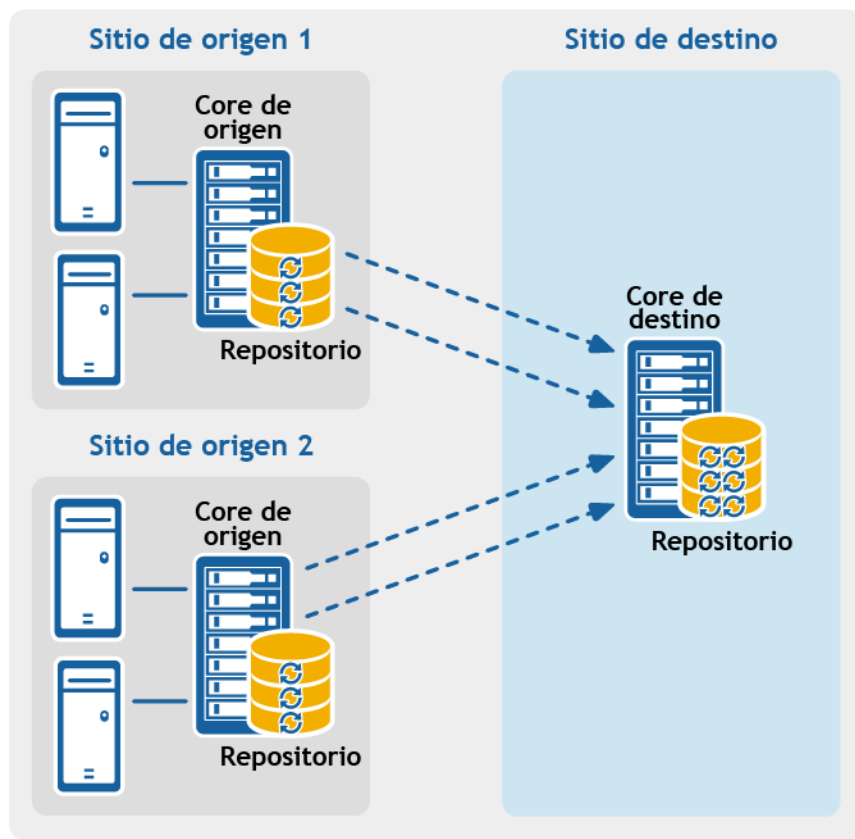


Ilustración 4. Configuración de la replicación de multipunto a punto.

- **Replicación de punto a multipunto.** Replica uno o más equipos protegidos desde un Core de origen único a más de un Core de destino.

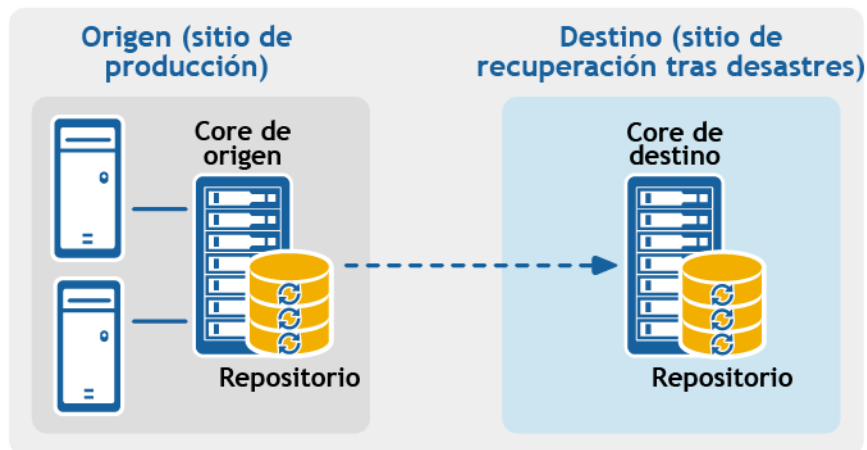


Ilustración 5. Configuración de la replicación de punto a multipunto

- **Replicación de salto múltiple.** Replica uno o más equipos protegidos desde un Core de destino a otro Core de destino, lo que produce opciones de conmutación por error o recuperación adicionales en el Core replicado.

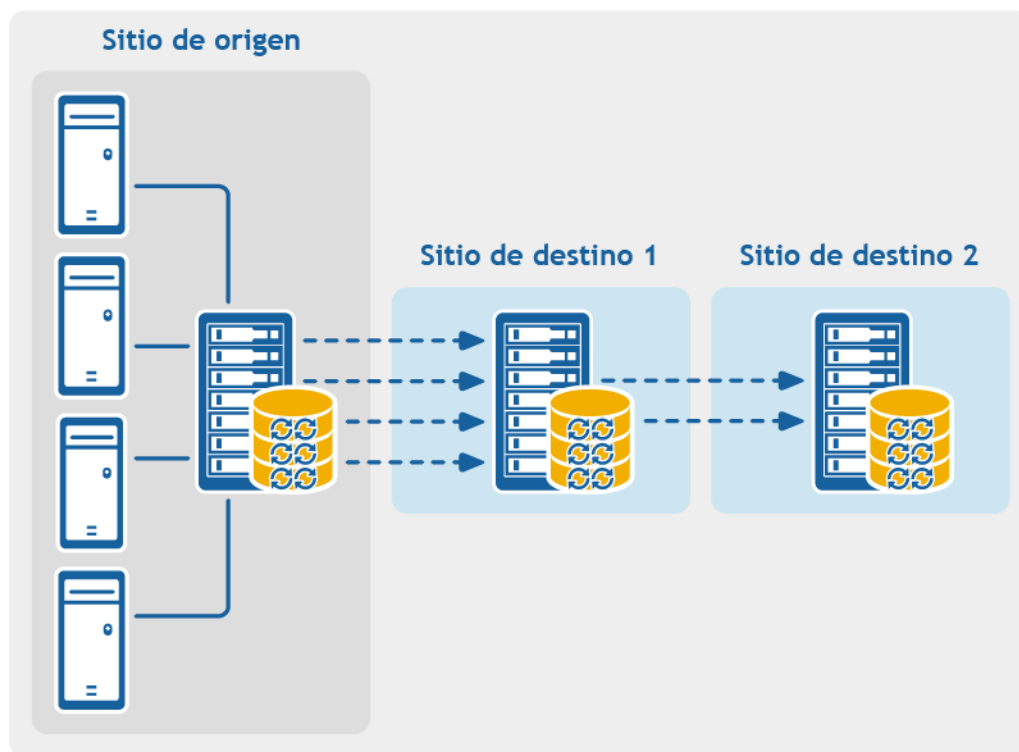


Ilustración 6. Configuración de replicación de salto múltiple

Si utiliza dispositivos de copia de seguridad de Dell Data Protection, como los de la serie DL1x00 o DL4x00, el Core de destino al que replique debe tener una licencia de software válida configurada. Estos dispositivos de hardware incluyen una licencia de destino de replicación con la compra. Compruebe la clave de licencia en el mensaje de correo electrónico de bienvenida que recibió cuando adquirió el dispositivo. Para obtener ayuda, visite el sitio web de Asistencia con las licencias en <https://support.software.dell.com/licensing-assistance> o envíe un correo electrónico a license@software.dell.com.

Retención y archivado

En el servidor, las políticas de copia de seguridad y retención son flexibles y, por tanto, fácilmente configurables. La capacidad de adaptar las políticas de retención a las necesidades de una organización no solo ayuda a cumplir los requisitos de cumplimiento sino que lo hace sin poner en peligro los RTO.

Las políticas de retención aplican los períodos durante los cuales las copias de seguridad se almacenan en medios a corto plazo (rápidos y caros). A veces, determinados requisitos empresariales y técnicos exigen ampliar la retención de estas copias de seguridad, pero el uso de almacenamiento rápido resulta inasequible. Por tanto, este requisito crea una necesidad de almacenamiento a largo plazo (lento y barato). Las empresas a menudo utilizan el almacenamiento a largo plazo para archivar tanto datos de cumplimiento como de no cumplimiento. La función de archivo se utiliza para admitir retenciones ampliadas de datos de cumplimiento y de no cumplimiento, y también se utiliza para inicializar los datos de replicación en un Core de destino.

Custom Retention Policy

☒ Enable Roll-up

Keep all Recovery Points for 3 Days ...

☒ ...and then keep one Recovery Point per hour for 3 Days ...

☒ ...and then keep one Recovery Point per day for 2 Days ...

☒ ...and then keep one Recovery Point per week for 4 Weeks ...

☒ ...and then keep one Recovery Point per month for 3 Months ...

☒ ...and then keep one Recovery Point per year for 1 Years ...

Newest Recovery Point: 5/16/2012

Resulting Retention Period

5/13/2012 | 5/10/2012 | 5/8/2012 | 4/10/2012 | 1/11/2012 | 1/11/2011

Oldest Recovery Point will be 1 year, 4 months, 6 days old

Ilustración 7. Custom Retention Policy (Política de retención personalizada)

En el servidor, las políticas de retención se pueden personalizar para especificar la duración de tiempo que se mantiene un punto de recuperación de copia de seguridad. Cuando la antigüedad de los puntos de recuperación se acerca al final de su período de retención, se quedan obsoletos y se quitan finalmente de la agrupación de retención. Normalmente, este proceso resulta ineficaz y acaba fallando, ya que la cantidad de datos y el período de retención empiezan a aumentar rápidamente. El servidor resuelve este problema de grandes datos administrando la retención de grandes cantidades de datos con políticas de retención complejas y realizando operaciones de mantenimiento periódico para datos con antigüedad mediante operaciones de metadatos eficaces.

Las copias de seguridad se pueden realizar con un intervalo de algunos minutos y a medida que estas copias de seguridad vayan envejeciendo a lo largo de los días, los meses y los años. Las políticas de retención administran el envejecimiento y la eliminación de las copias de seguridad antiguas. Un método de organización lineal simple define el proceso de antigüedad. Los niveles de organización lineal se definen en minutos, horas y días; semanas, meses y años. La política de retención es aplicada por el proceso de mantenimiento periódico nocturno.

Para el archivado a largo plazo, el servidor ofrece la posibilidad de crear un archivo del Core de origen y de destino en cualquier medio extraíble. El archivo se optimiza internamente y todos los datos del archivo se comprimen, cifran y deduplican. Si el tamaño total del archivo es superior al espacio disponible del medio extraíble, el archivo abarcará varios dispositivos en función del espacio disponible en el medio. El archivo también se puede bloquear con una frase de contraseña. La recuperación a partir de un archivo no requiere un nuevo Core; cualquier Core puede ingerir el archivo y recuperar los datos si el administrador tiene la frase de contraseña y las claves de cifrado.

Virtualización y nube

Core es compatible con la tecnología en nube, que le permite aprovechar la capacidad informática de la nube para recuperación.

El servidor puede exportar cualquier máquina protegida o replicada a una máquina virtual, como versiones con licencias de VMware o Hyper-V. Puede realizar una exportación virtual, o puede establecer una VM en espera virtual mediante el establecimiento de una exportación virtual continua. Con exportaciones continuas, la máquina virtual se actualiza de modo incremental después de cada instantánea. Las actualizaciones incrementales son muy rápidas y proporcionan clones en espera preparados para activarse con solo presionar un botón. Las exportaciones admitidas son tipos de máquina virtual VMware Workstation/Server en una carpeta, exportación directa a un host vSphere/VMware ESX (i); exportación a Oracle VirtualBox; y exportación a Microsoft Hyper-V Server en Windows Server 2008 (x64), 2008 R2, 2012 (x64) y 2012 R2 (incluido el soporte para VM Hyper-V de segunda generación)

Además, ahora puede archivar los datos del repositorio en la nube mediante plataformas como Microsoft Azure, Amazon S3, Rackspace Cloud Block Storage u otros servicios en la nube basados en OpenStack.

Administración de alertas y eventos

Además de HTTP REST API, el servidor también incluye un amplio conjunto de funciones para registro de eventos y notificación por correo electrónico, Syslog o Registro de eventos de Windows. Las notificaciones por correo electrónico pueden utilizarse para alertar a usuarios o grupos sobre la condición o estado de diferentes eventos en respuesta a una alerta. Los métodos Syslog y Registro de eventos de Windows se emplean para centralizar el registro en un repositorio en entornos con varios sistemas operativos; mientras que en entornos con Windows exclusivamente, solo se utiliza el Registro de eventos de Windows.

Portal de licencias

El Portal de licencias proporciona herramientas fáciles de usar para administrar los derechos de licencia. Puede descargar, activar, ver y administrar claves de licencia y crear un perfil de compañía para realizar un seguimiento de sus activos de licencia. Además, el portal permite a los proveedores de servicio y redistribuidores realizar un seguimiento y administrar sus licencias de cliente.

Consola web

Su dispositivo presenta una consola central basada en la web que administra Cores distribuidos desde una ubicación central. Los MSP y los clientes empresariales con varios Cores distribuidos pueden implementar la consola central para obtener una visión unificada de la administración central. La consola central permite la capacidad de organizar los núcleos administrados en unidades organizativas jerárquicas. Estas unidades jerárquicas pueden representar unidades de negocio, ubicaciones o clientes para MSP con acceso basado en la función. La consola central también puede ejecutar informes entre Cores administrados.

API de administración de servicios

El servidor incluye una API de administración de servicio y proporciona acceso programático a todas las funciones disponibles a través de la Central Management Console (Consola de administración central). La API de administración de servicio es una API de REST. Todas las operaciones de API se realizan sobre SSL y se autentican mutuamente mediante certificados X.509 v3. Se puede acceder al servicio de administración desde dentro del entorno o directamente a través de Internet desde cualquier aplicación que pueda enviar y recibir una solicitud y respuesta HTTPS. El enfoque facilita la fácil integración con aplicaciones web como herramientas de metodología de administración de relaciones (RMM) o sistemas de facturación. También se incluye un cliente de SDK para secuencias de comandos PowerShell.

Trabajar con el Core del Dispositivo DL

Descripción de la Core Console de Rapid Recovery

Esta sección describe los diversos elementos de la interfaz de usuario (IU) de la Core Console de Rapid Recovery.

Acceso a la Core Console de Rapid Recovery

Complete los pasos siguientes para acceder a la Core Console de Rapid Recovery.

- Realice una de las siguientes acciones para acceder a la Core Console de Rapid Recovery:
 - a Inicie sesión localmente en el servidor del Core de Rapid Recovery y haga doble clic en el icono Core Console.
 - b O bien, escriba una de las URL siguientes en el navegador web:
 - `https://<NombreServidorCore>:8006/apprecovery/admin/` o
 - `https://<DirecciónIPServidorCore>:8006/apprecovery/admin/`

NOTA: Como la interfaz de usuario de la Core Console de Rapid Recovery depende de JavaScript, el navegador web que utiliza para acceder a Core Console debe tener JavaScript habilitado.

Si ha cambiado el puerto predeterminado del servicio Rapid Recovery, actualice el puerto en la URL anterior según corresponda.

Comprensión de la Guía de inicio rápido

La Guía de inicio rápido es una función que indica un recorrido guiado de tareas sugeridas para configurar y utilizar el Core de Rapid Recovery.

La Guía de inicio rápido aparece automáticamente la primera vez que instala o actualiza el Core de Rapid Recovery y accede a la Core Console. Haga clic en **Iniciar guía** en la **página de bienvenida** para ver las distintas tareas de configuración sugeridas. Consulte la guía usando las opciones **Omitir paso** y **Atrás**. Cuando haya visto la última tarea sugerida, haga clic en **Finalizar** para cerrar la guía.

Puede volver a iniciar la guía de inicio rápido en cualquier momento desde el menú de ayuda de la Core Console. También puede optar por ocultar la página de **bienvenida** en la Guía de inicio rápido.

A no ser que la oculte, la Guía de inicio rápido aparece cada vez que inicia sesión en la Core Console de Rapid Recovery y que accede a la página **Inicio**. Para obtener más información, consulte [Cómo ocultar la Guía de inicio rápido](#).

No es necesario que realice los pasos sugeridos en la guía. Simplemente puede consultar las tareas sugeridas utilizando las opciones **Omitir paso** y **Atrás**. También puede ocultar la guía en cualquier momento y hacer clic en **Salir de la guía**.

Si elige realizar cualquier tarea de configuración sugerida en la Guía de inicio rápido, siga las indicaciones que aparecen en cualquier paso de la guía para mostrar el asistente o área correspondiente de la interfaz de usuario. Los procedimientos necesarios para completar todas las tareas sugeridas en la guía se describen en este documento, tal y como se indica en la siguiente tabla.

NOTA: No todos los usuarios necesitan realizar todas las tareas de configuración sugeridas en la Guía de inicio rápido. Debe entender qué tareas quiere cumplir según sus necesidades concretas.

La Guía de inicio rápido soluciona todas las siguientes tareas de configuración:

Tabla 2. Tareas de configuración de la Guía de inicio rápido

Función	Descripción corta	Resultado de seleccionar la tarea, enlace a procedimiento
Protección	Protección de un único equipo, protección de un clúster de servidor o protección de varios equipos usando la protección masiva	Haga clic en Proteger o seleccione Proteger equipo en el menú desplegable para abrir el Asistente para proteger un equipo. Para obtener más información sobre cómo completar el Asistente para proteger un equipo, consulte Cómo proteger una máquina. Seleccione Proteger clúster en el menú desplegable para abrir el cuadro de diálogo Conectarse al clúster. Para obtener más información sobre cómo proteger un clúster, consulte Protección de un clúster. Seleccione Protección masiva en el menú desplegable para abrir el Asistente para proteger varios equipos. Para obtener más información sobre cómo completar el Asistente para proteger varios equipos, consulte Acerca de la protección de varios equipos.
Replicación	Configuración de una replicación de un Core primario (origen) a uno secundario (destino)	Haga clic en Replicación para abrir la página Replicación. Le solicita que agregue un Core de destino mediante el asistente Replicación. Para obtener información sobre cómo usar el asistente Replicación para configurar la replicación en un Core administrado automáticamente, consulte Replicación a un Core de destino administrado automáticamente . Para obtener más información sobre la replicación, consulte Configuración de la replicación .
Exportación virtual	Realización de una exportación puntual o establecimiento de una exportación continua desde un equipo protegido a una máquina virtual	Haga clic en Exportar para realizar una exportación de datos de su equipo protegido a una máquina virtual. Puede realizar una única exportación puntual o establezca una espera virtual para la exportación continua a una máquina virtual. Para obtener información sobre la exportación virtual, consulte Información sobre la exportación a máquinas virtuales con Rapid Recovery .
Configuración	Le permite establecer la configuración adicional del Core de Rapid Recovery	Haga clic en Más para ver las funciones adicionales que puede configurar o administrar. Las funciones incluyen archivos comprimidos, montajes, CD de inicio, repositorios, claves de cifrado, cuentas de la nube, búsqueda de archivos, políticas de retención, notificaciones, informes, registros, etc.
Configuración: cifrado	Agregar o importar claves de cifrado que puede utilizar para uno o varios equipos protegidos	Haga clic en Claves de cifrado para gestionar la seguridad de los datos protegidos agregando o importando claves de cifrado. Puede aplicar claves de cifrado a uno o varios equipos protegidos. El cifrado se describe en el tema Descripción de las claves de cifrado .
Configuración: notificaciones	Configuración de las notificaciones para los eventos, advertencias y alertas.	Haga clic en Eventos para especificar grupos de notificación de eventos, advertencias y alertas. Para enviarlos por correo electrónico, también deberá establecer los ajustes del servidor SMTP. Para obtener más información sobre cómo administrar eventos, consulte el tema Eventos , incluidos los temas Configuración de grupos de notificación y Configuración de un servidor de correo electrónico .
Configuración: retención	Permite consultar o cambiar la política de retención predeterminada para el Core	Haga clic en Política de retención para abrir la página Política de retención para el Core. Desde aquí puede definir cuánto tiempo conservar un punto de recuperación antes de consolidarlo. Para obtener información sobre los conceptos de las políticas de retención, consulte el tema Administración de datos anteriores . Para obtener información sobre los procedimientos, consulte Administración de políticas de retención .
Restaurar	Restauración de datos desde un punto de recuperación del Core	Haga clic en Restaurar para abrir el Asistente para restaurar un equipo. Para obtener información sobre cómo restaurar datos, consulte el tema Restauración de volúmenes desde un punto de recuperación .

Cómo ocultar la Guía de inicio rápido

La Guía de inicio rápido aparece automáticamente la primera vez que instala o actualiza el Core de Rapid Recovery.

También aparece cuando selecciona Guía de inicio rápido en el menú desplegable Ayuda y cada vez que accede a la página Inicio de la Consola de Core.

Utilice el siguiente procedimiento para ocultar la Guía de inicio rápido.

- En la Core Console de Rapid Recovery, si está consultando la página **Bienvenido** de la Guía de inicio rápido, haga lo siguiente:
 - Si quiere ocultar la página **Bienvenido** de la Guía de inicio rápido, seleccione **No volver a mostrar**.

NOTA: Esta opción ocultará la página **Bienvenido** la próxima vez que se abra la Guía de inicio rápido y después hasta que actualice el Core de Rapid Recovery.

Si selecciona ocultar esta página y desea acceder a las opciones avanzadas de la función, seleccione **Atrás** en el asistente para ver esta página oculta.

- Si quiere ocultar la Guía de inicio rápido para esta sesión, a continuación haga clic en **Cerrar**.
Se cierra la Guía de inicio rápido. La siguiente vez que acceda a la página Inicio en la Consola de Core, volverá a aparecer la Guía de inicio rápido.

También puede abrir la Guía de inicio rápido desde el menú Ayuda.

- En cualquier página de la Guía de inicio rápido, haga clic en **Salir de la guía**.
Se cierra la Guía de inicio rápido. Aunque seleccione esta opción, podrá seguir abriendo la Guía de inicio rápido desde el menú Ayuda.

Desplazarse hasta la Rapid Recovery Core Console

Cuando inicia sesión en la Core Console y cada vez que hace clic en el icono **Inicio** , aparece la página **Inicio**. La página **Inicio** le brinda una vista del Core de Rapid Recovery con dos opciones. En el área de visualización principal, el contenido predeterminado es el nuevo panel del Core, que muestra un conjunto de informes en tiempo real en el sistema. Los informes predeterminados del panel incluyen el estado reciente del trabajo de transferencia, las transferencias por equipo, una descripción general del repositorio y el estado de la conectividad de equipos protegidos, replicados y con puntos de recuperación únicamente. También puede cambiar a la clásica vista Tablas de resumen. En esta vista, el título de la página muestra el nombre de visualización del Core de Rapid Recovery y puede ver tablas de resumen que muestran los equipos protegidos, repositorios y alertas recientes. Para obtener más información, consulte [Funcionamiento de la página Inicio \(vista de tablas de resumen\)](#) y [Comprensión del panel del Core](#), respectivamente.

En la página **Inicio** (y en cada página de la Core Console), el área de navegación de la izquierda muestra los elementos que están protegidos en el Core. Puede navegar a otras páginas en la IU mediante uno de estos procedimientos:

- Hacer clic en el icono correspondiente de la barra de iconos en el área de navegación de la izquierda. Las opciones a las que se puede acceder desde la barra de iconos incluyen Replicación, Servidor virtual en espera, Eventos, Configuración y Más.
- Expandir el menú  (Más) en la barra de iconos y, a continuación, seleccionar un destino
- Hacer clic en un botón u opción de menú de la barra de botones. Los botones incluyen Proteger, Restaurar, Archivar y Replicar.

Cuando selecciona un elemento en el área de navegación izquierda, el enfoque de la Core Console cambia para mostrar información de resumen sobre dicho elemento. Por ejemplo, si hace clic en el nombre de un equipo protegido, la Core Console muestra información únicamente sobre dicho equipo, en lugar de sobre el Core. En este ejemplo, el nombre de visualización del equipo protegido figura como el título de la página. Aparecerá un submenú a la derecha en el que puede ver información específica sobre el equipo protegido. Las opciones de menú incluyen: Resumen, Puntos de recuperación, Eventos, Configuración, Informes y Más.

Para volver a la visualización de la información sobre el Core, incluyendo los informes del panel o una vista de resumen de varios equipos protegidos o duplicados, haga clic en el icono **Inicio**  de la parte superior derecha de la UI. En la página **Inicio**, puede alternar entre la vista de panel y la de página de resumen haciendo clic en el enlace rojo de la parte superior derecha de la página.

Puede utilizar el título de la parte superior de la Core Console con el fin de proporcionar contexto para la información que está viendo en el Core. Por ejemplo:

- Cada vez que vea el nombre de visualización o la dirección IP del Core como título de la página, lo que está viendo es información de resumen del Core.
- Si el título es Panel, lo que ve es el panel del Core.
- Si aparece el nombre de visualización o la dirección IP de un equipo protegido, o un panel Resumen en la parte superior de una página, quiere decir que está viendo información acerca de un solo equipo protegido por o replicado en el Core.
- Si aparece el título Equipos protegidos, significa que se está viendo información acerca de todos los equipos protegidos en el Core de Rapid Recovery.
- Si aparece el título Equipos replicados de..., es que está viendo información sobre todos los equipos replicados en el Core de Rapid Recovery.
- Si aparece el título de página Solo puntos de recuperación, quiere decir que está viendo información acerca de todos los equipos con puntos de recuperación únicamente en este Core.

Para obtener información sobre las características y funciones disponibles en cada página, consulte la sección apropiada a continuación.

Para obtener más información sobre la visualización de equipos protegidos, consulte [Visualización del menú Equipos protegidos](#). Para obtener más información sobre la administración de equipos protegidos, consulte [Administración de equipos protegidos](#).

Para obtener más información sobre la visualización de equipos replicados, consulte [Visualización de la replicación entrante y saliente](#).

Para obtener más información sobre la visualización de equipos con puntos de recuperación únicamente, consulte [Visualización en el menú Solo puntos de recuperación](#)

Comprensión del área de navegación izquierda

El área de navegación izquierda aparece en Core Console, en el lado izquierdo de la interfaz de usuario. El contenido de esta área de navegación puede ser diferente según el tipo de objetos protegidos en el Core de Rapid Recovery.

El área de navegación izquierda siempre contiene lo siguiente:

- **Barra de iconos.** Para navegar entre las páginas principales de Core Console.
- **Filtro de texto.** El filtro de texto es un campo de texto que le permite filtrar los elementos que se muestran en los distintos menús que aparecen debajo del mismo. Al hacer clic en la flecha situada a la derecha del filtro de texto se expande y contrae cada uno de los menús que aparecen.

Al seguir estos elementos, el área de navegación izquierda muestra los menús para ayudarle a navegar, filtrar y ver los objetos protegidos en el Core. Esto incluye equipos protegidos y equipos replicados, entre otros.

Cada menú es contextual, es decir, el menú solo aparece en Core Console si es pertinente. Por ejemplo, si protege al menos un equipo, aparece el menú Equipos protegidos, y así sucesivamente.

Para obtener más información, consulte las tablas que figuran en el área de navegación de la izquierda [Visualización de la interfaz para el usuario de la Core Console](#).

Visualización de la página Inicio de la Core Console de Rapid Recovery

Cada vez que inicie sesión en la Core Console de Rapid Recovery, o cada vez que haga clic en el icono **Inicio**  de la barra de iconos, aparece la página **Inicio**.

La página **Inicio** de Core Console ofrece una nueva vista del **panel** y una vista conocida de las **tablas de resumen**. El panel es la vista predeterminada.

Puede alternar entre las vistas de la página **Inicio** al hacer clic en el vínculo rojo en la parte superior derecha de la página **Inicio**.

En la página Inicio, y cada dos páginas de Core Console, puede desplazarse hacia las funciones que desee utilizando el área de navegación izquierda.

Para obtener más información, consulte los siguientes temas:

- [Comprensión del área de navegación izquierda](#)
- [Comprensión del panel del Core](#)
- [Funcionamiento de la página Inicio \(vista de tablas de resumen\)](#)

Funcionamiento de la página Inicio (vista de tablas de resumen)

La página **Inicio** solo se aplica al Core. En la vista de panel, muestra informes gráficos en tiempo real. Cuando cambia a la vista Tablas de resumen, la página **Inicio** muestra todos los equipos o réplicas que protege el Core, los repositorios asociados al Core y las alertas para equipos de este Core.

La vista de cada panel en la página **Inicio** se puede ampliar o contraer. Por ejemplo, si hace clic en el icono  (contraer vista) que se encuentra en la parte superior derecha del panel Equipos protegidos, se contrae la vista de equipos protegidos y solo es visible el nombre del panel. Para expandir la vista para volver a ver todos los equipos protegidos, haga clic en el icono  (expandir vista).

La siguiente tabla describe los diversos elementos en la página **Inicio** cuando se encuentra en la vista de tablas de resumen.

Tabla 3. Opciones de la página Inicio

Elemento de la IU	Descripción
Equipos protegidos	El panel Equipos protegidos enumera los equipos que protege el Core. Este panel aparece independientemente de que se haya agregado algún equipo al Core para su protección o no. Esta sección incluye la siguiente información para cada equipo protegido: • Tipo de equipo. Un icono muestra si se trata de un equipo físico, de una máquina virtual o de un clúster protegido. • Estado. Los círculos de color en la columna Estado muestran si se puede acceder al equipo protegido, si se encuentra en pausa, fuera de línea o si no se puede contactar con él. • Nombre de visualización. El nombre que se muestra o la dirección IP del equipo protegido. • Nombre del repositorio. El nombre del repositorio que almacena los puntos de recuperación de ese equipo. • Última instantánea. La fecha y la hora a la que Rapid Recovery tomó la instantánea del punto de recuperación más reciente de ese equipo. • Puntos de recuperación. El número de puntos de recuperación almacenados en el repositorio y el uso de espacio para cada equipo protegido. • Versión. La versión del software Rapid Recovery Agent instalado en ese equipo. Si hace clic en un nombre de equipo específico que se muestra en este panel, aparece una página Resumen, que muestra la información de resumen del equipo seleccionado. Para obtener más información sobre lo que puede realizar en la página Resumen, consulte Visualización de información de resumen de un equipo protegido.
Equipos replicados	El panel Equipos replicados indica los equipos que este Core replica de otro Core. Este panel no aparece a menos que su Core replique equipos de otro Core. Esta sección incluye la siguiente información para cada equipo replicado: • Tipo de equipo. Un icono muestra si se trata de un equipo físico, de una máquina virtual o de un clúster protegido.

Elemento de la IU	Descripción
Equipos con puntos de recuperación únicamente	• Estado. Los círculos de color en la columna Estado muestran si se puede acceder al equipo replicado, si se encuentra en pausa, fuera de línea o si no se puede contactar con él. • Nombre de visualización. El nombre que se muestra o la dirección IP del equipo replicado. • Nombre de replicación. El nombre de visualización del Core de origen de los equipos que replica en este Core de destino. Puede definir este nombre cuando configure la replicación. • Nombre del repositorio. El nombre del repositorio que almacena los puntos de recuperación de ese equipo. • Última instantánea replicada. La fecha y la hora a la que Rapid Recovery realizó la réplica más reciente del equipo protegido original. • Puntos de recuperación. El número de puntos de recuperación almacenados en el repositorio y el uso de espacio para cada equipo replicado. • Versión. La versión del software Rapid Recovery Agent instalado en ese equipo. Si hace clic en un nombre de equipo específico que aparezca en este panel, se muestra la página Resumen, donde se enumera información de resumen de ese equipo replicado. El panel Equipos con puntos de recuperación únicamente enumera los equipos que muestran las máquinas que se retiran de la protección o replicación, si se han conservado los puntos de recuperación. Estos equipos pueden utilizarse para la recuperación a nivel de archivos, pero no pueden utilizarse para una recuperación completa bare metal, para restaurar volúmenes completos, o para agregar datos de instantáneas. Este panel no aparecerá a menos que tenga algún equipo que cumpla esta definición. Esta sección incluye la siguiente información para cada equipo con solo puntos de recuperación: • Tipo de equipo. Un icono muestra si se trata de un equipo físico, de una máquina virtual o de un clúster protegido. • Estado. Los círculos de color en la columna Estado muestran si se puede acceder al equipo con puntos de recuperación únicamente, si se encuentra en pausa, fuera de línea o si no se puede contactar con él. • Nombre de visualización. El nombre de visualización o dirección IP del equipo para el que mantuvo puntos de recuperación. • Nombre del repositorio. El nombre del repositorio que almacena el resto de puntos de recuperación de ese equipo. • Puntos de recuperación. El número de puntos de recuperación almacenados en el repositorio y el uso de espacio para cada equipo de puntos de recuperación únicamente. Si hace clic en un nombre de equipo específico que aparezca en este panel, se muestra la página Resumen para este equipo con puntos de recuperación únicamente.
Repositorios DVM	Este panel aparece para la configuración DL1000, independientemente de que se hayan creado repositorios DVM. Este panel no aparece a menos que el Core tenga uno o más repositorios DVM. Incluye la siguiente información para cada repositorio DVM: • Tipo. Un icono muestra un repositorio. • Estado. Los círculos coloreados en la columna Estado muestran si un repositorio está montado y puede aceptar transferencias de puntos de recuperación, o si no se puede contactar con él o tiene un estado de error. • Nombre del repositorio. El nombre de visualización del repositorio. • Uso del espacio. La cantidad total de espacio utilizado en el repositorio y el tamaño del volumen de almacenamiento o su ampliación. • Datos protegidos. La cantidad de espacio utilizada en el repositorio. • Equipos. El número de equipos para los que el repositorio almacena puntos de recuperación. • Puntos de recuperación. El número de puntos de recuperación almacenados en el repositorio. • Tasa de compresión. El índice al que el repositorio comprime los datos protegidos para ahorrar espacio. Para obtener más información, consulte Definición de los repositorios.

Elemento de la IU	Descripción
Alertas	Esta sección enumera las alertas importantes para el Core y cada equipo que protege. La sección incluye la siguiente información: • Iconos. La columna de iconos indica la naturaleza de la alerta. Estas alertas incluyen mensajes informativos y errores. • Fecha. Muestra la fecha y la hora a las que Rapid Recovery emitió la alerta. • Mensaje. Describe la alerta. También puede ver estos detalles en la página Eventos del Core. Para obtener más información, consulte Visualización de eventos mediante las tareas, las alertas y el diario.

Comprensión del panel del Core

El panel del Core muestra un conjunto de informes gráficos en tiempo real de datos relevantes para el Core y los equipos que protege. El panel incluye los siguientes informes:

- **Trabajo de transferencia.** Este informe muestra todas las transferencias de datos de instantáneas (incluidas las imágenes base e instantáneas incrementales) que se han completado en las últimas 24 horas. Las instantáneas incluyen imágenes base e instantáneas incrementales. Este informe del panel aparece como un gráfico de círculos.
- **Trabajo de transferencia por equipo.** Este trabajo indica, por equipo protegido, el número de operaciones correctas y trabajos de transferencia con fallos en las últimas 24 horas. Este informe del panel aparece como un gráfico de líneas.
- **Repositorio.** Este informe muestra los repositorios asociados con el Core. Muestra el número de repositorios, cuántos equipos están protegidos en cada uno, el número de puntos de recuperación y el porcentaje de compresión o deduplicación. Este informe se actualiza cada minuto.
- **Conectividad de equipo.** Este informe muestra el estado de la conectividad de los equipos protegidos y replicados en el Core. También muestra la conectividad de datos en [equipo con puntos de recuperación únicamente](#).

Puede contraer o ampliar la vista de los informes en el panel al hacer clic en la flecha hacia arriba o hacia abajo en el encabezado del informe. Algunos informes del panel (conectividad de equipo y de repositorio) tienen un signo más junto a la flecha, desde la que se puede agregar otro equipo protegido u otro repositorio, respectivamente.

También puede arrastrar y soltar para mover la ubicación de uno de los informes a otro lugar en el panel, para solicitar los informes de una forma más eficaz para su uso.

Visualización del menú Equipos protegidos

En la interfaz de usuario de Rapid Recovery, aparece un menú Equipos protegidos en el área de navegación izquierda. Al igual que con todas las etiquetas de menú en el área de navegación, la etiqueta de este menú aparece en todas las letras mayúsculas. Este menú está ampliado completamente de forma predeterminada, y muestra una lista de todos los equipos que están protegidos por este Core. Si tiene clústeres de servidores protegidos, estos también se incluyen en esta lista.

Puede contraer o ampliar la vista de cualquiera de estos equipos protegidos y clústeres de servidores en su Core haciendo clic en la fecha del lado izquierdo de este menú.

El menú Equipos protegidos incluye un menú desplegable en el lado derecho que muestra las funciones que se pueden realizar en todos los equipos protegidos. Haga clic en la flecha que aparece a la derecha de **Equipos protegidos** para ver el menú y realizar cualquiera de las siguientes acciones:

- Forzar una instantánea incremental de todos los equipos
- Forzar una imagen de base para todos los equipos
- Pausar la protección de todos los equipos (si la protección está activa)
- Reanudar la protección de todos los equipos (si la protección está en pausa)
- Actualizar los metadatos de todos los equipos protegidos
- Quitar la protección de todos los equipos en el Core

Todos los equipos que aparecen en el menú Equipos protegidos tienen un menú desplegable que controla las funciones de ese equipo exclusivamente. En el menú desplegable de cualquier equipo, puede realizar lo siguiente:

- Forzar una instantánea incremental del equipo seleccionado
- Pausar la protección del equipo seleccionado (si la protección está activa)
- Reanudar la protección (si la protección está en pausa)
- Actualizar metadatos
- Quitar la protección del equipo seleccionado en el Core
- Acceder a la página Resumen del equipo seleccionado
- Acceder a la página Puntos de recuperación del equipo seleccionado
- Acceder a la página Eventos del equipo seleccionado
- Acceder a la página Configuración del equipo seleccionado
- Generar informes específicos de ese equipo
- Acceder a más funciones específicas del equipo seleccionado, incluida información del sistema, montajes, política de retención, notificaciones o registro específico de un equipo
- Crear una etiqueta personalizada que se muestra en la lista Equipos protegidos

Si está gestionando clústeres de servidores desde el Core de Rapid Recovery, el clúster también aparece en el menú de navegación de la izquierda. En el menú desplegable de cualquier clúster, también puede:

- Acceder a la página **Nodos protegidos** del clúster seleccionado

Si hace clic en la flecha de la izquierda del menú Equipos protegidos, se contrae la lista de equipos protegidos y clústeres de servidores y dejan de mostrarse los equipos. Si vuelve a hacer clic en esta flecha, la lista de equipos vuelve a abrirse.

Si hace clic en cualquier nombre de equipo del menú Equipos protegidos, se abre la ficha Resumen de ese equipo. Para obtener más información sobre lo que puede realizar en la página Resumen, consulte [Visualización de información de resumen de un equipo protegido](#).

Por último, al hacer clic directamente en el menú **Equipos protegidos**, la página **Equipos protegidos** aparece en el área de contenido principal con un único panel que muestra los equipos protegidos en este Core. Para obtener más información sobre lo que puede hacer en el panel **Equipos protegidos** de la página Equipos protegidos, consulte [Visualización del panel de máquinas protegidas](#).

❗ NOTA: Desde la página Equipos protegidos, puede volver a una vista desde la perspectiva del Core haciendo clic en el icono Inicio de la barra de iconos.

Visualización de información de resumen de un equipo protegido

Si hace clic en el nombre de un equipo protegido en la Core Console, aparecerá la página **Resumen**. Esta página contiene, como mínimo, un panel [Resumen](#) y un panel [Volúmenes](#). Si se agrega un equipo a la replicación, también aparecerá un panel [Replicación](#).

Si dispone de uno o más servidores Exchange protegidos, también verá un panel [Información de Exchange Server](#), que contiene información sobre sus Exchange Servers protegidos.

Si dispone de uno o más SQL Servers protegidos, también verá un panel [Información de SQL Server](#), que contiene información sobre sus SQL Servers protegidos.

En la parte superior de esta página, hay un menú con acciones que puede realizar en el equipo protegido. Debajo, como mínimo, aparece un panel Resumen y un panel Volúmenes. Si se agrega un equipo a la replicación, también aparecerá un panel Replicación.

Cuando se muestra información de un equipo protegido (en la página Resumen y en el resto de vistas), aparece un menú situado en la parte superior de la página con las funciones que puede llevar a cabo. Dicho menú aparece justo debajo del nombre del equipo protegido.

Vínculos relacionados

- [Visualización en el panel Resumen](#)
- [Visualización de volúmenes en un equipo protegido](#)
- [Visualización de la información de replicación](#)
- [Visualización del panel Información de Exchange Server](#)
- [Visualización del panel Información de SQL Server](#)

Visualización en el panel Resumen

El panel **Resumen** contiene información de resumen sobre el equipo protegido, incluyendo el nombre de host, la fecha y la hora de la última instantánea, la fecha y la hora de la próxima instantánea programada, la información de la clave de cifrado y la información de la versión del software Rapid Recovery Agent. También existe un vínculo a una página detallada sobre información del sistema para el equipo.

Visualización de volúmenes en un equipo protegido

Puede realizar las siguientes acciones para cualquiera de los volúmenes enumerados desde la página Resumen en el panel Volúmenes para cualquier equipo protegido:

- Establecer o modificar una programación de protección de un volumen seleccionado. Las programaciones de protección se establecen normalmente cuando protege por primera vez un equipo. Para obtener más información sobre cómo modificar los calendarios de programación de protección, consulte [Modificación de los calendarios de programación de protección](#).
- Forzar una imagen base o instantánea. Las instantáneas se realizan normalmente en base a la programación de protección. Sin embargo, puede forzar la realización de una imagen base o una instantánea incremental de los volúmenes seleccionados siempre que quiera. Para obtener más información, consulte [Cómo forzar una instantánea](#).

Visualización de la información de replicación

El panel **Replicación** contiene información de resumen sobre el equipo replicado, incluidos el nombre de replicación, el estado de la replicación, el progreso y el espacio disponible.

Visualización del panel Información de Exchange Server

El panel **Información de Exchange Server** solo aparece en los equipos protegidos que son Exchange Server.

Este panel contiene información de resumen sobre el Exchange Server protegido, incluida la versión instalada de Microsoft Exchange, la ruta de acceso en la que está instalado Exchange y la ruta de acceso definida en los datos de correo de Exchange.

La cuadrícula de almacenes de correo muestra el nombre de la Base de datos de Exchange (EDB), la ruta de acceso del archivo EDB, la ruta de acceso en la que los archivos de registro están almacenados, el prefijo de registro, la ruta de acceso del sistema, el Grupo de disponibilidad de base de datos (DAG) y el tipo de almacén de correo.

Visualización del panel Información de SQL Server

El panel **Información de SQL Server** solo aparece para los equipos protegidos que sean servidores SQL Server.

Este panel contiene información de resumen sobre los servidores SQL Server protegidos. Puede ampliar la información de la base de datos para ver la información detallada de cada tabla en dicha base de datos. También puede ver la base de datos o el nombre de tabla y la ruta de acceso a la base de datos.

Visualización de los puntos de recuperación para un equipo

En la página Puntos de recuperación se muestra una lista de los puntos de recuperación recopilados para ese equipo protegido, así como los datos pertinentes de equipo y repositorio. En esta página puede montar, exportar y restaurar puntos de recuperación específicos, así como eliminar puntos de recuperación.

La pestaña se divide en dos paneles: resumen de puntos de recuperación y puntos de recuperación. El panel Resumen no incluye ningún vínculo para el usuario. Muestra los siguientes datos del equipo.

Tabla 4. Datos del panel Resumen de puntos de recuperación

Elemento de la IU	Descripción
Total de puntos de recuperación	El número de puntos de recuperación recopilados para este equipo protegido en particular.
Total de datos protegidos	La cantidad de datos de este equipo protegido que están almacenados en el repositorio.
Repositorio	El nombre del repositorio en el que Rapid Recovery almacena los puntos de recuperación de este equipo protegido.
Estado del repositorio	La barra de progreso muestra el porcentaje del espacio total utilizado en el repositorio. La cantidad de datos utilizada y el tamaño total del repositorio aparecen debajo de la barra de progreso.

Para obtener más información, consulte [Visualización del panel de máquinas protegidas](#).

Visualización de eventos de un equipo protegido

En la página **Eventos**, puede ver los trabajos que se han realizado o que están en curso en el equipo protegido que seleccionó. Los botones de la parte superior de la página le permiten navegar a listas de trabajos en cada una de las tres categorías de actividades:

- **Tareas.** Un trabajo que Rapid Recovery debe realizar para operar correctamente.
- **Alertas.** Una notificación relacionada con una tarea o evento que incluye errores y advertencias.
- **Diario.** Un compuesto de todas las tareas y alertas del equipo protegido.

La siguiente tabla incluye las descripciones de cada elemento de la página **Eventos**.

Tabla 5. Elementos de la página Eventos

Elemento de la IU	Descripción
Palabra clave de la búsqueda	Le permite buscar un elemento específico dentro de cada categoría. Solo disponible para tareas.
De	Para restringir los resultados, puede introducir una fecha en la que empezar la búsqueda. Solo disponible para tareas.
Hasta	Para restringir los resultados, puede introducir una fecha en la que detener la búsqueda. Solo disponible para tareas.
Iconos de estado	Cada icono representa un estado de trabajo diferente. En el caso de alertas y tareas, al hacer clic en uno de los iconos podrá filtrar la lista por ese estado, generando básicamente un informe. Al hacer clic en el icono una segunda vez elimina el filtro para ese estado. Puede filtrar por más de un estado. Los estados incluyen: • Activo. Un trabajo que está en curso. • En cola. Un trabajo que está esperando que otro trabajo finalice antes de poder iniciarse. • Esperando. Un trabajo que está esperando su aprobación o finalización, como una unidad de inicialización. (Para obtener más información acerca de las unidades de inicialización, consulte Replicación.) • Finalizado. Un trabajo que se ha realizado correctamente. • Con fallo. Un trabajo que ha fallado y no se completó.

Elemento de la IU	Descripción
Icono de servicio	Este botón agrega trabajos de servicios a la lista de trabajos. Cuando hace clic en este icono, aparece un icono de servicio más pequeño en cada icono de estado, que le permite filtrar por trabajos de servicio que tienen esos estados (si los hubiera). Los ejemplos de trabajos de servicios incluyen la eliminación de archivos de índice o retirar un equipo de la protección.
Lista desplegable Tipo de exportación	La lista desplegable incluye los formatos con los que puede exportar el informe del evento. Solo disponible para tareas. Incluye los siguientes formatos: • PDF • HTML • CSV • XLS • XLSX
 (icono Exportar)	Convierte el informe del evento al formato que seleccionó. Solo disponible para tareas.
Selección de página	Los informes de eventos pueden incluir varios trabajos en múltiples páginas. Los números y las flechas de la parte inferior de la página Eventos permiten navegar a las páginas adicionales del informe.

La página **Eventos** muestra todos los eventos de una tabla. La siguiente tabla enumera la información que se muestra para cada elemento.

Tabla 6. Información detallada para la tabla de resumen de los eventos

Elemento de la IU	Descripción
Estado	Muestra el estado de la tarea, alerta o el elemento diario. Está disponible para las alertas o los elementos diario; haga clic en el encabezado para filtrar los resultados por estado.
Nombre	Nombre está disponible solo para las tareas. Este campo de texto enumera el tipo de tarea que se ha completado para este equipo protegido. Algunos ejemplos incluyen la transferencia de volúmenes, el mantenimiento del repositorio, la consolidación, la realización de comprobaciones de la capacidad de montaje, la realización de comprobaciones de suma de comprobación, y así sucesivamente.
Hora de inicio	Disponible para las tareas, alertas y los elementos diario. Muestra la fecha y la hora en las que se inició el trabajo o la tarea.
Hora de finalización	Solo disponible para tareas. Muestra la fecha y la hora en las que se completó la tarea.
 Detalles del trabajo	Solo disponible para tareas. Se abre el cuadro de diálogo Supervisar tarea activa por lo que puede ver los detalles de un trabajo específico o una tarea. Estos detalles incluyen una ID para el trabajo, la velocidad a la que el Core transfirió los datos (si corresponde), el tiempo transcurrido para que el trabajo se complete, el trabajo total en cantidad de gigabytes y cualquier tarea secundaria relacionada con el trabajo.
Mensaje	Disponible para las alertas y los elementos diario. Este campo de texto proporciona un mensaje descriptivo de la alerta o el elemento diario.

Visualización de informes de un equipo protegido

El menú desplegable **Informes**  permite generar informes a petición para el equipo protegido seleccionado.

El informe de trabajos proporciona un informe del estado de trabajos correctos y de trabajos con fallos del equipo seleccionado. Los trabajos con fallos pueden verse más adelante en un informe de error. Para obtener más información sobre este tipo de informe, consulte [Descripción del informe de trabajo](#).

El informe de errores proporciona información sobre los trabajos del Core cancelados y con fallos del equipo especificado. Para obtener más información sobre este tipo de informe, consulte [Comprensión del informe de error](#).

Para obtener más información sobre cómo generar estos informes, consulte [Generación de un informe del Core a petición](#).

Visualización de equipos replicados en el menú de navegación

Si el Core replica equipos desde otro Core de Rapid Recovery, el nombre de visualización del Core de origen aparece como un menú que puede contraerse en el área de navegación izquierda de Core Console. Al igual que con todas etiquetas de menú del área de navegación, este nombre de menú de los equipos replicados aparece con todas las letras mayúsculas, debajo del menú Equipos protegidos. De manera predeterminada, el menú de los equipos replicados se expande completamente y muestra en una lista todos los equipos que derivan del Core de origen y que se replican en el Core de destino.

Puede contraer o expandir la vista de cualquiera de los equipos replicados del Core de origen haciendo clic en la fecha del lado izquierdo de este menú.

Cada menú de equipos replicados incluye un menú desplegable en el lado derecho que incluye las funciones que se pueden realizar de forma simultánea en todos los equipos replicados derivados de dicho Core. Haga clic en la flecha situada a la derecha del menú de equipos replicados para visualizar una lista desplegable de las funciones que puede realizar. Estas acciones incluyen lo siguiente:

- Realiza una pausa en la replicación. Si la replicación está activa en este momento, detiene la acción hasta que la reanuda.
- Reanuda la replicación. Si la replicación se ha puesto en pausa, comienza a replicar nuevamente.
- Forzar replicación. Replica a petición, en lugar de en una hora programada.
- Quitar replicación. Elimina la relación de replicación entre el Core de origen y el Core de destino. De forma opcional, puede eliminar los puntos de recuperación almacenados en este Core. Para obtener más información, consulte [Eliminación de replicación](#).

Si se hace clic directamente en el nombre del Core de origen en el menú de navegación, la página **Equipos replicados de [nombre del Core de origen]** aparece en el área de contenido principal. Para obtener más información sobre lo que puede realizar en dicha página, consulte [Visualización de la replicación entrante y saliente](#).

Vínculos relacionados

[Pausa y reanudación de la replicación](#)

[Forzado de la replicación](#)

[Eliminación de replicación](#)

Visualización en el menú Solo puntos de recuperación

El menú Solo puntos de recuperación aparece en el área de navegación izquierda si se cumple una de las siguientes condiciones:

- si su Core de Rapid Recovery conserva algunos puntos de recuperación de un equipo que estaba protegido previamente;
- si ha eliminado la replicación pero conserva los puntos de recuperación.

Al igual que con todas las etiquetas de menú del área de navegación, la etiqueta de este menú aparece en mayúsculas.

Puede contraer o ampliar la vista de los equipos con solo puntos de replicación haciendo clic en la fecha del lado izquierdo de este menú.

El menú incluye un menú desplegable en el lado derecho que muestra las funciones que se pueden realizar en todos los equipos solo con puntos de recuperación de forma simultánea. En este caso, la única función que puede realizar es eliminar puntos de recuperación desde el Core.

 **PRECAUCIÓN:** Esta acción elimina todos equipos con solo puntos de recuperación de su Core de Rapid Recovery, eliminándolos permanentemente y evitando que pueda restaurar información de esos puntos de recuperación desde este Core.

Visualización en el menú Grupos personalizados

El menú Grupos personalizados aparece en el área de navegación izquierda únicamente si ha definido uno o más grupos personalizados. Al igual que con todas las etiquetas de menú en el área de navegación, la etiqueta de este menú aparece en todas las letras mayúsculas.

Puede contraer o ampliar la vista de los elementos de este menú haciendo clic en la fecha del lado izquierdo de este menú.

El menú Grupos personalizados incluye un menú desplegable en el lado derecho que muestra las funciones que se pueden realizar de forma simultánea en todos los elementos parecidos de ese grupo.

Para obtener más información, consulte [Comprensión de los grupos personalizados](#).

Uso del cuadro de diálogo Error

Cuando se produce un error en la interfaz de usuario de la Core Console de Rapid Recovery, como al intentar introducir un parámetro no válido, se abre un cuadro de diálogo Error. El cuadro de diálogo normalmente indica la causa del error, incluye algunos vínculos para proporcionar más información sobre el error, e incluye un botón Cerrar. Debe cerrar el cuadro de diálogo Error antes de continuar, pero es posible que desee ver más información sobre el error.

En el cuadro de diálogo Error, seleccione entre las siguientes opciones:

Los errores de la interfaz de usuario que hacen que aparezca el cuadro de diálogo Error no se siguen en la pestaña Eventos de Rapid Recovery, ya que son simplemente errores de validación o de entrada de datos. Sin embargo, cuando hace clic en la opción Buscar base de conocimiento por cualquier error, el vínculo de URL que se proporciona para ese error se registra en el archivo CoreAppRecovery.log. Puede buscar en el registro la cadena de texto "KB article url generated" para ver la URL de cada error que se vio en un navegador. Para obtener más información sobre la descarga o visualización de registros de error del Core, consulte los temas [Descarga y visualización del archivo de registro del Core](#) o [Acceso a los registros del Core](#), respectivamente.

Configuración del Core

En esta sección se describe cómo gestionar y cambiar la configuración del Rapid Recovery Core desde el icono  Configuración.

Configuración del Core de Rapid Recovery

Los parámetros del Core de Rapid Recovery se configuran de forma predeterminada para obtener un rendimiento óptimo para la mayoría de los usuarios. Estos parámetros afectan al rendimiento del Core de Rapid Recovery o, en algunos casos, a la visualización de la

información en la Core Console de Rapid Recovery. Desde la barra de iconos, haga clic en  (Configuración) para acceder a la configuración del Core. Se mostrará a la izquierda una lista de todos los parámetros del Core. Puede hacer clic en el título de cualquiera de los valores de esta lista para saltar a la configuración completa de ese valor a la derecha. O bien, puede desplazarse hacia abajo a través de todos los parámetros del Core a la derecha para ver todas las opciones de configuración. Para obtener más información, consulte [Configuración del Core de Rapid Recovery](#).

También puede acceder a las herramientas del Core, por ejemplo, la visualización de un resumen de la información del sistema o la descarga de los archivos de registro del Core. Para obtener más información, consulte [Herramientas de nivel del Core](#).

La siguiente tabla describe el conjunto completo de parámetros del Core de Rapid Recovery que puede configurar.

Tabla 7. Opciones configurables del Core de Rapid Recovery

Parámetro de Configuración	Descripción
Configuración de copia de seguridad y restauración del Core	Rapid Recovery le permite realizar una copia de seguridad de los parámetros de configuración del Core en un archivo XML. Si tiene un archivo de copia de seguridad, puede utilizarlo para restaurar o migrar la configuración del Core. Para obtener más información acerca de cómo realizar una copia de seguridad y restauración de la configuración del Core, consulte Copia de seguridad y restauración de la configuración del Core.
General	La configuración general incluye las opciones de configuración que se aplican generalmente al Core de Rapid Recovery, incluyendo opciones de visualización y puertos para el servidor web y para el servicio Rapid Recovery. Para obtener más información acerca de la configuración general del Core de Rapid Recovery, incluyendo cómo configurar estos parámetros, consulte Configuración de los parámetros generales del Core.
Actualizaciones	Los parámetros de actualizaciones controlan el aspecto de la función Actualización automática, que comprueba si existen versiones actualizadas del software de Rapid Recovery. Para obtener más información acerca de la configuración para actualizar el Core de Rapid Recovery, incluyendo cómo configurar estos parámetros, consulte Configuración de los parámetros de actualización.
Trabajos nocturnos	La configuración de Trabajos nocturnos son tareas automatizadas que realiza el Core diariamente. Puede configurar la hora en la que comienzan los trabajos y qué trabajos se realizan. Dell recomienda programar los trabajos fuera de las horas laborales normales para reducir la carga en el sistema cuando la demanda de recursos es alta. Para obtener más información, consulte Descripción de los trabajos nocturnos, Configuración de trabajos nocturnos para el Core y Personalización de las tareas nocturnas de una máquina protegida.
Cola de transferencia	La configuración de Cola de transferencia controla el número de veces que se intentan las operaciones de transferencia si los trabajos fallan debido a la no disponibilidad de los recursos. Puede establecer el número máximo de transferencias simultáneas y el número máximo de reintentos para transferir datos. Para obtener más información acerca de la configuración de la cola de transferencia, consulte Modificación de la configuración de la cola de transferencias.
Tiempo de espera del cliente	La configuración de tiempo de espera del cliente determina la cantidad de tiempo que ha de transcurrir antes que se intenten esas solicitudes de conexión específicas u operaciones de lectura y escritura antes de que se agote el tiempo de espera. Para obtener más información acerca de la configuración del tiempo de espera del cliente, consulte Ajuste de la configuración del tiempo de espera de clientes.
Caché de deduplicación de DVM	La deduplicación garantiza que bloques únicos de información se almacenan solo una vez en su repositorio, creando referencias a bloques de datos repetidos. Las referencias se almacenan en una caché de deduplicación. Si se utilizan claves de cifrado, la deduplicación se produce dentro de cada dominio de cifrado. La configuración de la caché de deduplicación de DVM le permite configurar el tamaño y especificar las ubicaciones para la caché principal y secundaria, así como la ubicación de la caché de metadatos. Para obtener más información acerca de la caché de deduplicación, consulte Funcionamiento de la caché de deduplicación y las ubicaciones de almacenamiento. Para obtener más información sobre el ajuste de los parámetros, consulte Configuración de los valores de caché de la deduplicación de DVM.
Replay Engine	La configuración de Replay Engine controla la información relacionada con el canal de comunicación de Replay Engine, como las direcciones IP y los valores de tiempo, para ayudar a ajustar el rendimiento específico a sus necesidades de red. Para obtener más información acerca de la configuración del motor para Rapid Recovery, consulte Configuración de los parámetros del motor de Replay.

Parámetro de Configuración	Descripción
Implementar	Los parámetros de implementación le permiten establecer las opciones para implementar el software de Rapid Recovery Agent desde su Core en los equipos que desea proteger. Para obtener más información acerca de la configuración de los parámetros de implementación, consulte Configuración de los parámetros de implementación.
Conexión de base de datos	Rapid Recovery almacena la información de transacciones en una base de datos de servicio MongoDB que se instala localmente de forma predeterminada en el equipo del Core. Puede configurar estos parámetros para cambiar la cantidad de tiempo que se retiene la información en la base de datos, o para cambiar el tamaño del grupo de conexión para permitir más o menos conexiones simultáneas. Para obtener más información acerca del establecimiento o modificación de parámetros de conexión de bases de datos para la base de datos de servicio, consulte Configuración de los parámetros de conexión con la base de datos.
Base de datos local	Rapid Recovery muestra información sobre las tareas, eventos y alertas del Core en la página Eventos. Rapid Recovery almacena esta información de transacciones en una base de datos de servicio MongoDB que se instala localmente en el mismo equipo que el Core de Rapid Recovery. Puede configurar la información de credenciales (nombre de usuario y contraseña) para la base de datos de servicio MongoDB utilizando los parámetros de la base de datos local. Para obtener más información acerca de cómo ajustar la configuración de la base de datos local, consulte Modificación de la configuración de la conexión con la base de datos local.
Servidor SMTP	Configure los parámetros del servidor de protocolo sencillo de transferencia de correo (SMTP) para el Core, también podrá enviar la información de eventos del Core por correo electrónico. Para obtener más información acerca de la configuración de un servidor de correo electrónico SMTP, consulte Configuración de un servidor de correo electrónico. i NOTA: Para enviar información de eventos por correo electrónico, también deberá configurar los parámetros del grupo de notificación. Para obtener más información sobre cómo especificar eventos para recibir alertas de correo electrónico, consulte Configuración de grupos de notificación.
Configuración de nube	Los valores de Configuración de nube permiten especificar los valores de la configuración de las cuentas de almacenamiento en la nube compatibles. Estos parámetros no crean cuentas de nube. En su lugar, asocian las cuentas de almacenamiento en nube existentes con el Core de Rapid Recovery con el fin de facilitar acciones como el archivado de información de Rapid Recovery. Para obtener más información acerca de la administración de la información de cuentas de almacenamiento en la nube en el Core de Rapid Recovery, consulte Administración de cuentas de nube.
Informes	La configuración de informes incluye un único parámetro de configuración que le permite seleccionar el tipo de letra que se utiliza cuando se genera un informe a partir del Core de Rapid Recovery. Para obtener más información acerca de cómo cambiar la configuración de los informes, consulte Administración de la configuración de informes.
Conectabilidad	Los valores de conectabilidad le permiten especificar si llevar a cabo las comprobaciones de capacidad de conectabilidad de SQL en el equipo protegido, o si utilizar la instancia de SQL Server en el Core. Si se especifica SQL en el Core, deberá proporcionar la información de las credenciales. Para obtener más información acerca de cómo administrar la configuración de conectabilidad para el Core, consulte Administración de la configuración de conectabilidad de SQL del Core.
Trabajos	Los trabajos del Core se crean automáticamente cada vez que inicia operaciones como la replicación. Puede especificar la configuración de cada trabajo mediante la configuración del Core de los trabajos.

Parámetro de Configuración	Descripción
	Puede configurar el número de trabajos que hay que ejecutar a la vez. En caso de que se produzcan errores de red o de comunicación que eviten que se complete un trabajo la primera vez, puede establecer el número de veces que se debe intentar realizar un trabajo a través de la opción Recuento de intentos. Para obtener información acerca de los trabajos del Core, qué trabajos están disponibles y cómo configurarlos, consulte Configuración de trabajo de Core.
Licencias	Desde la Core Console, Rapid Recovery le permite cambiar la licencia asociada con su Core, limitar el número de instantáneas diarias, ver la información del grupo de licencias y ponerse en contacto con el servidor de licencias. Para obtener más información acerca de cómo administrar licencias desde el Core, consulte Administración de licencias. Para obtener más información acerca de la administración de licencias, consulte la guía Dell Data Protection Portal de licencias de Rapid Recovery. NOTA: El Dell Data Protection Portal de licencias de Rapid Recovery tiene un ciclo de publicación diferente al del software de Rapid Recovery. Para obtener la documentación del producto más reciente, consulte el sitio Web de documentación técnica de Dell.
Configuración de SNMP	Simple Network Management Protocol (SNMP) es un protocolo para administrar dispositivos en un red IP. Puede configurar el Core de Rapid Recovery como un agente SNMP. El Core puede informar sobre alertas, estado de repositorios y equipos protegidos. Para obtener más información acerca de cómo utilizar SNMP con Rapid Recovery, consulte Comprensión de la configuración de SNMP.
vSphere	La configuración del Core de vSphere se aplica solo a los usuarios de la protección sin agentes de las máquinas virtuales. Si se utiliza un host vSphere, estos valores incluyen las opciones de conexión que se aplican a las máquinas virtuales. Para obtener más información acerca de la configuración de vSphere para la protección sin agente de VMware o ESXi, consulte Configuración de los valores de vSphere.
Cargas de registros	Si esta opción se establece en Sí, el Rapid Recovery Core cargará los archivos de registro con el fin de que Dell los analice y así poder mejorar la calidad general del producto. Esta configuración es opcional.

Configuración de los parámetros generales del Core

La configuración general del Core de Rapid Recovery incluye el nombre de visualización del Core, el puerto del servidor web, el puerto de servicio y la configuración regional (el idioma de visualización de la Core Console).

- Desplácese hasta la Core Console de Rapid Recovery.
- En la barra de iconos, haga clic en  (Configuración) y, a continuación, lleve a cabo una de las acciones siguientes:
 - En la lista de configuración del Core, en el lado izquierdo de la página Configuración, haga clic en **General**.
 - Desplácese hacia abajo en el lado derecho de la página Configuración hasta poder ver el encabezado General. Se mostrará la configuración General del Core.
- Haga clic en la configuración general que desea cambiar. La configuración seleccionada se convierte en editable, como un campo de texto o un menú desplegable.
- Introduzca la información de configuración según se describe en la tabla siguiente.

Tabla 8. Información de configuración general

Cuadro de texto	Descripción
Nombre mostrado	Introduzca un nombre de visualización nuevo para el Core. Es el nombre que aparecerá en la Core Console de Rapid Recovery. Puede introducir hasta 64 caracteres.
Puerto del servidor Web	Introduzca un número de puerto para el servidor Web. El puerto predeterminado es 8006.
Puerto de servicio	Introduzca un número de puerto para el servicio Core de Rapid Recovery. El puerto predeterminado es 8006.
Configuración regional	En la lista desplegable Configuración regional, seleccione el idioma que desea mostrar. Puede elegir entre inglés, francés, alemán, japonés, coreano, portugués, chino simplificado y español.

NOTA: Si cambia el idioma, confirme el mensaje que indica que el servicio Core de Rapid Recovery debe reiniciarse antes de que el idioma actualizado se pueda mostrar en la Core Console. Puede reiniciar este servicio a partir del Administrador de tareas de Windows.

- 5 Para cada configuración, una vez esté satisfecho con los cambios, haga clic en  para guardar los cambios y salir del modo de edición o haga clic en  para salir del modo edición sin guardar.

Configuración de los parámetros de actualización

Rapid Recovery incluye la función Actualización automática. Al instalar el Core de Rapid Recovery, puede elegir si desea actualizar automáticamente el software del Core de Rapid Recovery cuando haya nuevas actualizaciones disponibles y la frecuencia con la que el sistema debe buscarlas.

Los números de versión de Rapid Recovery, normalmente, incluyen cuatro fragmentos de información, separados por puntos decimales: el número de la versión primaria, el número de la versión secundaria, el número de revisión y el número de compilación. Por ejemplo, el primer nombre de la versión de Rapid Recovery era 6.0.1.609. La versión siguiente era 6.0.2.142.

La función de actualización automática compara todos los dígitos de un número de versión. Si activa la actualización automática, el software del Core solo se actualiza sin intervención cuando los números de la versión primaria y secundaria son idénticos. Por ejemplo, la actualización automática se iniciaría de la versión del Core 6.0.1.609 a la 6.0.2.142 (ambas empiezan por 6.0). En el mismo equipo, el Core no se actualizaría automáticamente de 6.0.2.142 a 6.1.1.XXX, porque los dígitos siguientes al primer decimal no son iguales. En su lugar, aparecerá una notificación (en un banner en la parte superior de la Core Console) de que hay una actualización del software del Core disponible. Esta notificación le da la oportunidad de consultar las notas de la versión y determinar si actualizar el software a la última versión del Core es adecuado para sus necesidades.

NOTA: Para obtener información sobre cómo instalar el software del Core de Rapid Recovery, consulte la *Installation and Upgrade Guide (Guía de instalación y actualización)* de Dell Data Protection | Rapid Recovery.

Puede ver y cambiar los ajustes que utiliza el sistema para buscar actualizaciones en cualquier momento.

PRECAUCIÓN: Cuando utilice la replicación, la configuración de su sistema para instalar las actualizaciones automáticamente puede dar como resultado la actualización de su Core de origen antes que el Core de destino, lo que puede provocar fallos de replicación o la imposibilidad de configurar nuevas replicaciones entre Cores. Para los usuarios de la replicación, Dell recomienda que los administradores apliquen actualizaciones automáticas únicamente en el Core de destino, y luego actualizar manualmente el Core de origen, actualizando por último los equipos protegidos.

Complete los pasos de este procedimiento para configurar los ajustes de actualización.

- Desplácese hasta la Core Console de Rapid Recovery.
- En la barra de iconos, haga clic en  (Configuración) y, a continuación, realice una de las acciones siguientes:

- En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Actualizaciones**.
 - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Actualizaciones.
Aparece la configuración del Core de Actualizaciones.
- 3 Haga clic en la opción que desee cambiar.
La opción seleccionada se volverá editable.
- 4 Introduzca la información de configuración según se describe en la tabla siguiente.

Tabla 9. Información de configuración de actualizaciones

Cuadro de texto	Descripción
Comprobar nuevas actualizaciones	Seleccione la frecuencia con la que Rapid Recovery debe buscar e instalar actualizaciones. Puede seleccionar las opciones siguientes: • Nunca • Diariamente • Semanalmente • Mensualmente Si elige las actualizaciones automáticas, una vez que se supere el umbral temporal, si hay una actualización disponible, la función se instalará cuando se hayan completado los trabajos nocturnos.
Instalar actualizaciones	Especifique cómo se administran las actualizaciones disponibles eligiendo una de las siguientes opciones: • No buscar actualizaciones • Notificarme las actualizaciones, pero no instalar automáticamente • Instalar automáticamente actualizaciones
Estado	El estado indica si hay nuevas actualizaciones disponibles.
Última comprobación	El campo Última comprobación indica la fecha y la hora a la que se comprobó por última vez si había actualizaciones. Haga clic en Comprobar ahora para verificar inmediatamente si hay disponible una actualización de software. Esta comprobación se produce independientemente de la frecuencia que haya establecido.

- 5 Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en  para guardar los cambios y salir del modo edición, o haga clic en  para salir del modo sin guardar.

Descripción de los trabajos nocturnos

Los trabajos nocturnos son tareas automatizadas diarias que se producen en un momento determinado fuera del horario laboral normal. Estos trabajos exigen más memoria e incluyen varias comprobaciones de integridad y consolidación de datos que se realizan de forma óptica cuando el Rapid Recovery Core es menos activo.

Todos los trabajos nocturnos, así como su alcance de aplicación, se describen en la tabla siguiente. Los trabajos nocturnos pueden administrarse en el Core (que se aplica a todas las máquinas protegidas en el Core). Estos trabajos nocturnos también pueden aplicarse a un alcance en la lista de máquinas protegidas como "Máquina protegida".

Tabla 10. Información de los trabajos nocturnos

Nombre del trabajo	Alcance	Descripción
 Cambiar	N/A	Este control abre el cuadro de diálogo Nightly Jobs (Trabajos nocturnos), donde puede activar, desactivar o cambiar los valores de cada trabajo nocturno.
Hora de trabajos nocturnos	Todos	Este valor representa el tiempo de inicio de la ejecución de los trabajos nocturnos. Dell recomienda configurar el Core para ejecutar los trabajos nocturnos durante una hora de baja actividad. La hora predeterminada es 12:00
Rollup	Core o máquina protegida	Aplica la política de retención a los datos de su copia de seguridad mediante la combinación o "agregación" de puntos de recuperación en el programa establecido en la política. Puede personalizar la política en el Core, que se aplica de forma predeterminada a todas las máquinas protegidas. De manera predeterminada, el trabajo de agregación ejecuta el trabajo para todo el Core; o haga clic en  para definir las máquinas protegidas que se agregarán según la política de Core. Para obtener más información sobre cómo utilizar una política de retención en una máquina protegida que difiere de la política predeterminada establecida en el Core, consulte Personalización de la configuración de la política de retención de una máquina protegida .
Compruebe la capacidad de conexión de las bases de datos SQL	Máquina protegida	Comprueba la integridad de los puntos de recuperación que contienen las bases de datos SQL. Proceso: • Montar el punto de recuperación para los grupos de protección que contienen la bases de datos. • Conectarse a la base de datos desde el SQL Server. • Abrir la base de datos. • Cerrar la base de datos. • Desmontar el punto de recuperación. Para activar esta verificación nocturna, especifique un instancia de SQL Server que se utilizará para realizar las pruebas de conexión de las bases de datos de SQL Server en las máquinas protegidas.
 NOTA: Esta opción no aparece si no está protegiendo un SQL Server en su Core.		
Descargar registros de máquinas protegidas	Core	Descarga los registros de las máquinas protegidas en el Core, de forma que se puedan enviar a un servidor de registro.
Consolidar instantáneas de VMware para las máquinas virtuales protegidas	Core o máquina protegida	Este trabajo nocturno es relevante si utiliza API de VMware nativas para proteger máquinas sin el software Rapid Recovery Agent. Debe consolidar periódicamente las instantáneas de VMware. La activación de esta trabajo nocturno le permite realizar estas consolidaciones de forma diaria. Este trabajo nocturno contiene un parámetro (Consolidaciones simultáneas máximas), que debe establecerse a un número entre 1 y 100.
Verificar la integridad de los puntos de recuperación	Core o máquina protegida	Comprueba la integridad de los puntos de recuperación para cada máquina protegida. De manera predeterminada, la opción <code>Check integrity of recovery points</code> no está activada. Proceso: • Montar el punto de recuperación para cada grupo de protección. • Enumerar los archivos y carpetas para cada volumen. • Examina los puntos de recuperación para verificar que son válidos.

Nombre del trabajo	Alcance	Descripción
		Desmontar el punto de recuperación.
Comprobar la suma de comprobación de las bases de datos de Exchange	Máquina protegida	Comprueba la integridad de los puntos de recuperación que contiene archivos de base de datos Exchange (EDB). ① NOTA: Esta opción no aparece si no está protegiendo un Exchange Server en su Core.
Truncar registros SQL (sólo para el modelo de recuperación simple)	Máquina protegida	Mantiene el tamaño de los registros de SQL Server truncando el registro de transacciones de base de datos para que coincida con el último punto de recuperación. ① NOTA: Esta opción no aparece si no está protegiendo un SQL Server en su Core.
Truncar registros de Exchange	Máquina protegida	Mantiene el tamaño de los registros de Exchange, truncando el registro de transacciones de la base de datos Exchange para que coincida con el último punto de recuperación. ① NOTA: Esta opción no aparece si no están protegiendo un servidor Exchange en el Core.
Registrar estadísticas del repositorio	Core	Envía estadísticas del repositorio a un servidor de registro.
Eliminar eventos y trabajos antiguos	Core	Elimina los eventos antiguos para mantener la escala de la base de datos de eventos. El número de días es configurable (el valor predeterminado es 30 días).

Configuración de trabajos nocturnos para el Core

Quando se activa una opción de trabajo nocturno en el Core de Rapid Recovery, el trabajo seleccionado se ejecuta una vez al día a la hora especificada en todos los equipos que están protegidos por el Core. A la inversa, si desactiva cualquier trabajo nocturno a nivel del Core, el trabajo especificado ya no se ejecuta para todos los equipos que están protegidos por el Core.

① | NOTA: Si el ámbito de un trabajo nocturno, tal como se describe en el tema [Descripción de los trabajos nocturnos](#), incluye equipos protegidos, puede configurar ese trabajo nocturno únicamente para uno o más equipos protegidos específicos de forma individual. Para obtener más información sobre la aplicación de parámetros de trabajos nocturnos específicos para equipos protegidos, consulte [Personalización de las tareas nocturnas de una máquina protegida](#).

Debido a que los trabajos nocturnos utilizan gran cantidad de memoria, Dell recomienda configurar el Core para ejecutarlos durante un periodo de baja actividad. La programación predeterminada para la ejecución de trabajos nocturnos es las 12:00 am. Si alguna otra hora es más adecuada, cambie este parámetro en el campo Hora de trabajos nocturnos utilizando este procedimiento.

- Desplácese hasta la Core Console de Rapid Recovery.
- En la barra de iconos, haga clic en  (Configuración) y, a continuación, realice una de las acciones siguientes:
 - En la lista de configuración del Core del lado izquierdo de la página **Configuración** haga clic en **Trabajos nocturnos**.
 - Desplácese hacia abajo en el lado derecho de la página **Configuración** hasta que pueda ver el encabezado Trabajos nocturnos. Aparece la configuración del Core de Trabajos nocturnos.
- Para cambiar cualquier trabajo nocturno o para cambiar la hora a la que empiezan a ejecutarse los trabajos nocturnos, haga clic en  **Cambiar**.
Se abrirá el cuadro de diálogo **Trabajos nocturnos**.
- Si desea cambiar la hora de ejecución de los trabajos nocturnos, introduzca una nueva hora en el cuadro de texto **Horas de trabajos nocturnos**.

- 5 En la primera columna, haga clic para seleccionar cada opción de los trabajos nocturnos que desee configurar para el Core. Haga clic en cualquier opción seleccionada para borrarla.
- 6 Haga clic en **Aceptar**.
El cuadro de diálogo **Trabajos nocturnos** se cerrará y su configuración de trabajos nocturnos para el Core se guardará.

Modificación de la configuración de la cola de transferencias

La configuración de la cola de transferencias son ajustes a nivel de Core que establecen el número máximo de transferencias simultáneas y el número máximo de reintentos para transferir datos.

Complete los pasos de este procedimiento para modificar la configuración de la cola de transferencias.

- 1 Desplácese hasta la Core Console de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Configuración) y, a continuación, realice una de las acciones siguientes:
 - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Cola de transferencia**.
 - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Cola de transferencia. Aparece la configuración del Core de la cola de transferencias.
- 3 Haga clic en la opción que desee cambiar.
La opción seleccionada se volverá editable.
- 4 Introduzca la información de configuración según se describe en la tabla siguiente.

Tabla 11. Información de configuración de la cola de transferencias

Cuadro de texto	Descripción
Número máximo de transferencias simultáneas	Introduzca un valor para actualizar el número de transferencias simultáneas. Establezca un número del 1 al 60. Cuanto más pequeño sea el número, más pequeña será la carga en la red y en otros recursos del sistema. Conforme el número de Agents procesados aumenta, también lo hace la carga en el sistema.
Número máximo de reintentos	Introduzca un valor para establecer el número máximo de intentos antes de que la operación de transferencia se cancele. Establezca un número del 1 al 60.

- 5 Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en  para guardar el cambio y salir del modo edición, o haga clic en  para salir del modo edición sin guardar.

Ajuste de la configuración del tiempo de espera de clientes

La configuración del tiempo de espera de clientes controla la cantidad de tiempo en las que se intentan varias operaciones antes de que se agote el tiempo de espera.

NOTA: Dell recomienda no alterar la configuración predeterminada del tiempo de espera a no ser que se produzcan problemas específicos en su entorno, y que el soporte técnico de Dell aconseje modificar dicha configuración.

Complete los pasos de este procedimiento para ajustar la configuración del tiempo de espera del cliente.

- 1 Desplácese hasta la Core Console de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Configuración) y, a continuación, realice una de las acciones siguientes:
 - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Tiempo de espera del cliente**.

- Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Tiempo de espera del cliente.

Aparece la configuración del Core del tiempo de espera de clientes.

3 Haga clic en la opción que desee cambiar.

La opción seleccionada se volverá editable.

4 Introduzca la información de configuración según se describe en la tabla siguiente.

5

Tabla 12. Información de configuración del tiempo de espera del cliente

Configuración	Descripción
Tiempo de espera de conexión	Controla el tiempo de espera de una conexión entre el Core y los equipos protegidos cuando se envían datos mediante el protocolo de transferencia de hipertexto (http). Introduzca la cantidad de tiempo que desea que transcurra antes de que se agote el tiempo de espera de conexión. Utiliza el formato HH:MM:SS.
 NOTA: El valor predeterminado es 0:05:00 o cinco minutos.	
Tiempo de espera de lectura/escritura	Controla el tiempo de espera de una conexión entre el Core y los equipos protegidos cuando se leen o se escriben secuencias de datos mediante http. Un ejemplo es recibir bloques de datos cambiados de un equipo protegido al Core en una instantánea incremental. Introduzca la cantidad de tiempo que desea que transcurra antes de que se agote el tiempo de espera máximo durante un evento de lectura o escritura. Utiliza el formato HH:MM:SS.
 NOTA: El valor predeterminado es 0:05:00 o cinco minutos.	
Tiempo de espera de IU de conexión	Controla el tiempo de espera de una conexión entre la interfaz gráfica de usuario y el servicio del Core de Rapid Recovery mediante http. Introduzca la cantidad de tiempo que desea que transcurra antes de que se agote el tiempo de espera de IU de conexión. Utiliza el formato HH:MM:SS.
 NOTA: El valor predeterminado es 0:05:00 o cinco minutos.	
Tiempo de espera de IU de lectura/escritura	Controla el tiempo de espera de una conexión para leer y escribir secuencias de datos entre la interfaz gráfica de usuario y el servicio del Core de Rapid Recovery mediante http. Introduzca la cantidad de tiempo que desea que transcurra antes de que se agote el tiempo de espera máximo durante los eventos de lectura o escritura. Utiliza el formato HH:MM:SS.
 NOTA: El valor predeterminado es 0:05:00 o cinco minutos.	

6 Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en  para guardar los cambios y salir del modo edición, o haga clic en  para salir del modo sin guardar.

Funcionamiento de la caché de deduplicación y las ubicaciones de almacenamiento

La deduplicación global reduce la cantidad de espacio de almacenamiento en disco necesario para los datos de los cuales el Core realiza copias de seguridad. Cada repositorio se deduplica, almacenando cada bloque exclusivo una vez de forma física en disco, y empleando las referencias virtuales o punteros a esos bloques en copias de seguridad posteriores. Para identificar los bloques duplicados, Rapid Recovery incluye una caché de deduplicación para los repositorios del administrador de volúmenes de deduplicación (DVM). La caché mantiene las referencias a bloques exclusivos.

De manera predeterminada, la caché de deduplicación para repositorios DVM es de 1,5 GB. Este tamaño es suficiente para numerosos repositorios. Se deduplicarán sus datos en todo el repositorio hasta que se supere el tamaño de esta memoria caché. Si la cantidad de información redundante fuera tan grande que se llenara la caché de deduplicación, su repositorio dejaría de aprovechar todas las ventajas de la deduplicación para los datos recién añadidos. La cantidad de datos almacenados en su repositorio antes de que se llene la memoria caché de deduplicación varía dependiendo del tipo de datos que se incluyen en copia de seguridad y es diferente para cada usuario.

Puede aumentar el tamaño de la caché de deduplicación de DVM cambiando la configuración de la caché de deduplicación en el Core de Rapid Recovery. Para obtener información acerca de cómo aumentar el tamaño de la caché, consulte el tema [Configuración de los valores de caché de la deduplicación de DVM](#).

Cuando aumenta el tamaño de la caché de deduplicación de DVM hay dos factores a tener en cuenta: el espacio en disco y el uso de memoria RAM.

Espacio en disco. Se almacenan en disco dos copias de la caché de deduplicación de DVM: una memoria caché principal y una memoria caché secundaria que es una copia en paralelo. Por lo tanto, en el caso de utilizar el tamaño de la memoria caché predeterminada de 1,5 GB para un repositorio DVM, se utilizarán 3 GB de almacenamiento en disco en el sistema. A medida que aumenta el tamaño de la memoria caché, la cantidad de espacio en disco utilizada se mantiene proporcionalmente el doble del tamaño de la memoria caché. Para garantizar un rendimiento adecuado y resistente a los fallos, el Core cambia dinámicamente la prioridad de estas cachés. Ambas son necesarias, la única diferencia radica en que la memoria caché designada como principal se guarda primero.

Uso de memoria RAM. Cuando se inicia el Core de Rapid Recovery, carga la caché de deduplicación en la RAM. El tamaño de la caché, por lo tanto, afecta al uso de la memoria para el sistema. La cantidad total de RAM que utiliza el Core depende de muchos factores. Entre estos factores se incluyen qué operaciones se están ejecutando, el número de usuarios, el número de equipos protegidos y el tamaño de la caché de deduplicación. Cada operación realizada por el Core (transferencia, replicación, consolidación, etc.) consume memoria RAM. Una vez finalizada una operación, el consumo de memoria se ve reducido en consecuencia. Sin embargo, los administradores deberían tener en cuenta el requisito de carga de memoria RAM más alto para realizar operaciones de forma eficaz.

La configuración predeterminada para el Core de Rapid Recovery coloca la caché principal, la caché secundaria y la caché de metadatos para repositorios DVM en el directorio de AppRecovery. Esta carpeta está instalada en el equipo del Core.

NOTA: Dependiendo de su configuración, es posible que el directorio de AppRecovery no esté visible en el Core de Rapid Recovery. Para ver este directorio es posible que tenga que cambiar el panel de control de opciones de carpeta para que muestre archivos, carpetas y unidades ocultos.

Presuponiendo que el Core de Rapid Recovery esté instalado en la unidad C, estas ubicaciones son normalmente las siguientes:

Tabla 13. Ubicaciones de almacenamiento predeterminadas para la configuración de la caché de deduplicación de DVM

Configuración	Ubicación de almacenamiento predeterminada
Ubicación de la memoria caché principal	C:\ProgramData\AppRecovery\RepositoryMetadata\PrimaryCache
Ubicación de la memoria caché secundaria	C:\ProgramData\AppRecovery\RepositoryMetadata\SecondaryCache
Ubicación de la memoria caché de metadatos	C:\ProgramData\AppRecovery\RepositoryMetadata\CacheMetadata

Puede cambiar la ubicación de almacenamiento de estas memorias caché. Por ejemplo, para aumentar la tolerancia a fallos, puede cambiar la ubicación de su caché secundaria a una unidad física diferente a la principal, presuponiendo que el Core de Rapid Recovery tenga acceso a dicha ubicación.

Para obtener más información acerca del cambio de las ubicaciones de almacenamiento para cualquiera de estas configuraciones, consulte el tema [Configuración de los valores de caché de la deduplicación de DVM](#).

Dell recomienda planificar el almacenamiento de deduplicación por separado. La deduplicación solo se produce en un único repositorio (no en varios). Si se utiliza cifrado basado en el Core, la deduplicación se limita a los datos protegidos por una clave única, ya que por motivos de seguridad cada clave sirve para un único dominio de cifrado.

Para obtener más información acerca de la deduplicación, consulte [Deduplicación en Rapid Recovery](#).

Configuración de los valores de caché de la deduplicación de DVM

Complete los pasos de este procedimiento para configurar los parámetros de la caché de deduplicación para repositorios DVM.

- 1 Desplácese hasta la Core Console de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Configuración) y, a continuación, realice una de las acciones siguientes:
 - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Caché de deduplicación de DVM**. Esta opción solo aparece si el Core tiene uno o más repositorios DVM.
 - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Caché de deduplicación de DVM.
Aparece la configuración del Core de la caché de deduplicación de DVM.
- 3 Si desea restaurar los valores predeterminados de la caché de deduplicación de DVM en cualquier momento, haga lo siguiente:
 - a En la parte superior del área de configuración de la caché de deduplicación, haga clic en **Restaurar valores predeterminados**. Aparecerá el cuadro de diálogo Restaurar valores predeterminados.
 - b Haga clic en **Sí** para confirmar la restauración.
- 4 Haga clic en la opción de configuración que desee cambiar.
La opción seleccionada se volverá editable.
- 5 Para cambiar opciones de configuración individuales de la caché de deduplicación, introduzca la información de configuración según se describe en la tabla siguiente.

Tabla 14. Información de configuración de la caché de deduplicación de DVM

Configuración	Descripción
 Restaurar valores predeterminados	Este control restablece las ubicaciones de la caché DVM a las ubicaciones predeterminadas del sistema, que se describen para cada parámetro.
Ubicación de la caché principal	Si desea cambiar la ubicación de la memoria caché principal para repositorios DVM, en el cuadro de texto Ubicación de la memoria caché principal introduzca la ruta de acceso para una ubicación de almacenamiento accesible para el Core. La ubicación predeterminada es: C:\ProgramData\AppRecovery\RepositoryMetaData\PrimaryCache Ya que las memorias caché principal y secundaria son del mismo tamaño, el almacenamiento colectivo de estas dos memorias caché requiere el doble de espacio que la cantidad asignada para el tamaño de la memoria caché de deduplicación. Por ejemplo, si especifica 1,5 GB para el tamaño de deduplicación de la memoria caché de deduplicación, asegúrese de que cada una de las dos ubicaciones de almacenamiento cuenta con 1,5 GB como mínimo. En particular, si ambas ubicaciones pertenecen a la misma unidad (por ejemplo, la unidad C), debe haber al menos 3,0GB de espacio libre en el disco.
Ubicación de la caché secundaria	Si desea cambiar la ubicación de la memoria caché secundaria para repositorios DVM, en el cuadro de texto Ubicación de la memoria caché secundaria introduzca la ruta de acceso para una ubicación de almacenamiento accesible para el Core. La ubicación predeterminada es:

Configuración	Descripción
	C:\ProgramData\AppRecovery\RepositoryMetaData\SecondaryCache
Ubicación de metadatos de la caché	Si desea cambiar la ubicación de metadatos de la caché para repositorios DVM, en el cuadro de texto Ubicación de metadatos de la caché introduzca la ruta de acceso para una ubicación de almacenamiento accesible para el Core. La ubicación predeterminada es: C:\ProgramData\AppRecovery\RepositoryMetaData\CacheMetadata
Tamaño de la caché de deduplicación (GB)	Si desea cambiar el tamaño de la memoria caché de deduplicación para repositorios DVM, en el cuadro de texto Tamaño de caché de deduplicación introduzca una nueva cantidad (en GB). La ubicación predeterminada es: C:\ProgramData\AppRecovery\RepositoryMetaData\SecondaryCache El ajuste mínimo de tamaño de caché es 1,5GB. Además, el tamaño de la memoria caché no puede superar el 50% de la memoria RAM instalada.

- 6 Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en  para guardar el cambio y salir del modo edición, o haga clic en  para salir del modo edición sin guardar.

Configuración de los parámetros del motor de Replay

Puede configurar información referente al Replay Engine, que es el canal de comunicación de Rapid Recovery. Estos parámetros determinan la configuración del Core para que proporcione una comunicación eficaz.

En general, Dell recomienda el uso de la configuración predeterminada. En algunos casos, es posible que el soporte técnico de Dell le indique modificar estos parámetros para ayudar a ajustar el rendimiento a sus necesidades de red.

Complete los pasos de este procedimiento para configurar los parámetros del motor de Replay.

- Desplácese hasta la Core Console de Rapid Recovery.
- En la barra de iconos, haga clic en  (Configuración) y, a continuación, realice una de las acciones siguientes:
 - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Replay Engine**.
 - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Replay Engine. Aparecerá la configuración del Core de Replay Engine.
- Haga clic en la opción que desee cambiar.
La opción seleccionada se volverá editable.
- Introduzca la información de configuración según se describe en la tabla siguiente.

Tabla 15. Información de la configuración de Replay Engine

Cuadro de texto	Descripción
Dirección IP	El Core utiliza esta dirección IP cuando realiza el montaje y la restauración de un punto de recuperación para permitir reacciones entre los equipos protegidos y el Core. La dirección IP de Replay Engine se rellena automáticamente con la dirección IP del equipo del Core. Si introduce manualmente la dirección IP del servidor, este valor se utilizará en caso de que el equipo protegido no pueda resolver automáticamente la dirección IP facilitada.

Cuadro de texto	Descripción
	No hace falta establecer este valor manualmente a menos que los equipos protegidos tengan problemas para comunicarse con el Core.
Puerto de preferencia	Escriba un número de puerto o acepte el valor predeterminado. El puerto predeterminado es 8007. El puerto se utiliza para especificar el canal de comunicación del motor de Replay.
Puerto en uso	Representa el puerto que se utiliza para la configuración del motor de Replay.
Permitir autoasignación de puerto	Haga clic para permitir la autoasignación del puerto TCP.
Grupo de administración	Escriba un nuevo nombre para Grupo de administración. El nombre predeterminado es BUILTIN \Administrators.
Longitud mínima de E/S asíncrona	Escriba un valor o elija el valor predeterminado. Describe la longitud mínima de entrada y salida asíncrona. El valor predeterminado es 65536.
Tiempo de espera de lectura	Escriba un valor de tiempo máximo de espera de lectura o elija el valor predeterminado. El valor predeterminado es 0:05:00.
Tiempo de espera de escritura	Escriba un valor de tiempo máximo de espera de escritura o elija el valor predeterminado. El valor predeterminado es 0:05:00.
Tamaño del búfer de recepción	Escriba el tamaño del búfer de recepción o acepte el valor predeterminado. El valor predeterminado es 8192.
Tamaño del búfer de salida	Escriba el tamaño del búfer de salida o acepte el valor predeterminado. El valor predeterminado es 8192.
Sin demora	Se recomienda dejar esta casilla de verificación sin marcar, ya que, de lo contrario, la eficacia de la red podría verse afectada. Si desea modificar este ajuste, póngase en contacto con la asistencia técnica de Dell para que le asesoren.

- 5 Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en  para guardar los cambios y salir del modo edición, o haga clic en  para salir del modo sin guardar.

Configuración de los parámetros de implementación

Rapid Recovery le permite descargar instaladores desde el Core de Rapid Recovery en los equipos que desee proteger.

Puede configurar los parámetros relacionados con la implementación del software Rapid Recovery Agent desde el Core en los equipos que desee proteger.

Complete los pasos de este procedimiento para configurar los parámetros de implementación.

- Desplácese hasta la Core Console de Rapid Recovery.
- En la barra de iconos, haga clic en  (Configuración) y, a continuación, realice una de las acciones siguientes:
 - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Implementar**.
 - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Implementar. Aparece la configuración del Core de Implementar.
- Haga clic en la opción que desee cambiar.

La opción seleccionada se volverá editable.

- 4 Introduzca la información de configuración según se describe en la tabla siguiente.

Tabla 16. Información de configuración de implementaciones

Cuadro de texto	Descripción
Nombre de instalador de Agent	El nombre de archivo predeterminado es Agent-Web.exe. Si desea cambiar el nombre de este archivo por cualquier motivo, puede utilizar este parámetro para especificar un nuevo nombre del archivo ejecutable del instalador web del Core. Este archivo transmite una descarga de la última versión del instalador del Core de Rapid Recovery, que se inicia directamente desde Internet y le permite realizar una pausa y reanudar el proceso según lo necesite.
Dirección del Core	Introduzca la dirección de su servidor Core. Normalmente consta del protocolo, el nombre de su servidor Core y el puerto, así como el directorio donde residen los archivos del Core. Por ejemplo, si su servidor es Muestra, el parámetro es <code>https://muestra:8006/apprecovery/admin/Core</code>
Error de tiempo de espera de recepción	La cantidad de tiempo que la implementación del software Agent debe intentarse antes de agotar el tiempo de espera. El valor predeterminado es 00:25:00 o veinticinco minutos. Si desea cambiar este parámetro, introduzca la cantidad de tiempo que desea que el sistema pase intentando implementar el software Agent antes de que se agote el tiempo de espera máximo durante los eventos de lectura o escritura. Utiliza el formato HH:MM:SS.
Número máximo de instalaciones paralelas	Este parámetro controla el número máximo de implementaciones del software Agent que debe intentar el Core al mismo tiempo. El valor predeterminado es 100.

- 5 Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en  para guardar el cambio y salir del modo edición, o haga clic en  para salir del modo edición sin guardar.

Configuración de los parámetros de conexión con la base de datos

Rapid Recovery muestra información sobre las tareas, eventos y alertas del Core en la página Eventos. Rapid Recovery almacena esta información de transacciones en una base de datos de servicio MongoDB que se instala localmente de forma predeterminada en el equipo del Core. Puede configurar estos parámetros para cambiar la cantidad de tiempo que se retiene la información en la base de datos, o para cambiar el tamaño del grupo de conexión para permitir más o menos conexiones simultáneas.

Si está utilizando un segundo Core de Rapid Recovery, puede configurar los parámetros de conexión de la base de datos en el primer Core para que apunten al segundo equipo del Core. De esta manera, los datos de eventos de ambos Cores se almacenarán en MongoDB en el segundo Core.

También puede configurar los parámetros de conexión de la base de datos del Core para que apunten a otro equipo que tenga instalado MongoDB de forma separada y que esté accesible desde la red al Core de Rapid Recovery. Los datos de transacciones de eventos de su Core se guardan en esa base de datos de servicio, no de forma local. Para obtener más información acerca del establecimiento o modificación de parámetros de conexión de bases de datos para la base de datos de servicio, consulte [Configuración de los parámetros de conexión con la base de datos](#).

 **NOTA:** Para obtener más información sobre la visualización de información de eventos desde el Core de Rapid Recovery, consulte [Visualización de eventos mediante las tareas, las alertas y el diario](#).

Los clientes pueden elegir especificar la instalación de la base de datos de servicio MongoDB en otro equipo que sea accesible para el Core de Rapid Recovery en la red. Si la base de datos de servicio para su Core de Rapid Recovery se instala en otro equipo que no sea el que aloja el Core de Rapid Recovery, debe proporcionar credenciales para la base de datos (un nombre de usuario y una contraseña) en esta configuración.

Complete los pasos de este procedimiento para modificar los parámetros de conexión de base de datos de la base de datos de servicio que utiliza el Core de Rapid Recovery.

- 1 Desplácese hasta la Core Console de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Configuración) y, a continuación, realice una de las acciones siguientes:
 - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Conexión de base de datos**.
 - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Conexión de base de datos.
Aparece la configuración del Core de Conexión de base de datos.
- 3 En la parte superior del área de configuración de la conexión de base de datos, puede hacer lo siguiente:
 - Haga clic en **Probar conexión** para verificar la configuración.
Se recomienda probar la conexión si cambia alguno de los valores de conexión de la base de datos.
 - Haga clic en **Restaurar valores predeterminados** para restaurar todas las opciones de configuración de la base de datos a sus valores predeterminados.
Se le solicitará que confirme esta acción y, si lo hace, los valores personalizados de configuración de la conexión de la base de datos se descartarán.
- 4 Haga clic en la opción que desee cambiar.
La opción seleccionada se volverá editable.
- 5 Introduzca la información de configuración según se describe en la tabla siguiente.

Tabla 17. Información de configuración de la conexión de la base de datos

Cuadro de texto	Descripción
Nombre de host	Escriba un nombre de host para la conexión de la base de datos.  NOTA: Cuando localhost es el parámetro especificado como host, MongoDB se instala de forma local en el equipo que aloja al Core.
Puerto	Especifique un número de puerto para la conexión de la base de datos.  NOTA: El valor predeterminado es 27017.
Nombre de usuario	Introduzca un nombre de usuario con privilegios administrativos para la base de datos de servicio MongoDB.  NOTA: Si el parámetro de nombre de host es localhost, no se requiere este campo.
Contraseña	Introduzca la contraseña asociada con el nombre de usuario que haya especificado.  NOTA: Si el parámetro de nombre de host es localhost, no se requiere este campo.
Periodo de retención (día)	Introduzca el número de días que se conservará el historial de eventos y trabajos en la base de datos de servicio.
Tamaño máximo de grupo de conexiones	Establece el número máximo de conexiones de base de datos en caché para permitir la reutilización dinámica.  NOTA: El valor predeterminado es 100.
Tamaño mínimo de grupo de conexiones	Establece el número mínimo de conexiones de base de datos en caché para permitir la reutilización dinámica.  NOTA: El valor predeterminado es 0.

- 6 Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en  para guardar los cambios y salir del modo edición, o haga clic en  para salir del modo sin guardar.

Modificación de la configuración de la conexión con la base de datos local

Puede ver eventos del sistema relacionados con el Core de Rapid Recovery en la página Eventos. El Core de Rapid Recovery almacena esta información de transacciones en una base de datos de servicio MongoDB. De manera predeterminada, esta base de datos está instalada localmente en el equipo del Core y el nombre de host en la configuración de conexión de base de datos tiene los valores predeterminados del localhost. En esta situación, la interfaz de loopback omite el hardware de la interfaz de red local y no son necesarias las credenciales de la base de datos.

De manera opcional y para elevar la seguridad, puede especificar explícitamente credenciales de base de datos (un nombre de usuario y una contraseña) para la base de datos MongoDB que utiliza el Core de Rapid Recovery.

NOTA: Para obtener más información sobre la visualización de información de eventos desde el Core de Rapid Recovery, consulte [Visualización de eventos mediante las tareas, las alertas y el diario](#). Para obtener más información sobre la configuración de conexión de base de datos, consulte [Configuración de los parámetros de conexión con la base de datos](#).

Complete los pasos de este procedimiento para modificar la configuración de la conexión con la base de datos local con el fin de especificar credenciales de base de datos.

- 1 Desplácese hasta la Core Console de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Configuración) y, a continuación, realice una de las acciones siguientes:
 - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Parámetros de base de datos local**.
 - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Parámetros de base de datos local.
Aparece la configuración del Core de la base de datos local.
- 3 Haga clic en la opción que desee cambiar.
La opción seleccionada se volverá editable.
- 4 Introduzca las credenciales correspondientes para la conexión a la base de datos de servicio, tal como se describe en la tabla siguiente.

Tabla 18. Información de configuración de la base de datos local

Cuadro de texto	Descripción
Nombre de usuario	Introduzca un nombre de usuario con privilegios administrativos para la base de datos de servicio MongoDB.
Contraseña	Introduzca la contraseña asociada con el nombre de usuario que haya especificado.

- 5 Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en  para guardar el cambio y salir del modo edición, o haga clic en  para salir del modo edición sin guardar.

Administración de la configuración del servidor SMTP

Si configura los parámetros del servidor de protocolo sencillo de transferencia de correo (SMTP) para el Core, podrá enviar notificaciones de tareas, eventos y alertas por correo electrónico.

Puede encontrar información sobre cómo configurar un servidor de correo electrónico SMTP en el tema [Configuración de un servidor de correo electrónico](#).

NOTA: Para enviar información de eventos por correo electrónico, también deberá configurar los parámetros del grupo de notificación. Para obtener más información sobre cómo especificar eventos para recibir alertas de correo electrónico, consulte [Configuración de grupos de notificación](#).

Administración de los parámetros de configuración de nube

En Rapid Recovery, puede asociar las cuentas de almacenamiento que tenga con los proveedores de almacenamiento en la nube a su Core de Rapid Recovery. Esto le permite archivar información de equipos protegidos cuando los datos queden obsoletos.

Rapid Recovery se integra con Amazon™ S3, Microsoft Azure y proveedores de nube administrada mediante la tecnología de código abierto OpenStack.

Para obtener más información acerca de la administración de la información de cuentas de almacenamiento en la nube en el Core de Rapid Recovery, consulte [Administración de cuentas de nube](#).

Administración de la configuración de informes

Puede generar informes para el Core de Rapid Recovery o para máquinas protegidas. Para obtener información sobre los informes que puede generar, consulte [Creación y visualización de informes](#).

Complete los pasos de este procedimiento para administrar la configuración de informes de los informes de Core.

- 1 Desplácese hasta la Core Console de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Configuración) y, a continuación, realice una de las acciones siguientes:
 - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Informes**.
 - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Informes. Aparece la configuración del Core de **Informes**. La configuración de informes se describe en la siguiente tabla.

Opción	Descripción
Restaurar el valor predeterminado	Esta opción restaura la configuración de informes a sus valores predeterminados. Los valores predeterminados se enumeran a continuación para cada parámetro.
Tipo de letra	Esta opción controla el tipo de letra predeterminado que se utiliza para los informes. El valor predeterminado es la tipografía Trebuchet MS. Puede cambiar esta fuente por cualquier tipo de letra disponible para el sistema.
Tamaño del papel	Esta opción controla el tamaño del papel predeterminado utilizado para imprimir informes. El valor predeterminado es A4. Puede seleccionar los siguientes tamaños de papel: • Carta • Periódico • Libro de contabilidad • Legal • A3 • A4 • Ejecutivo • B4 • Sobre C3 • Sobre C4
Orientación de página	Esta opción controla la orientación de la página para informes exportados. La orientación predeterminada es Vertical. Puede seleccionar las opciones de diseño siguientes: • Portrait (Vertical)

Opción	Descripción
	• Landscape (Horizontal)
3	Para cambiar cualquiera de los parámetros de los informes, haga clic en el campo de configuración pertinente. El campo de configuración aparece como un menú desplegable configurable.
4	Haga clic en el menú desplegable y seleccione uno de los valores disponibles. Por ejemplo, en el campo Tipo de letra, haga clic en Times New Roman .
5	Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en  para guardar el cambio y salir del modo edición, o haga clic en  para salir del modo edición sin guardar. La opción seleccionada aparece ahora como la nueva configuración del parámetro Informes seleccionado.

Administración de la configuración de conectabilidad de SQL del Core

Las comprobaciones de conectabilidad SQL se realizan como parte de los trabajos nocturnos de Rapid Recovery. Con el fin de reducir los costos de licencia, Rapid Recovery propone dos opciones para realizar las comprobaciones de conectabilidad: utilizar una instancia de SQL Server con licencia instalada en el equipo del Core de Rapid Recovery o emplear la instancia de SQL Server que ya está instalada en el equipo protegido. Esta segunda opción es ahora el valor predeterminado. Sin embargo, si el equipo protegido ya se utiliza mientras se realizan los trabajos nocturnos, se recomienda realizar las comprobaciones con una instancia de SQL Server en el Core.

En resumen, el proceso de administración de la configuración de conectabilidad SQL del Core consta de las áreas siguientes:

- Montar el punto de recuperación más reciente para grupos de protección que contienen bases de datos.
 - Conectar con la base de datos desde SQL Server.
 - Abrir la base de datos.
 - Cerrar la base de datos.
 - Desmontar el punto de recuperación.
- Para activar esta comprobación nocturna, especifique una instancia de SQL Server que haya que utilizar para realizar comprobaciones de conectabilidad de las bases de datos SQL Server en equipos protegidos.

 **NOTA:** Esta opción no aparece si no está protegiendo un SQL Server en su Core.

Para configurar el Core con tal de realizar comprobaciones de la conectabilidad SQL como parte de las tareas nocturnas, realice los pasos siguientes.

 **NOTA:** Si selecciona la opción predeterminada para utilizar la instancia de SQL Server instalada en el equipo protegido, esa instancia de SQL Server administrará la conectabilidad de SQL de todos los equipos protegidos de SQL. Si no desea que este parámetro se aplique a todos los equipos SQL protegidos, seleccione Usar SQL Server en el Core. Para realizar comprobaciones de conectabilidad en el Core, debe instalar o utilizar una versión de SQL Server con licencia en el equipo del Core.

- 1 Desplácese hasta la Core Console de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Configuración) y, a continuación, realice una de las acciones siguientes:
 - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Conectabilidad**.
 - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Conectabilidad.
- 3 Para utilizar la instancia de SQL Server instalada en el equipo protegido de SQL Server, seleccione **Utilizar SQL Server en el equipo protegido**. Esta es la opción predeterminada.
- 4 Para utilizar la instancia de SQL Server instalada en el Core de Rapid Recovery, seleccione **Utilizar SQL Server en el Core** y, a continuación, introduzca la información de autenticación tal como se describe en la tabla siguiente.

Tabla 19. Información de credenciales de SQL Server

Cuadro de texto	Descripción
SQL Server	Desde el menú desplegable de SQL Server, seleccione la opción apropiada de la instancia de SQL Server desde el servidor del Core.
Tipo de credencial	Elija el método de autenticación pertinente para sus credenciales entre las siguientes opciones: - Windows - SQL
Nombre de usuario	Especifique un nombre de usuario para acceder a SQL Server en el Core según el tipo de credencial seleccionado.
Contraseña	Especifique una contraseña para acceder a SQL Server en el Core según el tipo de credencial seleccionado.

5 Haga clic en **Probar conexión**.

NOTA: Si no ha especificado las credenciales correctamente, aparece un mensaje que le indica que las credenciales son incorrectas. Corrija la información de credenciales y vuelva a probar la conexión.

6 Si está satisfecho con los cambios, haga clic en **Aplicar**.

Funcionamiento de los trabajos de Core

Los trabajos son procesos que el Core de Rapid Recovery realiza para dar soporte a sus operaciones, incluida la copia de seguridad en puntos de recuperación, la replicación de datos, el archivado de datos, la exportación de datos a máquinas virtuales, el mantenimiento de repositorios, etc. Los trabajos de Core se inician automáticamente para algunas operaciones, como la replicación o el archivado según un calendario de programación establecido. También puede abrir algunos trabajos a petición desde varios componentes en la Core Console.

- Cuando visualiza o edita la configuración de trabajo de Core, cada trabajo de Core tiene dos parámetros: N.º máximo de trabajos simultáneos y Recuento de intentos.
 - El parámetro N.º máximo de trabajos simultáneos determina cuántos trabajos de ese tipo se pueden ejecutar al mismo tiempo.
 - El parámetro Recuento de intentos determina el número de veces que un trabajo se debe intentar ejecutar antes de abandonarlo si un error de red u otro error de comunicación impide que el trabajo tenga éxito la primera vez.
- En la tabla de trabajos de Core, la columna Configuración indica si el trabajo que aparece está incluido en la configuración de trabajos de Core de manera predeterminada o si es necesario agregarlo explícitamente.

La siguiente tabla describe los trabajos del Core principal disponibles y sus funciones.

Tabla 20. Trabajos de Core

Nombre de trabajo	Descripción	N.º máximo de trabajos simultáneos	Recuento de intentos	Configuración
Comprobar la conectabilidad de bases de datos SQL en instantáneas	Permite al Core comprobar la coherencia de las bases de datos SQL y garantiza que todos los archivos MDF (datos) y LDF (registro) compatibles están disponibles en la instantánea de copia de seguridad. Proceso: • Montar el punto de recuperación más reciente para grupos de protección que contienen bases de datos SQL. • Montar la base de datos. Si se está realizando la conectabilidad desde el servidor SQL protegido, realice el montaje mediante la ruta de acceso UNC.	1	0	Predeterminado

Nombre de trabajo	Descripción	N.º máximo de trabajos simultáneos	Recuento de intentos	Configuración
	- Conectar con la base de datos desde SQL Server. - Realizar la comprobación de conectabilidad. - Realizar operaciones de limpieza. - Cerrar la base de datos. - Desmontar la base de datos. - Desmontar el punto de recuperación.			
Comprobar suma de comprobación de bases de datos de Exchange	Comprueba la integridad de los puntos de recuperación que contienen bases de datos de Exchange. Proceso: - Montar el punto de recuperación más reciente para grupos de protección que contienen bases de datos SQL. - Conectar con la base de datos desde SQL Server. - Abrir la base de datos. - Cerrar la base de datos. - Desmontar el punto de recuperación.	1	0	Predeterminado
Comprobar la capacidad de montaje de bases de datos de Exchange	Comprueba que las bases de datos de Exchange se pueden montar.	1	0	Predeterminado
Replicar datos de equipos protegidos desde origen remoto	Transfiere una copia de puntos de recuperación de un equipo protegido desde un Core de origen a un Core de destino. Este trabajo se ejecuta en el Core de destino y recibe los puntos de recuperación replicados entrantes.	3	0	Predeterminado
Replicar datos de equipos protegidos en destino remoto	Transfiere una copia de puntos de recuperación de un equipo protegido desde un Core de origen (en el que se guardaron originariamente) a un Core de destino. Este trabajo se ejecuta en el Core de origen y controla la replicación saliente.	1	3	Predeterminado
Consolidar puntos de recuperación	Aplica la política de retención a sus datos de copia de seguridad combinando la "consolidación" de puntos de recuperación en el programa definido en la política de retención.	1	0	Predeterminado
Comprobar puntos de recuperación	Comprueba la integridad de los puntos de recuperación.	1	0	Agregar
Eliminar todos los puntos de recuperación	Elimina el conjunto completo de puntos de recuperación en un equipo protegido.	1	0	Agregar
Eliminar cadena de puntos de recuperación	Elimina una cadena de puntos de recuperación completa en un equipo protegido.	1	0	Agregar
Eliminar intervalo de puntos de recuperación	Elimina un conjunto de puntos de recuperación en un equipo protegido, por identificador de punto de recuperación o por intervalo de fechas.	1	0	Agregar
Implementar software de Agent en equipos	Implementa el software Rapid Recovery Agent en el equipo o equipos especificados.	1	0	Agregar

Nombre de trabajo	Descripción	N.º máximo de trabajos simultáneos	Recuento de intentos	Configuración
Descargar bibliotecas de Exchange	Descarga las bibliotecas de Microsoft Exchange desde el equipo protegido al equipo del Core en la ruta de acceso C:\ProgramData\AppRecovery\ExchangeLibraries .	1	0	Agregar
Exportar a archivo comprimido	Crea una copia de seguridad en la ruta de acceso especificada con un archivo de los puntos de recuperación seleccionados. Proceso: • Puntos de recuperación de montaje. • Escribir datos en copias de seguridad. • Desmontar el punto de recuperación.	1	0	Agregar
Exportar a máquina virtual	Exporta los datos del punto de recuperación especificado del equipo protegido a la ruta de destino como una máquina virtual. Proceso: • Montar punto de recuperación. • Crear una máquina virtual a partir de los datos del punto de recuperación en la ruta de destino. • Desmontar el punto de recuperación.	1	0	Agregar
Importar archivos comprimidos	Importa el punto de recuperación a partir de la copia de seguridad especificada en un archivo comprimido del Core previamente creado.	1	0	Agregar
Mantener repositorio	Realiza una comprobación del repositorio. Proceso: • Comprobar el sistema de archivos de repositorio. • Montar punto de recuperación. • Volver a calcular el caché de deduplicación para el repositorio. • Cargar los puntos de recuperación del repositorio.	1	0	Agregar
Montar instantáneas de puntos de recuperación	Realiza el montaje del punto de recuperación en la ruta de acceso especificada.	1	0	Agregar
Proteger máquinas virtuales ESX®	Agrega todas las máquinas virtuales especificadas a la protección sin agente. El trabajo se realiza inmediatamente después de agregar la protección sin agente de una o más máquinas virtuales al Core mediante el asistente para proteger varios equipos. El trabajo establece el número de identificación para cada máquina virtual especificada, escribe información sobre el Core en un archivo de configuración y recupera los metadatos del archivo.	1	0	Agregar
Restaurar desde punto de recuperación	Realiza una restauración a partir de un punto de recuperación en un equipo de destino especificado. Proceso: • Montar punto de recuperación. • Escribir todos los datos del punto de recuperación en el equipo especificado.	1	0	Agregar

Nombre de trabajo	Descripción	N.º máximo de trabajos simultáneos	Recuentos de intentos	Configuración
	Desmontar el punto de recuperación.			
Carga de registros	Carga los registros al servidor especificado.	1	0	Agregar

Algunos trabajos de Core se incluyen en Configuración. La configuración de los trabajos le permite especificar cuántos trabajos simultáneos del mismo tipo puede ejecutar el Core y cuántos reintentos se deben realizar si falla el primer intento del trabajo.

Para obtener más información acerca de estos ajustes, consulte [Configuración de trabajo de Core](#).

Para obtener información sobre cómo agregar trabajos a la Configuración del Core, consulte [Incorporación de trabajos del Core a la configuración](#).

Para obtener más información sobre la edición de la configuración de los trabajos en la lista Configuración, consulte [Modificación de los parámetros de los trabajos del Core](#).

Configuración de trabajo de Core

Cuando se selecciona  (Configuración) en la barra de iconos, puede acceder a la configuración de algunos trabajos del Core. El área **Trabajos** en la página Configuración del Core permite determinar dos valores para cada tipo de trabajo enumerado:

- 1 El número máximo de trabajos de este tipo que el Core puede intentar al mismo tiempo. Se debe establecer en un valor entre 1 y 50.
- 2 El número de veces que un trabajo se debe intentar si un error de red u otro error de comunicación impide que el trabajo tenga éxito la primera vez. Se debe establecer en un valor entre 0 y 10.

Varios trabajos se incluyen automáticamente en la configuración del Core. Estos trabajos incluyen un valor de "Predeterminado" en la columna Configuración (tal como se muestra en el tema [Funcionamiento de los trabajos de Core](#)).

Puede agregar algunos otros trabajos en la configuración si desea ajustar dichos valores para controlar el número máximo de trabajos o reintentos para esas funciones. Estos trabajos incluyen un valor de "Agregar" en la columna Configuración. Para obtener información sobre cómo agregar estos trabajos a la tabla Configuración, consulte [Incorporación de trabajos del Core a la configuración](#).

Los trabajos del Core que no están disponibles en Configuración no proporcionan la capacidad de establecer estos dos parámetros.

Para los trabajos que se enumeran en Configuración, puede editar los valores existentes. Esto le permite personalizar los dos parámetros, eliminar un tipo de trabajo de la lista de configuración de trabajo o restaurar la configuración predeterminada. Para obtener información detallada, consulte el tema [Modificación de los parámetros de los trabajos del Core](#).

Incorporación de trabajos del Core a la configuración

La configuración de los trabajos del Core le permite definir, para cada tipo de trabajo, el número máximo de trabajos para el Core que pueden intentarse a la vez y cuántas veces se debe reintentar ese trabajo si falla el primer intento.

Cada tipo de trabajo del Core tiene valores predeterminados para estos dos parámetros, tal como se describe en el tema [Configuración de trabajo de Core](#). Esta lista también indica los tipos de trabajo que se incluyen en la configuración del Core de manera predeterminada.

Agregar un trabajo del Core a la configuración le permite cambiar estos parámetros para el tipo de trabajo que ha agregado.

Realice los pasos del procedimiento siguiente para agregar un trabajo a la configuración del Core.

- 1 Desplácese hasta la Core Console de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Configuración) y, a continuación, realice una de las acciones siguientes:

- En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Trabajos**.
 - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Trabajos. Aparece la configuración del Core de Trabajos.
- 3 En la página Configuración del Core, en Trabajos, haga clic en  **Agregar**. Aparece el cuadro de diálogo Configuración de trabajo.
 - 4 En el cuadro de diálogo **Configuración de trabajo**, en el campo **Trabajos**, seleccione el nombre del trabajo que desea agregar a la configuración del Core. Estos trabajos se describen en el tema [Configuración de trabajo de Core](#).
 - 5 Para establecer el número máximo de trabajos que el Core puede intentar al mismo tiempo, en el cuadro de texto **N.º máximo de trabajos simultáneos**, introduzca un nuevo valor entre 1 y 50.
 - 6 Para establecer el número de intentos que el Core debe realizar antes de abandonar el trabajo, en el cuadro de texto **Recuento de intentos**, introduzca un nuevo valor entre 0 y 10.
 - 7 Haga clic en **Guardar**. Se cerrará el cuadro de diálogo Configuración de trabajo y se aplicarán sus nuevos parámetros del trabajo.

Modificación de los parámetros de los trabajos del Core

La configuración de los trabajos del Core le permite definir, para cada tipo de trabajo, el número máximo de trabajos para el Core que pueden intentarse a la vez y cuántas veces se debe reintentar ese trabajo si falla el primer intento.

Cada tipo de trabajo del Core tiene valores predeterminados para estos dos parámetros, tal como se describe en el tema [Funcionamiento de los trabajos de Core](#). Esta lista también indica los tipos de trabajo que se incluyen en la configuración del Core de manera predeterminada. Al editar la configuración de los trabajos del Core, puede conseguir lo siguiente:

- Puede personalizar la configuración de cada tipo de trabajo del Core.
 - Puede eliminar un tipo de trabajo de la lista de configuración del Core. Esta función no está disponible si el tipo de trabajo está incluido en la configuración de manera predeterminada.
- ① **NOTA:** Eliminar un trabajo de la configuración del Core no hace más que quitar el tipo de trabajo de esa lista. Para volver a editar la configuración del Core para ese tipo de trabajo en el futuro, puede agregarlo a la lista tal como se describe en el tema [Incorporación de trabajos del Core a la configuración](#).
- Puede restablecer la configuración de cualquier tipo de trabajo a sus valores predeterminados.
- ① **NOTA:** Aunque solo puede utilizar esta función para los tipos de trabajo incluidos en la configuración del Core de manera predeterminada, sí que puede establecer otros tipos de trabajo en sus valores predeterminados si los elimina de la lista y los vuelve a agregar.

Realice los pasos del procedimiento siguiente para editar la configuración de un trabajo.

- 1 Desplácese hasta la Core Console de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Configuración) y, a continuación, realice una de las acciones siguientes:
 - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Trabajos**.
 - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Trabajos. Aparece la configuración del Core de Trabajos.
- 3 Desde la cuadrícula Trabajo, seleccione el trabajo que desee quitar de la lista. En el menú desplegable  de ese trabajo, seleccione **Eliminar**. El trabajo se eliminará de la lista.
- 4 Desde la cuadrícula Trabajo, seleccione en la lista el trabajo para el que desea restablecer la configuración. En el menú desplegable  de ese trabajo, seleccione **Restablecer a valores predeterminados**. La configuración de trabajo de este trabajo se restablecerá a sus valores predeterminados.
- 5 En la cuadrícula Trabajo, seleccione el trabajo que desee cambiar. En el menú desplegable  de ese trabajo, seleccione **Editar**.

- 6 Se abrirá el cuadro de diálogo Configuración de trabajo: [NombreDeTrabajo].
- 7 Para cambiar el número máximo de trabajos que el Core puede intentar al mismo tiempo, en el cuadro de texto Número máximo de trabajos simultáneos, introduzca un nuevo valor entre 1 y 50.
- 8 Para cambiar el parámetro del número de intentos adicionales que el Core debe realizar antes de abandonar el trabajo, en el cuadro de texto Recuento de intentos, introduzca un nuevo valor entre 0 y 10.
- 9 Haga clic en **Guardar**.
Se cerrará el cuadro de diálogo Configuración de trabajo y se aplicarán sus nuevos parámetros del trabajo.

Administración de licencias

Muchos usuarios del Core de Rapid Recovery comienzan con una licencia de prueba, que tiene funciones limitadas. Una licencia de prueba es válida durante 14 días, y el administrador del grupo puede ampliarla una vez hasta una licencia de 28 días. Una vez que vence el periodo de prueba, el Core de Rapid Recovery detiene la realización de instantáneas hasta que obtiene y registra una licencia válida que no sea de prueba.

NOTA: Para obtener información sobre cómo introducir la clave de licencia o la información del archivo (por ejemplo, para actualizar o cambiar una licencia de prueba por una licencia a largo plazo), consulte [Actualización o cambio de una licencia](#).

Las licencias se validan mediante el empleo de archivos de licencia o de claves de licencia.

Los **archivos de licencia** son archivos de texto que terminan con la extensión de archivo **.lic**. Estos son algunos ejemplos de archivos de licencia:

- Los archivos de licencia pueden aparecer con una longitud de nueve caracteres, que consiste en tres grupos de números arábigos separados entre sí por un guion; por ejemplo, `123-456-789.lic`.
- Las licencias basadas en software pueden aparecer con formato `Software<nombre de grupo>.lic`, y el grupo tendrá el nombre del cliente o de la cuenta; por ejemplo, `Software-YourCompany.lic`.
- Las licencias de dispositivos Dell pueden aparecer con formato `<Serie de dispositivo>-<Nombre de grupo>.lic`, y el grupo tendrá el nombre del cliente o de la cuenta; por ejemplo, `DL4X00 Series-YourCompany.lic`.

Las **claves de licencia** tienen 30 caracteres de longitud y constan de seis grupos de caracteres alfanuméricos ingleses separados entre sí por un guion. Por ejemplo, un formato de clave de licencia de muestra es `ESABC12-DEF3G-H45IJ-6K78L-9MN10-OPQ11`.

Rapid Recovery le permite administrar las licencias o ponerse en contacto con el servidor de licencias directamente desde la Core Console

seleccionando  (Configuración) en la barra de iconos y haciendo clic en **Licencias**.

La configuración de Licencias incluye la información siguiente:

Detalles de la licencia:

-  **Cambiar licencia.** Le permite cargar un archivo de licencia o introducir una clave de licencia para cambiar una licencia existente asociada con el Core.
-  **Agregar licencia.** Esta opción solo está disponible para dispositivos de copia de seguridad de Dell y le permite cargar un archivo de licencia o introducir una clave de licencia.
-  **Grupo de portal de licencias.** Esta opción abre el portal de licencias para la administración del grupo.
- **Tipo de licencia.** Los tipos de licencia incluyen Prueba, Suscripción y Empresa. Para obtener más información, consulte el tema sobre Dell Data Protection | Portal de licencias de Rapid Recovery los tipos de licencias de software en la Guía del usuario del Dell Data Protection | Portal de licencias de Rapid Recovery.
- **Estado de la licencia.** Indica el estado de la licencia. Un estado activo garantiza que las instantáneas pueden proseguir como está programado. Si la licencia está bloqueada o caducada, o si el Core no ha podido comunicarse con el Dell Data Protection | Portal de licencias de Rapid Recovery pasado el periodo de gracia, se realiza una pausa en las instantáneas hasta que se corrige el estado de la licencia.

Restricciones de licencia:

- **Máximo de instantáneas por día.** Indica el número de copias de seguridad, que está limitado por la licencia específica.

Grupo de licencias:

- **Tamaño de grupo.** El grupo de licencias es el número de licencias que no son de prueba disponibles para asignar en todos los grupos y subgrupos del Dell Data Protection | Portal de licencias de Rapid Recovery. El tamaño del grupo determina cuántas licencias se pueden asignar. Para obtener más información, consulte el tema “Funcionamiento de los grupos de licencias” en la Guía del usuario del *Dell Data Protection | Portal de licencias de Rapid Recovery*.
- **Protegidos por este Core.** Indica el número de equipos del grupo de licencias que están protegidos por este Core.
- **Total protegido en grupo.** Indica el número total de equipos protegidos dentro del mismo grupo de licencias que este Core.

Servidor de licencias. Estos parámetros se aplican a licencias estándar (llamada a casa). Estos parámetros no son aplicables a dispositivos y otras licencias que no son de llamada a casa:

- **Dirección del servidor de licencias.** Muestra una URL activa del servidor de licencias asociado con este Core.
- **Última respuesta del servidor de licencias.** Indica si la comunicación que se intentó por última vez con el portal del servidor de licencias fue correcta.
- **Último contacto con el servidor de licencias.** Muestra la fecha y la hora del último contacto correcto con el servidor de licencias.
- **Siguiente intento para ponerse en contacto con el servidor de licencias.** Indica las próximas fecha y hora programadas para intentar la comunicación con el servidor de licencias.
- **Póngase en contacto ahora.** Este botón entra en contacto con el servidor de licencias a petición. Utilice esta opción después de realizar cambios en la configuración de la licencia para registrar cambios inmediatamente en lugar de esperar al siguiente intento programado.

Para obtener más información sobre licencias, consulte la *Guía del usuario del Dell Data Protection | Portal de licencias de Rapid Recovery*.

Para obtener más información sobre cómo agregar o cambiar una clave o archivo de licencia, consulte [Actualización o cambio de una licencia](#).

Para obtener más información sobre cómo ponerse en contacto con el servidor del portal de licencias, consulte [Cómo ponerse en contacto con el servidor Dell Data Protection | Portal de licencias de Rapid Recovery](#)

También puede ver información de licencia para un único equipo protegido. Para obtener más información, consulte [Visualización de la información de licencia en un equipo](#).

Actualización o cambio de una licencia

Cuando haya actualizado o adquirido una licencia de Rapid Recovery de largo plazo, recibirá un archivo o una clave de licencia por correo electrónico.

Realice los pasos de este procedimiento para actualizar la licencia de prueba o cambiar la licencia existente, y asíóciela con la Core Console de Rapid Recovery.

NOTA: Si es necesario, los usuarios de dispositivos de copia de seguridad de Dell también pueden agregar licencias a la Core. Para obtener más información, consulte [Adición de una licencia](#).

Para obtener información sobre cómo obtener una clave de licencia o para conocer los detalles del uso del portal de licencias para descargar el software, registrar dispositivos, administrar suscripciones de licencia y grupos de licencias, y para generar informes del portal de licencias, consulte la guía del usuario del *Dell Data Protection | Portal de licencias de Rapid Recovery*.

Si ha instalado un nuevo Core y se le pide que elija un archivo o clave de licencia, vaya directamente al [paso 5](#).

- 1 Desplácese hasta la Core Console de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Configuración).
- 3 Desplácese hacia abajo en el lado derecho de la página **Configuración** hasta que pueda ver el encabezado Licencias.

Aparece la configuración del Core para las licencias.

- 4 Para actualizar o cambiar la licencia existente asociada con su Core, en la parte superior del área de configuración del Core Detalles de la licencia, haga clic en  **Cambiar licencia**. Aparecerá el cuadro de diálogo **Cambiar licencia**.
- 5 Para introducir una clave de licencia o para cargar un archivo de licencia, realice una de las acciones siguientes:
 - a Si desea *introducir manualmente* la clave de licencia, en el cuadro de diálogo Cambiar licencia, escriba cuidadosamente la clave y, a continuación, haga clic en **Continuar**.
El cuadro de diálogo se cierra, el archivo de licencia seleccionado se autentica y esa licencia se asocia a su Core.
 - b Si desea *cargar* un archivo de licencia, en el cuadro de diálogo Cambiar licencia, haga clic en **Seleccionar archivo**.
En el cuadro de diálogo **Carga de archivo**, desplácese por el sistema de archivos y localice el nuevo archivo de licencia que desea utilizar. Por ejemplo, `busqueSoftware-YourCompany.lic`.
 - c Haga clic en el archivo de licencia y, a continuación, haga clic en **Abrir**.
El cuadro de diálogo Carga de archivo se cerrará. El archivo de licencia seleccionado aparece en el cuadro de diálogo Cambiar licencia.
 - d En el cuadro de diálogo **Cambiar licencia**, haga clic en **Continuar**.
El cuadro de diálogo se cierra, el archivo de licencia seleccionado se autentica y esa licencia se asocia a su Core.
- 6 Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Servidor de licencias. Aparece la configuración del Core de Licencias.
- 7 En el área Servidor de licencias, haga clic en **Ponerse en contacto ahora**.
Una vez aplicada la licencia en el servidor de licencias, cualquier equipo protegido asociado se actualiza con la nueva licencia de manera automática.

Adición de una licencia

Los propietarios de dispositivos de copias de seguridad de Dell pueden agregar una o más licencias a la Core Console de Rapid Recovery.

Cuando haya actualizado la licencia de Rapid Recovery o haya adquirido una, recibirá un archivo o una clave de licencia por correo electrónico.

También puede actualizar o cambiar una licencia existente en la Core Console. Para obtener más información, consulte [Actualización o cambio de una licencia](#).

NOTA: Únicamente los usuarios de servidores de copias de seguridad de Dell pueden ver el botón Agregar servidor.

NOTA: Para obtener más información sobre cómo obtener una clave de licencia, consulte la guía del usuario del *Dell Data Protection | Portal de licencias de Rapid Recovery*.

- 1 Desplácese hasta la Core Console de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Configuración).
- 3 Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Licencias. Aparece la configuración del Core para las licencias.
- 4 Para agregar una licencia y asociarla con su Core, en la parte superior del área de configuración del Core Detalles de licencia, haga clic en **Agregar licencia**. En el cuadro de diálogo **Agregar licencia**, realice una de las siguientes acciones:
 - a Si desea *introducir manualmente* la clave de licencia, en el cuadro de diálogo Cambiar licencia, escriba cuidadosamente la clave y, a continuación, haga clic en **Continuar**.
El cuadro de diálogo se cierra, el archivo de licencia seleccionado se autentica y esa licencia se asocia a su Core.
 - b Si desea *cargar* un archivo de licencia, en el cuadro de diálogo Cambiar licencia, haga clic en **Seleccionar archivo**.
En el cuadro de diálogo **Carga de archivo**, desplácese por el sistema de archivos y localice el nuevo archivo de licencia que desea utilizar. Por ejemplo, `busqueSoftware-YourCompany.lic`.
 - c Haga clic en el archivo de licencia y, a continuación, haga clic en **Abrir**.

El cuadro de diálogo Carga de archivo se cerrará. El archivo de licencia seleccionado aparece en el cuadro de diálogo Cambiar licencia.

- d En el cuadro de diálogo **Cambiar licencia**, haga clic en **Continuar**.

El cuadro de diálogo se cierra, el archivo de licencia seleccionado se autentica y esa licencia se asocia a su Core.

- 5 Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Servidor de licencias. Aparece la configuración del Core de Licencias.
- 6 En el área Servidor de licencias, haga clic en **Ponerse en contacto ahora**.
Una vez aplicada la licencia en el servidor de licencias, cualquier equipo protegido asociado se actualiza con la nueva licencia de manera automática.

Cómo ponerse en contacto con el servidor Dell Data Protection | Portal de licencias de Rapid Recovery

La Core Console de Rapid Recovery se pone frecuentemente en contacto con el servidor del portal para mantenerse actualizada de cualquier cambio que se realice en el Dell Data Protection | Portal de licencias de Rapid Recovery.

Para licencias que no son de prueba, el Core de Rapid Recovery contacta con el portal de licencias cada hora. Si el Core no puede contactar con el portal de licencias tras un periodo de gracia de 10 días, el Core deja de tomar instantáneas.

Por lo general, la comunicación con el servidor del portal de licencias se produce de forma automática, en los intervalos establecidos; no obstante, puede iniciar la comunicación bajo demanda.

Complete los pasos de este procedimiento para establecer contacto con el servidor del portal de licencias.

- 1 Desplácese hasta la Core Console de Rapid Recovery.
- 2 En la barra de iconos, haga clic en **Configuración** y, a continuación, desplácese hacia abajo en la parte derecha de la página **Configuración** hasta que vea el encabezado Servidor de licencias.
- 3 En el área Servidor de licencias, haga clic en **Ponerse en contacto ahora**.

Comprensión de la configuración de SNMP

Simple Network Management Protocol (SNMP) es un protocolo para administrar dispositivos en una red IP. SNMP se utiliza principalmente para supervisar dispositivos en una red buscando condiciones que requieren atención. Este protocolo utiliza componentes de software (agentes) para remitir información a sistemas administrativos (gestores). Un agente SNMP administra las solicitudes del gestor para obtener o establecer ciertos parámetros. El agente SNMP puede enviar capturas (notificaciones sobre eventos específicos) al gestor.

Los objetos de datos que administran los agentes SNMP se organizan en un archivo de Base de información de administración (MIB) que contiene Identificadores de objetos (OID). Cada OID identifica una variable que se puede leer o establecer utilizando SNMP.

Rapid Recovery incluye compatibilidad con la versión de SNMP 1.0.

Puede configurar el Core de Rapid Recovery como un agente SNMP. El Core puede informar sobre alertas, estado de repositorios y equipos protegidos. Un host SNMP puede leer esta información mediante una aplicación independiente denominada explorador SNMP. Puede instalar el explorador SNMP en cualquier equipo que esté accesible para el Core de Rapid Recovery a través de la red.

Para garantizar que el explorador SNMP puede recibir las notificaciones de eventos del Core SNMP, compruebe que las opciones de notificación de un grupo de notificación están correctamente configuradas para notificar mediante captura de SNMP.

¡NOTA: Puede utilizar el grupo predeterminado o crear un grupo de notificación personalizada. El proceso es el mismo.

Abra el grupo de notificación, seleccione la pestaña **Opciones de notificación** y compruebe que la opción **Notificar por captura de SNMP** está activada. El grupo de notificación especifica el número de captura 1 de manera predeterminada. Si fuera necesario, puede cambiar el número de captura para garantizar que coincide con el valor que espera el explorador SNMP.

Para obtener más información y detalles específicos sobre opciones de notificación de configuración, consulte [Configuración de grupos de notificación](#).

De forma alternativa, puede descargar un archivo MIB del Core de Rapid Recovery. Este archivo se puede leer con un explorador SNMP de forma más sencilla para el usuario que con los datos que recibe directamente desde el Core.

Esta sección incluye los siguientes temas:

- [Configuración de los valores SNMP](#)
- [Descarga del archivo MIB de SNMP](#)

Configuración de los valores SNMP

Utilice los parámetros de SNMP para controlar la comunicación entre el Core y el explorador SNMP. Esto incluye el puerto de SNMP, el puerto receptor de capturas y el nombre de host del receptor de capturas.

Utilice este procedimiento para configurar los parámetros de SNMP para el Core.

- 1 Desplácese hasta la Core Console de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Configuración) y, a continuación, realice una de las acciones siguientes:
 - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **Configuración de SNMP**.
 - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado Configuración de SNMP. Aparecen los valores de Configuración de SNMP.
- 3 Modifique la configuración de SNMP según se describe en la tabla siguiente.

Tabla 21. Información de configuración de la conexión SNMP

Cuadro de texto	Descripción
Puerto entrante	Especifique un número de puerto para la conexión SNMP.  NOTA: El valor predeterminado es 8161.
Puerto de receptor de captura	Introduzca un número de puerto del receptor de captura. El valor predeterminado es 162.
Nombre de host de receptor de captura	Introduzca un nombre de host para la conexión SNMP.  NOTA: El nombre de host predeterminado es localhost.

- 4 Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en  para guardar el cambio y salir del modo edición, o haga clic en  para salir del modo edición sin guardar.

Descarga del archivo MIB de SNMP

El protocolo Simple Network Management Protocol se utiliza para controlar si existen condiciones que requieran su atención en los dispositivos de una red. Cuando el Core de Rapid Recovery se establece como un agente SNMP, el Core comunica información como alertas, el estado del repositorio y los equipos protegidos. Esta información la puede leer un host SNMP utilizando una aplicación autónoma denominada explorador SNMP.

Los objetos de datos administrados por los agentes SNMP se organizan en un archivo Base de información de administración (MIB) que contiene Identificadores de objetos (OID). Cada OID identifica una variable que se puede leer o establecer utilizando SNMP.

Puede descargar un archivo MIB del Core de Rapid Recovery. Un explorador SNMP puede entonces leer archivo, llamado dell-aa-core.mib, de forma más sencilla para el usuario que con los datos que recibe directamente desde el Core.

Siga este procedimiento para descargar el archivo MIB de SNMP del Core de Rapid Recovery.

- 1 Desplácese hasta la Core Console de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Más) y, a continuación, haga clic en **Descargas**. Aparece la página **Descargas**.
- 3 Desplácese hacia abajo al panel Otros archivos.
- 4 Para descargar el archivo MIB, haga clic en el vínculo de descarga **Archivo MIB de SNMP**. Aparecen los valores de Configuración de SNMP.
- 5 En el cuadro de diálogo **Abriendo dell-aa-core.mib**, realice una de las siguientes acciones:
 - Para abrir el archivo de registro, seleccione **Abrir con** y, a continuación, elija una aplicación de explorador SNMP para ver el archivo de texto MIB, y por último haga clic en **Aceptar**. El archivo dell-aa-core.mib se abre en la aplicación seleccionada.
 - Para guardar el archivo localmente, seleccione **Guardar archivo** y haga clic en **Aceptar**. El archivo dell-aa-core.mib se guardará en su carpeta Descargas. Puede abrirse mediante un explorador SNMP o un editor de texto.

Configuración de los valores de vSphere

VMware vSphere es una suite de software de virtualización desde la que puede administrar las máquinas virtuales ESXi o vCenter Server. Si utiliza vSphere, no es necesario cargar el software Rapid Recovery Agent en máquinas virtuales individuales para protegerlas. Esto se denomina la función de protección sin agente, que solo se aplica en máquinas virtuales.

Utilice este procedimiento para configurar los parámetros de vSphere para el Core.

- 1 Desplácese hasta la Core Console de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Configuración) y, a continuación, realice una de las acciones siguientes:
 - En la lista de configuración del Core del lado izquierdo de la página Configuración, haga clic en **vSphere**.
 - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado vSphere. Aparece la configuración de vSphere.
- 3 Modifique la configuración de vSphere según se describe en la tabla siguiente.

Tabla 22. Información de configuración de VSphere Core

Elemento de la IU	Tipo de módulo de la IU	Descripción
Duración de la conexión	Cuadro de rotación	Establece la duración antes de que se agote el tiempo de espera para la conexión con el servidor ESXi. Utiliza el formato HH:MM:SS.  NOTA: El valor predeterminado es 00:10:00 o diez minutos.
Consolidaciones máximas simultáneas	Campo de texto	Establece el número máximo de consolidaciones simultáneas para las máquinas virtuales protegidas.  NOTA: El valor predeterminado es 0.
Número máximo de reintentos	Campo de texto	Establece el número máximo de intentos para la conexión a un disco virtual o a las operaciones de lectura y escritura antes de que se agote el tiempo de espera.

Elemento de la IU	Tipo de módulo de la IU	Descripción

NOTA: El valor predeterminado es 10.

Permitir restauración en paralelo	Boolean (casilla de verificación)	Cuando esta opción está seleccionada, se activa una restauración paralela para una máquina virtual sin agente. Cuando esta opción está demarcada, la función está desactivada.

NOTA: El valor predeterminado es No (desmarcada).

- 4 Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en la marca de verificación para guardar los cambios y salir del modo edición, o haga clic en **X** para salir del modo sin guardar.

Copia de seguridad y restauración de la configuración del Core

Puede realizar una copia de seguridad de la información de la configuración del Core en un archivo, para luego restaurar dicha configuración si tiene problemas con el equipo del Core o si desea migrar esta configuración a un equipo diferente. La información que se incluye en la copia de seguridad incluye los metadatos de repositorios (como el nombre del repositorio, la ruta de acceso de los datos y la ruta de acceso de los metadatos); los equipos protegidos en el Core; las relaciones de replicación (orígenes y destinos); qué equipos están configurados para la espera virtual, así como información sobre las claves de cifrado.

Este proceso restaura solo los parámetros de configuración, no los datos. La información de seguridad (como las credenciales de autenticación) no se almacenan en el archivo de configuración. No hay riesgo de seguridad al guardar un archivo de configuración del Core.

NOTA: Debe realizar primero una copia de seguridad de la información de la configuración del Core antes de poder utilizar este proceso para restaurar configuraciones del Core.

Utilice este procedimiento para realizar una copia de seguridad y restaurar la configuración del Core.

- 1 Desplácese hasta la Core Console de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Configuración).
Aparecerá la página **Valores**. En la parte superior del panel Configuración, sobre las categorías de la configuración, verá dos botones, Configuración de copia de seguridad y Configuración de restauración.
- 3 Si desea realizar una copia de seguridad de la configuración del Core, vaya al [paso 4](#). Si desea restaurar la configuración del Core, vaya al [paso 6](#).
- 4 Para realizar una copia de seguridad de la configuración actual en un archivo XML, haga clic en **Configuración de copia de seguridad** en la parte superior de la página Configuración.
Aparece el cuadro de diálogo Configuración de copia de seguridad del Core.
- 5 En el cuadro de texto Ruta de acceso local, introduzca una ruta de acceso de un directorio accesible localmente del equipo del Core donde desea almacenar la configuración del Core como un archivo XML y, a continuación, haga clic en **Realizar copia de seguridad**.
Por ejemplo, introduzca `C:\Users\Your_User_Name\Documents\AA5CoreSettings` y después haga clic en **Realizar copia de seguridad**.
Se guardará un archivo denominado `AppRecoveryCoreConfigurationBackup.xml` en el destino local que especifique.
- 6 Para restaurar la configuración del Core desde un archivo XML de copia de seguridad guardado anteriormente empleando este método, realice los pasos siguientes.

NOTA: Cuando restaura los parámetros de configuración del Core, se reinicia el servicio del Core de Rapid Recovery.

- a En la parte superior de la página **Configuración**, haga clic en **Restaurar**.
Aparece el cuadro de diálogo **Restaurar configuración de Core**.
- b En el cuadro de texto **Ruta de acceso local**, introduzca la ruta de acceso local de la ubicación donde almacenó los parámetros de configuración del Core.

Por ejemplo, introduzca `C:\Users\Your_User_Name\Documents\AA5CoreSettings`.

- c Si no desea restaurar la información de repositorios, vaya al [paso g](#).
- d De forma opcional, si desea restaurar la información de repositorios según se haya configurado en el archivo de copia de seguridad, seleccione **Restaurar repositorios** y después haga clic en **Restaurar**.

Aparece el cuadro de diálogo **Restaurar repositorios**.

Si selecciona restaurar información de repositorios desde los datos de configuración en copia de seguridad, los repositorios configurados cuando se guardó la configuración del Core aparecerán para su verificación. Todos los repositorios existentes están seleccionados de forma predeterminada.

- e Verifique la información de los repositorios que desea restaurar. Si aparecen varios repositorios en las listas para su verificación y solo desea restaurar la información de algunos de ellos, anule la selección de cada repositorio que no desee.
- f Cuando esté satisfecho con la selección de repositorios que desea restaurar, haga clic en **Guardar**.

El cuadro de diálogo **Restaurar repositorios** se cierra.

- g En el cuadro de diálogo **Restaurar repositorios**, haga clic en **Restaurar**.

El cuadro de diálogo **Restaurar repositorios** se cierra y empieza el proceso de restauración. Aparecerá una alerta indicando que ha cambiado la configuración del servicio de repositorios.

- h Si no se puede restaurar cualquier parámetro de la configuración, verá un mensaje de error. Revise los detalles del error para ver si se requiere alguna acción por su parte. Para obtener más información, consulte [Visualización de eventos mediante las tareas, las alertas y el diario](#). Para continuar, haga clic en **Cerrar** para abandonar el cuadro de diálogo de error.
- i Después de restaurar la configuración, verifique lo siguiente:

- Desbloquee todas las claves de cifrado. Para obtener más información, consulte [Desbloqueo de una clave de cifrado](#).
- Si el estado en espera virtual está configurado para actualizar continuamente una VM a un destino de red, debe especificar las credenciales de red en la configuración del estado en espera virtual antes de realizar una sincronización satisfactoria. Para obtener más información, consulte [Exportación de VM](#).
- Si el archivo comprimido programado está configurado para archivar en una cuenta de almacenamiento de nube, debe especificar las credenciales para que el Core pueda conectarse a la cuenta de nube. Para obtener más información sobre la cuenta de almacenamiento de nube, consulte [Incorporación de una cuenta de nube](#).
- Si se ha establecido la replicación y desea restaurar en un Core de destino, verifique la configuración del Core (especialmente del host) de destino en el Core de origen. Para obtener más información, si administra su propio Core, consulte [Replicación a un Core de destino administrado automáticamente](#). Si está replicando a un Core administrado por un tercero, consulte [Replicación en un Core de destino externo](#).
- Si la comprobación de capacidad de conectabilidad de SQL está configurada y si la instancia de SQL Server que realiza la comprobación está en el equipo del Core, especifique las credenciales de SQL en la configuración Conectabilidad. Para obtener más información, consulte [Administración de la configuración de conectabilidad de SQL del Core](#).

Compruebe que la configuración del motor de reproducción se ha restaurado y actualice la configuración si no se garantizó una comunicación eficaz. Para obtener más información, consulte [Configuración de los parámetros del motor de Replay](#).

Herramientas de nivel del Core

Además de configurar las opciones del Core, también puede utilizar las herramientas a nivel del Core que se describen en la tabla siguiente.

Tabla 23. Otras herramientas a nivel del Core

Elemento de la IU	Descripción
Información del sistema	Rapid Recovery permite ver información sobre el Core de Rapid Recovery, que incluye información del sistema, volúmenes locales y montados, así como conexiones del motor de Replay. Para obtener más datos sobre la información que se muestra en la página Información del sistema, consulte Funcionamiento de la información del sistema para el Core.

Elemento de la IU	Descripción
	Para obtener más información sobre cómo acceder a la información del sistema, consulte Visualización de la información del sistema del Core .
Descarga de archivos de registro del Core	La información sobre diversas actividades del Core de Rapid Recovery se guarda en el archivo de registro del Core. Para diagnosticar posibles problemas, puede descargar y ver los registros del Core de Rapid Recovery. Para obtener más información sobre cómo acceder y ver los registros del Core, consulte Acceso a los registros del Core. Cada equipo protegido también guarda un registro de actividad. Este registro se puede cargar en el Core si selecciona el trabajo nocturno denominado Descargando los registros desde los equipos protegidos. Para obtener más información acerca de los trabajos nocturnos, consulte Descripción de los trabajos nocturnos. Para obtener más información sobre cómo configurar los parámetros de este trabajo nocturno para el Core, consulte Configuración de trabajos nocturnos para el Core. Para obtener más información sobre cómo configurar los trabajos nocturnos para equipos protegidos específicos, consulte Personalización de las tareas nocturnas de una máquina protegida.

Funcionamiento de la información del sistema para el Core

Rapid Recovery le permite ver información sobre el Core de Rapid Recovery. Puede ver la información general, información sobre volúmenes locales e información sobre volúmenes montados.

En el panel **General**, puede ver la información como se describe en la tabla siguiente.

Tabla 24. Información del sistema

Elemento de la IU	Descripción
Nombre de host	El nombre del equipo de su Core de Rapid Recovery.
Versión del sistema operativo	La versión del sistema operativo instalado en el Core de Rapid Recovery.
Arquitectura del sistema operativo	Enumera la estructura y el diseño subyacentes del equipo que aloja su Core de Rapid Recovery. También puede incluir el chipset y el sistema de 64 bits. El Core de Rapid Recovery solo es compatible con sistemas de 64 bits.
Memoria (física)	Enumera la cantidad de memoria de acceso aleatorio (RAM) instalada en el equipo del Core.
Nombre mostrado	Muestra el nombre de visualización del Core, que es configurable (consulte Configuración de los parámetros generales del Core).
Nombre de dominio totalmente cualificado	Muestra el nombre de dominio totalmente cualificado del equipo del Core.
Ubicación de la caché de metadatos	Muestra la ruta de acceso de la ubicación de la caché de metadatos. Para obtener más información, consulte Funcionamiento de la caché de deduplicación y las ubicaciones de almacenamiento.
Ubicación de la caché principal	Muestra la ruta de acceso de la ubicación de la caché de deduplicación principal. Para obtener más información, consulte Funcionamiento de la caché de deduplicación y las ubicaciones de almacenamiento.
Ubicación de la caché secundaria	Muestra la ruta de acceso de la ubicación de la caché de deduplicación secundaria. Para obtener más información, consulte Funcionamiento de la caché de deduplicación y las ubicaciones de almacenamiento.

El panel **Volúmenes** incluye la siguiente información sobre volúmenes de almacenamiento para la máquina del Core: nombre, ID de dispositivo, sistema de archivos, capacidad nativa, capacidad con formato, capacidad usada y puntos de montaje.

El panel **Conexiones del motor de reproducción** muestra información sobre los puntos de recuperación montados en estos momentos. Puede ver el Extremo local, el Extremo remoto, el Id. de Agent de la imagen montada, el Id. de imagen montada y el Nombre de visualización de la imagen montada. Puede ver si el montaje es escribible, ver el usuario autenticado, los bytes leídos y los bytes escritos.

Puede desmontar puntos de recuperación que estén montados localmente en un Core desde la página Montajes. Para obtener más información sobre el desmontaje de los puntos de recuperación, consulte [Desmontaje de puntos de recuperación](#).

Para obtener más información, consulte [Visualización de la información del sistema del Core](#).

Visualización de la información del sistema del Core

La información del sistema del Core incluye información general, información sobre volúmenes locales e información sobre los volúmenes montados en el Core. Para obtener una descripción detallada de la información disponible en esta página, consulte [Funcionamiento de la información del sistema para el Core](#).

Complete los pasos de este procedimiento para ver la información del sistema del Core.

❗ NOTA: También puede ver la información del sistema de un equipo protegido específico. Para obtener más información, consulte [Visualización de la información del sistema de un equipo protegido](#).

- 1 Desplácese hasta la Core Console de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Más) y haga clic en  **Información del sistema**.
Aparece la página Información del sistema.

Acceso a los registros del Core

La información sobre diversas actividades del Core de Rapid Recovery se guarda en el archivo de registro del Core. Este archivo, AppRecovery.log, se almacena de forma predeterminada en la ruta C:\ProgramData\AppRecovery\Logs.

❗ NOTA: Dependiendo de su configuración, es posible que el directorio de AppRecovery no esté visible en el Core de Rapid Recovery. Para ver este directorio es posible que tenga que cambiar el panel de control de opciones de carpeta para que muestre archivos, carpetas y unidades ocultos. Si esta configuración incluye la opción de ocultar extensiones de tipos de archivos conocidos, es posible que el archivo de registro del Core aparezca como AppRecovery sin la extensión .log.

El registro del Core incluye información sobre los trabajos completados del Core, fallos de conexión, los resultados de intentos por parte del Core para ponerse en contacto con el portal de licencias y otra información. Cada declaración almacenada en el archivo de registro del Core va precedida por uno de cuatro calificadores: INFORMACIÓN, DEPURAR, ERROR y ADVERTENCIA. Estos calificadores ayudan a organizar por categorías la naturaleza de la información almacenada en el registro a la hora de diagnosticar un problema.

❗ NOTA: De igual manera, un archivo de registro también se almacena en cada equipo protegido con información relativa a sus intentos de comunicarse con el Core. Para obtener más información acerca de los registros de equipos, consulte [Acceso a los diagnósticos de equipos protegidos](#).

La capacidad de acceder a registros puede ser útil al solucionar un problema o trabajar con el Soporte de Rapid Recovery de Dell. Para acceder a los registros, consulte los siguientes procedimientos:

- [Descarga y visualización del archivo de registro del Core](#)
- [Descarga y visualización del archivo de registro de un equipo protegido](#)

Descarga y visualización del archivo de registro del Core

Si se produce algún error o problema con el Core, puede descargar los registros del Core para verlos o consultarlos con su representante de Dell Support.

- 1 En la Rapid Recovery Core Console, en la barra de iconos, haga clic en  (Más) y, a continuación, haga clic en  **Registro del Core**.
- 2 En la página **Descargar registro del Core**, haga clic en  **Haga clic aquí para iniciar la descarga**.
- 3 Si se le solicita que abra o guarde el archivo `CoreAppRecovery.log`, haga clic en **Guardar**.
- 4 Si observa el cuadro de diálogo **Apertura de Opening CoreAppRecovery.log**, realice una de las siguientes acciones:
 - Para abrir el archivo de registro, seleccione **Abrir con** y, a continuación, seleccione una aplicación (como Bloc de notas) para visualizar el archivo de registro basado en texto y haga clic en **Aceptar**.
Se abre el archivo `CoreAppRecovery.log` en la aplicación seleccionada.
 - Para guardar el archivo localmente, seleccione **Guardar archivo** y haga clic en **Aceptar**.
El archivo `CoreAppRecovery.log` se guardará en su carpeta **Descargas**. Se puede abrir con un editor de texto.

Vínculos relacionados

[Descarga y visualización del archivo de registro del Core](#)

[Descarga y visualización del archivo de registro de un equipo protegido](#)

Planificación de la configuración del Core

La configuración incluye tareas como la creación y configuración del repositorio para almacenar instantáneas de copia de seguridad, definir claves de cifrado para asegurar los datos protegidos y configurar alertas y notificaciones. Después de completar la configuración del Core, puede proteger los Agents y realizar la recuperación.

La configuración del Core implica comprender varios conceptos y realizar las operaciones iniciales siguientes:

- Crear un repositorio
- Configurar claves de cifrado
- Configurar notificación de eventos
- Configurar la política de retención
- Configurar la conectabilidad de SQL

Repositorios

En esta sección se describe cómo trabajar con repositorios. Se describen las funciones y atributos del repositorio del administrador de volúmenes de deduplicación. Describe los tipos de deduplicación que se utilizan en Rapid Recovery y cómo se utilizan las deduplicaciones en la aplicación. A continuación, esta sección describe cómo administrar los repositorios DVM, incluidos la creación de un repositorio, la visualización y edición de detalles y la eliminación de repositorios. Puede conocer cómo se abre un repositorio de un Core en otro Core. Por último, esta sección describe cómo migrar los puntos de recuperación manualmente de un repositorio a otro.

Administración de un repositorio DVM

Antes de que pueda utilizar Rapid Recovery, debe configurar uno o más repositorios en el Core de Rapid Recovery. Un repositorio almacena los datos protegidos, más concretamente, las instantáneas que se capturan en los equipos protegidos del entorno.

La administración de un repositorio DVM implica las siguientes operaciones:

- 1 **Creación de un repositorio DVM.** Antes de crear un repositorio, tenga en cuenta el tipo de tecnología apropiado.
Para obtener información sobre los repositorios, consulte [Definición de los repositorios](#).

Para obtener información sobre cómo crear un repositorio DVM, consulte [Creación de un repositorio DVM](#).

- 2 **Adición de una nueva ubicación de almacenamiento.** Para obtener más información sobre cómo agregar una nueva ubicación de almacenamiento a un repositorio DVM, consulte [Cómo agregar una ubicación de almacenamiento a un repositorio DVM existente](#).
- 3 **Modificación de la configuración del repositorio.** Para obtener más información sobre la modificación de la configuración del repositorio de un repositorio, consulte [Ver o modificar los detalles de un repositorio](#).
- 4 **Comprobación de un repositorio.** Para obtener más información sobre cómo comprobar un repositorio DVM, consulte [Comprobación de un repositorio](#).
- 5 **Realización de un trabajo de optimización de repositorio.** Para obtener más información sobre el trabajo de optimización de repositorio, consulte [Acerca de del trabajo de optimización de repositorio](#). Para obtener información sobre los pasos para optimizar un repositorio DVM existente, consulte [Optimización de un repositorio DVM](#).
- 6 **Eliminación de un repositorio.** Para obtener más información sobre cómo eliminar un repositorio, consulte [Eliminación de un repositorio](#).

Creación de un repositorio DVM

Este proceso describe cómo crear un repositorio en el Core con la tecnología de repositorio del Deduplication Volume Manager (Administrador de volúmenes de deduplicación, DVM).

- Debe tener privilegios administrativos para acceder a la máquina en la que desea crear un repositorio de DVM.
- Este tipo de repositorio exigen un mínimo de 150 GB de espacio de almacenamiento disponible en el volumen que defina como ubicación de almacenamiento.
- La ubicación de almacenamiento para un repositorio de DVM debe estar en una unidad local conectada al servidor del Core.
- El servidor del Core puede ser un dispositivo de la serie DL (incluido el DL1000) o puede ser cualquier servidor Windows basado en software que cumpla los requisitos del sistema.

NOTA: Se recomienda crear el repositorio a través de la pestaña **Appliance (Dispositivo)**. Para obtener más información, consulte la sección [Aprovisionamiento de almacenamiento](#).

Complete los pasos siguientes para crear un repositorio de DVM.

- 1 Vaya a la Rapid Recovery Core Console.
- 2 En la barra de iconos, haga clic en  (Más) y, a continuación, seleccione **Repositories (Repositorios)**. Aparecerá la página **Repositories (Repositorios)**.

En la página **Repositories (Repositorios)**, aparece el panel de repositorios de DVM.

- 3 En la parte superior de la página, haga clic en **Add New DVM Repository (Agregar nuevo repositorio de DVM)**. Aparecerá el cuadro de diálogo **Add New Repository (Agregar nuevo repositorio)**.
- 4 Introduzca la información según se describe en la tabla siguiente.

Tabla 25. Agregar configuración del nuevo repositorio

Cuadro de texto	Descripción
Repository Name (Nombre del repositorio)	Escriba el nombre de pantalla del repositorio. De manera predeterminada, este cuadro de texto se compone de la palabra Repositorio y un número, que coincide con el número de repositorios que existen para este Core. Por ejemplo, si este es el primer repositorio, el nombre predeterminado es Repositorio 1. Cambie el nombre según sea necesario. Los nombres de repositorio deben contener entre 1 y 40 caracteres alfanuméricos, incluidos espacios. No utilice caracteres prohibidos ni frases prohibidas.
Concurrent Operations	Define el nombre de solicitudes simultáneas que desea que admita el repositorio. De manera predeterminada, el valor es 64.

Cuadro de texto	Descripción
(Operaciones simultáneas)	
Comments (Comentarios)	Opcionalmente, introduzca una nota descriptiva sobre este repositorio. Puede introducir hasta 254 caracteres. Por ejemplo, escriba DVM Repositorio 2 .

- 5 Haga clic en **Add Storage Location (Agregar ubicación de almacenamiento)** para definir la ubicación de almacenamiento específica o el volumen del repositorio. Este volumen debe ser la ubicación de almacenamiento principal.

PRECAUCIÓN: Defina una carpeta específica dentro de la raíz para la ubicación de almacenamiento del repositorio. No especifique la ubicación raíz. Por ejemplo, utilice E:\Repository\, no E:\. Si el repositorio que va a crear en este paso se elimina posteriormente, se eliminarán todos los archivos incluidos en la ubicación de almacenamiento de su repositorio. Si define la ubicación de almacenamiento en la raíz, todos los demás archivos en el volumen (ej., E:\) se eliminan, lo que podría provocar una pérdida de datos catastrófica.

Aparecerá el cuadro de diálogo **Add Storage Location (Agregar ubicación de almacenamiento)**.

- 6 Haga clic en **Add Storage Location (Agregar ubicación de almacenamiento)** para definir la ubicación de almacenamiento específica o el volumen del repositorio. Este volumen debe ser la ubicación de almacenamiento principal.
- 7 En el área **Storage Location (Ubicación de almacenamiento)**, especifique cómo desea agregar el archivo para la ubicación de almacenamiento. Puede agregar un volumen de almacenamiento conectado localmente (por ejemplo, un almacenamiento de conexión directa, una red de área de almacenamiento o un almacenamiento de red conectado). También puede especificar un volumen de almacenamiento en una ubicación compartida del Common Internet File System (Sistema de archivos de Internet común - CIFS)
- Haga clic en **Add the file on local disk (Agregar el archivo en disco local)** para especificar una máquina local y, a continuación, indique la información según se describe en la tabla siguiente.

Tabla 26. Configuración de disco local

Cuadro de texto	Descripción
Data Path (Ruta de datos)	Introduzca la ubicación para almacenar los datos protegidos. Por ejemplo, escriba X:\Repository\Data. Al especificar la ruta, escriba solo caracteres alfanuméricos, un guión o un punto (para separar los nombres de host y los dominios). Puede utilizar la barra diagonal invertida únicamente para definir los niveles en la ruta. No utilice espacios. No se admite ningún otro símbolo ni caracteres de puntuación.
Metadata path (Ruta de metadatos)	Introduzca la ubicación para almacenar los metadatos protegidos. Por ejemplo, escriba X:\Repository\Metadata. Al especificar la ruta, escriba solo caracteres alfanuméricos, un guión o un punto (para separar los nombres de host y los dominios). Puede utilizar la barra diagonal invertida únicamente para definir los niveles en la ruta. No utilice espacios. No se admite ningún otro símbolo ni caracteres de puntuación.

- O bien, seleccione **Add file on CIFS share (Agregar archivo en recurso compartido CIFS)** para especificar una ubicación compartida de red y, a continuación, indique la información según se describe en la tabla siguiente.

Tabla 27. Credenciales del recurso compartido CIFS

Cuadro de texto	Descripción
UNC Path (Ruta UNC)	Introduzca la ruta de acceso para la ubicación del recurso compartido de red. Si la ubicación se encuentra en la raíz, cree un nombre de carpeta específico (por ejemplo, Repository). La ruta debe empezar por \\. Al especificar la ruta, escriba solo caracteres alfanuméricos, un guión o un punto (para separar los nombres de host y los dominios). Las letras de la "a" a la "z" no distinguen

Cuadro de texto	Descripción
	mayúsculas de minúsculas. No utilice espacios. No se admite ningún otro símbolo ni caracteres de puntuación.
User name (Nombre de usuario)	Especifique un nombre de usuario para el acceso a la ubicación del recurso compartido de red.
Password (Contraseña)	Especifique una contraseña para acceder a la ubicación del recurso compartido de red.

- 8 En el área **Storage Configuration (Configuración de almacenamiento)**, haga clic en **More Details (Más detalles)** e introduzca los detalles de la ubicación de almacenamiento según se describe en la tabla siguiente.

Tabla 28. Detalles de la configuración de almacenamiento

Cuadro de texto	Descripción
Size (Tamaño)	Establezca el tamaño o capacidad de la ubicación de almacenamiento. El tamaño mínimo es 1 GB. El valor predeterminado es 250 GB. Puede elegir entre las opciones siguientes: - GB - TB NOTA: El tamaño que especifique no puede superar el tamaño del volumen. Si la ubicación de almacenamiento es un volumen de sistema de archivos de nueva tecnología (NTFS) que tiene Windows XP o Windows 7 instalado, el límite de tamaño de archivo es 16 TB. Si la ubicación de almacenamiento es un volumen NTFS que ejecuta Windows 8, 8.1, Windows 10 o Windows Server 2012, 2012 R2, el límite de tamaño de archivo es 256 TB. NOTA: Para que Rapid Recovery pueda validar el sistema operativo, el Instrumental de administración de Windows (WMI) debe estar instalado en la ubicación de almacenamiento deseada.
Write Caching Policy (Política de escritura en caché)	La política de escritura en caché de controla cómo se utiliza el Windows Cache Manager (Administrador de caché de Windows) en el repositorio y ayuda a ajustar el repositorio para un rendimiento óptimo en diferentes configuraciones. Establezca el valor en una de las opciones siguientes: - On (Activado) - Off (Desactivado) - Sync (Sincronizar) Si se establece en On (Activado), que es el valor predeterminado, Windows controla el almacenamiento en caché. Esto es adecuado para Windows 10, y para las versiones de Windows Server 2012 y posteriores. NOTA: Si se establece la política de escritura en caché en On (Activado), se mejora el rendimiento. Si utiliza Windows Server 2008 SP2 o Windows Server 2008 R2 SP2, el valor recomendado es Off (Desactivado). Si se establece en Off (Desactivado), Rapid Recovery controla el almacenamiento en caché. Si se establece en Sync (Sincronizar), Windows controla el almacenamiento en caché así como la entrada/salida sincrónica.
Bytes per sector (Bytes por sector)	Especifique el número de bytes que desee incluir en cada sector. El valor predeterminado es 512.
Average Bytes per Record (Número)	Especifique el número promedio de bytes por segundo. El valor predeterminado es 8192.

Cuadro de texto	Descripción

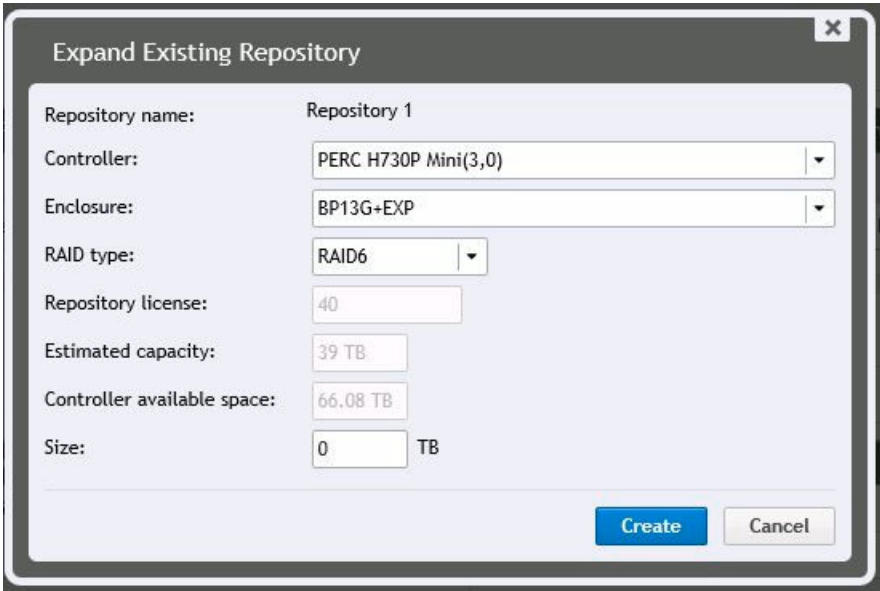
promedio de bytes por registro)	

- Haga clic en **Save (Guardar)**.
El cuadro de diálogo **Add Storage Location (Agregar ubicación de almacenamiento)** se cierra y se guardará la configuración. El cuadro de diálogo **Add New Repository (Agregar nuevo repositorio)** muestra la nueva ubicación de almacenamiento.
- De manera opcional, repita el paso 6 al paso 9 para agregar más ubicaciones de almacenamiento para el repositorio.
- Cuando haya definido todas las ubicaciones de almacenamiento que desee crear para el repositorio, haga clic en **Create (Crear)** en el cuadro de diálogo **Add New Repository (Agregar nuevo repositorio)**.
El cuadro de diálogo **Add New Repository (Agregar nuevo repositorio)** se cierra y se aplican los cambios. Se abre la página **Repositories (Repositorios)**, que muestra el repositorio recién agregado en la tabla de resumen de los repositorios de DVM.

Expansión del repositorio

La función de expansión del repositorio está disponible en todos los modelos DL (1300, 4300, 4000), excepto el DL 1000. El tipo de licencia que se aplica limita el tamaño del repositorio. Para ampliar el repositorio utilizando almacenamiento interno sin utilizar y almacenamiento en un gabinete externo, actualice la licencia. Para cambiar la clave de licencia, consulte la sección. [Actualización o cambio de una licencia](#). Para expandir el repositorio existente:

- Haga clic en **Appliance (Dispositivo) > Provisioning (Aprovisionamiento)**.
- En la sección **Repositories (Repositorios)**, haga clic en  → **Expand Existing Repository (Expandir repositorio existente)** junto al repositorio que desee ampliar.
Se muestra el cuadro de diálogo **Expand Existing Repository (Expandir repositorio existente)**.



- En el cuadro de diálogo **Expand Existing Repository (Expandir repositorio existente)**.

Tabla 29. Expansión del repositorio existente

Cuadro de texto	Descripción
Repository Name (Nombre del repositorio)	Se muestra el nombre del repositorio que se va a expandir.
Controller (Controladora)	Seleccione la controladora de almacenamiento en función de si está creando un repositorio en el almacenamiento interno o en el gabinete de almacenamiento de conexión directa.
Enclosure (Gabinete)	Seleccione el gabinete de almacenamiento adecuado.
RAID type (Tipo de RAID)	Seleccione la configuración de RAID. Dispone de las siguientes opciones para las configuraciones de RAID: 1, 5 o 6.
Repository license (Licencia del repositorio)	Se muestra la licencia del repositorio.
Estimated capacity (Capacidad estimada)	Muestra la capacidad estimada que hay disponible para crear un repositorio.
Controller available space (Espacio disponible en la controladora)	Muestra el espacio disponible en la controladora.
Size (Tamaño)	Introduzca el tamaño del repositorio que vaya a crearse.
4 Haga clic en Create (Chasquido; haga clicrear) .	
La nueva ubicación del repositorio se agrega al repositorio existente.	
El repositorio se expande al tamaño especificado.	

Ver o modificar los detalles de un repositorio

- Vaya a la Rapid Recovery Core Console.
- En la barra de iconos, haga clic en  (Más) y, a continuación, seleccione **Repositories (Repositorios)**. Aparecerá la página **Repositories (Repositorios)**.
Aparece el panel **DVM Repositories (Repositorios de DVM)**.
- En el menú de la página **Repositories (Repositorios)**, puede realizar las siguientes acciones generales:

Opción	Descripción
Add New DVM Repository (Agregar nuevo repositorio de DVM)	Agrega un nuevo repositorio de DVM
Open Existing DVM Repository (Abrir repositorio de DVM existente)	Abre un repositorio de DVM existente desde otro Core, que cambia la propiedad del repositorio a este Core. Para obtener más información, ver Abrir un repositorio DVM existente :
Refresh (Actualizar)	Permite ver o actualizar la lista de repositorios.

- En el panel **DVM Repositories (Repositorios de DVM)**, menú desplegable  para cualquier repositorio de DVM, puede realizar las siguientes acciones adicionales:

Opción	Descripción
Add Storage Location (Agregar ubicación de almacenamiento)	Amplía el repositorio existente agregando una ubicación de almacenamiento

 **NOTA:** Cuando amplíe un volumen del repositorio de DVM, en primer lugar detenga la protección. A continuación, amplíe el volumen y, finalmente, reanude la protección. Esta acción evita que se produzca un error infrecuente que sólo se produce cuando se amplía un volumen simultáneamente con una fase de transferencia.

Opción	Descripción
Check (Verificar)	Realiza una verificación repositorio
Settings (Configuración)	Permite ver o modificar la configuración del repositorio. Estos ajustes incluyen: • Visualización del nombre del repositorio • Visualización o modificación de las operaciones simultáneas máximas • Visualización o modificación de la descripción del repositorio • Activación o desactivación de la deduplicación • Activación o desactivación de la compresión de datos almacenados en el repositorio
Perform Optimization Job (Realizar trabajo de optimización)	Realiza un trabajo optimización en el repositorio
Delete (Eliminar)	Elimina un repositorio

NOTA: Cuando amplíe un volumen del repositorio de DVM, en primer lugar detenga la protección. A continuación, amplíe el volumen y, finalmente, reanude la protección. Esta acción evita que se produzca un error infrecuente que puede producirse cuando se amplía un volumen con una fase de transferencia específica.

Puede realizar las siguientes acciones generales en la página Repositories (Repositorios):

- Permite ver o actualizar la lista de repositorios.
- Add a new repository (Agregar un nuevo repositorio)
- Abra un repositorio existente desde otro Core, lo cual cambia la propiedad a este repositorio

Cómo agregar una ubicación de almacenamiento a un repositorio DVM existente

NOTA: Se recomienda que expanda el repositorio a través de la pestaña Servidor. Para obtener más información, consulte [Expansión del repositorio](#)

Agregar una ubicación de almacenamiento a un repositorio DVM permite definir dónde se almacenará el repositorio o volumen.

Complete los pasos del procedimiento siguiente para especificar la ubicación de almacenamiento para el repositorio o volumen.

- 1 Desplácese hasta la Core Console de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Más información), y, a continuación, seleccione **Repositorios**. Aparecerá la página Repositories (Repositorios).

Aparece el panel Repositorios DVM.
- 3 En la tabla de resumen de los repositorios, en la fila que representa el repositorio DVM para el que desea agregar una ubicación de almacenamiento, haga clic en **Configuración** y seleccione **Agregar ubicación de almacenamiento**. Aparece el cuadro de diálogo **Agregar ubicación de almacenamiento**.
- 4 Especifique cómo agregar el archivo a la ubicación de almacenamiento. Puede elegir agregar el archivo en el disco local o en un recurso compartido CIFS.
 - Seleccione **Agregar el archivo en disco local** para especificar un equipo local y, a continuación, introduzca la información según se describe en la siguiente tabla.

Tabla 30. Parámetros de Disco local

Cuadro de texto	Descripción
Ruta de acceso a datos	Introduzca la ubicación para almacenar los datos protegidos. Por ejemplo, introduzca X:\Repository\Data.

Cuadro de texto	Descripción
	Se aplican las mismas limitaciones en la ruta de acceso; utilice solo caracteres alfanuméricos, guiones o puntos, sin espacios ni caracteres especiales.
Ruta de acceso a metadatos	Introduzca la ubicación para almacenar los metadatos protegidos. Por ejemplo, introduzca X:\Repository\Metadata. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guión y el punto (solo para separar nombres de host y dominios). Las letras de la a la z no distinguen entre mayúsculas y minúsculas. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.
O, seleccione Agregar archivo en recurso compartido CIFS para especificar una ubicación de uso compartido de red y, a continuación, introduzca la información según se describe en la siguiente tabla.	

Tabla 31. Credenciales de recurso compartido CIFS

Cuadro de texto	Descripción
Ruta de acceso de UNC	Introduzca la ruta de acceso de la ubicación de uso compartido de red. Si esta ubicación está en la raíz, defina un nombre de carpeta específico (por ejemplo, Repository). La ruta de acceso debe comenzar por \\. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guión y el punto (solo para separar nombres de host y dominios). Las letras de la a la z no distinguen entre mayúsculas y minúsculas. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.
Nombre de usuario	Especifique un nombre de usuario para el acceso a la ubicación compartida de red.
Contraseña	Especifique una contraseña para acceder a la ubicación de uso compartido de red.

- 5 En el panel Configuración de almacenamiento, haga clic en **Más detalles** e introduzca los detalles para la ubicación de almacenamiento según se describen en la siguiente tabla.

Tabla 32. Detalles de ubicación de almacenamiento

Cuadro de texto	Descripción
Tamaño	Establezca el tamaño o capacidad de la ubicación de almacenamiento. El tamaño predeterminado es 250 GB. Puede elegir entre las siguientes opciones: - GB - TB NOTA: El tamaño mínimo es de 1 GB. El tamaño que especifique no puede superar el tamaño del volumen. Si la ubicación del almacenamiento es un volumen New Technology File System (NTFS) utilizando Windows XP o Windows 7, el límite de tamaño del archivo es 16 TB. Si la ubicación del almacenamiento es un volumen NTFS utilizando Windows 8, 8.1 o Windows Server 2012, 2012 R2, el límite de tamaño del archivo es 256 TB. NOTA: Para que Rapid Recovery pueda validar el sistema operativo, el Instrumental de administración de Windows (WMI) debe estar instalado en la ubicación de almacenamiento deseada.
Política de almacenamiento en caché de escritura	La política de almacenamiento en caché de escritura controla cómo se utiliza el Administrador de caché de Windows en el repositorio y ayuda a ajustar el repositorio para un rendimiento óptimo en diferentes configuraciones. Establezca el valor en una de las opciones siguientes: - Activado - Desactivado

Cuadro de texto	Descripción
	Sincronización Si se establece como Activado, que es el valor predeterminado, Windows controla el almacenamiento en caché. Es apropiado para Windows 10 y para las versiones de Windows Server 2012 y posteriores. NOTA: si se establece la política de escritura en caché en Activado, se mejora el rendimiento; no obstante, el valor recomendado es Desactivada. Si utiliza Windows Server 2008 SP2 o Windows Server 2008 R2 SP2, la configuración recomendada es desactivado. Si se establece en Desactivado, Rapid Recovery controla el almacenamiento en caché. Si se establece en Sincronización, Windows controla el almacenamiento en caché así como la entrada/salida sincrónica.
Bytes por sector	Especifique el número de bytes que desea que incluya cada sector. El valor predeterminado es 512.
Promedio de bytes por registro	Especifique el promedio del número de bytes por registro. El valor predeterminado es 8192.
6	De manera opcional, si desea realizar el trabajo de optimización de repositorio para el repositorio seleccionado, seleccione Ejecutar trabajo de optimización de repositorio para [nombre del repositorio]. Dell recomienda que realice el trabajo de optimización de repositorio al agregar ubicaciones de almacenamiento a un repositorio existente. Este trabajo optimiza el espacio libre aplicando la deduplicación a los datos almacenados en el repositorio. En función de varios factores, como el tamaño del repositorio, la cantidad de datos en el repositorio, el ancho de banda de red disponible y la carga existente en la entrada y salida del sistema, realizar un trabajo de optimización de repositorio podría tardar una cantidad considerable de tiempo y consumir gran parte del ancho de banda en su entorno. Para obtener más información sobre el trabajo de optimización de repositorio, consulte Acerca de del trabajo de optimización de repositorio.
7	Haga clic en Guardar. El cuadro de diálogo se cierra y la ubicación del almacenamiento se guarda. En la tabla de resumen de los repositorios, la ubicación de almacenamiento que ha creado es visible si expande los detalles de un repositorio.

Comprobación de la integridad de los repositorios de DVM

Los usuarios de Rapid Recovery Core pueden establecer distintas políticas de retención entre los Core de origen y de destino. Para que la replicación funcione correctamente con diferentes políticas de retención, el Core de destino debe tener la misma versión de software (o más reciente) que el Core de origen.

NOTA: Los Cores deben compartir los mismos tres dígitos para el número de publicación (por ejemplo, 6.0.1.xxxx o 5.4.3.xxxx). El número de compilación (representado por xxxx) puede ser diferente únicamente si el Core de destino es más reciente.

Los administradores pueden configurar la agregación a un Core de destino a una velocidad diferente que en el Core de origen. De forma similar, ahora puede definir una política de retención personalizada para cualquier máquina replicada. Por ejemplo, puede agregar puntos de recuperación en el Core de destino a una velocidad mayor y con menos resolución que en el Core de origen, lo que ahorra espacio. O bien puede agregar los puntos de recuperación para cualquier máquina replicada seleccionada a una velocidad más lenta en el Core de destino y mantener una mayor resolución, lo que puede ser útil para fines de cumplimiento. Para obtener más información acerca de cómo utilizar una política de retención diferente de la predeterminada en el Core, consulte [Personalización de la configuración de la política de retención de una máquina protegida](#).

Si el Core se ha actualizado desde AppAssure 5.3.x y ha utilizado la replicación, debe ejecutar este trabajo antes de poder configurar las políticas de retención diferentes entre el Core de origen y un Core de destino, o configurar una política de retención personalizada en una máquina replicada.

No podrá ver ni ejecutar este trabajo a menos que tenga uno o varios repositorios que cumplan los requisitos (creado antes de la versión 5.4.x pero no ejecutados).

La ejecución de este trabajo verifica la integridad de todos los datos almacenados en el repositorio especificado, lo que garantiza que puede recuperar datos de cada instantánea o imagen base. Si la comprobación de la integridad detecta un problema con los datos incluidos en el repositorio, el trabajo se detiene inmediatamente. Los detalles de evento de ese trabajo en el Core solicitarán que se ponga en contacto con el Servicio de asistencia de Dell para que pueda programar una hora para trabajar con un representante de asistencia con el fin de realizar procedimientos adicionales para identificar y solucionar incoherencias de datos.

⚠ PRECAUCIÓN: Es previsible que sea necesario un largo período de tiempo para ejecutar este trabajo. La cantidad de tiempo varía en función de la cantidad y el tipo de datos en el repositorio, así como del sistema de almacenamiento subyacente. Mientras el trabajo se está ejecutando, no puede llevar a cabo otras transacciones en ese repositorio, incluidas las transferencias (copia de seguridad de instantáneas e imágenes base y replicación), trabajos nocturnos, etc.

Puede realizar otras operaciones en otros repositorios mientras este trabajo se está ejecutando.

📘 NOTA: Este trabajo comprueba la integridad de todos los contenidos dentro de un repositorio. Para obtener más información sobre el trabajo de Integrity Check que puede utilizar para verificar el montaje y uso de un repositorio, consulte [Comprobación de un repositorio](#).

Comprobación de un repositorio

Rapid Recovery proporciona la capacidad de realizar una comprobación de diagnóstico de un volumen de repositorio DVM cuando se producen errores. Los errores del Core pueden ser el resultado de que se haya cerrado inadecuadamente, un fallo de hardware u otros factores de entorno de la pila IP inferiores que pueden exponerse en las funciones de Rapid Recovery.

📘 NOTA: Este procedimiento se debe realizar únicamente con fines de diagnóstico. Por ejemplo, ejecute esta comprobación en el caso de un error de hardware, apagado incorrecto del Core o error de importación de un repositorio.

- 1 Desplácese hasta la Core Console de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Más) y, a continuación, seleccione **Repositorios**. Aparecerá la página **Repositories (Repositorios)**.

Aparece el panel Repositorios DVM.
- 3 Para comprobar un repositorio DVM, en el panel **Repositorios DVM**, en cualquier fila de la tabla de resumen que representa un repositorio DVM, haga clic en  y, a continuación, seleccione **Comprobar**. Aparecerá el cuadro de diálogo **Check Repository (Comprobar repositorio)**.
- 4 En el cuadro de diálogo **Comprobar repositorio** confirme que entiende que se cancelan todas las tareas activas asociadas con este repositorio y que desea continuar.
Los trabajos activos se cancelan y el trabajo de comprobación de repositorio se inicia.
- 5 De manera opcional, se puede realizar un seguimiento del estado del trabajo haciendo clic en la barra de botones del menú desplegable **Tareas en ejecución**, y seleccionando el trabajo de mantenimiento del repositorio.

Acerca de del trabajo de optimización de repositorio

Cuando se utiliza un repositorio DVM, los datos que capture en cada instantánea se deduplican. Esta deduplicación se produce de manera gradual, a medida que las instantáneas se guardan en el repositorio. Se guarda una aparición de cada cadena de información en el repositorio. Cuando una cadena de información se deduplica, se utiliza una referencia a la cadena original en la caché de deduplicación, ahorrando así espacio en el repositorio.

Si la caché de deduplicación de DVM se llena, solo se deduplican los datos de instantánea que ya se han referenciado en la caché. A medida que se produce la deduplicación, la caché continúa la actualización con los nuevos valores exclusivos y sobrescribe los valores más antiguos de la caché. Esto da lugar a una menor deduplicación óptima.

Para obtener más información acerca de la deduplicación, consulte [Funcionamiento de la caché de deduplicación y las ubicaciones de almacenamiento](#).

Puede elegir aumentar la caché de deduplicación de DVM antes de que se llene, lo que garantiza la continuidad de una deduplicación óptima de los datos del repositorio. Para obtener más información, consulte [Configuración de los valores de caché de la deduplicación de DVM](#).

También puede aumentar la caché de deduplicación después de que se llene. Si desea reclamar espacio en el repositorio después de aumentar la caché, puede optimizar el repositorio. Esta acción fuerza una comparación de los datos en sus instantáneas con la información de la caché de deduplicación. Si hubiera cadenas repetidas en el repositorio, los datos se sustituyen con referencias a los datos, lo que ahorra espacio de almacenamiento en el repositorio. Este proceso se denomina a veces como deduplicación sin conexión, ya que el proceso de deduplicación se produce bajo solicitud, en lugar de gradualmente a medida que se transfieren los datos de instantánea.

El proceso de optimización hace un uso intensivo del procesador. La cantidad de tiempo que tarda en ejecutarse este trabajo depende de varios factores. Entre estos factores se incluye el tamaño del repositorio, la cantidad de datos en el repositorio, el ancho de red disponible y la carga existente en la entrada y salida del sistema. Cuantos más datos haya en el repositorio, más tardará el trabajo en ejecutarse.

Las siguientes acciones se sustituyen o cancelan cuando se produce un trabajo de optimización de repositorio.

- Trabajo de eliminación de puntos de recuperación
- Trabajo de mantenimiento de repositorio
- Trabajo de comprobación de la integridad del repositorio

Las siguientes acciones se sustituyen o cancelan cuando se produce un trabajo de optimización.

- Trabajo de eliminación de todos los puntos de recuperación
- Trabajo de eliminación de cadena de puntos de recuperación
- Trabajo de mantenimiento de repositorio
- Trabajo base de eliminación de puntos de recuperación
- Trabajo de comprobación de la integridad del repositorio

Para obtener información sobre los pasos del proceso de optimización de un repositorio DVM existente, consulte [Optimización de un repositorio DVM](#).

Puede interrumpir el trabajo de optimización de repositorio durante un tiempo limitado si es necesario. Para obtener más información, consulte [Interrupción o reanudación del trabajo de optimización del repositorio](#).

Optimización de un repositorio DVM

Debe tener un repositorio DVM en el Core para realizar este procedimiento.

Puede realizar deduplicación sin conexión de datos guardados en un repositorio DVM existente. Esto se consigue mediante el inicio del Trabajo de optimización de repositorio.

NOTA: Dell recomienda que realice el trabajo Optimizar repositorio solo después de aumentar el tamaño de la caché de deduplicación. Esta acción le permite recuperar espacio de repositorio y utilizar de forma más eficaz la caché de deduplicación de DVM.

Lleve a cabo los pasos de este procedimiento para optimizar un repositorio DVM.

- 1 Desplácese hasta la Core Console de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Más), y, a continuación, seleccione **Repositorios**. Aparecerá la página **Repositorios**.
- 3 En el panel Repositorios DVM, en la fila que representa el repositorio que quiere actualizar, haga clic en  y, a continuación, seleccione **Realizar trabajo de optimización**.

Aparece un mensaje de aviso que le pide que confirme la optimización.

- 4 Haga clic en confirmar la optimización.

El trabajo de optimización tiene prioridad sobre la mayoría de los otros trabajos. Si es necesario, puede interrumpir un trabajo de optimización en progreso. Para obtener más información sobre la interrupción o reanudación de este trabajo, consulte [Interrupción o reanudación del trabajo de optimización del repositorio](#).

Interrupción o reanudación del trabajo de optimización del repositorio

Al iniciar el Trabajo de optimización de repositorio, el repositorio DVM seleccionado se desduplica. Esta optimización de la desduplicación es un trabajo intensivo del procesador para ahorrar espacio en el repositorio. Para obtener más información, consulte [Acerca de del trabajo de optimización de repositorio](#).

Una vez que este trabajo se ha iniciado, puede interrumpir el trabajo mediante el procedimiento siguiente. Esto pausa la desduplicación. Si ya ha interrumpido una optimización, puede reanudar el proceso mediante este procedimiento.

NOTA: Este procedimiento se aplica solo a repositorios DVM y solo cuando el trabajo de optimización de repositorio se ha iniciado.

Complete los pasos de este procedimiento para interrumpir o reanudar un trabajo de optimización de repositorio.

- 1 Desplácese hasta la Core Console de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Más) y, a continuación, seleccione **Repositorios**.
Aparecerá la página **Repositorios (Repositorios)**.

Aparece el panel Repositorios DVM.
- 3 Si desea interrumpir un trabajo de optimización, haga lo siguiente:
 - a En la tabla de resumen de repositorios, desde la fila que representa el repositorio apropiado, haga clic en  y, a continuación, seleccione **Interrumpir trabajo de optimización**.
Aparece un mensaje de aviso que le pide que confirme la interrupción.
 - b Haga clic en confirmar la optimización.
- 4 Si desea reanudar un trabajo de optimización interrumpido, haga lo siguiente:
 - a En la tabla de resumen de repositorios, desde la fila que representa el repositorio apropiado, haga clic en  y, a continuación, seleccione **Continuar trabajo de optimización**.
Aparece un mensaje de aviso que le pide que confirme la interrupción.
 - b En el cuadro de diálogo, seleccione la opción **Continuar trabajo desde el punto de interrupción** y, a continuación, haga clic en **Sí**.

El cuadro de diálogo se cierra y el trabajo de optimización de repositorio se reanuda desde el punto donde se interrumpió por última vez.

Abrir un repositorio DVM existente

Como la tecnología del repositorio principal de Rapid Recovery, el repositorio DVM contiene datos de la instantánea (en forma de puntos de recuperación) de los equipos protegidos en Rapid Recovery Core específico. Puede abrir un repositorio existente de un Core (por ejemplo, Core A) en un segundo Core (Core B).

NOTA: Al abrir un repositorio desde otro Core cambia el propietario del repositorio. Al abrir un repositorio existente, la información es accesible únicamente en el segundo Core.

En el caso de un repositorio DVM, el Core original (Core A) no debe estar en uso actual. Por ejemplo, el equipo debe estar apagado, no se puede acceder a la red o los servicios de Core deben estar detenidos.

El repositorio puede estar en una ubicación de red compartida o en un dispositivo de almacenamiento accesible para el segundo Core.

Realice el procedimiento siguiente para abrir un repositorio existente.

- 1 Desplácese hasta la Core Console de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Más información), y, a continuación, seleccione **Repositorios**. Aparecerá la página **Repositorios**.

El panel de repositorios DVM también aparece.
- 3 Para abrir un repositorio DVM existente, en la parte superior de la página, haga clic en **Abrir repositorio DVM existente**. Aparecerá el cuadro de diálogo **Abrir repositorio DVM existente**.
- 4 En el cuadro de diálogo **Abrir repositorio DVM existente**, introduzca la siguiente información en el repositorio que desea abrir y, a continuación, haga clic en **Abrir**.

Tabla 33. Opciones de Abrir repositorio DVM existente

Cuadro de texto	Descripción
Ruta	La ruta de acceso del repositorio (por ejemplo, D:\trabajo\maquina de una ruta de acceso local, \10.10.99.155\repositorios por dirección IP o \\nombreservidor\nombre recurso compartido de una ruta de red).
Nombre de usuario	Si el repositorio tiene una ruta de acceso de red, introduzca el nombre de usuario para iniciar sesión en el recurso compartido de red.
Contraseña	Si el repositorio tiene una ruta de acceso de red, introduzca la contraseña para iniciar sesión en el recurso compartido de red.

El cuadro de diálogo se cierra y el repositorio seleccionado se agrega al Core actual.

Eliminación de un repositorio

Lleve a cabo los pasos de este procedimiento para eliminar un repositorio.

- 1 Desplácese hasta la Core Console de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Más) y, a continuación, seleccione **Repositorios**. Aparecerá la página **Repositorios**.

En la página **Repositorios**, aparece el panel Repositorios DVM.
- 3 En la tabla de resumen de repositorios, desde la fila que representa el repositorio que quiere eliminar, haga clic en  para expandir el menú desplegable y, a continuación, seleccione **Eliminar**. Aparece un mensaje de advertencia para confirmar la eliminación.
- 4 Haga clic en **Sí** para confirmar la eliminación del repositorio.

 **PRECAUCIÓN:** Cuando se elimina un repositorio los datos del mismo se descartan y no se pueden recuperar.

Ejecución de un trabajo de comprobación de repositorio en un repositorio DVM

Realice este procedimiento para comprobar la integridad de todo el repositorio DVM. Se recomienda para Cores de destino replicados cuando actualice de AppAssure 5.3.x a la versión 5.4. Durante la ejecución de la comprobación de integridad, que puede tardar cierto tiempo, no es posible realizar otras acciones en el repositorio.

Si tiene múltiples repositorios DVM para un Core de destino, realice este proceso una vez para cada repositorio.

NOTA: Si tiene otro repositorio DVM en el Core de destino para el que ya se ha completado el trabajo de comprobación de integridad o si crea un nuevo repositorio adicional para este Core de destino, puede realizar operaciones en ese repositorio secundario mientras el trabajo de comprobación de integridad se ejecuta en el repositorio DVM especificado.

- 1 Desplácese hasta la Core Console de Rapid Recovery.
 - 2 En la barra de iconos, haga clic en  (Más) y, a continuación, seleccione **Repositorios**.
Aparecerá la página **Repositorios (Repositorios)**.

Aparece el panel Repositorios DVM.
 - 3 En la tabla de resumen de repositorios, en la fila que representa al repositorio que desea comprobar, haga clic en  y en el menú desplegable, seleccione **Trabajo de comprobación de repositorio**.
Aparecerá un mensaje de confirmación.
- PRECAUCIÓN:** Antes de confirmar que desea realizar el trabajo, debe considerar con cuidado la duración de tiempo necesaria. Mientras el trabajo se está ejecutando, no es posible realizar ninguna otra transacción en ese repositorio, incluyendo las transferencias (instantáneas, copias de seguridad de imagen base y replicación), trabajos nocturnos, etc.
- 4 En el cuadro de diálogo **Trabajo de comprobación de repositorio**, para realizar la comprobación de integridad, haga clic en **Sí**.
El cuadro de diálogo se cierra. Cualquier trabajo que esté en cola o en progreso se cancelará y comenzará el trabajo de comprobación de integridad.
 - 5 Para supervisar el progreso del trabajo de comprobación de un repositorio, incluyendo la determinación de si es necesario realizar pasos adicionales tras la comprobación, en la barra de iconos, haga clic en  (Eventos).
 - 6 En la página **Eventos**, haga clic en  **Detalles del trabajo** de dicho trabajo para ver más información acerca de su estado.
 - Si ve un error en las tareas secundarias de este trabajo, anote el error y proporcione la información a un representante de asistencia técnica de Dell.
 - Si el trabajo de comprobación de repositorio termina todas las tareas secundarias con éxito, podrá establecer una política de retención personalizada para este repositorio.

Administración de la seguridad

Core puede cifrar datos de instantáneas de máquinas protegidas en el repositorio. En lugar de cifrar todo el repositorio, puede especificar una clave de cifrado durante la protección de una máquina en un repositorio, lo que le permite volver a utilizar las claves para diferentes máquinas protegidas. El cifrado no afecta al rendimiento, porque cada clave de cifrado activa crea un dominio de cifrado. Esto permite que un Core individual admita varios clientes al alojar varios dominios de cifrado. En un entorno con múltiples clientes, los datos se particionan y deduplican dentro de los dominios de cifrado. Puesto que usted administra las claves de cifrado, la pérdida del volumen no puede revelar las claves. Entre los conceptos y consideraciones sobre la seguridad de las claves se incluyen:

- El cifrado se realiza mediante AES de 256 bits en el modo Encadenamiento de bloques de cifrado (CBC) que cumple SHA-3.
- La deduplicación funciona en el dominio de Core para garantizar la privacidad.
- El cifrado se realiza sin afectar al rendimiento.
- Puede agregar, quitar, importar, exportar, modificar y eliminar las claves de cifrado que se han configurado en el Core.
- No hay límite en el número de claves de cifrado que pueden crearse en el Core.

Aplicación o retirada del cifrado de un equipo protegido

Puede asegurar los datos protegidos en su Core en cualquier momento definiendo una clave de cifrado y aplicándola a uno o más equipos protegidos de su repositorio. Puede aplicar una única clave de cifrado a cualquier número de equipos protegidos, pero un equipo protegido solo puede tener aplicada una clave de cifrado a la vez.

El ámbito de deduplicación de Rapid Recovery se limita a los equipos protegidos con el mismo repositorio y clave de cifrado. Por lo tanto, para potenciar al máximo el valor de la deduplicación, Dell recomienda aplicar una única clave de cifrado al máximo número de equipos

protegidos posible. Sin embargo, no hay límite en el número de claves de cifrado que pueden crearse en el Core. Por ello, si el cumplimiento normativo, las reglas de seguridad, las políticas de privacidad u otras circunstancias lo requieren, puede agregar y administrar cualquier número de claves de cifrado. Luego podrá aplicar cada clave a un único equipo protegido o a cualquier conjunto de equipos de su repositorio.

En el momento que aplica una clave de cifrado a un equipo protegido o disocia una clave de cifrado de un equipo protegido, Rapid Recovery toma una nueva imagen base para ese equipo en la siguiente instantánea programada o forzada. Los datos que se almacenan en esa imagen de base (y todas las instantáneas incrementales posteriores que se tomen mientras se aplica una clave de cifrado) están protegidos por un estándar de cifrado avanzado de 256 bits. No existen métodos conocidos para poner en peligro este método de cifrado.

Si cambia el nombre de la frase de contraseña por una clave de cifrado existente y que se usa actualmente para proteger un equipo, a continuación, en la siguiente instantánea programada o forzada, el Core de Rapid Recovery captura y refleja las propiedades actualizadas de la clave. Los datos que se almacenan en esa imagen (y todas las instantáneas incrementales posteriores que se tomen mientras se aplica una clave de cifrado) están protegidos por un estándar de cifrado avanzado de 256 bits. No existen métodos conocidos para poner en peligro este método de cifrado.

Una vez que se crea y se aplica una clave de cifrado a un equipo protegido, existen dos conceptos que se aplican para retirar ese cifrado. El primero es desasociar la clave del equipo protegido. Opcionalmente, una vez que se desasocia la clave de cifrado de todos los equipos protegidos, puede eliminarse del Core de Rapid Recovery.

Esta sección incluye los siguientes temas:

- [Asociación de una clave de cifrado con un equipo protegido](#)
- [Aplicación de una clave de cifrado desde la página Equipos protegidos](#)
- [Desasociación de una clave de cifrado de un equipo protegido](#)

Asociación de una clave de cifrado con un equipo protegido

Puede aplicar una clave de cifrado a un equipo protegido empleando uno de los dos métodos siguientes:

- **Como parte de la protección de un equipo.** Cuando se utiliza este método, puede aplicar el cifrado a uno o varios equipos de forma simultánea. Este método le permite agregar una nueva clave de cifrado o aplicar una clave existente al equipo o equipos seleccionados. Para utilizar el cifrado cuando se define inicialmente la protección de un equipo, debe seleccionar las opciones avanzadas en el Asistente para proteger equipo relevante. Esta selección agrega una página Cifrado al flujo de trabajo del asistente. Desde esta página, seleccione **Activar cifrado** y, a continuación, seleccione una clave de cifrado existente o especifique parámetros para una nueva clave. Para obtener más información, consulte [Cómo proteger una máquina](#) o [Acerca de la protección de varios equipos](#), respectivamente.
- **Modificando los parámetros de configuración de un equipo.** Este método aplica una clave de cifrado a un equipo protegido a la vez. Existen dos enfoques para modificar los parámetros de configuración de un equipo en la interfaz de usuario de Rapid Recovery:
 - Modificar los parámetros de configuración de un equipo protegido específico. La clave de cifrado que desee utilizar para este enfoque debe existir en el Core de Rapid Recovery, ser un tipo de clave universal y estar en un estado de desbloqueo. El cifrado forma parte de la configuración general. Para obtener más información, consulte [Visualización y modificación de la configuración de equipos protegidos](#).
 - Haga clic en  **No cifrado** de la página Equipos protegidos. Empleando este enfoque puede crear y aplicar una nueva clave de cifrado, o asignar una clave existente desbloqueada existente al equipo protegido especificado. Para obtener más información, consulte [Aplicación de una clave de cifrado desde la página Equipos protegidos](#).

Aplicación de una clave de cifrado desde la página Equipos protegidos

Una vez se ha agregado una clave de cifrado a un Core de Rapid Recovery, puede utilizarse para cualquier número de equipos protegidos.

Si selecciona una clave de cifrado durante la protección inicial de uno o más equipos, esa clave se aplica automáticamente a cualquier equipo que proteja utilizando ese asistente. En dichos casos, no se requiere este procedimiento.

Realice este procedimiento:

- Si desea aplicar una clave de cifrado existente, universal, desbloqueada para cualquier equipo protegido en el Core.
- Si acaba de agregar una nueva clave de cifrado mediante el proceso que se describe en el tema [Incorporación de una clave de cifrado](#) y desea aplicar esa clave a un equipo protegido.
- Si el cifrado ya se aplica a un equipo protegido en el Core, pero desea cambiar la clave a una clave universal desbloqueada diferente disponible en el Core.

⚠ PRECAUCIÓN: Después de aplicar una clave de cifrado a un equipo protegido, Rapid Recovery toma una nueva imagen de base para ese equipo en la siguiente instantánea programada o forzada.

- 1 Desplácese hasta el Core de Rapid Recovery y haga clic en **Equipos protegidos**.

Aparece la página **Equipos protegidos** enumerando todos los equipos protegidos por este Core. Aparece un Candado abierto 

para todos los equipos que no tienen aplicada una clave de cifrado. Un candado cerrado  indica que un equipo protegido tiene el cifrado aplicado.

- 2 En el panel Equipos protegidos, haga clic en el icono de candado del equipo protegido que desee configurar.

Aparece el cuadro de diálogo **Configuración de cifrado**.

- 3 Realice una de las siguientes acciones:

- Si desea aplicar una clave de cifrado existente a esa máquina, seleccione **Cifrar los datos mediante un cifrado basado en Core con una clave existente** y en el menú desplegable, seleccione la clave adecuada. Haga clic en **Aceptar** para confirmar.
- Si desea cambiar una clave de cifrado existente a una clave universal, desbloqueada diferente seleccione **Cifrar los datos mediante un cifrado basado en Core con una clave nueva** y en el menú desplegable, seleccione la clave adecuada. Haga clic en **Aceptar** para confirmar.
- Si desea crear una nueva clave de cifrado y aplicarla a este equipo protegido, haga clic en **Cifrar los datos mediante un cifrado basado en Core con una clave nueva**. A continuación, introduzca los detalles para la clave según se describe en la tabla siguiente.

Tabla 34. Detalles de la nueva clave de cifrado

Cuadro de texto	Descripción
Nombre	Escriba un nombre para la clave de cifrado. Los nombres de las claves de cifrado contienen entre 1 y 64 caracteres alfanuméricos. No utilice caracteres no permitidos o frases no permitidas.
Descripción	Escriba un comentario descriptivo para la clave de cifrado. Esta información aparece en el campo Descripción cuando al visualizar una lista de claves de cifrado en la Rapid Recovery Core Console. Las descripciones pueden contener hasta 254 caracteres. La práctica recomendada es evitar el uso de caracteres no permitidos y frases no permitidas.
Frase de contraseña	Introduzca una frase de contraseña usada para controlar el acceso. La práctica recomendada es evitar el uso de caracteres no permitidos. Registre la frase de contraseña en lugar seguro. Dell Support no puede recuperar frases de contraseña. Una vez cree una clave de cifrado y la aplique a uno o más equipos protegidos no podrá recuperar los datos si pierde la frase de contraseña.
Confirmar frase de contraseña	Como confirmación, vuelva a escribir la Frase de contraseña. Se utiliza para confirmar la entrada de frase de contraseña.

- 4 Haga clic en **Aceptar**.

El cuadro de diálogo se cierra. La clave de cifrado que especificó se ha aplicado a copias de seguridad futuras en este equipo protegido, y el candado ahora aparece como cerrado.

De forma opcional, si desea que se aplique una clave de cifrado de forma inmediata, fuerce una instantánea. Para obtener más información, consulte [Cómo forzar una instantánea](#).

PRECAUCIÓN: Rapid Recovery utiliza cifrado AES de 256 bits en el modo Encadenamiento de bloques de cifrado (CBC) con claves de 256 bits. Si bien el uso de cifrado es opcional, Dell recomienda que establezca una clave de cifrado y que proteja la frase de contraseña que defina. Almacene la frase de contraseña en una ubicación segura, dado que es clave para la recuperación de datos. Sin una frase de contraseña, la recuperación de datos no es posible.

Desasociación de una clave de cifrado de un equipo protegido

Una vez se aplica una clave de cifrado a un equipo protegido, se cifran todos los datos de instantáneas posteriores que se almacenan en el Core de Rapid Recovery.

Puede desasociar una clave de cifrado de un equipo protegido. Esta acción no descifra los datos de copia de seguridad existentes, pero da como resultado una nueva imagen de base para ese equipo en el momento de que se realice la siguiente instantánea programada o forzada.

NOTA: Si desea retirar una clave de cifrado del Core, según se describe en el tema [Eliminación de una clave de cifrado](#), debe desasociar primero esa clave de cifrado de todos los equipos protegidos.

Realice este procedimiento para desasociar una clave de cifrado de un equipo protegido específico.

- 1 Desplácese hasta el Core de Rapid Recovery y haga clic en **Equipos protegidos**.

Aparece la página Equipos protegidos enumerando todos los equipos protegidos por este Core. Aparece un Candado abierto  para todos los equipos que no tienen aplicada una clave de cifrado. Un candado cerrado  indica que un equipo protegido tiene el cifrado aplicado.

- 2 En el panel Equipos protegidos, haga clic en el icono  **Cifrado** del equipo protegido que quiere configurar.
Aparece el cuadro de diálogo **Configuración de cifrado**.
- 3 Seleccione **Cifrar datos mediante un cifrado basado en el Core con una clave existente** y, desde el menú desplegable, seleccione **(Ninguno)** y, a continuación, haga clic en **Aceptar**.
- 4 Si desea retirar esta clave de cifrado del Core de Rapid Recovery, primero repita este procedimiento para todos los equipos protegidos que utilicen esta clave. A continuación, realice el procedimiento que se describe en el tema [Eliminación de una clave de cifrado](#).

Administración de las claves de cifrado

Para administrar las claves de cifrado del Core de Rapid Recovery, en la barra de iconos haga clic en  (Más) y, a continuación, seleccione **Claves de cifrado**. Aparece la página **Claves de cifrado**. Para cada clave de cifrado que se haya agregado al Core de Rapid Recovery (si ya se ha definido alguna), verá la información que se describe en la siguiente tabla.

Tabla 35. Información sobre cada clave de cifrado

Elemento de la IU	Descripción
Select Item (Seleccionar elemento)	Para cada clave de cifrado, puede seleccionar la casilla de verificación para realizar acciones de la lista de opciones del menú situada encima de la tabla.
Nombre	El nombre asociado con la clave de cifrado.
Huella digital	Este parámetro es una cadena alfabética de 26 caracteres de caracteres latinos en mayúsculas y minúsculas generado aleatoriamente que ayuda a identificar de forma exclusiva cada clave de cifrado.
Tipo	El tipo describe el punto de origen de una clave de cifrado y su capacidad de aplicarse. Una clave de cifrado puede contener uno de los dos tipos posibles:

Elemento de la IU	Descripción
	Universal. El tipo Universal es la condición predeterminada cuando crea una clave de cifrado. Una clave con un tipo de Universal, combinado con un estado Desbloqueado, indica que la clave puede aplicarse a un equipo protegido. No es posible bloquear un tipo de clave universal manualmente; en su lugar, debe primero cambiar su tipo según se describe en el procedimiento Cambio de los tipos de clave de cifrado. Replicación. Cuando un equipo protegido en un Core de origen tiene activado el cifrado, y los puntos de recuperación de ese equipo se replican en un Core de destino, cualquier clave de cifrado empleada en el origen aparece automáticamente en el Core de destino con un tipo de Replicación. El estado predeterminado después de recibir una clave replicada es bloqueado. Puede desbloquear una clave de cifrado con un tipo de Replicación proporcionando la frase de contraseña. Si una clave tiene un tipo de desbloqueo, puede bloquearla manualmente. Para obtener más información, consulte el tema Desbloqueo de una clave de cifrado.
Estado	El estado indica si se puede utilizar una clave de cifrado. Los dos estados posibles incluyen: - Desbloqueado. Un estado Desbloqueado indica que la clave puede utilizarse de forma inmediata. Por ejemplo, puede cifrar instantáneas de un equipo protegido, o realizar una recuperación de los datos desde un punto de recuperación replicado en el Core de destino. - Bloqueado. Un estado Bloqueado indica que la clave no puede utilizarse hasta que se desbloquee proporcionando la frase de contraseña. Bloqueado es el estado predeterminado de una nueva clave de cifrado importada o replicada. Si el estado de una clave de cifrado es Bloqueado, debe desbloquearse antes de poder utilizarse. Si ha desbloqueado previamente una clave de cifrado bloqueada, y la duración para permanecer desbloqueada ha transcurrido, el estado cambia de Desbloqueado a Bloqueado. Después de que la clave se bloquee automáticamente, debe desbloquear la clave de nuevo para utilizarla. Para obtener más información, consulte el tema Desbloqueo de una clave de cifrado.
Descripción	La descripción es un campo opcional que se recomienda para proporcionar información útil sobre la clave de cifrado, como su destino o una pista de la frase de contraseña.

En el nivel superior del panel Claves de cifrado puede agregar una clave de cifrado o importar una clave utilizando un archivo exportado desde otro Core de Rapid Recovery. También puede eliminar las claves seleccionadas en la tabla de resumen.

Una vez haya una clave de cifrado para un Core, puede administrar las claves existentes modificando el nombre o las propiedades de descripción, cambiando la frase de contraseña, desbloqueando una clave de cifrado bloqueada o bien eliminando la clave del Core de Rapid Recovery. También puede exportar una clave a un archivo, que puede importarse en otro Core de Rapid Recovery.

Cuando agrega una clave de cifrado desde la página **Claves de cifrado**, la clave aparece en la lista de claves de cifrado, pero no se aplica a un equipo protegido específico. Para obtener información sobre cómo aplicar una clave de cifrado que cree desde el panel **Claves de cifrado**, o para eliminar una clave completamente del Core de Rapid Recovery, consulte [Aplicación o retirada del cifrado de un equipo protegido](#).

Desde el panel **Claves de cifrado** puede administrar la seguridad para los datos de copia de seguridad guardados en el Core de cualquier equipo protegido de su repositorio realizando lo siguiente:

- [Incorporación de una clave de cifrado](#)
- [Importación de una clave de cifrado](#)
- [Desbloqueo de una clave de cifrado](#)
- [Modificación de una clave de cifrado](#)
- [Cambio de la frase de contraseña de la clave de cifrado](#)
- [Exportación de una clave de cifrado](#)
- [Eliminación de una clave de cifrado](#)
- [Cambio de los tipos de clave de cifrado](#)

Incorporación de una clave de cifrado

Rapid Recovery utiliza cifrado AES de 256 bits en el modo Encadenamiento de bloques de cifrado (CBC) con claves de 256 bits. Si bien el uso de cifrado es opcional, Dell recomienda que establezca una clave de cifrado y que proteja la frase de contraseña que defina.

⚠ PRECAUCIÓN: Guarde la frase de contraseña en un lugar seguro. Sin una frase de contraseña, no podrá recuperar los datos de los puntos de recuperación cifrados.

Tras definir una clave de cifrado, puede utilizarla para salvaguardar sus datos. Las claves de cifrado pueden utilizarse en cualquier número de equipos protegidos.

Este paso describe cómo agregar una clave de cifrado desde la Core Console de Rapid Recovery. Este proceso no aplica la clave a ningún equipo que se esté protegiendo en esos momentos en el Core. También puede agregar una clave de cifrado durante el proceso de protección de un equipo. Para obtener más información sobre la incorporación del cifrado como parte de la protección de un equipo, consulte [Cómo proteger una máquina](#). Para obtener más información sobre la incorporación del cifrado a dos o más equipos protegiéndolos inicialmente, consulte [Acerca de la protección de varios equipos](#).

Complete los pasos de este procedimiento para agregar una clave de cifrado.

- 1 Desplácese hasta la Core Console de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Más) y, a continuación, seleccione **Claves de cifrado**. Aparece la página **Claves de cifrado**.
- 3 Haga clic en **Agregar clave de cifrado**. Se abrirá el cuadro de diálogo **Crear clave de cifrado**.
- 4 En el cuadro de diálogo **Crear clave de cifrado**, escriba los detalles para la clave según se describe en la tabla siguiente.

Tabla 36. Detalles de Crear clave de cifrado

Cuadro de texto	Descripción
Nombre	Escriba un nombre para la clave de cifrado. Los nombres de las claves de cifrado contienen entre 1 y 64 caracteres alfanuméricos. No utilice caracteres no permitidos o frases no permitidas .
Descripción	Escriba un comentario para la clave de cifrado. Esta información aparece en el campo Descripción cuando se ven claves de cifrado desde la Core Console. Puede introducir hasta 254 caracteres. La práctica recomendada es evitar el uso de caracteres no permitidos y frases no permitidas .
Frase de contraseña	Introduzca una frase de contraseña usada para controlar el acceso. La práctica recomendada es evitar el uso de caracteres no permitidos .
⚠ PRECAUCIÓN: Registre la frase de contraseña en lugar seguro. El soporte técnico de Dell no puede recuperar frases de contraseña. Una vez cree una clave de cifrado y la aplique a uno o más equipos protegidos no podrá recuperar los datos si pierde la frase de contraseña.	
Confirmar la frase de contraseña	Como confirmación, vuelva a escribir la Frase de contraseña. Se utiliza para confirmar la entrada de frase de contraseña.

- 5 Haga clic en **Aceptar**.
El cuadro de diálogo se cierra y la clave de cifrado creada aparece en la página Claves de cifrado.
- 6 Si desea aplicar la clave de cifrado a un equipo protegido, consulte [Aplicación de una clave de cifrado desde la página Equipos protegidos](#).

Importación de una clave de cifrado

Puede importar una clave de cifrado desde otro Core de Rapid Recovery y utilizar esa clave para cifrar los datos de un equipo protegido en su Core. Para importar la clave debe primero poder acceder a ella desde el equipo del Core, ya sea localmente o a través de la red. También debe saber la frase de contraseña de la clave de cifrado.

Complete los pasos de este procedimiento para importar una clave de cifrado.

NOTA: Este proceso no aplica la clave a ningún equipo protegido. Para obtener más información sobre la aplicación de la clave, consulte [Aplicación de una clave de cifrado desde la página Equipos protegidos](#).

- 1 Vaya al Core de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Más) y, a continuación, seleccione **Claves de cifrado**. Aparece la página **Claves de cifrado**.
- 3 Haga clic en  **Importar**. Aparece el cuadro de diálogo **File Upload** (Carga de archivos).
- 4 En el cuadro de diálogo **File Upload** (Carga de archivos), vaya a la red o al directorio local que contiene la clave de cifrado que quiere importar. Por ejemplo, vaya a la carpeta **Descargas** del usuario que ha iniciado sesión.

El nombre de archivo de la clave comienza por "EncryptionKey-," seguido del Id. de la clave, y termina con la extensión de archivo .key. Por ejemplo, un nombre de clave de cifrado de muestra es EncryptionKey-CaracteresAlfabeticosAleatorios.key.

- 5 Seleccione la clave que desea importar y luego haga clic en **Abrir**.
- 6 En el cuadro de diálogo **Importar clave**, haga clic en **Aceptar**. El cuadro de diálogo se cierra y la clave de cifrado importada aparece en la página **Claves de cifrado**. Si la clave de cifrado se utilizó para proteger un volumen antes de exportarla, el estado de la clave es Bloqueado.

Desbloqueo de una clave de cifrado

Las claves de cifrado pueden contener un estado de bloqueo o desbloqueo. Puede aplicarse una clave de cifrado desbloqueada a un equipo protegido para asegurar los datos de copia de seguridad guardados para ese equipo en el repositorio. También puede recuperar datos de un punto de recuperación desde un Core de Rapid Recovery que utiliza una clave de cifrado desbloqueada.

Cuando importa una clave de cifrado a un Core de Rapid Recovery, su estado predeterminado es bloqueado. Esto es así sin que sea relevante si importó explícitamente la clave o si la clave de cifrado se agregó al Core de Rapid Recovery replicando equipos protegidos cifrados o importando un archivo comprimido de puntos de recuperación cifrados.

Para claves de cifrado agregadas al Core de Rapid Recovery solo por replicación, cuando desbloquea una clave, puede especificar una duración de tiempo (en horas, días o meses) para que la clave de cifrado permanezca desbloqueada. Cada día tiene un periodo de 24 horas, a contar desde la hora que se guardó la solicitud de desbloqueo en el Core de Rapid Recovery. Por ejemplo, si se desbloquea la clave a las 11:24 AM del martes y la duración seleccionada es 2 días, la clave se volverá a bloquear automáticamente a las 11:24 AM del jueves.

NOTA: No es posible utilizar una clave de cifrado bloqueada para recuperar datos o para aplicarla a un equipo protegido. Primero debe proporcionar la frase de contraseña, lo que desbloqueará la clave.

También puede bloquear una clave de cifrado desbloqueada, lo que garantiza que no podrá aplicarse a ningún equipo protegido hasta que se desbloquee. Para bloquear una clave de cifrado con estado Universal, debe cambiar primero su tipo a Replicada.

Si una clave de cifrado desbloqueada se está utilizando en ese momento para proteger un equipo en el Core, primero debe desasociar esa clave de cifrado del equipo protegido antes de que pueda bloquearla.

Complete los pasos de este procedimiento para desbloquear una clave de cifrado bloqueada.

- 1 Acceda al Core de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Más) y, a continuación, seleccione **Claves de cifrado**. Aparece la página **Claves de cifrado**. La columna Estado indica qué claves de cifrado están bloqueadas.
- 3 Localice la clave de cifrado que desee desbloquear, haga clic en su menú desplegable  y seleccione **Desbloquear**. Aparecerá el cuadro de diálogo **Desbloquear clave de cifrado**.
- 4 En el cuadro de diálogo, en el campo Frase de contraseña, introduzca la frase de contraseña para desbloquear esta clave.
- 5 Para especificar la cantidad de tiempo que la clave permanece desbloqueada, en la opción Duración, realice una de las acciones siguientes:
 - Para especificar que la clave permanezca desbloqueada hasta que la bloquee explícitamente en Rapid Recovery, seleccione **Hasta que se bloquee manualmente**.
 - Para especificar que la clave permanezca bloqueada durante el tiempo que configure en horas, días o meses, haga lo siguiente:
 - Seleccione el campo de número e introduzca un valor entre 1 y 999.
 - Especifique la duración en horas, días o meses, respectivamente.
 - A continuación, haga clic en **Aceptar**.Esta opción está disponible para claves de cifrado que se incorporaron por replicación.

El cuadro de diálogo se cierra y los cambios de la clave de cifrado seleccionada aparecen en la página Claves de cifrado.

- Para especificar que la clave permanezca bloqueada hasta una fecha y hora que especifique, haga lo siguiente:
 - Seleccione la opción **Hasta**.
 - En el campo de texto o a través de los widgets de calendario y reloj, especifique explícitamente los datos y la hora a la que desee que se bloquee la clave de cifrado.
 - A continuación, haga clic en **Aceptar**.Esta opción está disponible para claves de cifrado que se incorporaron por replicación.

El cuadro de diálogo se cierra y los cambios de la clave de cifrado seleccionada aparecen en la página Claves de cifrado.

Bloqueo de una clave de cifrado

Cuando el estado de una clave de cifrado está bloqueado, no se puede aplicar a ningún equipo protegido hasta que se desbloquee. Para bloquear una clave de cifrado con el tipo Universal, debe cambiar primero su tipo a Replicado.

Complete los pasos de este procedimiento para bloquear una clave de cifrado.

- 1 Vaya al Core de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Más) y, a continuación, seleccione **Claves de cifrado**. Aparece la página **Claves de cifrado**. La columna Estado indica qué claves de cifrado están desbloqueadas y muestra el tipo de cada clave.
- 3 Localice la clave de cifrado que desea bloquear. Si su tipo es Universal, haga clic en el menú desplegable  y seleccione **Cambiar el tipo a Replicado**. Aparece el cuadro de diálogo **Cambiar tipo de clave de cifrado**.
- 4 En el cuadro de diálogo, confirme que desea cambiar el tipo de clave a **Replicado**.
- 5 Si ha cambiado correctamente el estado de la clave de cifrado a Replicado, haga clic en su menú desplegable  y seleccione **Bloquear**. Aparece el cuadro de diálogo **Bloquear clave de cifrado**.
- 6 En el cuadro de diálogo, confirme que quiere bloquear la clave.

Se cerrará el cuadro de diálogo y el estado de la clave de cifrado seleccionada será ahora Bloqueado.

 **NOTA:** Esta opción está disponible para claves de cifrado que se incorporaron por replicación.

Modificación de una clave de cifrado

Después de definir una clave de cifrado, puede modificar el nombre de la clave de cifrado o la descripción de la clave. Estas propiedades están visibles cuando ve la lista de claves de cifrado del panel Claves de cifrado.

Complete los pasos de este procedimiento para editar el nombre o la descripción de una clave de cifrado desbloqueada existente.

 **PRECAUCIÓN:** Después de modificar el nombre o la descripción de una clave de cifrado que se utiliza para proteger a uno o más equipos, Rapid Recovery toma una nueva imagen base. La instantánea de la imagen base se produce en ese equipo en la siguiente instantánea programada o forzada.

- 1 Vaya al Core de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Más) y, a continuación, seleccione **Claves de cifrado**.
Aparece la página **Claves de cifrado**.
- 3 Ubique la clave de cifrado que desea editar y, haga lo siguiente:
 - Si la clave está bloqueada, primero debe desbloquearla. Consulte [Desbloqueo de una clave de cifrado](#)
 - Si la clave está desbloqueada, continúe como se describe a continuación.
- 4 Haga clic en el menú desplegable  en la clave de cifrado especificada y seleccione **Editar**.
Aparecerá el cuadro de diálogo **Editar clave de cifrado**.
- 5 En el cuadro de diálogo, edite el nombre o la descripción de la clave de cifrado y, a continuación, haga clic en **Aceptar**.
El cuadro de diálogo se cierra y los cambios de la clave de cifrado seleccionada aparecen en la página **Claves de cifrado**.

Cambio de la frase de contraseña de la clave de cifrado

Para mantener el máximo de seguridad, puede cambiar la frase de contraseña de cualquier clave de cifrado. Complete los pasos de este procedimiento para cambiar la frase de contraseña de una clave de cifrado.

 **PRECAUCIÓN:** Después de modificar la frase de contraseña de una clave de cifrado que se utiliza para proteger a uno o más equipos, el Core de Rapid Recovery captura una instantánea incremental para ese equipo en la siguiente instantánea programada o forzada.

- 1 Vaya al Core de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Más) y, a continuación, seleccione **Claves de cifrado**.
Aparece la página **Claves de cifrado**.
- 3 Localice la clave de cifrado que desea actualizar, haga clic en el menú desplegable  y seleccione **Cambiar frase de contraseña**.
Aparecerá el cuadro de diálogo **Cambiar frase de contraseña**.
- 4 En el cuadro de diálogo, en el campo **Frase de contraseña**, introduzca la nueva frase de contraseña para el cifrado.
- 5 En el campo **Confirmar la frase de contraseña**, vuelva a escribir la misma frase de contraseña.
- 6 Haga clic en **Aceptar**.
El cuadro de diálogo se cierra y la frase de contraseña se actualiza.
- 7 De manera opcional, si utiliza una sugerencia en el campo Descripción, edite la clave de cifrado para actualizar la sugerencia. Para obtener más información, consulte [Modificación de una clave de cifrado](#).

 **PRECAUCIÓN:** Rapid Recovery utiliza cifrado AES de 256 bits en el modo Encadenamiento de bloques de cifrado (CBC) con claves de 256 bits. Dell recomienda que guarde la frase de contraseña en un lugar seguro y mantenga esta información actualizada. Dell Support no puede recuperar frases de contraseña. Sin la frase de contraseña, no podrá recuperar información de los puntos de recuperación cifrados.

Exportación de una clave de cifrado

Puede exportar una clave de cifrado desde cualquier Core de Rapid Recovery con el propósito expreso de utilizarla en otro Core. Cuando realiza este procedimiento, la clave se guarda en la carpeta **Descargas** de la cuenta de usuario activa de Windows.

Complete los pasos de este procedimiento para exportar una clave de cifrado.

- 1 Vaya al Core de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Más) y, a continuación, seleccione **Claves de cifrado**. Aparece la página **Claves de cifrado**.
- 3 Localizar la clave de cifrado que desea exportar, haga clic en el menú desplegable  y seleccione **Exportar**. Aparece el cuadro de diálogo **Abrir clave de cifrado-[name.key]**.
- 4 En el cuadro de diálogo, seleccione **Guardar archivo** para guardar y almacenar las claves de cifrado en una ubicación segura y, a continuación, haga clic en **Aceptar**.
La clave de cifrado se descarga como un archivo de texto en la ubicación predeterminada, como la carpeta **Descargas** de la cuenta de usuario de Windows activa.
- 5 De forma opcional, si desea importar esta clave en un Core diferente, copie el archivo en una ubicación accesible desde ese Core.

Eliminación de una clave de cifrado

Al eliminar una clave de cifrado de la página claves de cifrado, la clave se borra del Core de Rapid Recovery.

 **NOTA:** La eliminación de una clave de cifrado no descifra los puntos de recuperación ya guardados con la clave. Todavía debe conservar y proporcionar la frase de contraseña de la clave para recuperar los datos para los puntos de recuperación encriptados existentes.

No es posible eliminar una clave de cifrado que ya esté asociada con cualquier equipo protegido. Primero debe ver la configuración del cifrado de cada equipo protegido que utilice la clave, y desasociar la clave de cifrado que desea eliminar. Para obtener más información, consulte el tema [Desasociación de una clave de cifrado de un equipo protegido](#).

Complete los pasos de este procedimiento para quitar una clave de cifrado.

- 1 Vaya al Core de Rapid Recovery.
 - 2 En la barra de iconos, haga clic en  (Más) y, a continuación, seleccione **Claves de cifrado**. Aparece la página **Claves de cifrado**.
 - 3 Localice la clave de cifrado que desea quitar. Haga clic en su menú desplegable , y seleccione **Quitar**. Se abrirá el cuadro de diálogo **Eliminar clave de cifrado**. Verá un mensaje que confirma la acción para quitar la clave de cifrado.
 - 4 En el cuadro de diálogo, confirme que desea quitar la clave de cifrado.
-  **NOTA:** La eliminación de una clave de cifrado no descifra los puntos de recuperación ya guardados con la clave. Todavía debe conservar y proporcionar la clave para recuperar los datos para los puntos de recuperación encriptados existentes.

El cuadro de diálogo se cierra y la clave de cifrado quitada deja de aparecer en la página **Claves de cifrado**.

Cambio de los tipos de clave de cifrado

Las claves de cifrado enumeran uno de los dos tipos posibles en el panel Claves de cifrado: Universal o Replicación. El tipo indica que origen probable de la clave de cifrado y determina si puede cambiar sus detalles o la frase de contraseña. Puede modificar estos atributos únicamente si el tipo es Universal. Si necesita modificar estos atributos para una clave con el tipo Replicación, debe cambiar su tipo a Universal mediante este procedimiento. Cuando cambia el tipo de una clave de cifrado a Universal, se desbloquea manualmente y puede utilizarse para cifrar otros equipos protegidos.

 **NOTA:** Debe conocer la frase de contraseña para cambiar el tipo de Replicación a Universal.

Las claves de cifrado también tienen dos posibles estados: Bloqueado o Desbloqueado. El estado controla su capacidad de aplicar una clave de cifrado a un equipo protegido, o para restaurar datos desde un punto de recuperación con cifrado. Puede cambiar el tipo de una clave de cifrado manualmente únicamente si el estado es Desbloqueado.

Cuando crea por primera vez una clave de cifrado, su tipo es Universal y su estado Desbloqueado. Puede utilizar dicha clave inmediatamente (por ejemplo, para cifrar copias de seguridad de un equipo protegido). Sin embargo, una clave de tipo Universal no se puede bloquear manualmente. Si desea bloquear manualmente una clave de cifrado con el tipo Universal, deberá cambiar el tipo a Replicación mediante este procedimiento.

No se puede cambiar una clave de cifrado tipo si ya está en uso cifrando puntos de recuperación para uno o más equipos protegidos.

Siga este procedimiento para cambiar el tipo de una clave de cifrado.

- 1 Vaya al Core de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Más) y, a continuación, seleccione **Claves de cifrado**.
Aparece la página **Claves de cifrado**. Todas las claves de cifrado accesibles al Core aparecen en una tabla de resumen. Cada una muestra un tipo de Universal o Replicación.
- 3 Localice la clave de cifrado que quiere actualizar.
- 4 Si quiere cambiar una clave de cifrado de Universal a Replicación, haga lo siguiente:
 - a Haga clic en su menú desplegable  y seleccione **Cambiar el tipo a Replicado**.
Aparece el cuadro de diálogo **Cambiar tipo de clave de cifrado**. Se muestra un mensaje que confirma que desea cambiar el tipo a Replicación.
 - En el cuadro de diálogo, confirme que desea cambiar el tipo a Replicación.

El cuadro de diálogo se cierra y se actualiza el tipo de clave de cifrado a Replicación.
- 5 Si quiere cambiar una clave de cifrado de Replicación a Universal, haga lo siguiente:
 - a Haga clic en su menú desplegable  y seleccione **Cambiar el tipo a Universal**.
Aparece el cuadro de diálogo **Cambiar tipo de clave de cifrado**. Se muestra un mensaje que confirma que desea cambiar el tipo a Universal.
 - En el cuadro de diálogo, en el campo **Frase de contraseña**, introduzca la frase de contraseña y, a continuación, haga clic en **Aceptar** para confirmar que desea cambiar el tipo a Universal.

El cuadro de diálogo se cierra y se actualiza el tipo de clave de cifrado a Universal.

Administración de cuentas de nube

Esta sección describe cómo definir vínculos a cuentas de proveedores de almacenamiento en la nube existentes y cómo administrar esas cuentas de nube para utilizarlas con Rapid Recovery. Por ejemplo, puede archivar datos de Rapid Recovery en la nube, o importar datos archivados desde la nube.

Acerca de las cuentas de servicios en la nube

Rapid Recovery le permite archivar datos en una variedad de proveedores de nube, o importar datos archivados almacenados en una cuenta de nube. Las nubes compatibles son Microsoft Azure, Amazon™, Rackspace y cualquier proveedor con tecnología basada en OpenStack.

Puede agregar una cuenta de nube existente a la Core Console de Rapid Recovery. Una vez agregada, puede modificar la información, configurar las opciones de conexión de cuenta o eliminar la cuenta de Rapid Recovery.

Incorporación de una cuenta de nube

Antes de que pueda mover datos en ambas direcciones entre una cuenta en la nube y su Core, debe agregar información de la cuenta del proveedor de la nube a la Rapid Recovery Core Console. Esta información identifica la cuenta en la nube en la Core Console al mismo tiempo que almacena en la caché la información de la conexión de forma segura. Este proceso permite al Rapid Recovery Core conectarse a la cuenta en la nube para realizar las operaciones que especifique.

Para añadir una cuenta de nube, realice estos pasos en el procedimiento siguiente.

- 1 En la barra de iconos de la Rapid Recovery Core Console, haga clic en el icono  **Más** y, a continuación, seleccione **Cuentas en la nube**.
Aparece la página **Cuentas en la nube**.
- 2 En la página **Cuentas en la nube**, haga clic en **Agregar cuenta nueva**.
Se abrirá el cuadro de diálogo **Agregar cuenta nueva**.
- 3 Seleccione un proveedor de nube compatible en la lista desplegable Tipo de nube.
- 4 Basándose en el tipo de nube que haya seleccionado en el paso 3, introduzca los detalles que se describen en la tabla siguiente.

Tabla 37. Detalles de cuenta de nube

Tipo de nube	Cuadro de texto	Descripción
Microsoft Azure	Nombre de cuenta de almacenamiento	Introduzca el nombre de su cuenta de almacenamiento de Microsoft Azure. NOTA: El nombre debe coincidir precisamente con el nombre de la cuenta de almacenamiento de Azure. Debe contener solo números y letras en minúsculas y tener entre 3 y 24 caracteres de longitud.
	Clave de acceso	Introduzca la clave de acceso para su cuenta. NOTA: Puede introducir la clave principal o secundaria. Para obtener la clave de acceso de su cuenta de Azure, consulte Claves en Configuración.
	Utilizar protocolo https	Seleccione esta opción para usar el protocolo https seguro, en lugar del protocolo http estándar.
	Nombre mostrado	Introduzca un nombre de visualización para esta cuenta de nube para que se muestre en la Core Console de Rapid Recovery; por ejemplo, Microsoft Azure 1.
Amazon™ S3	Clave de acceso	Introduzca la clave de acceso para su cuenta de nube de Amazon™.
	Clave secreta	Introduzca la clave secreta para esta cuenta.

Tipo de nube	Cuadro de texto	Descripción
Nubes con tecnología OpenStack	Nombre mostrado	Introduzca un nombre de visualización para esta cuenta de nube para que se muestre en la Core Console de Rapid Recovery; por ejemplo, Amazon 1.
	Región	Introduzca la región para su cuenta de nube.
	Nombre de usuario	Introduzca el nombre de usuario para su cuenta de nube basada en OpenStack.
	Contraseña o clave de API	Seleccione si quiere utilizar una contraseña o una clave de API y, a continuación, introduzca su selección para esta cuenta.
	Id. de inquilino	Introduzca la identificación de inquilino para esta cuenta.
	URL de autenticación	Introduzca la dirección URL de autenticación para esta cuenta.
Archivos de nube de Rackspace	Nombre mostrado	Introduzca un nombre de visualización para esta cuenta de nube para que se muestre en la Rapid Recovery Core Console; por ejemplo, OpenStack 1.
	Región	Utilice la lista desplegable para seleccionar la región para su cuenta.
	Nombre de usuario	Introduzca el nombre de usuario para su cuenta de nube de Rackspace.
	Contraseña o clave de API	Seleccione si quiere utilizar una contraseña o una clave de API y, a continuación, introduzca su selección para esta cuenta.
	Id. de inquilino	Introduzca la identificación de inquilino para esta cuenta.
	URL de autenticación	Introduzca la dirección URL de autenticación para esta cuenta.
	Nombre mostrado	Introduzca un nombre de visualización para esta cuenta de nube para que se muestre en la Core Console de Rapid Recovery; por ejemplo, Rackspace 1.

5 Haga clic en **Guardar**.

Se cerrará el cuadro de diálogo y su cuenta aparecerá en la página **Cuentas en la nube** de la Core Console.

Modificación de una cuenta de nube

Si necesita cambiar la información para conectar con su cuenta de nube, como por ejemplo para actualizar la contraseña o modificar el nombre mostrado, puede hacerlo en la página Cuentas en la nube de la Rapid Recovery Core Console. Complete los pasos del siguiente procedimiento para modificar una cuenta de nube.

- 1 En la barra de iconos de la Rapid Recovery Core Console, haga clic en el icono  **Más** y, a continuación, seleccione **Cuentas en la nube**.
Aparece la página **Cuentas en la nube**.
- 2 Haga clic en el menú desplegable que hay junto a la cuenta de nube que desea modificar y, a continuación, haga clic en **Editar**.
Se abre la ventana **Editar cuenta**.
- 3 Modifique los detalles apropiados y a continuación haga clic en **Guardar**.

 **NOTA:** No puede modificar el tipo de nube.

Configuración de los parámetros de cuentas de nube

La configuración de la nube permite determinar cuánto tiempo debe transcurrir entre que Rapid Recovery intenta conectarse a su cuenta de nube antes de que el tiempo se agote. Realice los pasos del procedimiento siguiente para configurar los ajustes de conexión para su cuenta de nube.

- 1 En la barra de iconos de la Core Console de Rapid Recovery, haga clic en  **Configuración**. Aparecerá la página Configuración.
- 2 En el menú izquierdo, haga clic en **Cuentas de nube**.
- 3 En la tabla Cuentas de nube, haga clic en el menú desplegable junto a la cuenta de nube que desee configurar y, a continuación, complete una de las siguientes acciones:
 - Para cambiar la configuración de la conexión de la cuenta de nube, haga clic en **Editar**.
 - 1 En el cuadro de diálogo Configuración de la nube, complete cualquiera de las siguientes acciones:
 - En **Tiempo de espera agotado de la solicitud**, utilice las flechas hacia arriba y hacia abajo para determinar la cantidad de tiempo en minutos y segundos que Rapid Recovery debe invertir en cada intento de conexión con la cuenta de nube cuando hay un retraso. Los intentos de conexión cesarán transcurrida la cantidad de tiempo introducida.
 - En **Tamaño del búfer de escritura**, introduzca el tamaño del búfer que desea reservar para escribir los datos archivados en la nube.
 - En **Tamaño del búfer de lectura**, introduzca el tamaño del bloque que desea reservar para leer los datos archivados desde la nube.
 - 2 Haga clic en **Aceptar**.
 - Para restablecer los siguientes valores predeterminados de la configuración de la nube, haga clic en **Restablecer**.
 - **Tiempo de espera agotado de la solicitud:** 01:30 (minutos y segundos)
 - **Tamaño del búfer de escritura:** 8388608 (bytes)
 - **Tamaño del búfer de lectura:** 8388608 (bytes)

Eliminación de una cuenta de nube

Si deja de usar su servicio de nube o decide dejar de usarlo para un Core en particular, es posible que desee eliminar su cuenta de nube de la Core Console. Complete los pasos del siguiente procedimiento para eliminar una cuenta de nube.

- 1 En la barra de iconos de la Rapid Recovery Core Console, haga clic en el icono  **Más** y, a continuación, seleccione **Cuentas en la nube**. Aparece la página **Cuentas en la nube**.
- 2 Haga clic en el menú desplegable que hay junto a la cuenta de nube que desea modificar y, a continuación, haga clic en **Eliminar**.
- 3 En el cuadro de diálogo **Eliminar cuenta**, haga clic en **Sí** para confirmar que desea eliminar la cuenta.
- 4 Si la cuenta de nube está en uso en esos momentos, un segundo cuadro de diálogo le pedirá confirmación sobre la eliminación. Haga clic en **Sí** para confirmar.

 **NOTA:** La eliminación de una cuenta que está en uso hace que todos los trabajos de archivación para esta cuenta fallen.

Archivado

En esta sección se describen los modelos de negocio para crear un archivo, cómo crear un archivo con Rapid Recovery y dónde puede archivarlos.

Cómo funciona la archivación

Las políticas de retención ejecutan los períodos en los que las copias de seguridad se almacenan en medios a corto plazo (rápidos y caros). A veces, los requisitos empresariales y técnicos exigen una retención ampliada de esas copias de seguridad, pero utilizar un almacenamiento rápido tiene un coste prohibitivo. Por tanto, ese requisito crea la necesidad de un almacenamiento a largo plazo (lento y barato). Las empresas suelen utilizar almacenamiento a largo plazo para archivar tanto los datos de conformidad como los de no conformidad. La función de archivo de Rapid Recovery se utiliza para ofrecer compatibilidad la retención ampliada para la conformidad y la no conformidad de los datos. También se utiliza para inicializar los datos de replicación en un Core de réplica remoto.

Una vez se haya creado un archivo, puede utilizarse de las siguientes maneras:

- Un archivo puede montarse como un sistema de archivos de recuperación simple de archivo o carpeta.
- Un archivo puede utilizarse como el origen de una restauración sin sistema operativo.
- Un archivo puede importarse a un repositorio.

Creación de una archivación

Puede utilizar este procedimiento para crear un archivo comprimido único o programado.

Si tiene pensado crear un archivo comprimido en una ubicación en la nube, primero se debe agregar su cuenta de nube a la Core Console de Rapid Recovery. Para obtener más información, consulte [Incorporación de una cuenta de nube](#).

Una archivación única es un archivo comprimido creado a petición para un equipo especificado. Un archivo comprimido programado es un archivo comprimido que aparece automáticamente en la fecha y hora especificadas en el asistente. Con la capacidad de programar un archivo comprimido periódico, se engloban situaciones donde se desea que se guarden archivos frecuentes de un equipo, sin la incomodidad de tener que crear archivos manualmente cada vez.

- 1 En la barra de botones de la Core Console de Rapid Recovery, haga clic en  **Archivo comprimido**. Se abre el Asistente de archivación.
- 2 En la página **Tipo de archivación** del asistente, seleccione una de las siguientes opciones:
 - Archivación única
 - Archivación continua (por programación)
- 3 Haga clic en **Siguiente**.
- 4 En la página **Ubicación**, seleccione la opción de la lista desplegable **Tipo de ubicación** y, a continuación, introduzca la información tal y como se describe en la tabla siguiente.

Tabla 38. Opciones del tipo de ubicación del archivo comprimido

Opción	Cuadro de texto	Descripción
Local	Ubicación	Escriba la ubicación de la salida. Se utiliza para definir la ruta de acceso de la ubicación en la que desea que resida el archivo; por ejemplo, d:\trabajo\archivación.
Red	Ubicación	Escriba la ubicación de la salida. Se utiliza para definir la ruta de acceso de la ubicación en la que desea que resida el archivo; por ejemplo, \\nombreservidor\nombre recursocompartido.
	Nombre de usuario	Escriba un nombre de usuario. Se utiliza para establecer las credenciales de inicio de la sesión del recurso compartido de red.

Opción	Cuadro de texto	Descripción
	Contraseña	Escriba una contraseña para la ruta de acceso de red. Se utiliza para establecer las credenciales de inicio de la sesión del recurso compartido de red.
Nube	Cuenta	Seleccione una cuenta de la lista desplegable.
		NOTA: Para seleccionar una cuenta de nube, debe añadirla primero en Core Console. Para obtener más información, consulte Incorporación de una cuenta de nube .
	Contenedor	Seleccione un contenedor asociado con su cuenta en el menú desplegable.
	Nombre de carpeta	Introduzca un nombre para la carpeta en la que hay que guardar los datos archivados.

- 5 Haga clic en **Siguiente**.
- 6 En la página **Equipos** del asistente, seleccione los equipos protegidos o equipos que desea archivar.
- 7 Haga clic en **Siguiente**.
- 8 Realice una de las siguientes acciones:
 - Si elige crear un archivo comprimido único, omita el [Paso 15](#).
 - Si elige crear un archivo comprimido programado, continúe con el [Paso 9](#)
- 9 En la página **Calendario de programación**, seleccione una de las siguientes opciones de la lista desplegable **Enviar datos**:
 - Diariamente
 - Semanalmente
 - Mensualmente
- 10 Introduzca la información que se describe en la siguiente tabla en base a lo que seleccionó en el [Paso 9](#).

Tabla 39. Opciones enviar datos

Opción	Cuadro de texto	Descripción
Diariamente	Una hora	Seleccione la hora del día a la que desea crear un archivo diario.
Semanalmente	Un día a la semana	Seleccione un día de la semana en el que crear automáticamente el archivo.
	Una hora	Seleccione la hora del día a la que desea crear una archivación.
Mensualmente	Un día al mes	Seleccione el día del mes en el que crear automáticamente el archivo.
	Una hora	Seleccione la hora del día a la que desea crear una archivación.

- 11 De manera opcional, si no desea que el trabajo de archivación empiece a la hora programada siguiente después de completar el asistente, seleccione **Realizar pausa en archivación inicial**.

NOTA: Si desea realizar una pausa en un archivo programado si necesita más tiempo para preparar la ubicación de destino antes de que se reanude la archivación. Si no desea seleccionar esta opción, la archivación comenzará a la hora programada.

- 12 Haga clic en **Siguiente**.
- 13 En la página **Opciones**, seleccione una de las acciones de reciclaje descritas en la tabla siguiente.

Tabla 40. Opciones de reciclaje de archivos comprimidos continuos

Cuadro de texto	Descripción
Incremental (Incremental)	Le permite añadir puntos de recuperación a un archivo existente. Compara los puntos de recuperación para evitar duplicar datos que ya hay en el archivo.
Reemplazar este Core	Sobrescribe los datos archivados que ya existan y que pertenezcan a este Core, pero deja intactos los datos del resto de Cores.
Borrar completamente	Borra todos los datos archivados del directorio antes de escribir el nuevo archivo.

- 14 De manera opcional, seleccione **Crear cadenas de puntos de recuperación (reparar huérfanos)** y, a continuación, omita el [Paso 18](#).
- 15 En la página **Opciones** para una archivación única, introduzca la información que se describe en la tabla siguiente.

Tabla 41. Opciones de archivación única

Cuadro de texto	Descripción
Tamaño máximo	Los grandes archivos de datos se pueden dividir en varios segmentos. Seleccione el tamaño máximo de espacio que desea reservar para crear el archivo realizando una de las siguientes acciones: • Seleccione Destino completo para reservar todo el espacio disponible en la ruta de acceso que se introdujo en el destino del Paso 4. (Por ejemplo, si la ubicación es D:\trabajo\archivo, se reservará todo el espacio disponible en la unidad D:). • Seleccione el cuadro de texto en blanco, utilice las flechas de dirección arriba y abajo para introducir una cantidad y, a continuación, seleccione una unidad de medida en la lista desplegable para personalizar el espacio que desea reservar.  NOTA: Los archivos de la nube de Amazon™ se dividen automáticamente en segmentos de 50 GB. Los archivos de la nube de Microsoft Azure se dividen automáticamente en segmentos de 200 GB.
Acción de reciclaje	Seleccione una de las opciones de la acción de reciclaje siguientes: • No reutilizar. No sobrescribe ni borra datos archivados existentes de la ubicación. Si la ubicación no está vacía, Rapid Recovery permite seleccionar una ubicación diferente. • Reemplazar este Core. Sobrescribe los datos archivados que ya existan y que pertenezcan a este Core, pero deja intactos los datos del resto de Cores. • Borrar completamente. Borra todos los datos archivados del directorio antes de escribir el nuevo archivo. • Incremental. Le permite añadir puntos de recuperación a un archivo existente. Compara los puntos de recuperación para evitar duplicar datos que ya hay en el archivo.
Comentario	Escriba comentarios o información adicional que sea necesaria capturar para el archivo. El comentario aparecerá si importa el archivo más tarde.
Crear cadenas de puntos de recuperación (reparar huérfanos)	Seleccione esta opción para archivar la cadena de punto de recuperación completa. Esta opción se selecciona de forma predeterminada.

- 16 Haga clic en **Siguiente**.
- 17 En la página **Intervalo de fechas**, introduzca de forma manual la fecha de inicio y la de finalización de los puntos de recuperación que se van a archivar o seleccione la fecha y hora haciendo clic en el icono de calendario seguido por el icono de reloj después de la ventana calendario.
- 18 Haga clic en **Finalizar**.
El Asistente se cerrará.

Archivar en la nube

Cuando los datos alcanzan la finalización de un periodo de retención, es posible que desee ampliar dicho plazo archivando los datos. Cuando se archivan datos, siempre se presenta el problema de su almacenamiento. Rapid Recovery le permite cargar su archivo en varios proveedores de nube directamente desde Core Console. Las nubes compatibles son Microsoft Azure, Amazon™, Rackspace y cualquier proveedor con tecnología basada en OpenStack.

La exportación de un archivo a una nube empleando Rapid Recovery lleva aparejados los siguientes procedimientos:

- Añadir su cuenta de nube a la Core Console de Rapid Recovery. Para obtener más información, consulte [Incorporación de una cuenta de nube](#).
- Archivar sus datos y exportarlos a su cuenta de nube. Para obtener más información, consulte [Creación de una archivación](#).
- Recuperar los datos archivados importándolos desde la ubicación de nube. Para obtener más información, consulte [Importación de un archivo](#).

Modificación de una archivación programada

Rapid Recovery permite cambiar los detalles de una archivación programada. Para modificar una archivación programada, realice estos pasos en el procedimiento siguiente.

- 1 En la Core Console de Rapid Recovery, haga clic en el menú desplegable  **Más** en la barra de iconos y, a continuación, haga clic en **Archivos comprimidos**.
- 2 En la página Archivos comprimidos, en Archivaciones programadas, haga clic en el menú desplegable junto al archivo que desea cambiar y, a continuación, haga clic en **Editar**.
Se abre **Agregar asistente de archivo**.
- 3 En la página **Ubicación** del Asistente de archivación, seleccione una de las siguientes opciones de la lista desplegable **Tipo de ubicación**:
 - Local
 - Red
 - Nube
- 4 En función del tipo de ubicación que haya seleccionado en el [Paso 3](#), introduzca los detalles para el archivo según se describen en la tabla siguiente.

Tabla 42. Detalles de archivación

Opción	Cuadro de texto	Descripción
Local	Ubicación	Escriba la ubicación de la salida. Se utiliza para definir la ruta de acceso de la ubicación en la que desea que resida el archivo; por ejemplo, d:\trabajo\archivación.
Red	Ubicación	Escriba la ubicación de la salida. Se utiliza para definir la ruta de acceso de la ubicación en la que desea que resida el archivo; por ejemplo, \\nombreservidor\nombre recursocompartido.
	Nombre de usuario	Escriba un nombre de usuario. Se utiliza para establecer las credenciales de inicio de la sesión del recurso compartido de red.
	Contraseña	Escriba una contraseña para la ruta de acceso de red. Se utiliza para establecer las credenciales de inicio de la sesión del recurso compartido de red.
Nube	Cuenta	Seleccione una cuenta de la lista desplegable.

Opción	Cuadro de texto	Descripción
NOTA: Para seleccionar una cuenta de nube, debe añadirla primero en Core Console. Para obtener más información, consulte Incorporación de una cuenta de nube.		
	Contenedor	Seleccione un contenedor asociado con su cuenta en el menú desplegable.
	Nombre de carpeta	Introduzca un nombre para la carpeta en la que desea guardar los datos archivados; por ejemplo, Rapid-Recuperación -Archivo comprimido- [FECHA DE CREACIÓN] - [HORA DE CREACIÓN].

- 5 Haga clic en **Siguiente**.
- 6 En la página **Equipos** del asistente, seleccione los equipos protegidos o equipos que contienen los puntos de recuperación que desea archivar. Borre los equipos que no desea archivar.
- 7 Haga clic en **Siguiente**.
- 8 En la página **Calendario de programación**, seleccione una de las siguientes opciones de la lista desplegable **Enviar datos**:
 - Diariamente
 - Semanalmente
 - Mensualmente
- 9 Introduzca la información que se describe en la siguiente tabla en base a lo que seleccionó en el [Paso 8](#).

Tabla 43. Opciones enviar datos

Opción	Cuadro de texto	Descripción
Diariamente	Una hora	Seleccione la hora del día a la que desea crear un archivo diario.
Semanalmente	Un día a la semana	Seleccione un día de la semana en el que crear automáticamente el archivo.
	Una hora	Seleccione la hora del día a la que desea crear un archivo diario.
Mensualmente	Un día al mes	Seleccione el día del mes en el que crear automáticamente el archivo.
	Una hora	Seleccione la hora del día a la que desea crear un archivo diario.

- 10 De manera opcional, para aplazar la archivación y que se reanude más tarde, seleccione **Realizar pausa en archivación inicial**.

NOTA: Si desea realizar una pausa en un archivo programado si necesita más tiempo para preparar la ubicación de destino antes de que se reanude la archivación. Si no desea seleccionar esta opción, la archivación comenzará a la hora programada.

- 11 Haga clic en **Siguiente**.
- 12 En la página **Opciones**, utilice la lista desplegable **Acción de reciclaje** para seleccionar una de las opciones descritas en la tabla siguiente:

Tabla 44. Opciones de reciclar archivo comprimido

Cuadro de texto	Descripción
Incremental (Incremental)	Le permite añadir puntos de recuperación a un archivo existente. Compara los puntos de recuperación para evitar duplicar datos que ya hay en el archivo.
Reemplazar este Core	Sobrescribe los datos archivados que ya existan y que pertenezcan a este Core, pero deja intactos los datos del resto de Cores.

Cuadro de texto	Descripción
Borrar completamente	Borra todos los datos archivados del directorio antes de escribir el nuevo archivo.
13	Seleccione de manera opcional Crear cadenas de puntos de recuperación (reparar huérfanos) .
14	Haga clic en Finalizar . Rapid Recovery se aplica a los cambios en el archivo comprimido.

Cómo realizar una pausa o reanudar un archivo programado

Si tiene un trabajo programado de archivado para que se repita, puede pausar o resumir esta acción según sea necesario.

Hay veces que es necesario realizar una pausa en un trabajo de archivación programado, como cuando tiene que cambiar la ubicación de archivación de destino. Del mismo modo, si estableció una pausa inicial en la archivación cuando realizó el procedimiento [Creación de una archivación](#), es probable que desee reanudar el archivo comprimido programado más adelante. Realice los pasos del procedimiento siguiente para realizar una pausa o reanudar la archivación programada.

- Desde la Core Console de Rapid Recovery, haga clic en el menú en la barra de iconos  **Más** y, a continuación, haga clic en **Archivos comprimidos**.
- En la página **Archivos comprimidos**, en las archivaciones programadas, realice una de las acciones siguientes:
 - Seleccione el archivo que prefiera y, a continuación, haga clic en la acción que desee:
 - Realizar pausa
 - Reanudar
 - Junto al archivo que desee, haga clic en el menú desplegable y haga clic en una de las siguientes acciones:
 - Realizar pausa
 - Reanudar

El estado del archivo se muestra en la columna Programar.

Forzar un trabajo de archivación

Mediante este procedimiento, puede forzar Rapid Recovery para realizar el trabajo de archivación en un archivo comprimido programado en cualquier momento.

Para forzar un trabajo de archivación, debe tener un archivo programado en el Core.

- En la Core Console de Rapid Recovery, en la barra de iconos, haga clic en el menú desplegable  **Más** y, a continuación, seleccione **Archivos comprimidos**.
- En la página Archivos comprimidos, en Archivaciones programadas, haga clic en el menú desplegable junto al archivo comprimido que desea forzar y, a continuación, haga clic en **Forzar**.
Rapid Recovery archiva los puntos de recuperación en función de la configuración que ha elegido para ese archivo comprimido, independientemente de la hora de archivo comprimido programado que estableció.

Comprobación de una archivación

La comprobación de un archivo comprimido verifica si un archivo comprimido y su contenido se encuentran lo suficientemente saludables para que se restauren.

Puede explorar un archivo comprimido para la integridad de su estructura, los segmentos de datos y archivos de índice al realizar una comprobación de archivo comprimido. La comprobación de archivo comprimido verifica la presencia de todos los archivos necesarios en el archivo y que los archivos se encuentran en buen estado. Para realizar una comprobación de archivo, realice los pasos del siguiente procedimiento.

- 
- Desde la Core Console de Rapid Recovery, haga clic en el menú desplegable **Más** en la barra de iconos y, a continuación, haga clic en **Archivos comprimidos**.
 - En la página **Archivos comprimidos**, haga clic en **Comprobar**.
Aparecerá el cuadro de diálogo **Comprobar archivado**.
 - Para **Tipo de ubicación**, seleccione una de las opciones siguientes en la lista desplegable:
 - Local
 - Red
 - Nube
 - En función del tipo de ubicación que haya seleccionado en el [paso 3](#), introduzca los detalles para el archivo comprimido según se describen en la siguiente tabla.

Tabla 45. Detalles de archivación

Opción	Cuadro de texto	Descripción
Local	Ubicación	Introduzca la ruta de acceso para el archivo.
Red	Ubicación	Introduzca la ruta de acceso para el archivo.
	Nombre de usuario	Escriba el nombre de usuario. Se utiliza para establecer las credenciales de inicio de la sesión del recurso compartido de red.
	Contraseña	Escriba una contraseña para la ruta de acceso de red. Se utiliza para establecer las credenciales de inicio de la sesión del recurso compartido de red.
Nube	Cuenta	Seleccione una cuenta de la lista desplegable.
	 NOTA: Para seleccionar una cuenta de nube, debe añadirla primero en Core Console. Para obtener más información, consulte Incorporación de una cuenta de nube.	
	Contenedor	Seleccione un contenedor asociado con su cuenta en el menú desplegable.
	Nombre de la carpeta	Seleccione la carpeta en la que se guardan los datos archivados; por ejemplo, Archivo-Rapid Recovery-5-[FECHA CREACIÓN]-[HORA CREACIÓN]

- Seleccione o borre las comprobaciones que se describen en la siguiente tabla. Todos están seleccionados de forma predeterminada.

 **NOTA:** No borre todas las comprobaciones. Debe seleccionar al menos una opción.

Opción	Descripción
Desplazamiento de asignación de archivos de índice	Esta opción comprueba que todos los datos de la estructura interna del archivo están en la ubicación correcta.
Integridad de estructura	Esta opción verifica la presencia de determinados archivos internos y las estructuras de las carpetas del archivo comprimido. Si faltan los archivos o las carpetas, la comprobación falla.

Opción	Descripción
Integridad de suma de comprobación	Esta opción comprueba la integridad de los segmentos de datos en el archivo comprimido para asegurarse de que los segmentos se encuentran en buen estado.

- 6 Haga clic en **Comprobar archivo**.
Rapid Recovery comprueba el archivo comprimido según las selecciones efectuadas.

Adición de un archivo comprimido

La adición de un archivo comprimido le permite ver los puntos de recuperación de dicho archivo.

Deberá tener un archivo comprimido ya existente creado en el Core Rapid Recovery 6.0.1 o posterior para completar este procedimiento. Para obtener más información, consulte [Creación de una archivación](#).

Cuando adjunte un archivo comprimido, el nombre que le proporcione aparecerá como un archivo comprimido de menú en el menú de navegación que se encuentra a la izquierda de la Core Console. Cada equipo protegido con puntos de recuperación del archivo comprimido se muestra por separado debajo del menú de archivo. Puede hacer clic en cualquier nombre de equipo en el archivo comprimido y examinar sus puntos de recuperación. A continuación, puede realizar las mismas acciones que con cualquier otro punto de recuperación visible en el Core.

Al adjuntar el archivo comprimido también se almacenan las credenciales para acceder a la información. Hasta que elimine la definición del archivo comprimido adjunto, podrá volver a adjuntar o desvincular dicho archivo para hacer que se pueda acceder a sus puntos de recuperación con mayor facilidad.

Utilice este procedimiento para adjuntar un archivo comprimido.

- 1 En la Core Console de Rapid Recovery, haga clic en el menú desplegable  **Archivo comprimido** y, a continuación, seleccione  **Adjuntar archivo comprimido**.

Aparecerá el cuadro de diálogo **Adjuntar archivo comprimido**.

- 2 En el cuadro de texto **Nombre**, introduzca un nombre para dicho archivo comprimido.
El valor que escriba en este campo aparecerá en el menú de navegación que se encuentra a la izquierda como el nombre del menú del archivo comprimido.

Si se sigue la práctica recomendada de los nombres de visualización, el nombre del archivo comprimido debería contener entre 1 y 64 caracteres alfanuméricos, espacios incluidos. No utilice [caracteres prohibidos](#) ni [frases prohibidas](#).

- 3 En la lista desplegable **Tipo de ubicación**, seleccione el tipo de ubicación del archivo comprimido de entre las opciones siguientes:
 - Local
 - Red
 - Nube
- 4 En función del tipo de ubicación que haya seleccionado en el [Paso 3](#), introduzca los detalles para el archivo según se describen en la tabla siguiente.

Tabla 46. Detalles del tipo de ubicación

Opción	Cuadro de texto	Descripción
Local	Ubicación	Introduzca la ruta de acceso al archivo comprimido; por ejemplo, D:\work\archive .
Red	Ubicación	Introduzca la ruta de acceso al archivo comprimido; por ejemplo, \\servername\sharename .
	Nombre de usuario	Introduzca el nombre de usuario para iniciar sesión en el recurso compartido de red.
	Contraseña	Introduzca la contraseña para iniciar sesión en el recurso compartido de red.

Opción	Cuadro de texto	Descripción
Nube	Cuenta	Seleccione una cuenta de la lista desplegable.
NOTA: Para seleccionar una cuenta de nube, debe añadirla primero en Core Console. Para obtener más información, consulte Incorporación de una cuenta de nube.		
	Contenedor	En el menú desplegable, seleccione el contenedor del archivo comprimido asociado con su cuenta.
	Nombre de carpeta	Introduzca el nombre de la carpeta de los datos del archivo comprimido; por ejemplo, Rapid-Recovery-Archive-[FECHA CREACIÓN]-[HORA CREACIÓN].

- 5
- Presione **Attach (Conectar)**.

El archivo comprimido se adjunta a este Core y monta el contenido como un sistema de archivos.

Importación de un archivo

Puede utilizar este procedimiento para importar un archivo una sola vez, o programar un archivo que se va a importar de manera recurrente.

Cuando desee recuperar los datos archivados, puede importar todo el archivo en una ubicación especificada.

PRECAUCIÓN: Realice este paso sólo después de una cuidadosa consideración. La importación de un archivo completa el repositorio con el contenido del archivo, sustituyendo los datos nuevos en el repositorio a partir de la captura del archivo.

Para importar un archivo, realice los pasos que se indican en el siguiente procedimiento.

- 1

En la barra de menú de la Rapid Recovery Core Console, haga clic en el **menú desplegable Archive (Archivo)** y, a continuación, seleccione **Import Archive (Importar archivo)**.

Se abre el **Impot Archive Wizard (Asistente de importación de archivo)**.

2

En la página **Import Type (Tipo de importación)**, seleccione una de las opciones siguientes:

 - One-time import (Importación única)
 - Continuous import (by schedule) (Importación continua [por programa])

3

Haga clic en **Next (Siguiente)**.

4

En la página **Location (Ubicación)**, seleccione la ubicación del archivo que desea importar en la lista desplegable y, a continuación, introduzca la información tal y como se describe en la tabla siguiente:
- Tabla 47. Opciones del tipo de ubicación del archivo importado
- | Opción | Cuadro de texto | Descripción |
|---------------|-------------------|--|
| Local (Local) | Ubicación | Especifique la ubicación de salida, que se utiliza para definir la ruta de acceso a la ubicación en la que desea que resida el archivo; por ejemplo, d:\work\archive. |
| Network (Red) | Ubicación | Especifique la ubicación de salida, que se utiliza para definir la ruta de acceso a la ubicación en la que desea que resida el archivo; por ejemplo, \\servername\sharename. |
| | Nombre de usuario | Introduzca un nombre de usuario. Se utiliza para establecer las credenciales de inicio de sesión para el recurso compartido de red. |
| | Contraseña | Introduzca una contraseña para la ruta de acceso de red. Se utiliza para establecer las credenciales de inicio de sesión para el recurso compartido de red. |
- 104

Trabajar con el Core del Dispositivo DL
- DELLEM

Opción	Cuadro de texto	Descripción
Cloud (Nube)	Cuenta	Seleccione una cuenta en la lista desplegable.
		 NOTA: Para seleccionar una cuenta en la nube, debe haberla agregado primero en la Core Console. Para obtener más información, consulte Incorporación de una cuenta de nube .
	Contenedor	En el menú desplegable, seleccione un contenedor asociado con la cuenta.
	Nombre de carpeta	Introduzca un nombre para la carpeta en la que desea guardar los datos archivados.

- 5 Haga clic en **Next (Siguiente)**.
- 6 Si desea importar cada máquina incluida en el archivo, en la página **Archive Information (Información de archivo)** seleccione **Import all machines (Importar todas las máquinas)**.
- 7 Realice una de las opciones siguientes en función de la selección:
 - Si ha seleccionado **One-time import (Importación única)** en el Paso 2, ha seleccionado **Import all machines (Importar todas las máquinas)** en el Paso 6, y todas las máquinas están presentes en el Core (como máquinas protegidas, replicadas, o máquinas con sólo puntos de recuperación), vaya al Paso 12.
 - Si ha seleccionado **Continuous import (by schedule) (Importación continua [por programa])** en el Paso 2, ha seleccionado **Import all machines (Importar todas las máquinas)** en el Paso 6, y al menos una máquinas no está presente en el Core (como máquina protegida, replicada, o máquina con sólo puntos de recuperación), haga clic en **Next (Siguiente)** y vaya al Paso 9.
 - Si no ha importado todas las máquinas en el Paso 6, haga clic en **Next (Siguiente)** y, a continuación, vaya al Paso 8.
- 8 En la página **Machines (Máquinas)**, seleccione las máquinas las máquinas que desee importar desde el archivo.
 - Si ha seleccionado **One-time import (Importación única)** en el Paso 2, y al menos una máquinas no está presente en el Core (como máquina protegida, replicada, o máquina con sólo puntos de recuperación), utilice las listas desplegables para seleccionar un repositorio para cada una de las máquinas que desee importar y, a continuación, vaya al Paso 12.
 - Si todas las máquinas ya están presente en Core (como máquinas protegidas, replicadas, o máquinas con sólo puntos de recuperación), vaya al Paso 12.
- 9 Haga clic en **Next (Siguiente)**.
- 10 En la página **Repository (Repositorio)**, lleve a cabo uno de las opciones siguientes:
 - Si un repositorio está asociado al Core, seleccione una de las opciones de la tabla siguiente.

Tabla 48. Opciones de repositorio

Opción	Descripción
Use an existing repository (Usar un repositorio existente)	Seleccione un repositorio asociado actualmente a este Core en la lista desplegable.
Create a Repository (Crear un repositorio)	En el cuadro de texto Server (Servidor), introduzca el nombre del servidor en el que desea guardar el nuevo repositorio, por ejemplo servername o localhost, y consulte Creación de un repositorio DVM .
	• Si no ningún repositorio está asociado al Core, introduzca el nombre del servidor en la que desea guardar el nuevo repositorio, por ejemplo servername o localhost, y consulte Creación de un repositorio DVM .

- 11 Si selecciona **Continuous import (by schedule) (Importación continua [por programa])** en el Paso 2, seleccione las opciones descritas en la tabla siguiente en la página **Schedule (Programa)**,

Tabla 49. Opciones de programar importación

Opción	Descripción
Daily (Diariamente)	Haga clic en el icono del reloj y utilice las flechas hacia arriba y hacia abajo para seleccionar la hora a la que desea iniciar el trabajo de archivo.
)	

Opción	Descripción
	Si está utilizando un sistema de hora de 12 horas, haga clic en el botón AM/PM para especificar la hora del día.
Weekly (Semanalmente)	Seleccione el día de la semana y, a continuación, la hora a la que desea iniciar el trabajo de archivo. Si está utilizando un sistema de hora de 12 horas, haga clic en el botón AM/PM para especificar la hora del día.
Monthly (Mensualmente)	Seleccione el día del mes y la hora a la que desea iniciar el trabajo de archivo. Si está utilizando un sistema de hora de 12 horas, haga clic en el botón AM/PM para especificar la hora del día.
Pause initial importing (Pausar la importación inicial)	Seleccione esta opción si no desea que el trabajo de importación se inicie a la hora programada después de completar el asistente. NOTA: Es posible que desee pausar la importación programada si necesita tiempo para preparar la ubicación de destino antes de archivar las reanudaciones. Si no selecciona esta opción, el archivado comenzará a la hora programada.

12 Haga clic en **Finalizar**.

Eventos

El Rapid Recovery Core incluye conjuntos predefinidos de eventos. Estos eventos se pueden utilizar para notificar a los administradores de los problemas críticos en el Core o con trabajos que pertenecen a copias de seguridad, a la exportación virtual, la replicación, etc.

En esta sección se describe cómo ver los eventos que se muestran en la Rapid Recovery Core Console. También puede obtener más información sobre los métodos y la configuración de la notificación de eventos, incluida la configuración de las notificaciones por correo electrónico. Por último, puede configurar las notificaciones para cambiar la cantidad de registros de eventos de tiempo que se conservan y reducir las notificaciones de eventos repetitivas.

Rapid Recoveryde Rapid Recovery

El Core de Rapid Recovery contiene conjuntos de eventos predefinidos que pueden utilizarse para notificar a los administradores problemas graves del Core o de las tareas de copia de seguridad en máquinas protegidas.

- Defina los tipos de eventos que desencadenan las alertas, así como los métodos utilizados por el sistema para estas notificaciones (correo electrónico, alertas de notificaciones, etc.), mediante la configuración grupos de notificaciones. Para obtener más información, consulte [Configuración de grupos de notificación](#).
- Si desea que los administradores reciban notificaciones mediante correo electrónico, configure un grupo de notificación, así como un servidor de correo electrónico, y configure una plantilla de notificaciones de correo electrónico. Para obtener más información, consulte [Configuración de un servidor de correo electrónico](#) y [Configuración de una plantilla de notificaciones por correo electrónico](#), respectivamente.
- Puede reducir el número de eventos del mismo tipo y el alcance en que aparecen en la página Eventos mediante la función de reducción de repeticiones. La función de reducción de repeticiones está activada de forma predeterminada. Puede desactivar esta función, o puede controlar el periodo en que los eventos se combinen en una sola ocurrencia en el registro de eventos. Para obtener más información, consulte [Acerca de la configuración de la reducción de repeticiones](#).
- Puede controlar por cuánto tiempo eventos y historial de trabajos información se conservan en la página Eventos en la Core Console. Para obtener más información, consulte [Configuración de la retención de eventos](#).

Visualización de eventos mediante las tareas, las alertas y el diario

En la Consola de Core, puede ver los eventos para el Core y puede ver los eventos de un equipo protegido o replicado específico.

La página **Eventos** de la Consola de Core muestra un registro de todos los eventos del sistema relacionados con el Core de Rapid

Recovery. Para acceder a los eventos del Core y verlos, haga clic en  (Eventos).

La página **Eventos** para un equipo protegido o replicado específico muestra un registro de eventos relacionados con este equipo protegido. Para acceder y ver los eventos de un equipo seleccionado, haga clic en el nombre del equipo en el menú Equipos protegidos y, desde la página **Resumen**, haga clic en el menú **Eventos**.

El contenido de la página Eventos (en el Core o en un equipo especificado) se divide en tres secciones: las tareas, las alertas y el diario. Estas vistas permiten filtrar los detalles sobre diversos sucesos, según corresponda.

Puede definir cómo se le notificarán los distintos eventos mediante la configuración de grupos de notificación. Para obtener más información, consulte [Configuración de grupos de notificación](#).

Realice los pasos de los procedimientos siguientes para ver tareas, alertas o un diario de todos los eventos:

- [Visualización de tareas](#)
- [Visualización de alertas](#)
- [Visualización de todos los eventos](#)

Visualización de tareas

Una tarea es un trabajo que el Core de Rapid Recovery debe realizar, como transferir datos en una copia de seguridad programada con regularidad o realizar una restauración desde un punto de recuperación.

Cuando una tarea se está ejecutando, se enumera en el menú desplegable **Tareas en ejecución** de la parte superior de Core Console. Al hacer clic en una tarea en ejecución, se abre el cuadro de diálogo Supervisar tarea activa.

También puede ver todas las tareas del Core de Rapid Recovery o todas las tareas asociadas con un equipo específico.

- 1 Para ver todas las tareas del Core de Rapid Recovery, en la barra de iconos haga clic en  (Eventos).
Si desea ver las tareas de un equipo protegido específico, vaya a la página **Resumen** del equipo especificado y, a continuación, haga clic en el menú **Eventos**.
- 2 Para ver únicamente tareas, en la parte superior izquierda de la página, haga clic en **Tareas**. Esta es la vista predeterminada.
La lista de eventos se filtrará para mostrar únicamente las tareas del Core o del equipo que seleccione.
- 3 Opcionalmente, para filtrar la lista de tareas por palabra clave, fecha de inicio, fecha de finalización o cualquier combinación, haga lo siguiente:
 - a Para filtrar por palabra clave, introduzca la palabra clave en el cuadro de texto **Palabra clave de la búsqueda**.
Por ejemplo, puede filtrar por palabras clave como "consolidando", "archivo comprimido" o "transferencia".
 - b Para filtrar por la fecha y hora de inicio, introduzca la fecha y hora de inicio mediante una de las siguientes opciones:
 - En el cuadro de texto **Desde**, escriba la fecha y hora con el formato MM/DD/AAAA HH:MM AM/PM. Por ejemplo, para buscar desde el 1 de enero de 2016 a las 08:00, introduzca 1/1/2016 8:00 AM.
 - Para seleccionar la fecha y hora actuales, haga clic en el widget  **Calendario** en el cuadro de texto **Desde** y, a continuación, haga clic en la fecha actual. La hora actual aparecerá automáticamente.
 - Haga clic en el widget  **Calendario**, seleccione la fecha y, a continuación, haga clic en el widget  **Reloj** y seleccione la hora deseada que utilizarán los controladores. Haga clic fuera del calendario para aceptar los cambios seleccionados.
 - c Para definir más la lista de tareas que aparece, también puede definir una fecha y hora de finalización con el mismo formato.
La lista de tareas se filtrará inmediatamente según los criterios que seleccione.
- 4 Opcionalmente, puede filtrar las tareas que aparecen en la lista de la manera siguiente:

Opción Descripción

	Para ver únicamente las tareas activas, haga clic en el icono Tarea activa .
	Para ver únicamente las tareas que estén en cola para ser realizadas, haga clic en el icono En cola .
	Para ver únicamente las tareas que estén a la espera de ser realizadas, haga clic en el icono Tareas en espera .
	Para ver únicamente las tareas que se hayan completado, haga clic en el icono Tareas completadas .
	Para ver únicamente las tareas que hayan fallado, haga clic en el icono Tareas con errores .

- 5 Para exportar la lista de tareas, seleccione un formato de la lista y, a continuación, haga clic en  **Exportar**. En el cuadro de diálogo resultante, confirme la exportación y, a continuación, haga clic en **Aceptar**.

Puede exportar utilizando los siguientes formatos:

Tabla 50. Formatos de exportación

Formato	Descripción
PDF	Portable Document Format (formato de exportación predeterminado)
HTML	Formato de página web
CSV	Valores separados por comas
XLS	Libro de Microsoft Excel® 1997 - 2003
XLSX	Libro de Excel

El archivo del tipo que haya seleccionado se descarga en la ubicación predeterminada del servidor del Core.

- 6 Haga clic en el widget  **Detalles del trabajo** de cualquier tarea para iniciar una nueva ventana con información detallada de la tarea, que incluye:
- Estado
 - Trabajo total (tamaño o porcentaje completado)
 - Fecha y hora de inicio
 - Fecha y hora de finalización
 - Velocidad
 - Tiempo transcurrido
 - Fase (para tareas secundarias)

Visualización de alertas

Una alerta es una notificación relacionada con una tarea o evento. Los tipos de alertas incluyen errores, advertencias o información.

Puede ver un diario de alertas importantes del Core de Rapid Recovery o de alertas importantes asociadas con un equipo específico.

- 1 Para ver las alertas del Core de Rapid Recovery, desde la barra de iconos, haga clic en  (Eventos), y, a continuación, haga clic en **Alertas**.
- Si desea ver las alertas de un equipo protegido específico, vaya a la página **Resumen** del equipo especificado, haga clic en el menú **Eventos** y, a continuación, haga clic en **Alertas**.

La lista de eventos se filtrará para mostrar únicamente las alertas importantes del Core o del equipo que seleccione.

- 2 De manera opcional, para filtrar la lista de alertas importantes por fecha de inicio, fecha de finalización, descripción del mensaje de alerta o cualquier combinación, haga lo siguiente:
 - a Para filtrar por la fecha y hora de inicio, introduzca la fecha y hora de inicio mediante una de las siguientes opciones:
 - En el cuadro de texto **De**, escriba la fecha y hora con el formato MM/DD/AAAA HH:MM AM/PM. Por ejemplo, para buscar desde el 1 de enero de 2016 a las 8:00 AM, introduzca 1/1/2016 8:00 AM.
 - Para seleccionar la fecha y la hora actual, haga clic en el widget  **Calendario** en el cuadro de texto **De** y, a continuación, haga clic en la fecha actual. La hora actual aparecerá automáticamente.
 - Haga clic en la flecha  **Calendario**, seleccione la fecha y, a continuación, haga clic en  y seleccione la hora deseada que utilizarán los controladores. Haga clic fuera del calendario para aceptar los cambios seleccionados.
 - b Para filtrar por descripción de alerta de mensaje, introduzca la descripción en el cuadro de texto **Search message** (Buscar mensaje).
Por ejemplo, para ver solo las alertas relacionadas con los Agents, introduzca "Agent"; para ver las alertas relacionadas con las transferencias, introduzca "transferencia", etc.
 - c Para definir más la lista de alertas que aparece, también puede definir una fecha y hora de finalización con el mismo formato.
La lista de alertas se filtra inmediatamente según los criterios que seleccione.
- 3 De manera opcional, si quiere quitar todas las alertas, haga clic en **Descartar todo**.

Visualización de todos los eventos

Puede ver todos los eventos del Core de Rapid Recovery o todos los eventos asociados con un equipo específico.

- 1 Para ver un diario de todos los eventos del Core de Rapid Recovery, desde la barra de iconos, haga clic en  (Eventos) y, a continuación, haga clic en **Diario**. Para ver todos los eventos del Core de Rapid Recovery, vaya a la página de inicio del Core de Rapid Recovery y haga clic en  (Eventos).
Si desea ver un diario de todos los eventos de un equipo protegido, vaya a la página **Resumen** del equipo especificado, haga clic en el menú **Eventos** y, a continuación, haga clic en **Diario**.
- 2 De manera opcional, para filtrar la lista de todos los eventos por fecha de inicio, fecha de finalización, descripción del mensaje de alerta o cualquier combinación, haga lo siguiente:
 - a Para filtrar por la fecha y hora de inicio, introduzca la fecha y hora de inicio mediante una de las siguientes opciones:
 - En el cuadro de texto **De**, escriba la fecha y hora con el formato MM/DD/AAAA HH:MM AM/PM. Por ejemplo, para buscar desde el 1 de enero de 2016 a las 8:00 AM, introduzca 1/1/2016 8:00 AM.
 - Para seleccionar la fecha y la hora actual, haga clic en el widget  **Calendario** en el cuadro de texto **De** y, a continuación, haga clic en la fecha actual. La hora actual aparecerá automáticamente.
 - Haga clic en la flecha  **Calendario**, seleccione la fecha y, a continuación, haga clic en  y seleccione la hora deseada que utilizarán los controladores. Haga clic fuera del calendario para aceptar los cambios seleccionados.
 - b Para filtrar por descripción de alerta de mensaje, introduzca la descripción en el cuadro de texto **Search message** (Buscar mensaje).
Por ejemplo, para ver solo las alertas relacionadas con los Agents, introduzca "Agent"; para ver las alertas relacionadas con las transferencias, introduzca "transferencia", etc.
 - c Para refinar más la lista de eventos que aparece, también puede definir una fecha y hora de finalización con el mismo formato.
La lista de eventos se filtra inmediatamente según los criterios que seleccione.

Información sobre las notificaciones por correo electrónico

Puede configurar el Core de Rapid Recovery para que le notifique eventos específicos mediante mensajes de correo electrónico a una dirección de correo electrónico que ha especificado. Los eventos que desencadenan las alertas se definen en el grupo de notificación, al igual que los otros métodos de notificación.

NOTA: Los grupos de notificación se deben establecer independientemente si utiliza el correo electrónico como un método de notificación. Para obtener más información, consulte [Configuración de grupos de notificación](#).

Si elige usar el correo electrónico como una de las opciones de notificación, también debe configurar un servidor de correo electrónico SMTP. El Core de Rapid Recovery utiliza el servidor que define para enviar alertas según los parámetros del grupo de notificación.

Además, también debe definir una plantilla de notificaciones de correo electrónico. El Core utiliza esta plantilla para definir la línea del asunto para cada alerta, y el contenido del cuerpo del mensaje de correo electrónico. La plantilla tiene los valores predeterminados y puede utilizar el valor predeterminado como está, o puede probar y realizar modificaciones para atender a sus necesidades.

Esta sección consta de los temas siguientes:

- [Configuración de un servidor de correo electrónico](#)
- [Configuración de una plantilla de notificaciones por correo electrónico](#)

Configuración de un servidor de correo electrónico

Complete los pasos de este procedimiento para configurar un servidor de correo electrónico.

NOTA: También debe configurar los ajustes del grupo de notificación, incluida la activación de la opción **Notificar por correo electrónico**, antes de que los mensajes de alerta por correo electrónico los envíe el sistema. Para obtener más información sobre cómo especificar eventos para recibir alertas de correo electrónico, consulte [Configuración de grupos de notificación](#).

1 Desplácese hasta la Core Console de Rapid Recovery.

2 En la barra de iconos, haga clic en  (Configuración) y, a continuación, realice una de las acciones siguientes:

- En la configuración de la Lista de Cores del lado izquierdo de la página Configuración, haga clic en **Servidor SMTP**.
- Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado **Servidor SMTP**.

Aparece la configuración del Core del servidor SMTP.

3 Haga clic en la opción que desee cambiar.

La opción seleccionada se volverá editable.

4 Introduzca la información de configuración según se describe en la tabla siguiente.

Opción	Descripción
Servidor SMTP	Introduzca el nombre del servidor de correo electrónico que debe utilizar la plantilla de notificación de correo electrónico. La convención de asignación de nombres incluye el nombre de host, dominio y sufijo; por ejemplo, smtp.gmail.com.
De	Escriba una dirección de correo electrónico de remite. Se utiliza para especificar la dirección de correo electrónico de respuesta en la plantilla de notificaciones de correo electrónico; por ejemplo, noreply@localhost.com.
Nombre de usuario	Escriba un nombre de usuario para el servidor de correo electrónico.
Contraseña	Introduzca la contraseña asociada con el nombre de usuario necesaria para acceder al servidor de correo electrónico.
Puerto	Escriba un número de puerto. Se utiliza para identificar el puerto para el servidor de correo electrónico; por ejemplo, el puerto 587 para Gmail. El valor predeterminado es 25.

Opción	Descripción
Tiempo de espera (en segundos)	Introduzca un valor entero para especificar durante cuánto tiempo se debe intentar la conexión con el servidor de correo electrónico. Se utiliza para establecer el tiempo de espera en segundos. El valor predeterminado es 60 segundos.
TLS	Seleccione esta opción si el servidor de correo utiliza una conexión segura como Transport Layer Security (TLS) o Secure Sockets Layer (SSL).

- 5 Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en  para guardar los cambios y salir del modo edición, o haga clic en  para salir del modo edición sin guardar.

 **PRECAUCIÓN:** Si no confirma cada cambio, la configuración no cambiará.

- 6 Haga clic en **Enviar correo electrónico de prueba** y, a continuación, haga lo siguiente:
- En el cuadro de diálogo **Enviar correo electrónico de prueba**, introduzca una dirección de correo electrónico de destino para el mensaje de prueba y, a continuación, haga clic en **Enviar**.
 - Si falla el mensaje de prueba, cierre el cuadro de diálogo de error y de **Enviar correo electrónico de prueba** y revise la configuración del servidor de correo electrónico. A continuación, envíe el mensaje de prueba otra vez.
 - Una vez que el mensaje de prueba es correcto, haga clic en **Aceptar** para confirmar que la operación se ha realizado correctamente.
 - Compruebe la cuenta de correo electrónico a la que ha enviado el mensaje de correo electrónico de prueba.

Configuración de una plantilla de notificaciones por correo electrónico

Cuando se habilita las notificaciones de los eventos de Rapid Recovery por correo electrónico, se crea una plantilla predeterminada de forma predeterminada. El servidor de correo electrónico SMTP definido para el Core utiliza esta plantilla para enviar notificaciones de los eventos de Rapid Recovery por correo electrónico.

En este tema se describe el proceso de configuración de la plantilla de notificaciones por correo electrónico predeterminada o del proceso de personalización del contenido. Mediante la opción **Restore Default** (Restaurar ajuste predeterminado) puede restaurar la plantilla de notificación predeterminada en cualquier momento.

 **PRECAUCIÓN:** Modifique la plantilla bajo su propia responsabilidad. Usted es responsable de comprobar todas modificaciones realizadas en la plantilla. Sólo se admite la plantilla predeterminada.

Complete los pasos de este procedimiento para configurar una plantilla de notificaciones por correo electrónico.

 **NOTA:** También debe configurar un servidor de correo electrónico y los ajustes de los grupos de notificación, incluida la opción **Notify by email** (Notificar por correo electrónico), antes de que se envíen los mensajes de alerta de correo electrónico. Para obtener más información sobre cómo configurar un servidor de correo electrónico para el envío de alertas, consulte [Configuración de un servidor de correo electrónico](#). Para obtener más información sobre la especificación de eventos para recibir alertas por correo electrónico, consulte [Configuración de grupos de notificación](#).

- Vaya a la Rapid Recovery Core Console.
- En la barra de iconos, haga clic en  (Más información), y, a continuación, seleccione  **Notificaciones (Notificaciones)**. Aparece la página **Notifications (Notificaciones)**.
- En el panel **Email Settings** (Configuración del correo electrónico), haga clic en  **Change (Cambiar)**. Aparecerá el cuadro de diálogo **Edit Email Notification Configuration** (Editar configuración de notificación por correo electrónico).
- Seleccione **Enable Email Notifications** (Habilitar notificaciones por correo electrónico). La plantilla de correo electrónico se activa y se muestra. Los valores de la plantilla de correo electrónico predeterminada se describen en el paso siguiente.
- Revise el contenido en el cuadro de diálogo **Edit Email Notification Configuration** (Editar configuración de notificación por correo electrónico) y determine si el contenido predeterminado se adapta a sus necesidades.

Opción	Descripción
Enable email notifications (Activar notificaciones por correo electrónico)	Este parámetro activa o desactiva la plantilla de notificaciones por correo electrónico. - Para activar la notificación por correo electrónico, seleccione esta opción. - Para desactivar la notificación por correo electrónico, desactive esta opción.
Email Subject (Asunto del correo electrónico)	El contenido de este campo de texto controla la línea de asunto de los mensajes de correo electrónico enviados como notificaciones de los eventos del sistema. La línea de asunto del correo electrónico predeterminado es la siguiente: <pre><hostName> <level>: <name> for <agentName></pre>
Email (Correo electrónico)	El contenido de esta área de texto controla el cuerpo de los mensajes de correo electrónico enviados como notificaciones de los eventos del sistema. El mensaje del cuerpo del correo electrónico predeterminado es el siguiente: <pre> <shortCompanyName> <coreProductName> on <hostName> has reported the <level> event "<name>" Date/Time: <localTimestamp> <message> <if(details.errorDetails)> <details.ErrorDetails.Message> <details.ErrorDetails.Details> <endif> ---</pre> About this event: <description> <pre><coreAdminUrl></pre>
Send Test Email (Enviar correo electrónico de prueba)	Al hacer clic en este botón se envía un mensaje de correo electrónico de prueba a la dirección de correo electrónico especificada en el cuadro de diálogo Send Test Email (Enviar correo electrónico de prueba) .
Restore defaults (Restaurar valores predeterminados)	Al hacer clic en este botón se eliminan los cambios personalizados de la plantilla de correo electrónico y se restauran los campos Email Subject (Asunto del correo electrónico) e Email (Correo electrónico) con el contenido predeterminado que se describe en esta tabla.
OK (Aceptar)	Al hacer clic en este botón se confirma y se guarda la configuración en el cuadro de diálogo Edit Email Notification Configuration (Editar configuración de notificación por correo electrónico).
Cancel (Cancelar)	Al hacer clic en este botón se cancelan los cambios efectuados en el cuadro de diálogo Edit Email Notification Configuration (Editar configuración de notificación por correo electrónico).

- 6 Si desea personalizar la plantilla de correo electrónico, realice los cambios en el texto o las variables que se han descrito en el paso anterior. Las variables utilizadas en el valor predeterminado se describen en la tabla siguiente.

Opción	Descripción
hostName	El nombre de host del Core
details	El objeto de detalles del evento específico.
agentName	El nombre de la máquina protegida asociada a este evento, si el evento tiene un ámbito de una única máquina protegida.
repositoryName	El nombre del repositorio asociado a este evento, si el evento tiene un alcance de repositorio.
jobSummary	El resumen de la tarea asociada con este evento, si el evento tiene un alcance de trabajo.
remoteSlaveCoreName	El nombre del Core de destino remoto asociado a este evento, si el evento tiene un alcance de core de destino.
remoteMasterCoreName	El nombre del Core de origen remoto asociado a este evento, si el evento tiene un alcance de core de origen.
productName	El nombre del producto, 'Rapid Recovery Core.' Este nombre de producto pueden cambiarse a efectos de denominación de marca con etiquetas blancas.
companyName	El nombre de la empresa que vende el producto.

- 7 En el cuadro de texto **Email Subject (Asunto del correo electrónico)** introduzca un asunto para la plantilla de correo electrónico. El asunto del correo electrónico se utiliza para definir el asunto de la plantilla de notificación por correo electrónico, por ejemplo, <nombre del host> - <nivel> <nombre>.
- 8 En el cuadro de texto **Email (Correo electrónico)**, introduzca la información para el texto de la plantilla que describa el evento, cuándo se ha producido y la gravedad.
- 9 Haga clic en **Send Test Email (Enviar correo electrónico de prueba)** y realice lo siguiente:
 - a En este cuadro de diálogo, escriba una dirección de correo electrónico de destino para el mensaje de prueba y, a continuación, haga clic en **Send (Enviar)**.
 - b Si el mensaje de prueba falla, salga del cuadro de diálogo de error y del cuadro de diálogo Send Test Email (Enviar correo electrónico de prueba), haga clic en **OK (Aceptar)** para guardar la configuración actual de la plantilla de correo electrónico. A continuación, modifique la configuración del servidor de correo electrónico tal y como se describe en el procedimiento. [Configuración de un servidor de correo electrónico](#) Verifique que ha vuelto a introducir la contraseña de esa cuenta de correo electrónico. Guarde esta configuración y, a continuación, vuelva a este procedimiento.
 - c Una vez que el mensaje de prueba se ha realizado correctamente, haga clic en **OK (Aceptar)** para confirmar que la operación se ha realizado correctamente.
 - d Compruebe la cuenta de correo electrónico a la que envió el mensaje de correo electrónico de prueba.

Una vez esté satisfecho con los resultados de las pruebas, vuelva al cuadro de diálogo Edit Email Notification Configuration (Editar configuración de notificación por correo electrónico) y haga clic en **OK (Aceptar)** para cerrar el cuadro de diálogo y guardar la configuración.

Grupos de notificación, valores del SMTP y plantillas de notificaciones de eventos del sistema

Los grupos de notificación le permiten definir conjuntos de eventos específicos que se les informa a los usuarios y la forma en la que la notificación se lleva a cabo. Para configurar o editar los grupos de notificación, consulte [Configuración de grupos de notificación](#).

También debe configurar los valores del servidor del Protocolo simple de transferencia de correo (SMTP) si desea enviar alertas como los mensajes de correo electrónico. Para obtener más información sobre cómo configurar valores de configuración del servidor de correo electrónico, consulte [Configuración de un servidor de correo electrónico](#).

Al enviar notificaciones de eventos, el sistema utiliza una notificación por correo electrónico. Puede personalizar esta plantilla. Para obtener más información sobre la configuración o la personalización la plantilla de notificaciones de correo electrónico, consulte [Configuración de una plantilla de notificaciones por correo electrónico](#).

Configuración de grupos de notificación

NOTA: También debe configurar el protocolo simple de transferencia de correo (SMTP) si desea enviar alertas como mensajes de correo electrónico, según se describe en este procedimiento. Para obtener más información sobre cómo establecer la configuración del servidor de correo electrónico, consulte [Configuración de un servidor de correo electrónico](#).

Los grupos de notificación le permiten definir conjuntos de eventos específicos en los que se alerta a los usuarios, y el modo en que esta notificación tiene lugar. Puede configurar alertas para que se envíen con los siguientes métodos:

- Por correo electrónico
- En el registro de eventos de Windows
- Utilizando syslogd
- Utilizando alertas de toast
- Utilizando alertas
- Utilizando captura SNMP

Puede configurar más de un grupo de notificaciones con diferentes parámetros de notificación.

Los grupos de notificación pueden establecerse al nivel del Core o para cada equipo protegido específico.

Realice los pasos de este procedimiento para configurar los grupos de notificación de las alertas.

1 Realice una de las siguientes acciones:

- Para establecer las notificaciones en el nivel del Core, desde la barra de iconos, haga clic en  (Más) y, a continuación, seleccione **Notificaciones**.
Aparecerá la página **Notificaciones**.
- Para establecer notificaciones para un equipo protegido específico, haga lo siguiente:
 - 1 A partir del menú de los equipos protegidos, haga clic en el equipo para el que quiera especificar las notificaciones.
Aparecerá la página **Grupos de notificación personalizada**.
 - 2 En la página de resumen del equipo protegido, en el menú desplegable Más, seleccione **Notificaciones**.
Aparecerá la página **Grupos de notificación personalizada**.

2 Haga clic en  **Agregar grupo**

Aparecerá el cuadro de diálogo **Agregar grupo de notificación**.

Los grupos de notificación le permiten definir conjuntos de eventos específicos en los que se alerta a los usuarios, y el modo en que esta notificación tiene lugar. Puede configurar alertas para que se envíen con los siguientes métodos:

El cuadro de diálogo **Agregar grupo de notificación** contiene un área de descripción general y dos fichas:

- Activar alertas
- Opciones de notificación

3 En el área de descripción general, introduzca la información básica para el grupo de notificación, según se describe en la siguiente tabla.

Opción	Descripción

Nombre	Introduzca un nombre para el grupo de notificación de eventos. Esta información es obligatoria.

 **PRECAUCIÓN:** El valor que introduzca para el nombre del grupo de notificación se puede cambiar más tarde.

Descripción	Introduzca una descripción que clarifique el propósito del grupo de notificación de eventos. Esta información es opcional.

4 En la ficha **Activar alertas**, defina el conjunto de eventos del sistema que desea registrar, para el que desea crear informes y por el cual desea recibir alertas de la siguiente forma:

Opción	Descripción
Todas las alertas	Para crear alertas de todos los eventos, seleccione All Alerts (Todas las alertas) .
Errores	Para crear alertas de errores, en el menú Seleccionar tipos , haga clic en Error . Esto se representa con una X roja. 
Advertencia	Para crear alertas de errores, en el menú Seleccionar tipos , haga clic en Aviso . Esto se representa mediante un icono de signo de admiración amarillo. 
Información	Para crear alertas de mensajes informativos, en el menú Seleccionar tipos , haga clic en Información . Esto se representa con una i azul. 
Restaurar el valor predeterminado	Para restaurar los tipos de alerta a los valores predeterminados, desde el menú Seleccionar tipos , haga clic en Restaurar valores predeterminados . Esto se representa con una flecha hacia la izquierda en azul oscuro. 

5 Para crear alertas de un tipo de evento específico (error, aviso o mensaje informativo), haga lo siguiente:

- a Si la opción **Todas las alertas** no muestra los grupos de alertas, haga clic en el símbolo mayor que > anterior a la etiqueta Todas las alertas. El símbolo cambia a una flecha hacia abajo y la vista se expande para mostrar los grupos.
- b A continuación, haga clic en el símbolo mayor que > junto a cualquier grupo de alertas específico para visualizar los eventos relacionados en el grupo.
Las categorías de grupos de eventos incluyen:

- Archivado
- Informe automático
- Conectabilidad
- Actualización automática
- Realizar copia de seguridad de repositorio
- CD de inicio
- Nubes
- Clústeres
- Servicio de Core
- Retención de base de datos
- Caché de deduplicación
- Repositorio DVM
- Exchange
- Exportación
- Trabajos
- Licencias
- Montaje local
- Truncamiento del registro
- Metadatos
- Trabajos nocturnos
- Notificación
- Persistir estado de Core
- Secuencias de comandos de PowerShell
- Protección
- Instalación automática
- Comprobación del punto de recuperación
- Montaje remoto
- Común de repositorio
- Replicación
- Restaurar
- Consolidación
- Archivaciones programadas
- Seguridad
- Registros de servidor
- vSphere

- Para definir alertas para todos los eventos en cada grupo, seleccione la casilla de verificación para **Todas las alertas**.
- Para definir alertas para todos los eventos de cualquier grupo de alerta, seleccione la casilla de verificación junto a ese grupo.
- Para seleccionar solo algunos tipos de alerta dentro de un grupo de alertas, expanda el grupo y, a continuación, seleccione solo aquellos sucesos específicos para los que desea log, informes y establecer alertas.

6 Haga clic en la pestaña **Opciones de notificación**.

7 En la pestaña **Opciones de notificación**, especifique cómo se gestionará el proceso de notificación.

Opción	Descripción
Notificar por correo electrónico	Designar los receptores de la notificación por correo electrónico. Puede elegir separar varias direcciones de correo electrónico, así como copias y copias ocultas. Puede elegir: • A: • CC:

Opción	Descripción
	BCC:
Notificar mediante registro de sucesos de Windows.	Seleccione esta opción si desea que las alertas se entreguen mediante el registro de eventos de Windows.
Notificar por syslogd	Seleccione esta opción si desea que las alertas se entreguen mediante syslogd. Especifique los detalles de syslogd en los cuadros de texto siguientes: - Host: - Puerto:
Notificar por alerta del sistema	Seleccione esta opción si desea que la alerta aparezca como un mensaje emergente en la esquina inferior derecha de la pantalla.
Notificar por alertas	Seleccione esta opción si desea que las alertas aparezcan como ventanas emergentes ubicadas en la parte inferior derecha de la Core Console.
Notificar por captura de SNMP	El Core de Rapid Recovery sirve como agente SNMP, que envía capturas (notificaciones sobre eventos específicos) a un gestor SNMP. El resultado es que el Core informa sobre alertas, estado de repositorios y equipos protegidos. Seleccione esta opción si desea notificar eventos del Core por captura SNMP. También debe especificar un número de captura. Por ejemplo, el número de captura predeterminado que utiliza el Core de Rapid Recovery es 162.

8 Haga clic en **Aceptar**.

Verá un mensaje que indica que el nombre del grupo de notificación definido no puede cambiar después de crear el grupo. Puede cambiar otras propiedades del grupo de notificación en cualquier momento.

- Si está satisfecho con el nombre del grupo, confirme este mensaje y guarde su trabajo.
- Si desea cambiar el nombre del grupo, haga clic en **No** para volver a la ventana Crear grupo de notificación, actualice el nombre del grupo y cualquier otro ajuste del grupo de notificación y guarde su trabajo.

El grupo de notificación aparece en la tabla de resumen. Puede crear diferentes grupos de notificación por medio de cualquier conjunto de parámetros.

Acerca de la configuración de la reducción de repeticiones

La capacidad de los administradores de recibir alertas cuando se producen ciertos eventos es de vital importancia. Sin embargo, en ciertas circunstancias, la recepción de una notificación repetida de eventos de los que ya está al tanto puede ser también frustrante e incómodo. Incluso si se genera una alerta debido a un error del entorno que desee conocer inmediatamente, es posible que el mismo estado de error genere cientos o miles de eventos en el mismo registro de eventos. Para reducir la repetición en el registro de eventos y reducir los inconvenientes de recibir notificaciones de correo electrónico repetidas para el mismo evento en Core Console, Rapid Recovery incluye una configuración de reducción de repeticiones que se habilita de forma predeterminada y se establece a los 5 minutos. Este parámetro puede ajustarse tan bajo como 1 minuto y tan alto como 60 minutos. También puede desactivarse completamente.

Cuando la reducción de repeticiones está desactivada, cada vez que se produzca un evento del mismo tipo y ámbito, se registrará en la base de datos. Sin importar la cantidad de tiempo que haya transcurrido desde que se produjo el evento anteriormente, cada nueva incidencia se mostrará en la parte Alertas de la pestaña Eventos.

Cuando se habilita la reducción de repeticiones (por ejemplo, con el tiempo predeterminado de 5 minutos), la primera vez que se produzca ese evento específico, se registrará en la base de datos de eventos y se mostrará en el registro de alertas. Si más tarde se registra de nuevo un evento del mismo tipo y ámbito dentro del umbral de tiempo establecido, el recuento del evento en la base de datos aumentará en 1 por cada incidencia de repetición dentro de ese umbral. El registro se muestra en la parte Alertas de la página Eventos. Sin embargo, muestra el evento una única vez, con la fecha y la hora de la aparición más reciente. El registro de eventos no está actualizado con el mismo evento hasta que caduque el umbral de tiempo desde la primera aparición. Por ejemplo, si se establece en 5 minutos y el evento ocurre de nuevo 6 minutos más tarde, aparecerá en el registro y recibirá otro mensaje de correo electrónico.

Configuración de la reducción de repeticiones

Complete los pasos de este procedimiento para configurar la reducción de repeticiones de los eventos.

- 1 Desplácese hasta la Core Console de Rapid Recovery. En la barra de iconos, haga clic en  (Más) y, a continuación, seleccione **Notificaciones**.
Aparecerá la página **Notificaciones**.
 - 2 En el panel Reducción de repeticiones, verá la configuración existente.
 - 3 Para activar, desactivar o cambiar el tiempo umbral de los eventos guardados, haga clic en  **Cambiar**.
Aparece el cuadro de diálogo **Editar reducción de repeticiones**
 - 4 Realice una de las siguientes acciones:
 - Para desactivar la reducción de repeticiones, desmarque la opción **Habilitar reducción de repeticiones**.
 - Para activar la reducción de repeticiones, seleccione la opción **Habilitar reducción de repeticiones**.
 - Para cambiar el umbral de tiempo (en minutos) para el que se ignoran los eventos idénticos repetidos, en el cuadro de texto **___ minutos**, introduzca un número entre 1 y 60.
-  **NOTA:** La opción **Habilitar reducción de repeticiones** debe estar seleccionada para cambiar este valor.
- 5 Haga clic en **Aceptar** para guardar la configuración y cerrar el cuadro de diálogo.

Configuración de la retención de eventos

Los eventos y trabajos a los que se les realiza un seguimiento en el Core se guardan durante una cantidad de tiempo determinada. La configuración predeterminada es 30 días. Este número se puede establecer entre los 0 y 3652 días (aproximadamente 10 años).

Complete los pasos de este procedimiento para configurar la retención de los eventos.

- 1 Desplácese hasta la Core Console de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Configuración), y, a continuación, realice una de las acciones siguientes:
 - En la configuración de la Lista de Cores en el lado izquierdo de la página Configuración, haga clic en **Conexión de base de datos**.
 - Desplácese hacia abajo en el lado derecho de la página Configuración hasta que pueda ver el encabezado **Conexión de base de datos**.

Aparecerá la configuración de conexión de base de datos.
- 3 Para cambiar la cantidad de días durante los cuales la información de eventos se guarda en la base de datos, haga clic en el campo de texto **Periodo de retención (días)**, introduzca un valor entre 0 y 3652 y, a continuación, haga clic en  para guardar cambios.
El periodo de retención de eventos se ajusta según lo especificado.

Recuperación automática rápida del dispositivo (RASR)

La Recuperación automática rápida del dispositivo (RASR) es un proceso de restauración desde cero que rápidamente restaura el dispositivo a un estado operativo.

RASR ofrece dos opciones de recuperación:

- Restaurar configuración de fábrica

- Recuperar el dispositivo de un estado error justo antes de que se produzca el error (se recuperan el SO, las configuraciones y los valores de configuración)

Creación de la memoria USB de RASR

Para crear una memoria USB de RASR:

- Vaya a la pestaña **Appliance (Dispositivo)**.
- Seleccione **Appliance (Dispositivo) > Backup (Copia de seguridad)** en el panel de navegación de la izquierda.
Se muestra la ventana **Create RASR USB Drive (Crear unidad USB de RASR)**.
NOTA: Inserte una memoria USB de 16 GB o mayor antes de intentar crear la clave RASR.
- Después de insertar una memoria USB de 16 GB o más, haga clic en **Create RASR USB Drive now (Crear unidad USB de RASR ahora)**.
Se muestra el mensaje **Prerequisite Check (Verificación de requisitos previos)**.
Después de que se hayan comprobado los requisitos previos, se abrirá la ventana **Create the RASR USB Drive (Crear la unidad USB de RASR)**, que muestra el tamaño mínimo requerido para crear la unidad USB y una **List of Possible target paths (Lista de posibles rutas de destino)**.
- Seleccione el destino y haga clic en **Create (Crear)**.
Aparece un cuadro de diálogo de advertencia.
- Haga clic en **Sí**.
Se ha creado la memoria de la unidad USB de RASR.
- NOTA:** Asegúrese de utilizar la función Extracción de la unidad de Windows para preparar la memoria USB para su extracción. De lo contrario, el contenido de la memoria USB puede dañarse y la memoria USB no funcionará como se espera.
Extraiga la memoria USB de RASR que se ha creado para cada dispositivo DL, etiquétela y guárdela para su uso en el futuro.

Ejecución de RASR

- NOTA:** Dell recomienda crear una clave USB RASR después de haber configurado el dispositivo. Para crear una clave USB RASR, consulte el apartado [Creación de la clave USB RASR](#).
- NOTA:** Asegúrese de contar con los más recientes RUU a los que pueda acceder el dispositivo.
- NOTA:** Para realizar la recuperación del sistema mediante RASR, consulte el documento *Recuperación de un dispositivo de recuperación y copia de seguridad™ DL mediante un dispositivo de Copia de seguridad y recuperación mediante Recuperación automática rápida del dispositivo (RASR)* en Dell.com/support/home.

Para restablecer la configuración predeterminada de fábrica:

- Introduzca la llave USB RASR creada.
- Reinicie el dispositivo y seleccione **Boot Manager (F11) (Administrador de arranque [F11])**.
- En el **Boot Manager Main Menu (Menú principal del administrador de arranque)**, seleccione **One-shot BIOS Boot Menu (Menú de inicio de BIOS único)**.
- En el **Boot Manager Boot Menu (Menú del administrador de arranque)**, seleccione la unidad USB conectada.
- Seleccione el diseño del teclado.
- Haga clic en **Troubleshoot (Solución de problemas) > Rapid Appliance Self Recovery (Recuperación automática rápida del dispositivo)**.
- Seleccione el sistema operativo de destino (SO).
RASR se inicia y aparece la pantalla de **bienvenida**.
- Haga clic en **Siguiente**.

Se muestra la pantalla de verificación **Prerequisites (Prerrequisitos)**.

❗ **NOTA:** Antes de ejecutar la RASR, asegúrese de que se verifican todos los prerrequisitos de hardware y otros.

9 Haga clic en **Siguiente**.

Se muestra la pantalla **Recovery Mode Selection (Selección de modo de recuperación)** con tres opciones:

- **System Recovery (Recuperación del sistema)**
- **Windows Recovery Wizard (Asistente de recuperación de Windows)**
- **Factory Reset (Restablecer valores de fábrica)**

10 Seleccione la opción **Factory Reset (Restablecer valores de fábrica)**.

Esta opción recuperará el disco del sistema operativo desde la imagen de fábrica.

11 Haga clic en **Siguiente**.

Aparece el siguiente mensaje de aviso en un cuadro de diálogo: `This operation will recover the operating system. All OS disk data will be overwritten .`

12 Haga clic en **Sí**.

El disco del sistema operativo inicia la restauración de las configuraciones de fábrica.

13 La página **RASR completada** aparece una vez finalizado el proceso de recuperación. Haga clic en **Finalizar**.

14 Iniciar el sistema después restaurar.

15 ❗ **NOTA:** Continúe configurando solo si aparece el Asistente de configuración del dispositivo AppAssure. Si no, vaya al paso 17.

Espera a que cargue el Asistente de configuración del dispositivo AppAssure. Cierre el asistente utilizando el Administrador de tareas de Windows.

16 Ejecute el archivo **launchRUU.exe** del paquete RUU. Siga las instrucciones y seleccione la opción para continuar con la instalación de RUU y finalice la instalación de RUU.

17 Se inicia el **Asistente de configuración del dispositivo DL** y le guiará a través del resto del proceso de restauración.

El dispositivo funciona correctamente ahora.

Local Mount Utility

En esta sección se describe cómo descargar, instalar y utilizar la Utilidad de montaje local (LMU) de Rapid Recovery basada en Windows para montar puntos de recuperación y explorar el contenido de un nivel de archivos con un equipo que es el host del Rapid Recovery Core.

Acerca de Local Mount Utility

LMU es un aplicación basada en Windows que se puede descargar y que permite montar un punto de recuperación de Rapid Recovery en cualquiera de los tres modos disponibles en los equipos con Windows. La utilidad ligera se puede instalar en operativos Windows de 32 bits y 64 bits. Incluye el `rapidrecovery-vdisk` (anteriormente, `aavdisk`) y controladores de `aavstor`, aunque no se ejecuta como un servicio. Cuando la instale, de manera predeterminada, se instala en el directorio **C:\Program Files\AppRecovery\Local Mount Utility** y coloca un acceso directo en el escritorio del equipo.

Aunque la utilidad ha sido diseñada para el acceso remoto a un Rapid Recovery Core, también puede instalar LMU en el mismo equipo que un Rapid Recovery Core. Cuando se ejecuta en un Core, la aplicación reconoce y muestra todos los montajes de ese Core, incluidos los montajes realizados por medio de la Rapid Recovery Core Console. De la misma forma, los montajes realizados en LMU también aparecerán en la Core Console.

Cuando LMU se instala en el mismo equipo que Mailbox Restore, LMU inicia automáticamente Mailbox Restore cuando se usa para abrir una base de datos de Exchange. Mailbox Restore es la aplicación de Dell Rapid Recovery que se utiliza para restaurar almacenes de datos y elementos de Microsoft Exchange. Puede instalarla después de instalar LMU o el Rapid Recovery Core. Para obtener más información sobre Mailbox Restore, consulte la *Dell Data Protection | Rapid Recovery*.

NOTA: En los equipos con Linux se usa una utilidad de línea de comandos, `local_mount`, para hacer consultas en el Core para equipos protegidos y sus puntos de recuperación correspondientes. De la misma forma, la herramienta permite a los usuarios montar un volumen de puntos de recuperación de forma remota, explorar el contenido del volumen en los niveles de archivo y restaurar archivos concretos o todo un volumen desde el punto de recuperación, incluida una restauración BMR del volumen del sistema. Para obtener más información, consulte [Montaje de un volumen de punto de recuperación en un equipo Linux](#), [Restauración de volúmenes para un equipo Linux mediante la línea de comandos](#), y [Realización de una restauración Bare Metal Restore para Linux](#), respectivamente.

Cómo trabajar con equipos Rapid Recovery Core en la Utilidad de montaje local

La Utilidad de montaje local (LMU) le permite trabajar con un número ilimitado de equipos Core de forma local o remota. Si instala la LMU en un equipo Rapid Recovery Core, el equipo aparece automáticamente en la LMU como host local. Todos los demás Core remotos aparecen con sus nombres de equipo o direcciones IP, en función de la información que se haya especificado al agregarlos. Con la LMU, puede agregar, modificar y eliminar equipos Core. Para obtener más información, consulte los siguientes procedimientos:

Vínculos relacionados

- [Incorporación de un equipo Core a Local Mount Utility](#)
- [Cambio de las opciones de Local Mount Utility](#)
- [Edición de la configuración de conexión de un Core en Local Mount Utility](#)
- [Cómo volver a conectarse a un Core](#)
- [Eliminación de un equipo Rapid Recovery Core de Local Mount Utility](#)

Incorporación de un equipo Core a Local Mount Utility

Para montar un punto de recuperación, debe agregar un equipo Core a la LMU. No hay límite en el número de Cores que puede agregar. Realice el procedimiento siguiente para configurar LMU agregando un Core.

- En el equipo en el que esté instalada la utilidad LMU, ejecútela haciendo doble clic en el icono del escritorio.
- Realice una de las siguientes acciones:
 - En el menú de Local Mount Utility en la esquina superior izquierda, haga clic en **Agregar Core**.
 - Haga clic con el botón derecho en el panel de la izquierda y, a continuación, haga clic en **Agregar Core**.Aparecerá el cuadro de diálogo **Agregar Core**.
- En el cuadro de diálogo **Agregar Core**, escriba las credenciales solicitadas que se describen en la tabla siguiente:

Tabla 51. Credenciales de Rapid Recovery Core

Opción	Descripción
Nombre de host	El nombre o la dirección IP del Core desde el que quiere montar puntos de recuperación. NOTA: Si instala LMU en un equipo Rapid Recovery Core, LMU agrega automáticamente el equipo de host local.
Puerto	Número de puerto usado para comunicar con el Core. El número de puerto predeterminado es 8006.
Utilizar mis credenciales de usuario de Windows	Seleccione esta opción si las credenciales que utiliza para acceder al Core son las mismas que sus credenciales de Windows.

Opción	Descripción
Utilizar credenciales específicas	Seleccione esta opción si las credenciales que utiliza para acceder al Core son distintas de las credenciales de Windows.
Nombre de usuario	Nombre de usuario utilizado para acceder al equipo del Core.
<i>i</i> NOTA: Esta opción solo está disponible si elije usar credenciales específicas.	
Contraseña	Contraseña utilizada para acceder al equipo del Core.
<i>i</i> NOTA: Esta opción solo está disponible si elije usar credenciales específicas.	

- Haga clic en **Conectar**.
- Si agrega varios Cores, repita todos los pasos según sea necesario.

Cambio de las opciones de Local Mount Utility

Lleve a cabo el siguiente procedimiento para cambiar las opciones para todos los Rapid Recovery Cores conectados a LMU.

- Desde la interfaz de usuario de Local Mount Utility, haga clic en **Opciones**.
- En el cuadro de diálogo **Opciones**, puede cambiar la configuración descrita en la siguiente tabla.

Tabla 52. Configuración del Core

Opción	Descripción
Repositorio predeterminado de punto de montaje	Utilice el botón Examinar o introduzca una ruta de acceso a la ubicación que desee utilizar para los puntos de recuperación de montaje.
Utilizar mis credenciales de cuenta de usuario de Windows	Seleccione esta opción para utilizar siempre las credenciales de Windows de manera predeterminada al iniciar sesión en un Core.
Utilizar credenciales específicas	Seleccione esta opción para usar las siguientes credenciales para cada Core conectado: Nombre de usuario: introduzca el nombre de usuario para utilizar con todos los Cores. Contraseña: introduzca la contraseña para utilizar con todos los Cores.
Tiempo de inactividad de Core (seg.)	Introduzca la cantidad de tiempo que LMU debe continuar intentando conectarse a un Core antes de que se agote el tiempo de conexión (en minutos : segundos : milisegundos).
Idioma	Seleccione el idioma en el que desea que LMU aparezca. Puede seleccionar las opciones siguientes: - Inglés - Francés - Alemán - Portugués - Español - Chino simplificado - Japonés - Coreano

Edición de la configuración de conexión de un Core en Local Mount Utility

Para editar la configuración que se ha establecido al agregar un Core a LMU, realice el siguiente procedimiento.

NOTA: Este procedimiento no se aplica al Core de host local. Sólo se aplica a las máquinas de Core remoto.

- 1 En la interfaz de usuario de Local Mount Utility, haga clic con el botón derecho en el Core para el que desee editar la configuración y, a continuación, haga clic en **Editar Core**.
- 2 En el cuadro de diálogo **Editar Core**, puede cambiar la configuración descrita en la siguiente tabla.

Tabla 53. Configuración del Core

Opción	Descripción
Nombre de host	El nombre del Core desde el que desee montar puntos de recuperación. NOTA: Si instala LMU en un equipo de Rapid Recovery Core, LMU agrega automáticamente el equipo de host local.
Puerto	Número de puerto usado para comunicar con el Core. El número de puerto predeterminado es 8006.
Utilizar mis credenciales de usuario de Windows	Seleccione esta opción si las credenciales que utiliza para acceder al Core son las mismas que sus credenciales de Windows.
Utilizar credenciales específicas	Seleccione esta opción si las credenciales que utiliza para acceder al Core son distintas de las credenciales de Windows.
Nombre de usuario	Nombre de usuario utilizado para acceder al equipo del Core. NOTA: Esta opción solo está disponible si elige usar credenciales específicas.
Contraseña	Contraseña utilizada para acceder al equipo del Core. NOTA: Esta opción solo está disponible si elige usar credenciales específicas.

- 3 Después de realizar los cambios, haga clic en **Aceptar**.

Cómo volver a conectarse a un Core

Si pierde la conexión a un equipo Rapid Recovery Core, puede actualizar la conexión haciendo lo siguiente.

Desde la interfaz de usuario de la Utilidad de montaje local, realice una de las acciones siguientes:

- Si el Core está sin conexión, haga doble clic en el Core cuya conexión desea restablecer.
La utilidad trata de restablecer la conexión con el Core.
- Si el Core está en línea, haga clic con el botón derecho en el Core y, a continuación, haga clic en la opción para volver a conectarse al Core.
La Utilidad de montaje local actualiza la conexión.

Eliminación de un equipo Rapid Recovery Core de Local Mount Utility

Lleve a cabo el siguiente procedimiento para eliminar un Core de LMU.

NOTA: Esta opción no está disponible para un Rapid Recovery Core localizado en el host local y etiquetado como tal.

- 1 Desde la interfaz de usuario de la utilidad de Local Mount Utility, haga clic con el botón derecho en el Core que desee eliminar y, a continuación, haga clic en **Eliminar Core**.
- 2 Para confirmar el comando, haga clic en **Sí** en el cuadro de diálogo.

LMU elimina el Core y sus equipos protegidos del árbol de navegación.

Cómo trabajar con equipos protegidos en Local Mount Utility

Con la Local Mount Utility, puede montar y examinar los puntos de recuperación de los equipos protegidos sin tener que haber iniciado sesión en la Rapid Recovery Core Console asociada a ese equipo. Para obtener más información, consulte los siguientes procedimientos:

- [Montaje de un punto de recuperación mediante Local Mount Utility](#)
- [Exploración de un punto de recuperación montado mediante Local Mount Utility](#)
- [Actualización de puntos de recuperación](#)
- [Desmontaje de puntos de recuperación individuales mediante Local Mount Utility](#)
- [Desmontaje de todos los puntos de recuperación desde un Rapid Recovery Core único o equipo protegido](#)
- [Desmontaje de todos los puntos de recuperación montados mediante Local Mount Utility](#)

Montaje de un punto de recuperación mediante Local Mount Utility

Con la LMU, puede montar cualquier punto de recuperación asociado a un equipo Core conectado, incluyendo equipos protegidos, equipos replicados y equipos con puntos de recuperación únicamente.

Antes de montar un punto de recuperación, Local Mount Utility (LMU) debe conectarse al Core en el que se almacena el punto de recuperación. Según se describe en el procedimiento [Incorporación de un equipo Core a Local Mount Utility](#), el número de Cores que se puede agregar a LMU no está limitado; no obstante, la aplicación solo puede conectar a un Core en cada momento. Por ejemplo, si monta un punto de recuperación de un equipo protegido por un Core y, a continuación, monta un punto de recuperación de otro equipo protegido por un Core distinto, LMU se desconecta automáticamente del primer Core para establecer una conexión con el segundo.

- 1 En la interfaz de usuario de Local Mount Utility, abra el Core en el árbol de navegación para mostrar los equipos protegidos.
- 2 En el árbol de navegación, seleccione el equipo desde el que desea montar un punto de recuperación.
Los puntos de recuperación aparecen en el marco principal.
- 3 Opcionalmente, expanda el punto de recuperación que desee montar para revelar volúmenes de disco o bases de datos individuales.
- 4 Haga clic con el botón derecho del ratón en el punto de recuperación que desee montar y seleccione una de las siguientes opciones:

Opción	Descripción
Montar	Esta opción le permite montar el punto de recuperación como de solo lectura.
Montaje editable	Esta opción le permite realizar cambios en el punto de recuperación montado.
Montaje de solo lectura con escrituras anteriores	Esta opción monta el punto de recuperación como de solo lectura e incluye los cambios que se realizaron previamente.
Montaje avanzado...	Esta opción abre el cuadro de diálogo Montajes avanzados.

- 5 Si ha seleccionado **Montaje avanzado**, complete las opciones que se describen en la siguiente tabla.

Tabla 54. Opciones de montaje avanzado

Opción	Descripción
Ruta de acceso de punto de montaje	Haga clic en el botón Examinar para seleccionar una ruta de acceso del punto de montaje predeterminado o introduzca manualmente la ruta de acceso preferida.
Tipo de montaje	Seleccione una de las opciones siguientes: • Montaje de solo lectura • Montaje editable • Montaje de solo lectura con escrituras anteriores

Opción	Descripción
	Para obtener descripciones de cada opción, consulte el Paso 4 .

- Haga clic en **Montar**.
LMU abre automáticamente la carpeta que contiene el punto de recuperación montado.

NOTA: Si selecciona un punto de recuperación ya montado hará que el cuadro de diálogo Montaje solicite o no desmontar el punto de recuperación.

Exploración de un punto de recuperación montado mediante Local Mount Utility

La exploración de un punto de recuperación abre los datos de copia de seguridad en una ventana del Explorador de Windows, y le permite buscar los volúmenes y las carpetas para el tema o los temas que desea recuperar.

A continuación, puede recuperar elementos copiándolos en la ubicación que desee por medio de un administrador de archivos, como por ejemplo, Explorador de Windows (o mediante programación con las API de Windows). Realice el procedimiento siguiente para examinar un punto de recuperación montado actualmente.

NOTA: este procedimiento no es necesario si está explorando un punto de recuperación justo después de montarlo, ya que la carpeta que contiene el punto de recuperación se actualiza automáticamente al completar el procedimiento de montaje.

- Desde la interfaz de usuario de la utilidad de montaje local, haga clic en **Montajes activos**.
Se abre la ventana Montajes activos y muestra todos los puntos de recuperación montados.
- Expanda el árbol de navegación para mostrar los puntos de recuperación montados para cada equipo y sus volúmenes.
- Haga clic en **Explorar** junto al volumen que desea explorar.

Actualización de puntos de recuperación

La LMU no recibe actualizaciones en tiempo real desde el Core y los equipos protegidos. Para actualizar un equipo protegido y ver los puntos de recuperación más recientes, realice el siguiente procedimiento.

Desde la interfaz de usuario de la utilidad de montaje local, haga clic con el botón derecho en el equipo protegido que desea actualizar y, a continuación, haga clic en Actualizar puntos de recuperación.

Desmontaje de puntos de recuperación individuales mediante Local Mount Utility

Realice el procedimiento siguiente para desmontar un punto de recuperación en un Core remoto usando LMU.

- Desde la interfaz de usuario de la utilidad de montaje local, haga clic en **Montajes activos**.
Se abre la ventana **Montajes activos** y muestra todos los puntos de recuperación montados.
- En la ventana **Montajes activos**, de forma opcional, puede hacer clic en los iconos más o menos para expandir o contraer la vista de volúmenes en cada punto de recuperación montado.
- En la ventana **Montajes activos**, junto a cada punto de recuperación o volumen que desee desmontar, haga clic en **Desmontar**.
Una ventana de progreso muestra si los puntos de recuperación seleccionados se han desmontado.
- Haga clic en la **x** en la parte superior derecha de la ventana **Montajes activos** para cerrar la ventana y volver a LMU.

Desmontaje de todos los puntos de recuperación desde un Rapid Recovery Core único o equipo protegido

Realice el procedimiento siguiente para desmontar solo los puntos de recuperación que están montados desde un único Core o equipo protegido.

- 1 Desde la interfaz de usuario de Local Mount Utility, realice una de las acciones siguientes:
 - Haga clic con el botón derecho en el Core para el que desee desmontar todos los puntos de recuperación.
 - Haga clic con el botón derecho en el equipo protegido para el que desee desmontar todos los puntos de recuperación.
- 2 Haga clic en **Desmontar todo para [nombre_equipo]**.
- 3 Para confirmar el comando, en el cuadro de diálogo, haga clic en **Sí**.

 **NOTA: Si hay tareas activas que utilizan los montajes existentes, desmontarlos hace que las tareas no se realicen.**

Se desmontan todos los puntos de recuperación montados para equipo que haya seleccionado.

Desmontaje de todos los puntos de recuperación montados mediante Local Mount Utility

Hay dos maneras principales de desmontar todos los puntos de recuperación de una sola vez en la LMU. Puede desmontar todos los puntos de recuperación sin necesidad de ver qué puntos de recuperación están montados actualmente. También puede ver todos los puntos de recuperación montados actualmente y, a continuación, desmontarlos todos. Consulte el procedimiento correspondiente a cada uno.

Desmontaje de todos los puntos de recuperación con el botón Desmontar todos los montajes

Realice el siguiente procedimiento para desmontar a la vez todos los puntos de recuperación montados.

- 1 Desde el menú de Utilidad de montaje local, haga clic en **Desmontar todos los montajes**.
- 2 Para confirmar el comando, en el cuadro de diálogo, haga clic en **Sí**.

 **NOTA: Si hay tareas activas que utilizan los montajes existentes, desmontarlos hace que las tareas no se realicen.**

Desmontaje de todos los puntos de recuperación con la ventana Montajes activos

Realice el siguiente procedimiento para desmontar a la vez todos los puntos de recuperación montados desde la ventana Montajes activos.

- 1 Desde la interfaz de usuario de la utilidad de montaje local, haga clic en **Montajes activos**.
- 2 En la sección **Montajes activos**, haga clic en **Desmontar todo**.
- 3 Para confirmar el comando, en la ventana, haga clic en **Sí**.
- 4 En la ventana **Montajes activos**, haga clic en **Cerrar**.

Uso del menú de bandeja de Local Mount Utility

El menú de bandeja de LMU se encuentra en la barra de tareas de su escritorio. Haga clic con el botón derecho del ratón en el icono para ver las opciones que se describen en la tabla siguiente.

Tabla 55. Opciones del menú de bandeja

Opción	Descripción
Examinar puntos de recuperación	Abre la ventana principal de LMU.
Montajes activos	Abre el cuadro de diálogo Montajes activos en la parte superior de la ventana principal de LMU.
Opciones	Abre el cuadro de diálogo Opciones en la parte superior de la ventana principal de LMU. En el cuadro de diálogo Opciones puede cambiar el directorio predeterminado de punto de montaje y las credenciales predeterminadas del Core para la interfaz de usuario de LMU.
Acerca de	Muestra información sobre la licencia de Local Mount Utility.
Salir	Cierra la aplicación LMU.

Administración del servidor

En la Core Console se incluye la pestaña **Appliance**, que permite aprovisionar espacio, supervisar el estado del servidor y acceder a herramientas de administración.

Temas:

- Supervisión del estado del dispositivo
- Copia de seguridad de Windows
- Aprovisionamiento de almacenamiento
- Eliminación de asignación de espacio para un disco virtual
- Utilidad de recuperación y actualización

Supervisión del estado del dispositivo

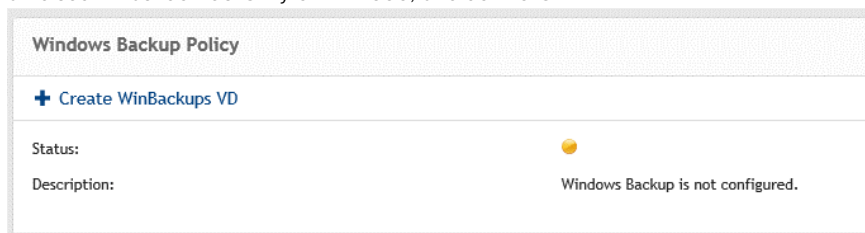
Puede supervisar el estado de los subsistemas del dispositivo en la página **Appliance (Dispositivo) > Health (Estado)**. En la página **Health (Estado)** se muestra un indicador de estado al lado de cada subsistema, junto con una descripción que indica el estado de condición del subsistema.

En la página **Health (Estado)** también se incluyen enlaces a herramientas que permiten profundizar en los detalles de cada subsistema, lo que puede ser útil para la solución de problemas de advertencias o errores. El enlace **Provisioning Status (Estado de aprovisionamiento)**, disponible para el subsistema de aprovisionamiento de almacenamiento, abre la pantalla **Provisioning (Aprovisionamiento)**, que muestra el estado de aprovisionamiento de ese subsistema. El enlace a **Rapid Appliance Self Recovery (Recuperación automática y rápida del dispositivo)** para la recuperación automática y rápida del dispositivo abre la página **Backup (Copia de seguridad)**, donde puede crear llave USB de RASR, supervisar el estado, y configurar la política de copia de seguridad de Windows. El enlace a Administración de máquinas virtuales abre la página Virtual **Standby (Espera virtual)**, donde puede administrar las máquinas virtuales. El enlace al **Administrador del servidor** disponible para el subsistema de hardware de almacenamiento abre la página **Health (Estado)**, donde ese puede analizar la condición del controlador, el gabinete, las unidades físicas, etc. El enlace a **Controladores**, disponible para el hardware del servidor abre la página **Controllers (Controladores)**, la cual le concede los detalles de los controladores y las unidades físicas asociadas con la controladora.

Copia de seguridad de Windows

La copia de seguridad de Windows está disponible en todas las versiones DL excepto DL 1000. La pestaña **Appliance (Dispositivo) > Backup (Copia de seguridad)** le permite configurar la política de copia de seguridad de Windows y muestra el estado de la última copia de seguridad y también los elementos de los que se ha hecho copia de seguridad previamente. Para usar esta función de copia de seguridad de Windows, debe existir el disco virtual de copia de seguridad de Windows.

- Una vez que haya actualizado el dispositivo con la utilidad RUU más reciente (3.0 .x), y si la copia de seguridad de Windows VD (creada en un entorno de AppAssure) no existe, el disco virtual de copia de seguridad de Windows se ha creado una vez que haya completado el Asistente de configuración del servidor DL. En este caso, si el disco virtual de la copia de seguridad de Windows no existe, haga clic en **+ Create WinBackups VD (Crear disco virtual de la copia de seguridad de Windows)** en la página **Backup (Copia de seguridad)** en la sección **Windows Backup Policy (Política de copia de seguridad de Windows)**. En los dispositivos DL 4000 y DL 4300, se crea un disco virtual de 295 GB y en DL 1300, uno de 210 GB.



- Una vez que haya actualizado el dispositivo con la utilidad RUU más reciente y si existe el disco virtual de la copia de seguridad de Windows creado en el entorno de AppAssure, realice estos pasos para crear el disco virtual de la copia de seguridad de Windows en el entorno de Rapid Recovery:

- a Edite **ApplianceProvisioningConfiguration.xml** (este archivo se encuentra en la raíz de cada volumen, por lo que puede editar una vez y, a continuación, copie en caso necesario):

⚠ PRECAUCIÓN: No elimine el disco virtual existente de la copia de seguridad de Windows.

- 1 Elimine todo el texto entre las etiquetas **<BackupVolumes>**.
 - 2 Elimine la etiqueta **</BackupVolumes>**.
 - 3 Edite la etiqueta **<BackupVolumes>** de forma que quede como **<Backupvolume/>**.
 - 4 Guarde y cierre.
- b Vaya a la Core Console.
 - c Haga clic en la pestaña **Appliance (Dispositivo) > RASR**.
 - d Haga clic en el botón **Create Windows Backup volume (Cear volumen de copia de seguridad de Windows)**.
 - e se crea el disco virtual de la copia de seguridad de Windows si hay suficiente espacio.

ⓘ NOTA: También puede configurar la Copia de seguridad de Windows mediante la función Copias de seguridad de Windows Server y almacenar copias de seguridad en cualquier ubicación, pero en este caso se muestra un error en la página RASR, ya que las copias no se pueden controlar y no se puede garantizar si serán coherentes para llevar a cabo restauraciones con RASR.

Estado de la copia de seguridad

El estado de la copia de seguridad de Microsoft Windows está disponible en la pestaña **Last Backup (Última copia de seguridad)**. Si se está ejecutando una copia de seguridad, la información se muestra en la pestaña **Current Backup (Copia de seguridad actual)**. Para ver la última copia de seguridad, lleve a cabo los siguientes pasos:

- 1 En la Core Console, acceda a la pestaña **Appliance (Dispositivo) > Backup (Copia de seguridad)**.
- 2 Haga clic en la flecha situada junto al botón **Status (Estado)** para ver el estado de la copia de seguridad.
- 3 El panel **Last Backup (Última copia de seguridad)** muestra la siguiente información:
 - Estado
 - Estado
 - Ubicación de la copia de seguridad
 - Hora de inicio
 - Hora de finalización
 - Descripción del error
 - Los elementos que se respaldaron

ⓘ NOTA: La información anterior se muestra si Windows Backup Policy se ejecuta o no.

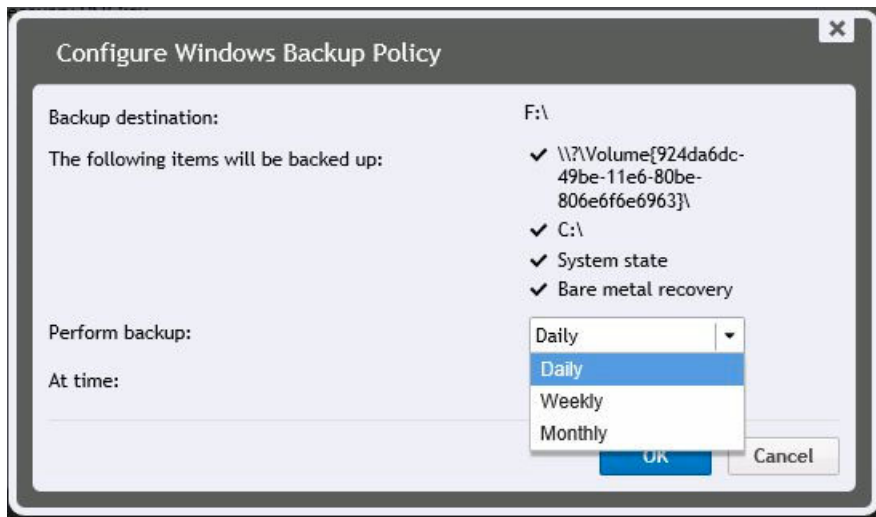
Backup Status	
Last Backup	
Status:	🟢 (Completed successfully)
Backup Location:	F:
Start Time:	8/16/2016 7:34:00 PM
End Time:	8/16/2016 7:39:00 PM
Error Description:	
Error Action:	
Items Backed Up	
State	Name
1	VolumeList
1	SystemState
1	BareMetalRecovery

Si se está ejecutando una copia de seguridad, se mostrará información sobre **Current Backup Progress (Progreso de la copia de seguridad actual)** y **Start Time (Hora de inicio)**.

Política de copia de seguridad de Windows

Para configurar una política de copia de seguridad de Windows, lleve a cabo los siguientes pasos:

- 1 En la Core Console, acceda a **Appliance > Backup**(Dispositivo / Copia de seguridad).
- 2 Haga clic en el botón **Configure Policy (Configurar política)**.
Se muestra la ventana **Windows Backup Policy (Política de copia de seguridad de Windows)**.



- 3 Introduzca los parámetros tal y como se describe a continuación:

Cuadro de texto	Descripción

Following items will be backed up (Copia de seguridad de los siguientes elementos):	· Volumen OS · Partición de recuperación · Archivos binarios de recuperación completa Todos los elementos anteriores estarán seleccionados de forma predeterminada.

Perform backup (Realizar una copia)	Seleccione la frecuencia de ejecución de Winbackup. Tiene las siguientes opciones: diariamente, semanalmente y mensualmente.

Select the time to schedule the backup (Período para programar la copia de seguridad):	Introduzca el período para programar una copia de seguridad.

- 4 Haga clic en **Configure (Configurar)**.
La política Winbackup está configurada y se mostrarán los detalles en la sección **Windows Backup Policy (Política de copia de seguridad de Windows)**.

Una vez configurada, puede realizar la copias de seguridad de los elementos seleccionados en cualquier momento con la opción **Backup now (Hacer copia de seguridad ahora)** y eliminar la política de copia de seguridad en **Delete policy (Eliminar política)** de la sección

Windows Backup Policy (Política de copia de seguridad de Windows).

Windows Backup Policy	
Backup now Delete Configure	
Backup destination:	F:\
Perform backup:	Daily
At time:	1:00 PM
The following items will be backed up:	✓ \\?\Volume{924da6dc-49be-11e6-80be-806e6f6e6963}\ ✓ C:\ ✓ System state ✓ Bare metal recovery

Aprovisionamiento de almacenamiento

El dispositivo configura el almacenamiento internodisponible y cualquier gabinete de almacenamiento externo conectado para:

- Repositorios\
- Volúmenes de disco para máquinas virtuales en espera o cualquier otra finalidad

Antes de empezar a aprovisionar almacenamiento en el disco, determine la cantidad de almacenamiento que desea asignar a las máquinas virtuales en espera. Puede asignar cualquier porcentaje de la capacidad disponible restante después de crear el repositorio de Rapid Recovery para alojar máquinas virtuales en espera. Por ejemplo, si está utilizando la administración de recursos de almacenamiento (SRM), puede asignar hasta el 100 por ciento de su capacidad de almacenamiento que queda después de crear el repositorio de Rapid Recovery. Se puede asignar espacio a máquinas virtuales en espera solo en los dispositivos que están abastecidos para alojar máquinas virtuales. Mediante la función de Recuperación dinámica de Rapid Recovery, puede usar estas máquinas virtuales para reemplazar un servidor con fallos que proteja el dispositivo.

Gracias a un entorno de tamaño medio que no necesita máquinas virtuales en espera, puede usar todo el almacenamiento para realizar copias de seguridad de un número considerable de Agents. No obstante, si precisa más recursos para las máquinas virtuales en espera y tiene que realizar copias de seguridad de un número menor de máquinas de Agent, puede asignar más recursos para máquinas virtuales más grandes.

Al seleccionar la pestaña **Appliance (Dispositivo) > Provisioning (Aprovisionamiento)**, el software del dispositivo de Rapid Recovery detecta el espacio de almacenamiento disponible para todas las controladoras compatibles con el sistema y verifica que el hardware cumpla con los requisitos.

Para completar al aprovisionamiento de discos del almacenamiento disponible:

- 1 Haga clic en **Appliance (Dispositivo) > Provisioning (Aprovisionamiento)**.
La pantalla **Provisioning (Aprovisionamiento)** muestra las secciones **Repositories (Repositorios)** y **Storage Volumes (Volúmenes de almacenamiento)**.
- 2 **PRECAUCIÓN:** Antes de proceder, asegúrese de seguir del paso 2 al 4 en este procedimiento.
- 2 Aprovisiona almacenamiento disponible para crear:
 - Repository (Repositorio)
 - Volúmenes de disco para máquinas virtuales en espera o cualquier otra finalidad
- 3 Para crear un repositorio:
 - a En la página **Provisioning (Aprovisionamiento)**, en la sección **Repositories (Repositorios)**, haga clic en **Add New Repository (Agregar nuevo repositorio)**.
Aparecerá el cuadro de diálogo **Add New Repository (Agregar repositorio nuevo)**.
 - b Introduzca la información según se describe en la tabla siguiente.

Tabla 56. Aprovisionamiento de almacenamiento

Cuadro de texto	Descripción
Repository Name	Escriba el nombre del repositorio. De manera predeterminada, este cuadro de texto contiene la palabra Repositorio y un número, que corresponde al número de repositorios de este Core. Por ejemplo, si se trata del segundo repositorio, el nombre predeterminado es 2. Cambie el nombre según sea necesario. Los nombres de los repositorios deben contener entre 1 y 40 caracteres alfanuméricos, incluidos espacios. No utilice caracteres o frases no permitidos. Para obtener más información, consulte los temas "Caracteres no permitidos" y "Frases prohibidas" en <i>Protección de datos de Dell Guía de usuario de Rapid Recovery 6.0 en dispositivos DL</i>.
Controladora	Seleccione el controlador de almacenamiento que corresponda si está creando un repositorio en el almacenamiento interno o en un gabinete de almacenamiento de conexión directa.
Gabinete	Seleccione el gabinete de almacenamiento que corresponda.
Tipo de RAID	Seleccione el nivel de RAID que corresponda. Dispone de las siguientes opciones para la configuración de RAID: 1, 5 o 6.

NOTA: El sistema le permite crear repositorios solo en los niveles de RAID en el que el almacenamiento está configurado como disponible y de fábrica. Para crear repositorios en la configuración RAID deseada, debe configurar su almacenamiento en el nivel de RAID deseado. Para configurar el almacenamiento en el nivel de RAID deseado, consulte la documentación de [Adaptadores de Dell](http://www.dell.com/support/home) en www.dell.com/support/home.

Capacidad estimada Muestra la capacidad estimada disponible para crear un repositorio.

Espacio disponible del controlador Muestra el espacio disponible del controlador.

Tamaño Introduzca el tamaño del repositorio.

c Haga clic en **Crear**.

Se crea un nuevo repositorio.

4 Para crear volúmenes de disco en máquinas virtuales en espera o para cualquier otra finalidad:

a En la sección **Storage Volume (Volumen de almacenamiento)** haga clic en **Create Volume (Crear volumen)**.

b En el campo de texto **Create Volume (Crear volumen)**, especifique la siguiente información para un nuevo volumen de disco: Volume name (Nombre de volumen), Controller (Controlador), Enclosure (Gabinete), RAID type (Tipo de RAID) y Size (Tamaño).

El espacio disponible del controlador se muestra de manera predeterminada. Puede seleccionar una de las siguientes configuraciones RAID: 1, 5 o 6.

c Haga clic en **Crear**.

Se crea un nuevo volumen de almacenamiento.

Eliminación de asignación de espacio para un disco virtual

Si necesita cambiar la configuración de aprovisionamiento, póngase en contacto con el servicio de asistencia técnica. Para obtener más información, consulte la sección **Cómo ponerse en contacto con Dell**.

Utilidad de recuperación y actualización

La utilidad Recovery and Update Utility (Utilidad de actualización y recuperación, RUU) es un instalador todo en uno para recuperar y actualizar el software de dispositivos DL (DL1000, DL1300, DL4000 y DL4300). Incluye el software Rapid Recovery y componentes específicos del dispositivo.

La utilidad RUU se compone de versiones actualizadas de funciones y características de Windows Server, .Net 4.5.2, LSI Provider, DL Applications, OpenManage Server Administrator y el software Rapid Recovery Core. Además, la utilidad Recovery and Update Utility (Utilidad de recuperación y actualización, RUU) también actualiza el contenido de Rapid Appliance Self Recovery (Recuperación automática rápida del dispositivo, RASR).

NOTA: Si actualmente utiliza cualquiera de las versiones del Core de AppAssure, la versión de Rapid Recovery 6.0.2.144 o anterior, la utilidad RUU actualiza a la versión más reciente disponible en la carga útil. No es posible omitir la actualización y esta actualización no es reversible. Si no desea actualizar el software del Core, no ejecute la utilidad RUU.

Actualización del dispositivo

Para actualizar el dispositivo, realice las tareas siguientes:

- 1 Vaya al portal de licencias en la sección Downloads (Descargas) o abra **support.dell.com** y descargue el instalador RUU.
- 2 Copie la utilidad al escritorio del dispositivo y extraiga los archivos.
- 3 Haga doble clic en el icono **launchRUU (Abrir RUU)**.
- 4 Cuando se le solicite, haga clic en **Yes (Sí)** para aceptar que no está ejecutando ninguno de los procesos enumerados.
- 5 Cuando aparezca la pantalla de la **Recovery and Update Utility (Utilidad de recuperación y actualización)**, haga clic en **Start (Inicio)**.
- 6 Cuando se le solicite reiniciar, haga clic en **OK (Aceptar)**.

Las versiones actualizadas de Windows Server Roles and Features, .Net 4.5.2, LSI Provider, DL Applications, OpenManage Server Administrator y Rapid Recovery Core Software se instalan como parte de la utilidad de recuperación y actualización. Además, la Recovery and Update Utility (Utilidad de recuperación y actualización) también actualiza el contenido RASR.

NOTA: Si utiliza actualmente una de las versiones de AppAssure Core, Recovery Core versión 6.0.2.144 o anterior, la utilidad RUU fuerza una actualización a la versión más reciente que hay en el contenido. No es posible omitir la actualización, que tampoco es reversible. Si no desea actualizar el software Core, no ejecute la utilidad RUU.

- 7 Reinicie el sistema, si se le solicita.
- 8 Haga clic en **Proceed (Continuar)** cuando todos los servicios y aplicaciones estén instalados.
La Core Console se inicia.

Reparación del dispositivo

Para reparar el dispositivo, realice las tareas siguientes:

- 1 Vaya al portal de licencias en la sección Descargas o vaya a **support.dell.com** y descargue la utilidad instalador de RUU.
- 2 Copie la utilidad al escritorio del dispositivo y extraiga los archivos.
- 3 Haga doble clic en el icono **launchRUU (Abrir RUU)**.
- 4 Cuando se le solicite, haga clic en **Yes (Sí)** para aceptar que no está ejecutando ninguno de los procesos enumerados.
- 5 Cuando aparezca la pantalla de la utilidad de recuperación y actualización, haga clic en **Start (Inicio)**.
- 6 Cuando se le solicite reiniciar, haga clic en **OK (Aceptar)**.

Las versiones actualizadas de Windows Server Roles and Features, .Net 4.5.2, LSI Provider, DL Applications, OpenManage Server Administrator y Rapid Recovery Core Software se instalan como parte de la utilidad de recuperación y actualización.

- 7 Si la versión integrada de la utilidad es la misma que la versión instalada, la utilidad de recuperación y actualización le solicitará que confirme si desea ejecutar una instalación de reparación. Este paso se puede omitir si no se necesita una instalación de reparación en el Rapid Recovery Core.
- 8 Si la versión integrada de la utilidad es superior a la versión instalada, la utilidad de recuperación y actualización le solicitará que confirme si desea actualizar el software Rapid Recovery Core.

 **NOTA: No se admiten actualizaciones a versiones anteriores del software Rapid Recovery Core.**

- 9 Reinicie el sistema, si se le solicita.
- 10 Haga clic en **Proceed (Continuar)** cuando todos los servicios y aplicaciones estén instalados.
El DL Appliance Configuration Wizard (Asistente de configuración del dispositivo DL) se inicia si el sistema debe configurarse de nuevo después de la reparación. De lo contrario, se iniciará la Core Console.

Protección de estaciones de trabajo y servidores

Protección de máquinas

Esta sección describe cómo proteger, configurar y administrar los equipos protegidos en su entorno de Rapid Recovery.

Acerca de la protección de los equipos con Rapid Recovery

Para proteger sus datos mediante Rapid Recovery, debe agregar las estaciones de trabajo y los servidores para la protección en la Core Console de Rapid Recovery; por ejemplo, su Exchange Server, SQL Server, servidor Linux, etc.

Debe instalar el software Rapid Recovery Agent en todos los equipos físicos o virtuales que desee proteger en el Core.

NOTA: Como excepción a la regla, si protege máquinas virtuales en VMware o un host ESXi, puede utilizar protección sin agentes. Para obtener más información, incluidas las restricciones para la protección sin agentes, consulte [Descripción Rapid Snap para Virtual](#).

En la Core Console de Rapid Recovery, mediante uno de los asistentes para proteger un equipo, puede identificar los equipos que desea proteger. Puede hacer lo siguiente:

- Puede proteger un solo equipo con el asistente para proteger un equipo, que se conecta al equipo que utiliza un nombre de host de red o dirección IP. Para obtener más información sobre cómo proteger un único equipo, [Cómo proteger una máquina](#).
- Puede proteger un clúster de red con la función Proteger clúster, que se conecta al clúster y sus nodos mediante un nombre de host de red o dirección IP.
- Puede proteger varios equipos simultáneamente mediante el asistente para proteger varios equipos, que se conecta al equipo mediante Microsoft Active Directory®, o a un vCenter o host ESXi; o puede especificar el nombre de host de red o las direcciones IP de una lista de equipos que introduzca manualmente.

NOTA: Dell recomienda limitar el número de equipos para proteger de manera simultánea a 50 o menos para evitar experimentar restricciones de recursos que puedan provocar que falle la operación de protección.

Cuando identifique los requisitos de protección de un equipo individual en el asistente, puede especificar qué volúmenes desea proteger. Al proteger varios equipos, todos los volúmenes se protegen de manera predeterminada. (Puede cambiar esto más adelante en base al equipo individual).

El asistente también le permite definir un programa personalizado de protección (o volver a utilizar un programa existente).

Mediante las opciones avanzadas, puede agregar medidas de seguridad adicionales al especificar o aplicar una clave de cifrado a las copias de seguridad de los equipos que desea proteger.

Finalmente, si no hay ninguno, puede definir un repositorio utilizando el asistente.

Después de instalar el software de Agent, cada máquina debe reiniciarse tras la instalación.

Para obtener más información sobre cómo proteger las estaciones de trabajo y los servidores, consulte [Cómo proteger una máquina](#).

PRECAUCIÓN: Rapid Recovery no admite bare metal restore (BMR) de equipos Linux con particiones de arranque EXT2. Cualquier BMR realizada en un equipo con este tipo de partición dará como resultado un equipo que no puede iniciarse. Si desea realizar una BMR en un equipo Linux con una partición de arranque EXT2, debe convertir la partición de arranque EXT2 a una EXT3 o EXT4 antes de comenzar a proteger el equipo y a realizar copias de seguridad.

Acerca de la protección de equipos Linux con Rapid Recovery

El software Agent de Rapid Recovery es compatible con varios sistemas operativos basados en Linux (para obtener más detalles, consulte los requisitos del sistema que se incluyen en la Installation and Upgrade Guide [Guía de instalación y actualización] de *Rapid Recovery* o en las Release Notes [Notas de versión de *Rapid Recovery*). El Core de Rapid Recovery solo es compatible con equipos Windows. Aunque puede administrar equipos protegidos Linux desde la Core Console de Rapid Recovery, varios procedimientos para equipos Linux tienen pasos que difieren de sus equivalentes Windows. También puede realizar algunas acciones directamente en equipos protegidos Linux mediante la utilidad de la línea de comandos `local_amount`.

❗ **NOTA:** Anteriormente, la utilidad `local_amount` se llamaba `aamount`.

Acerca de la administración de servidores Exchange Server y SQL Server en el Rapid Recovery Core

Las opciones específicas para Exchange Server y SQL Server aparecen en la Rapid Recovery Core Console cuando se detecta una instancia del software y los archivos en servidores protegidos. En esos casos, hay disponibles opciones adicionales al seleccionar el equipo protegido en Core Console.

Por ejemplo: si selecciona un Exchange Server protegido en el menú de navegación izquierdo, las opciones de menú que aparecen para ese equipo protegido incluyen la opción del menú desplegable **Exchange**.

Si selecciona un SQL Server protegido en el menú de navegación izquierdo, las opciones de menú que aparecen para ese equipo protegido incluyen la opción del menú desplegable **SQL**.

Aunque estas opciones funcionen de forma diferente, hay algunas características comunes. Entre las funciones que puede realizar en los servidores Exchange y SQL (y no en otros equipos protegidos) se incluye:

- **Forzado de truncamiento de registros.** Tanto los servidores SQL Server como los Exchange incluyen registros de servidor. El proceso para trunca registros de SQL identifica el espacio disponible en el servidor. Cuando trunca registros de un servidor Exchange, además de la identificación del espacio disponible, el proceso también libera más espacio en el servidor.
- **Establecimiento de credenciales para el servidor apropiado.** Los servidores Exchange le permiten establecer las credenciales para el equipo protegido en la página Resumen del servidor protegido. Los servidores SQL Server permiten establecer credenciales para un equipo SQL Server protegido por separado, o establecer las credenciales predeterminadas para todos los servidores SQL Server protegidos.
- **Visualización del estado de las comprobaciones en los puntos de recuperación de Exchange Server o SQL Server.** Los puntos de recuperación capturados del SQL o Exchange Server protegido se corresponden con los indicadores de estado de color. Los colores indican el éxito o el error de las diversas comprobaciones relevantes para los servidores SQL Server o Exchange.

Esta sección incluye los siguientes temas específicos para la administración de equipos protegidos que utilizan Exchange Server o SQL Server:

- [Comprensión de los indicadores de estado de puntos de recuperación](#)
- [Configuración y funciones en servidores de Exchange protegidos](#)
- [Configuración y funciones en servidores SQL Server protegidos](#)

Acerca de la protección de clústeres de servidor

En Rapid Recovery, la protección de clúster de servidor está asociada con los equipos protegidos de Rapid Recovery instalados en nodos de clúster individuales (esto es, equipos individuales en el clúster), y el Core de Rapid Recovery, que protege dichos equipos, todo ello como si fueran un único equipo compuesto.

Puede configurar fácilmente un Core de Rapid Recovery para proteger y administrar un clúster. En la Core Console, un clúster está organizado como una entidad aparte, que actúa como un contenedor, para incluir los nodos relacionados. Por ejemplo, en el área de

navegación izquierda, en el menú **Equipos protegidos**, se enumeran los clústeres protegidos. Justo debajo de cada clúster, aparecen los equipos Agent o los nodos individuales asociados. Cada uno de estos es un equipo protegido en el que está instalado el software Rapid Recovery Agent. Si hace clic en el clúster, aparece la página **Resumen** de la Core Console.

En los niveles de Core y clúster, puede ver información sobre el clúster, como la lista de nodos relacionados y volúmenes compartidos. Al mostrar la información de un clúster en la Core Console, puede hacer clic en **Nodos protegidos**, en la parte superior del menú, para ver una tabla de resumen de los nodos individuales del clúster. En la tabla de resumen, en cada nodo, puede realizar funciones como forzar una instantánea, realizar una exportación única o configurar un servidor virtual en espera, montar o visualizar puntos de recuperación, realizar una restauración desde un punto de recuperación, convertir el nodo de clúster en su propio equipo protegido o eliminar el nodo de la protección. Si el nodo es un servidor Exchange o SQL Server, podrá ver las opciones de los registros de truncamiento.

A nivel de clúster, también puede ver los metadatos correspondientes del clúster de Exchange y SQL para los nodos del clúster. Puede especificar la configuración de todo el clúster y los volúmenes compartidos de dicho clúster.

Si hace clic en cualquier nodo del clúster en el menú de navegación izquierdo, la información que se muestra en la Core Console es específica de ese nodo del clúster. Aquí puede ver la información específica de ese nodo o establecer la configuración solo de ese nodo.

Compatibilidad con los volúmenes compartidos en el clúster

En la versión 6.x de Rapid Recovery, la compatibilidad con volúmenes compartidos en el clúster (CSV) se limita a copias de seguridad originales de CSV que ejecutan Windows Server 2008 R2. También puede restaurar volúmenes CSV que ejecutan Windows Server 2008 R2 desde un punto de recuperación, o realizar una exportación virtual a una Hyper-V CSV que ejecutan Windows Server 2008 R2. No se puede realizar una exportación virtual de un volumen compartido en el clúster. Una novedad de Rapid Recovery versión 6.0.1 y posterior es la capacidad para realizar una exportación virtual a un CSV Hyper-V que ejecuta Windows Server 2012 o Windows Server 2012 R2.

NOTA: La función Hyper-V sin Agent es compatible sólo con Windows Server 2012 R2 y posterior.

Para otros sistemas operativos, el servicio del Agent de Rapid Recovery se puede ejecutar en todos los nodos en un clúster, y el clúster se puede protegerse como un clúster dentro del Core de la Rapid Recovery. Sin embargo, los CSV no se muestran en la Core Console y no se pueden proteger. Todos los discos locales (como el volumen del sistema operativo) pueden protegerse.

La siguiente tabla muestra la compatibilidad actual del Core de Rapid Recovery con volúmenes compartidos en el clúster.

Tabla 57. Rapid Recovery con volúmenes compartidos en el clúster

Asistencia volúmenes compartidos de clúster con Rapid Recovery	Proteger, replicar, consolidar, montar, archivar	Restaurar volúmenes CSV	Exportación virtual a CSV Hyper-V
Rapid Recovery	6.0	6.0	6.0.x
Windows Server 2008 R2	Sí	Sí	Sí
Windows Server 2012	No	No	Sí
Windows Server 2012 R2	No	No	Sí

¹ Excluye la función Hyper-V sin Agent, que es compatible solo con Windows Server 2012 R2 y posterior.

Rapid Recovery le permite proteger otros sistemas operativos en volúmenes compartidos en el clúster, pero lo hace bajo su propia responsabilidad. Dell solo ofrece asistencia para las configuraciones de la tabla anterior.

Compatibilidad con volúmenes básicos y dinámicos

Rapid Recovery permite tomar instantáneas de todos los volúmenes básicos y dinámicos. Rapid Recovery también admite la exportación de volúmenes dinámicos sencillos que se encuentren en un único disco físico. Como su nombre indica, los volúmenes dinámicos sencillos no son volúmenes seccionados, reflejados, extendidos ni RAID.

El comportamiento de la exportación virtual de los discos dinámicos es diferente en función de si el volumen que desea exportar está protegido por el software Rapid Recovery Agent o es una VM con protección sin agentes. Esto se debe a que los volúmenes dinámicos complejos o que no son simples disponen de una geometría de disco arbitraria que Rapid Recovery Agent no puede interpretar por completo.

Cuando se intenta exportar un disco dinámico complejo desde un equipo con el software Rapid Recovery Agent, aparece una notificación en la interfaz de usuario que le avisa de que las exportaciones están limitadas y restringidas a los volúmenes dinámicos sencillos. Si intenta exportar otra cosa que no sea un volumen dinámico sencillo con Rapid Recovery Agent, el trabajo de exportación fallará.

En contraposición, los volúmenes dinámicos para VM con protección sin agentes son compatibles para la protección, exportación virtual, restauración de datos y BMR, y almacenamiento repositorio con algunas restricciones importantes. Por ejemplo:

- **Protección:** en el caso de que un volumen dinámico abarque varios discos, debe proteger dichos discos juntos para mantener la integridad del volumen.
- **Exportación virtual:** puede exportar volúmenes dinámicos complejos seccionados, reflejados, extendidos o RAID desde un host ESXi mediante la protección sin agentes.
Sin embargo, los volúmenes se exportan al nivel del disco, sin análisis del volumen. Por ejemplo, si se exporta un volumen dinámico expandido en dos discos, la exportación incluirá dos volúmenes de disco distintos.

 **PRECAUCIÓN:** Al exportar un volumen dinámico expandido en varios discos, debe exportar los discos dinámicos con los volúmenes del sistema original para conservar los tipos de discos.

- **Restauración de datos:** al exportar un volumen dinámico expandido en varios discos, debe restaurar los discos dinámicos con los volúmenes del sistema original para conservar los tipos de discos. Si se restaura solo un disco, se interrumpirá la configuración del disco.

Almacenamiento repositorio: además, Rapid Recovery es compatible con la creación de repositorios en volúmenes dinámicos complejos (seccionados, reflejados, extendidos o RAID). El sistema de archivos del equipo que aloja el repositorio debe ser NTFS o ReFS.

Funcionamiento del instalador del software Rapid Recovery Agent

Rapid Recovery le permite descargar instaladores del Core de Rapid Recovery. En la página **Descargas**, puede elegir entre descargar Agent Installer, Local Mount Utility (LMU) o un archivo MIB de SNMP. Para obtener más información acerca de la LMU, consulte [Local Mount Utility](#). Para obtener más información acerca de la SNMP, consulte [Comprensión de la configuración de SNMP](#).

 **NOTA:** Para acceder a Agent Installer, consulte [Descarga del instalador Agent de Rapid Recovery](#). Para obtener más información sobre la implementación de Agent Installer, consulte la *Installation and Upgrade Guide (Guía de instalación y actualización)* de Dell Data Protection | Rapid Recovery.

Agent Installer se utiliza para instalar la aplicación Rapid Recovery Agent en los equipos que el Core de Rapid Recovery debe proteger. Si determina que tiene un equipo que necesita el Agent Installer, puede descargar el instalador web desde la página Descargas de la Core Console de Rapid Recovery.

 **NOTA:** La descarga del Core se realiza desde el Dell Data Protection | Portal de licencias de Rapid Recovery. Para descargar el instalador del Core de Rapid Recovery, visite <https://licenseportal.com>. Para obtener más información, consulte la guía del usuario del Dell Data Protection | Portal de licencias de Rapid Recovery.

Descarga del instalador Agent de Rapid Recovery

Descargue el Instalador Agent de Rapid Recovery e impleméntelo en cualquier equipo que desee proteger en el Core de Rapid Recovery. Complete los pasos de este procedimiento para descargar el instalador web.

- 1 Para descargar el instalador web de Agent directamente desde el equipo que desea proteger, haga lo siguiente:
 - a En un navegador web, abra el Dell Data Protection | Portal de licencias de Rapid Recovery en <https://licenseportal.com>.
 - b En el menú de navegación izquierdo, haga clic en **Descargas**.
 - c Desde el panel **Aplicaciones basadas en Windows**, desplácese hasta la fila **Windows Agent** y haga clic en **Descargar** según el instalador apropiado (sistemas de 32 bits o de 64 bits).

El archivo del instalador, por ejemplo ,Agent-X64-6.0.1.xxxx.exe, se guarda en la carpeta de destino de descargas.

- 2 Para descargar el instalador web desde el Core, en la barra de iconos de la Consola de Core, haga clic en el icono  **Más** y, a continuación, seleccione **Descargas**.
- 3 En la página **Descargas**, en el panel **Agent**, haga clic en **Descargar instalador web**.
- 4 En el cuadro de diálogo **Abrir LocalMountUtility-Web.exe**, haga clic en **Guardar archivo**.
El archivo del instalador, por ejemplo ,Agent-X64-6.0.1.xxxx.exe, se guarda en la carpeta de destino de descargas.
- 5 Mueva el instalador al equipo adecuado e instale el software de Rapid Recovery Agent.
Para obtener más información acerca de la instalación del software Rapid Recovery, consulte la *Installation and Upgrade Guide* (Guía de actualización y de instalación) de Rapid Recovery.

Implementación simultánea del Agente en varias máquinas desde la Core Console

Puede implementar el software Rapid Recovery Agent de forma simultánea en varios equipos Windows. Los equipos pueden formar parte de un dominio de Active Directory o host virtual vCenter o ESX(i); o bien pueden ser equipos ya protegidos por el Rapid Recovery Core, como en el caso de una actualización del software Rapid Recovery Agent. También tiene la opción de implementar manualmente el software en equipos que no están necesariamente asociados con un dominio específico o el host.

También puede implementar manualmente el software Rapid Recovery Agent en uno o varios equipos Linux desde la Core Console.

⚠ PRECAUCIÓN: Si AppAssure Agent se ha instalado previamente en un equipo Linux, antes de instalar Rapid Recovery Agent, elimine el AppAssure Agent del equipo mediante una secuencia de comandos de shell. Para obtener información sobre cómo eliminar el Agent de un equipo Linux, consulte el tema [Desinstalar el software de AppAssure Agent de un equipo Linux](#). Para implementar correctamente el software Agent en equipos Linux, consulte los requisitos previos en el tema [Información sobre la instalación de software Agent en equipos Linux](#). Estos temas se encuentran en la *Guía de instalar y actualización de Dell Data Protection | Rapid Recovery*

La implementación del software Rapid Recovery Agent no protege los equipos automáticamente. Tras la implementación, debe seleccionar la opción **Protect Multiple Machines (Proteger varios equipos)** en la barra de botones de Core Console.

① NOTA: La función de implementación simultánea de varios equipos se denominaba “implementación masiva”. La función de protección simultánea de varios equipos se denominaba “protección masiva”.

Para implementar y proteger simultáneamente varios equipos, debe realizar las tareas siguientes:

- Implementar el Rapid Recovery Agent en varios equipos. Consulte [Implementación del software Rapid Recovery Agent en uno o más equipos](#).
- Supervise la implementación. Consulte [Verificación de la implementación en varios equipos](#).
- Proteger varios equipos. Consulte [Acerca de la protección de varios equipos](#).

① NOTA: Si ha seleccionado la opción **Protect machine after install (Proteger máquina tras la instalación)** durante la implementación, omita este paso.

- Supervisar la actividad de la protección masiva. Consulte [Supervisión de la protección de varios equipos](#).

Implementación del software Rapid Recovery Agent en uno o más equipos

Puede simplificar la tarea de implementar el software Rapid Recovery Agent en uno o más equipos de Windows mediante el empleo del asistente de implementación del software Agent.

① NOTA: En el pasado, esta función se denominaba "implementación masiva."

Cuando utiliza el asistente de implementación del software Agent, Rapid Recovery puede detectar automáticamente equipos en un host y seleccionar los equipos en los que desea implementar. En el caso de equipos en dominios o hosts que no sean Active Directory, vCenter o

ESX(i), puede conectarse manualmente a equipos individuales utilizando sus direcciones IP y las credenciales pertinentes. También puede enviar actualizaciones del software en equipos que ya protege el Core de Rapid Recovery.

Desde el interior de la Core Console, puede completar cualquiera de las siguientes tareas:

- [Implementación en equipos de un dominio de Active Directory](#)
- [Implementación en equipos de un host virtual VMware vCenter/ESX\(i\)](#)
- [Implementación de una actualización de software de Agent Rapid Recovery para los equipos protegidos](#)
- [Implementación en equipos manualmente](#)

NOTA: Dell recomienda limitar el número de equipos en los que implementa de forma simultánea a 50 o menos para evitar sufrir limitaciones de recursos que pueden provocar el fracaso de la operación de implementación.

NOTA: Los equipos objetivo deben tener acceso a Internet para descargar e instalar bits, ya que Rapid Recovery utiliza la versión web del instalador de Rapid Recovery Agent para implementar los componentes de instalación. Si no dispone de acceso a Internet, utilice la Core Console para descargar el instalador en un soporte, como una unidad USB y, a continuación, instale físicamente el software en los equipos que desea proteger. Para obtener más información, consulte [Descarga del instalador Agent de Rapid Recovery](#).

Implementación en equipos de un dominio de Active Directory

Utilice este procedimiento para implementar simultáneamente el software Rapid Recovery Agent en uno o más equipos en un dominio Active Directory.

Antes de iniciar este procedimiento, debe tener a mano la información del dominio y las credenciales de inicio de sesión para el servidor de Active Directory.

- 1 En la Core Console de Rapid Recovery, haga clic en el menú desplegable **Proteger** y luego haga clic en **Implementar el software de Agent**.

Se abre el asistente para implementar el software de Agent.

- 2 En la página **Conexión** del asistente, en la lista desplegable **Origen**, seleccione **Active Directory**.
- 3 Introduzca la información de dominio y las credenciales de inicio de sesión según se describe en la tabla siguiente.

Tabla 58. Información y credenciales de dominio

Cuadro de texto	Descripción
Host	Nombre de host o dirección IP del dominio de Active Directory.
Nombre de usuario	El nombre de usuario utilizado para conectarse con el dominio; por ejemplo, Administrator (o, si el equipo se encuentra en un dominio, [nombre de dominio]\Administrator).
Contraseña	La contraseña segura que se utiliza para conectar con el dominio.

- 4 Haga clic en **Siguiente**.
- 5 En la página **Equipos**, seleccione los equipos en los que quiere implementar el software Rapid Recovery Agent.
- 6 De manera opcional, para reiniciar automáticamente los equipos protegidos una vez que el agente está instalado, seleccione **Después de la instalación, reiniciar los equipos automáticamente (recomendado)**.
- 7 Haga clic en **Finalizar**.

El sistema comprueba de forma automática cada uno de los equipos que haya seleccionado.

Si Rapid Recovery detecta cualquier laguna durante la verificación automática, el asistente avanza a la página Avisos, donde puede borrar los equipos de la selección y comprobar manualmente los equipos seleccionados. Si los equipos que ha agregado pasan la verificación automática, aparecerán en el panel Implementar Agent en los equipos.

- 8 Si ha aparecido la página Advertencia pero está satisfecho con la selección de repositorios, haga clic de nuevo en **Finalizar**.

El software Rapid Recovery Agent se implementa en los equipos especificados. Los equipos todavía no están protegidos. La protección se inicia una vez que se haya completado [Protección de varias máquinas en un dominio de Active Directory](#).

Implementación en equipos de un host virtual VMware vCenter/ESX(i)

Utilice este procedimiento para implementar simultáneamente el software de Agent Rapid Recovery en uno o más equipos en un host virtual VMware vCenter/ESX(i).

Antes de iniciar este procedimiento, debe tener la siguiente información:

- Las credenciales de inicio de sesión para el host virtual VMware vCenter/ESX(i).
- La ubicación del host.
- Las credenciales de inicio de sesión para cada uno de los equipos que desee proteger.

NOTA: Todas las máquinas virtuales deben tener herramientas de VMware instaladas; de lo contrario, Rapid Recovery no podrá detectar el nombre de host de la máquina virtual en la que se realizará la implementación. En lugar del nombre de host, Rapid Recovery utiliza el nombre de máquina virtual, lo cual puede causar problemas si el nombre de host es diferente del nombre de la máquina virtual.

- 1 En la Core Console de Rapid Recovery, haga clic en el menú desplegable **Proteger** y luego haga clic en **Implementar el software de Agent**.
Se abre el asistente para **Implementar el software de Agent**.
- 2 En la página del asistente **Conexión**, de la lista desplegable **Origen**, seleccione **vCenter/ESX(i)**.
- 3 Introduzca la información de host y las credenciales de inicio de sesión, según se describe en la siguiente tabla.

Tabla 59. Configuración de conexión vCenter/ESX(i)

Cuadro de texto	Descripción
Host	Nombre o dirección IP del host virtual VMware vCenter Server/ESX(i).
Puerto	Número de puerto usado para conectar con el host virtual. El valor predeterminado es 443.
Nombre de usuario	El nombre de usuario utilizado para conectarse con el host virtual; por ejemplo, Administrator o, si el equipo se encuentra en un dominio, [nombre de dominio]\Administrator.
Contraseña	La contraseña segura que se utiliza para conectarse con este host virtual.

- 4 Haga clic en **Siguiente**.
- 5 En la página **Equipos** del asistente, seleccione una de las opciones siguientes en el menú desplegable:
 - Hosts y clústeres
 - Máquinas virtuales y plantillas
- 6 Expanda la lista de equipos y, a continuación, seleccione las máquinas virtuales en las que desea implementar el software.
Aparece una notificación si Rapid Recovery detecta que un equipo está fuera de línea o que las herramientas de VMware no están instaladas.
- 7 Si desea reiniciar los equipos automáticamente después de la implementación, seleccione **Después de la instalación, reiniciar el equipo automáticamente (recomendado)**.
- 8 Haga clic en **Siguiente**.
Rapid Recovery comprueba de forma automática cada uno de los equipos que haya seleccionado.
- 9 En la página **Ajustes** del asistente, escriba las credenciales de cada equipo en el siguiente formato:
hostname::username::password.

NOTA: Introduzca un equipo por línea.

- 10 Haga clic en **Finalizar**.
El sistema comprueba de forma automática cada uno de los equipos que haya seleccionado.
Si Rapid Recovery detecta cualquier laguna durante la verificación automática, el asistente avanza a la página Avisos, donde puede borrar los equipos de la selección y comprobar manualmente los equipos seleccionados. Si los equipos que ha agregado pasan la verificación automática, aparecerán en el panel Implementar Agent en los equipos.

- 11 Si ha aparecido la página Advertencia pero está satisfecho con la selección de repositorios, haga clic de nuevo en **Finalizar**.

El software Rapid Recovery Agent se implementa en los equipos especificados. Los equipos todavía no están protegidos. La protección se inicia una vez que se haya completado [Protección de varias máquinas en un host virtual VMware vCenter/ESX\(i\)](#).

Implementación de una actualización de software de Agent Rapid Recovery para los equipos protegidos

Puede utilizar el Asistente de implementación del software de Agent para realizar una actualización del software de Agent Rapid Recovery a equipos que ya están protegidos por el Core de Rapid Recovery local.

- 1 En la Core Console de Rapid Recovery, haga clic en el menú desplegable **Proteger** y luego haga clic en **Implementar el software de Agent**.
Se abre el asistente para **Implementar el software de Agent**.
- 2 En la página del asistente **Conexión**, de la lista desplegable **Origen**, seleccione **Core local**.
- 3 Haga clic en **Siguiente**.
- 4 En la página **Equipos** del asistente, seleccione los equipos protegidos en los que desea implementar una actualización del software de Agent Rapid Recovery.
- 5 Haga clic en **Finalizar**.
El sistema comprueba de forma automática cada uno de los equipos que haya seleccionado.
Si Rapid Recovery detecta cualquier laguna durante la verificación automática, el asistente avanza a la página **Avisos**, donde puede borrar los equipos de la selección y comprobar manualmente los equipos seleccionados. Si los equipos que ha agregado pasan la verificación automática, aparecerán en el panel **Implementar el Agent en los equipos**.
- 6 Si apareció la página **Aviso** y sigue satisfecho con las selecciones, haga clic en **Finalizar** otra vez.

Implementación en equipos manualmente

Utilice el siguiente procedimiento para implementar Rapid Recovery Agent en varios equipos en cualquier tipo de host distinto del Core local, Active Directory o vCenter/ESXi.

- 1 En la Core Console de Rapid Recovery, seleccione el menú desplegable **Proteger** y, a continuación, haga clic en **Deploy Agent Software** (Implementar el software de Agent).
Se abre el asistente para **Implementar el software de Agent**.
- 2 En la página del asistente **Conexión**, de la lista desplegable **Origen**, seleccione **Manualmente**.
- 3 Haga clic en **Siguiente**.
- 4 En la página del asistente **Equipos**, escriba los detalles de equipo en el cuadro de diálogo en el formato `hostname::username::password::port`. Los ejemplos incluyen:
`10.255.255.255::administrator::&11@yYz90z::8006`
`abc-host-00-1::administrator::99!zU$o83r::168`
- 5 Si desea reiniciar los equipos automáticamente después de la implementación, seleccione **Después de la instalación, reiniciar el equipo automáticamente (recomendado)**.
- 6 Haga clic en **Finalizar**.
El sistema comprueba de forma automática cada uno de los equipos que haya seleccionado.
Si Rapid Recovery detecta cualquier laguna durante la verificación automática, el asistente avanza a la página **Avisos**, donde puede borrar los equipos de la selección y comprobar manualmente los equipos seleccionados. Si los equipos que ha agregado pasan la verificación automática, aparecerán en el panel **Implementar el Agent en los equipos**.
- 7 Si apareció la página **Aviso** y sigue satisfecho con las selecciones, haga clic en **Finalizar** otra vez.

El software Rapid Recovery Agent se implementa en los equipos especificados. Los equipos todavía no están protegidos. La protección se inicia una vez que se haya completado [Protección de varios equipos manualmente](#).

Verificación de la implementación en varios equipos

Una vez haya implementado de forma simultánea el software Rapid Recovery Agent en dos o más equipos, podrá verificar si se ha hecho correctamente visualizando cada equipo indicado en el menú Equipos protegidos.

También puede ver información relativa al proceso de implementación masiva desde la página Eventos. Realice los pasos de este procedimiento para verificar la implementación.

- 1 Desplácese hasta la Core Console de Rapid Recovery, haga clic en  (Eventos), y, a continuación, haga clic en **Alertas**. Los eventos de alerta aparecerán en la lista, mostrando el tiempo en que se inició el evento y un mensaje. Por cada implementación correcta del software de Agent, verá una alerta indicando que el equipo protegido se ha agregado.
- 2 También puede hacer clic en cualquier enlace de un equipo protegido. Aparece la pestaña **Resumen** del equipo seleccionado, que muestra la información pertinente, entre la que se incluye:
 - El nombre de host del equipo protegido.
 - La última instantánea, si es aplicable.
 - La hora de la siguiente instantánea programada, basada en el calendario de programación de protección del equipo seleccionado
 - La clave de cifrado, si la hubiera, utilizada para este equipo protegido.
 - La versión del software de Agent.

Modificación de la configuración de implementación

Complete los pasos de este procedimiento para modificar la configuración de implementación.

- 1 Desde la Core Console de Rapid Recovery, haga clic en  (Configuración).
- 2 En la página **Configuración**, en la columna izquierda, haga clic en **Implementar** para ir a la sección Implementar.
- 3 Modifique cualquiera de las opciones siguientes haciendo clic en la configuración que quiere cambiar para que se puede editar como un cuadro de texto o una lista desplegable y, a continuación, haga clic en  para guardar la configuración.

Tabla 60. Opciones de implementación

Opción	Descripción
Agent Installer Name	Escriba el nombre del archivo ejecutable del agente. El valor predeterminado es Agent-web.exe.
Core Address	Introduzca la dirección para el Core.
Error de tiempo de espera de recepción	Especifique el número de minutos que hay que esperar sin actividad antes del tiempo de espera.
Número máximo de instalaciones paralelas	Especifique un número para el máximo de instalaciones que quiere instalar de forma simultánea. El valor predeterminado y límite es 100.
Reinicio automático después de la instalación	Marque la casilla de verificación para Sí o desmárquela para No.
Proteger tras implementación	Marque la casilla de verificación para Sí o desmárquela para No.

Comprensión del calendario de programación de protección.

El programa de protección define cuándo se transfieren las copias de seguridad desde las máquinas protegidas al Core de Rapid Recovery.

La primera transferencia de copia de seguridad guardada en el Core se denomina una instantánea de imagen base. Todos los datos de todos los volúmenes especificados (incluidos el sistema operativo, las aplicaciones y la configuración) se guardan en el Core, lo que puede tardar una cantidad de tiempo considerable en función de la cantidad de datos que se transfieran. En lo sucesivo, las instantáneas incrementales (copias de seguridad más pequeñas, compuestas únicamente por datos cambiados en el equipo protegido desde la última copia de seguridad) se guardarán en el Core con regularidad, basándose en el intervalo definido (por ejemplo, cada 60 minutos). Esta copia de seguridad contiene menos datos que una imagen base y, por tanto, tarda menos tiempo en transferirse.

Los calendarios de programación de protección se definen inicialmente mediante el Asistente para proteger un equipo o el Asistente para proteger varios equipos. Al utilizar un asistente, puede personalizar los calendarios de programación de protección (seleccionando períodos o una hora de protección diaria) para ajustarse a sus necesidades empresariales. Es posible modificar el calendario de programación existente o crear un nuevo calendario de programación en cualquier momento en el cuadro de diálogo Calendario de programación de protección de la página de resumen en un equipo protegido específico.

Rapid Recovery proporciona un calendario de programación de protección predeterminado, que incluye un único periodo que abarca todos los días de la semana, con un único periodo de tiempo definido (desde las 12:00 hasta las 23:59). El intervalo predeterminado (el período de tiempo entre instantáneas) es de 60 minutos. La primera vez que habilita la protección también está activando el calendario de programación. De este modo, cuando se utiliza la configuración predeterminada, independientemente de la hora del día actual, la primera copia de seguridad se producirá cada hora, a la hora en punto (12:00, 13:00, 14:00, etc.).

La selección de periodos le permite ver el calendario de programación de protección predeterminado y realizar los ajustes pertinentes. Seleccionar una hora de protección diaria hace que el Core de Rapid Recovery cree una copia de seguridad de los equipos protegidos indicados una vez a diario a la hora que especifique.

Es posible personalizar el calendario de programación para definir las horas punta y no punta utilizando los periodos disponibles de días laborables y fines de semana. Por ejemplo, si utiliza mayormente sus equipos protegidos los días laborables, podría disminuir el intervalo del periodo de días laborables a 20 minutos, dando lugar a tres instantáneas cada hora. También puede incrementar el intervalo del periodo de los fines de semanas de 60 minutos a 180 minutos, con lo que obtendrá instantáneas una vez cada tres horas cuando el tráfico sea reducido.

También puede cambiar la programación predeterminada para definir horas pico y no pico diariamente. Para hacerlo, cambie la hora de inicio y la hora de finalización predeterminadas a un rango de tiempo menor (por ejemplo, de las 12:00 hasta las 16:59) y establezca un intervalo adecuado (por ejemplo, 20 minutos). Esto hará que se realicen copias de seguridad frecuentes durante el periodo de horas pico. A continuación puede añadir un intervalo de tiempo adicional para los días laborables para el periodo de tiempo restante (desde las 17:00 hasta las 23:59) y establezca un intervalo apropiado (posiblemente mayor, como por ejemplo, 180 minutos). Estos parámetros definen un periodo fuera de las horas de pico que incluye las 5:00 PM hasta la media noche todos los días. Esta personalización da como resultado instantáneas cada tres horas desde las 17:00 hasta las 23:59, e instantáneas cada 20 minutos desde las 12:00 hasta las 16:59.

Al modificar o crear un calendario de programación de protección por medio del cuadro de diálogo Calendario de programación de protección, Rapid Recovery le ofrece la opción de guardar ese calendario de programación como una plantilla reutilizable que puede aplicar después a otros equipos protegidos.

Otras opciones del asistente de protección incluyen el ajuste de una hora de protección diaria. El resultado es una única copia de seguridad diaria en el período definido (el ajuste predeterminado es 00:00).

Al proteger uno o varios equipos utilizando un asistente, puede realizar pausa en la protección inicialmente, lo cual define el calendario de programación de protección sin proteger los equipos. Cuando esté listo para empezar a proteger sus equipos basándose en el calendario de programación de protección establecido, deberá reanudar la protección de manera explícita. Para obtener más información sobre cómo reanudar la protección, consulte [Puesta en pausa y reanudación de la protección](#). Asimismo, si quiere proteger un equipo inmediatamente, puede forzar una instantánea. Para obtener más información, consulte [Cómo forzar una instantánea](#).

Cómo proteger una máquina

Si ya tiene instalado el software Rapid Recovery Agent en la máquina que desea proteger pero aún no la ha reiniciado, reiniciela ahora.

En este tema se describe cómo iniciar la protección de los datos en una sola máquina que especifique mediante el Protect Machine Wizard (Asistente de protección de máquina).

NOTA: A menos que se utilice una protección sin agente en un host VMware o ESXi, la máquina que desee proteger debe tener instalado el software Rapid Recovery Agent para este fin. Puede instalar el software Agent antes de realizar este procedimiento, o bien puede implementar el software en la máquina de destino durante la ejecución del Protect Machine Wizard (Asistente de protección de máquina).

Para obtener más información sobre la protección y sus restricciones, consulte [Descripción Rapid Snap para Virtual](#).

Para obtener más información acerca de la instalación del software Agente, consulte "Instalación del Rapid Recovery Agent" en *Dell Data Protection | Portal de licencias de Rapid Recovery Installation and Upgrade Guide*. Si el software Agent no está instalado antes de proteger una máquina, no podrá seleccionar volúmenes específicos para la protección como parte de este asistente. De forma predeterminada, todos los volúmenes de la máquina Agent se incluirán para su protección. Rapid Recovery es compatible con la protección y recuperación de máquinas configuradas con particiones EISA. También se ha ampliado el soporte para máquinas Windows 8 y 8.1 y Windows 2012 y 2012 R2 que utilizan un Entorno de recuperación de Windows (Windows RE).

Para proteger simultáneamente varias máquinas mediante un solo proceso, consulte [Acerca de la protección de varios equipos](#).

Cuando agrega protección, tiene que definir la información de conexión, como la dirección IP y el puerto, y proporcionar las credenciales de la máquina que desea proteger. Opcionalmente, puede proporcionar un nombre para mostrar en la Core Console en lugar de la dirección IP. Si lo cambia, no verá la dirección IP de la máquina protegida cuando vea los detalles en la Core Console. También podrá definir el programa de protección de la máquina.

El proceso de protección incluye pasos opcionales a los que puede acceder si selecciona una configuración avanzada. Las opciones avanzadas incluyen funciones repositorio y cifrado. Por ejemplo, puede especificar un repositorio de Rapid Recovery para guardar las instantáneas o crear un nuevo repositorio. También puede especificar una clave de cifrado existente (o agregar una nueva clave de cifrado) para aplicar a los datos almacenados en el Core de esta máquina. Para obtener más información sobre las claves de cifrado, consulte [Descripción de las claves de cifrado](#).

El flujo de trabajo del asistente de protección pueden variar ligeramente en función de su entorno. Por ejemplo, si se instala el software Rapid Recovery Agent en la máquina que desea proteger, no se le solicitará que lo instale desde el asistente. De forma similar, si ya existe un repositorio en el Core, no se le solicitará que cree uno.

PRECAUCIÓN: Rapid Recovery no es compatible con restauraciones completas (BMR) de máquinas Linux con particiones de inicio ext2. Un BMR realizado en una máquina con este tipo de partición hará que no se inicie la máquina. Si desea realizar una BMR en esta máquina en el futuro, deberá convertir todas las particiones ext2 a ext3 o ext4 antes de comenzar a proteger y realizar una copia de seguridad de la máquina.

1 Realice uno de los siguientes pasos:

- Si comienza desde el Protect Machine Wizard (Asistente de protección de máquina), vaya al [Paso 2](#).
- Si comienza desde la Rapid Recovery Core Console, en la barra de botones haga clic en **Protect (Proteger)**.

Se abrirá el asistente **Protect Machine Wizard (Asistente de protección de máquina)**.

2 En la página **Welcome (Bienvenido)**, seleccione las opciones de instalación adecuadas:

- Si no necesita definir un repositorio o establecer el cifrado, seleccione **Typical (Típica)**.
- Si necesita crear un repositorio, o definir un repositorio diferente para las copias de seguridad de la máquina seleccionada, o si desea establecer el cifrado con el asistente, seleccione **Advanced (show optional steps) (Avanzad [mostrar pasos opcionales])**.
- Si no desea ver la página **Welcome (Bienvenido)** del para el Protect Machine Wizard Asistente de protección de máquina) en el futuro, seleccione la opción **Skip this Welcome page the next time the wizard opens (Omitir esta página de bienvenida la próxima vez que se abra el asistente)**.

- 3 Cuando esté satisfecho con las opciones en la página de bienvenida, haga clic en **Next (Siguiente)**. Aparecerá la página **Connection (Conexión)**.
- 4 En el cuadro de diálogo **Connection (Conexión)**, introduzca la información sobre la máquina a la que desea conectarse, tal como se describe en la tabla siguiente y haga clic en **Next (Siguiente)**.

Tabla 61. Configuración de conexión de la máquina

Cuadro de texto	Descripción
Host (Host)	El nombre de host o la dirección IP de la máquina que desea proteger.
Port (Puerto)	El número de puerto por el que el Rapid Recovery Core se comunica con el Agent en la máquina. El número de puerto predeterminado es 8006.
User name (Nombre de usuario)	El nombre de usuario que se utiliza para conectar a esa máquina; por ejemplo, Administrador (o, si la máquina está en un dominio, [nombre de dominio]\Administrador).
Password (Contraseña)	La contraseña que se utiliza para conectar a esa máquina.

Si se abre la página **Install Agent** en el Protect Machine Wizard (Asistente de protección de máquina), significa que Rapid Recovery no detecta el Rapid Recovery Agent en la máquina y se instalará la versión actual del software. Vaya al [Paso 7](#).

Si se abre la página **Upgrade Agent (Actualizar Agente)** en el asistente, significa que hay instalada una versión anterior del software Agent en la máquina que desea proteger.

NOTA: El software Agent debe estar instalado en la máquina que desea proteger, y debe reiniciar máquina antes de que pueda hacer su copia de seguridad en el Core. Para que el instalador reinicie la máquina protegida, seleccione la opción **After installation, restart the machine automatically (recommended) (Reiniciar la máquina automáticamente después de la instalación)** antes de hacer clic en **Next (Siguiente)**.

- 5 En la página **Upgrade Agent (Actualizar Agente)**, realice una de las acciones siguientes:
 - Para implementar la nueva versión del software Agent (con la misma versión que Rapid Recovery Core), seleccione **Upgrade the Agent to the latest version of the software (Actualizar el Agent a la versión más reciente del software)**.
 - Para continuar protegiendo la máquina sin actualizar la versión del software Agent, desactive la opción **Upgrade the Agent to the latest version of the software (Actualizar el Agent a la versión más reciente del software)**.
- 6 Haga clic en **Next (Siguiente)**.
- 7 Opcionalmente, en la página **Protection (Protección)**, si desea mostrar un nombre en lugar de la dirección IP en la Rapid Recovery Core Console para esta máquina protegida, en el campo **Display Name (Nombre)** escriba un nombre en el cuadro de diálogo. Puede introducir hasta 64 caracteres. No utilice los caracteres especiales indicados en el tema [caracteres prohibidos](#). Además, no utilice ninguna de las combinaciones de caracteres que se describen en el tema [frases prohibidas](#).
- 8 Seleccione el programa de protección adecuado tal como se describe a continuación:
 - Para usar el programa de protección predeterminado, en la opción **Schedule Settings (Configuración de programación)**, seleccione **Default protection (Protección predeterminada)**.

Con un programa de protección predeterminado, el Core realizará instantáneas de todos los volúmenes en la máquina protegida una vez cada hora. Para cambiar la configuración de la protección en cualquier momento después de cerrar el asistente (y seleccionar los volúmenes para proteger), vaya a la página **Summary (Resumen)** de la máquina protegida específica.

- Para definir un programa de protección diferente, en la opción **Schedule Settings (Configuración de programación)**, seleccione **Custom protection (Protección personalizada)**.

- 9 Continúe con la configuración de la manera siguiente:
 - Si en el asistente Protect Machine Wizard (Asistente de protección de máquina) ha seleccionado una configuración típica y ha especificado la protección predeterminada, haga clic en **Finish (Finalizar)** para confirmar la selección, cerrar el asistente y proteger la máquina especificada.
La primera vez que se agrega protección para una máquina, se inicia de inmediato la transferencia de una imagen base (una instantánea de todos los datos de los volúmenes protegidos) al repositorio en el Rapid Recovery Core, salvo que haya especificado pausar la protección inicialmente.

- Si ha seleccionado una configuración típica en el Protect Machine Wizard (Asistente de protección de máquina) y ha especificado una protección personalizada, haga clic en **Next (Siguiente)** para configurar un programa de protección personalizado. Para obtener más información sobre cómo definir un programa de protección, consulte [Creación de calendarios de programación de protección personalizados](#).
 - Si ha seleccionado Advanced configuration en el asistente y ha especificado una protección personalizada, haga clic en **Next (Siguiente)** y vaya al [Paso 14](#) para ver las opciones de repositorio y cifrado.
 - Si ha seleccionado la opción Advanced configuration (Configuración avanzada) en el asistente y ha especificado la protección predeterminada, haga clic en **Next (Siguiente)** y vaya al [Paso 11](#) para elegir los volúmenes para proteger.
- 10 En la página **Protection Volumes (Volúmenes con protección)**, seleccione los volúmenes que desea proteger. Si en la lista se incluye algún volumen que no desea incluir en la protección, haga clic en la columna Check (Marcar) para quitar la selección. A continuación, haga clic en **Next (Siguiente)**.

NOTA: Por lo general se recomienda proteger como mínimo el volumen System Reserved (Reservado para el sistema) y el volumen con el sistema operativo (por lo general, la unidad C).

- 11 En la página **Protection Schedule (Programa de protección)**, defina un programa personalizado y haga clic en **Next (Siguiente)**. Para obtener más información sobre cómo definir un programa de protección personalizado, consulte [Creación de calendarios de programación de protección personalizados](#).
- Si ya tiene configurada la información del repositorio y ha seleccionado la opción Advanced (Avanzado) en el Paso 1, se abrirá la página Encryption (Cifrado). Vaya al [Paso 13](#).
- 12 En la página **Repository (Repositorio)**:
- Si ya tiene un repositorio y desea guardar los datos de esta máquina para protegerlos en el repositorio existente, realice lo siguiente:
 - 1 Seleccione **Use an existing repository (Usar un repositorio existente)**.
 - 2 Seleccione un repositorio existente de la lista.
 - 3 Haga clic en **Next (Siguiente)**.

Aparece la página **Encryption (Cifrado)**. Vaya al [Paso 13](#) para definir opcionalmente el cifrado.

- Si desea crear un repositorio existente), seleccione **Create a Repository (Crear un repositorio)** y, a continuación, realice los pasos siguientes.
 - 1 En la página **Repository (Repositorio)**, introduzca la información que se describe en la tabla siguiente.

Tabla 62. Agregar configuración del nuevo repositorio

Cuadro de texto	Descripción
Repository Name (Nombre del repositorio)	Escriba el nombre de pantalla del repositorio. De manera predeterminada, este cuadro de texto se compone de la palabra Repositorio y un número, que coincide con el número de repositorios que existen para este Core. Por ejemplo, si este es el primer repositorio, el nombre predeterminado es Repositorio 1. Cambie el nombre según sea necesario. Los nombres de repositorio deben contener entre 1 y 40 caracteres alfanuméricos, incluidos espacios. No utilice caracteres prohibidos ni frases prohibidas.
Concurrent Operations (Operaciones simultáneas)	Define el nombre de solicitudes simultáneas que desea que admita el repositorio. De manera predeterminada, el valor es 64.
Comments (Comentarios)	Opcionalmente, introduzca una nota descriptiva sobre este repositorio. Puede introducir hasta 254 caracteres. Por ejemplo, escriba DVM Repositorio 2.

- 2 Haga clic en **Add Storage Location (Agregar ubicación de almacenamiento)** para definir la ubicación de almacenamiento específica o el volumen del repositorio. Este volumen debe ser la ubicación de almacenamiento principal.

PRECAUCIÓN: Defina una carpeta específica dentro de la raíz para la ubicación de almacenamiento del repositorio. No especifique la ubicación raíz. Por ejemplo, utilice E:\Repository\, no E:\. Si el repositorio que va a crear en este paso se elimina posteriormente, se eliminarán todos los archivos incluidos en la ubicación de almacenamiento de su repositorio. Si define la ubicación de almacenamiento en la raíz, todos los demás archivos en el volumen (ej., E:\) se eliminan, lo que podría provocar una pérdida de datos catastrófica.

Aparecerá el cuadro de diálogo **Add Storage Location (Agregar ubicación de almacenamiento)**.

- 3 Haga clic en **Add Storage Location (Agregar ubicación de almacenamiento)** para definir la ubicación de almacenamiento específica o el volumen del repositorio. Este volumen debe ser la ubicación de almacenamiento principal.
- 4 En el área **Storage Location (Ubicación de almacenamiento)**, especifique cómo desea agregar el archivo para la ubicación de almacenamiento. Puede agregar un volumen de almacenamiento conectado localmente (por ejemplo, un almacenamiento de conexión directa, una red de área de almacenamiento o un almacenamiento de red conectado). También puede especificar un volumen de almacenamiento en una ubicación compartida del Common Internet File System (Sistema de archivos de Internet común - CIFS)
 - Haga clic en **Add the file on local disk (Agregar el archivo en disco local)** para especificar una máquina local y, a continuación, indique la información según se describe en la tabla siguiente.

Tabla 63. Configuración de disco local

Cuadro de texto	Descripción
Data Path (Ruta de datos)	Introduzca la ubicación para almacenar los datos protegidos. Por ejemplo, escriba X:\Repository\Data. Al especificar la ruta, escriba solo caracteres alfanuméricos, un guión o un punto (para separar los nombres de host y los dominios). Puede utilizar la barra diagonal invertida únicamente para definir los niveles en la ruta. No utilice espacios. No se admite ningún otro símbolo ni caracteres de puntuación.
Metadata path (Ruta de metadatos)	Introduzca la ubicación para almacenar los metadatos protegidos. Por ejemplo, escriba X:\Repository\Metadata. Al especificar la ruta, escriba solo caracteres alfanuméricos, un guión o un punto (para separar los nombres de host y los dominios). Puede utilizar la barra diagonal invertida únicamente para definir los niveles en la ruta. No utilice espacios. No se admite ningún otro símbolo ni caracteres de puntuación.

- O bien, seleccione **Add file on CIFS share (Agregar archivo en recurso compartido CIFS)** para especificar una ubicación compartida de red y, a continuación, indique la información según se describe en la tabla siguiente.

Tabla 64. Credenciales del recurso compartido CIFS

Cuadro de texto	Descripción
UNC Path (Ruta UNC)	Introduzca la ruta de acceso para la ubicación del recurso compartido de red. Si la ubicación se encuentra en la raíz, cree un nombre de carpeta específico (por ejemplo, Repository). La ruta debe empezar por \\. Al especificar la ruta, escriba solo caracteres alfanuméricos, un guión o un punto (para separar los nombres de host y los dominios). Las letras de la "a" a la "z" no distinguen mayúsculas de minúsculas. No utilice espacios. No se admite ningún otro símbolo ni caracteres de puntuación.
User name (Nombre de usuario)	Especifique un nombre de usuario para el acceso a la ubicación del recurso compartido de red.
Password (Contraseña)	Especifique una contraseña para acceder a la ubicación del recurso compartido de red.

- 5 En el área **Storage Configuration (Configuración de almacenamiento)**, haga clic en **More Details** (Más detalles) e introduzca los detalles de la ubicación de almacenamiento según se describe en la tabla siguiente.

Tabla 65. Detalles de la configuración de almacenamiento

Cuadro de texto	Descripción
Size (Tamaño)	Establezca el tamaño o capacidad de la ubicación de almacenamiento. El tamaño mínimo es 1 GB. El valor predeterminado es 250 GB. Puede elegir entre las opciones siguientes: • GB

Cuadro de texto	Descripción
	TB ① NOTA: El tamaño que especifique no puede superar el tamaño del volumen. Si la ubicación de almacenamiento es un volumen de sistema de archivos de nueva tecnología (NTFS) que tiene Windows XP o Windows 7 instalado, el límite de tamaño de archivo es 16 TB. Si la ubicación de almacenamiento es un volumen NTFS que ejecuta Windows 8, 8.1, Windows 10 o Windows Server 2012, 2012 R2, el límite de tamaño de archivo es 256 TB. ① NOTA: Para que Rapid Recovery pueda validar el sistema operativo, el Instrumental de administración de Windows (WMI) debe estar instalado en la ubicación de almacenamiento deseada.
Write Caching Policy (Política de escritura en caché)	La política de escritura en caché de controla cómo se utiliza el Windows Cache Manager (Administrador de caché de Windows) en el repositorio y ayuda a ajustar el repositorio para un rendimiento óptimo en diferentes configuraciones. Establezca el valor en una de las opciones siguientes: - On (Activado) - Off (Desactivado) - Sync (Sincronizar) Si se establece en On (Activado), que es el valor predeterminado, Windows controla el almacenamiento en caché. Esto es adecuado para Windows 10, y para las versiones de Windows Server 2012 y posteriores. ① NOTA: Si se establece la política de escritura en caché en On (Activado), se mejora el rendimiento. Si utiliza Windows Server 2008 SP2 o Windows Server 2008 R2 SP2, el valor recomendado es Off (Desactivado). Si se establece en Off (Desactivado), Rapid Recovery controla el almacenamiento en caché. Si se establece en Sync (Sincronizar), Windows controla el almacenamiento en caché así como la entrada/salida sincrónica.
Bytes per sector (Bytes por sector)	Especifique el número de bytes que desee incluir en cada sector. El valor predeterminado es 512.
Average Bytes per Record (Número promedio de bytes por registro)	Especifique el número promedio de bytes por segundo. El valor predeterminado es 8192.

6 Haga clic en **Next (Siguiente)**.

Si ha seleccionado la opción **Advanced (Avanzado)** en el paso 1, aparece la página **Encryption (Cifrado)**.

13 De manera opcional, para **activar** el cifrado en la página de cifrado, seleccione **Enable Encryption (Activar cifrado)**.

Aparecerán los campos de clave de cifrado en la página **Encryption (Cifrado)**.

① | NOTA: Si activa el cifrado, se aplicará a los datos para todos los volúmenes protegidos de esta máquina. Puede cambiar la configuración posteriormente en el Rapid Recovery Core Para obtener más información sobre el cifrado, consulte el tema [Descripción de las claves de cifrado](#).

⚠ PRECAUCIÓN: Rapid Recovery utiliza cifrado AES de 256 bits en el modo Encadenamiento de bloques de cifrado (CBC) con claves de 256 bits. Mientras el uso de cifrado es opcional, Dell recomienda encarecidamente que establezca una clave de cifrado y que proteja la frase de contraseña que defina. Guarde la frase de contraseña en un lugar seguro, ya que es fundamental para la recuperación de datos. Sin una frase de contraseña, la recuperación de datos no es posible.

14 En la página **Encryption (Cifrado)**, seleccione una de las opciones siguientes:

- Si desea cifrar esta máquina protegida con una clave de cifrado que ya está definida en este Rapid Recovery Core, seleccione **Encrypt data using an existing Encryption key** (Cifrar los datos mediante una clave de cifrado existente) y seleccione la clave apropiada en el menú desplegable. Vaya al [paso siguiente](#).

- Si desea agregar una clave de cifrado para el Core y aplicar dicha clave a esta máquina protegida, Introduzca la información según se describe en la tabla siguiente.

Tabla 66. Configuración de clave de cifrado

Cuadro de texto	Descripción
Name (Nombre)	Introduzca un nombre para la clave de cifrado. Los nombres de la clave de cifrado debe contener entre 1 y 130 caracteres alfanuméricos. No se podrá incluir caracteres especiales, tales como la barra diagonal inversa, barra diagonal, barra vertical, dos puntos, asterisco, comilla, signo de interrogación, paréntesis de apertura o cierre o almohadilla.
Description (Descripción)	Escriba un comentario para la clave de cifrado. Esta información se muestra en el campo Description (Descripción) cuando se visualizan las claves de cifrado desde Core Console.
Passphrase (Frase de contraseña)	Introduzca la frase de contraseña usada para controlar el acceso. Se recomienda evitar el uso de los caracteres especiales indicados anteriormente. Registre la frase de contraseña en un lugar seguro. Dell Support no puede recuperar una frase de contraseña. Una vez que haya creado una clave de cifrado y la haya aplicado a una o varias máquinas protegidas, no podrá recuperar los datos si pierde la frase de contraseña.
Confirm Passphrase (Confirmar frase de contraseña)	Vuelva a introducir la frase de contraseña que acaba de introducir.

- 15 Haga clic en **Finish (Finalizar)** para guardar y aplicar la configuración.

La primera vez que se agrega protección para una máquina, se inicia de inmediato la transferencia de una imagen base (una instantánea de todos los datos de los volúmenes protegidos) al repositorio en el Rapid Recovery Core, salvo que haya especificado pausar la protección inicialmente.

Protección de un clúster

En este tema se describe cómo agregar un clúster para protección en Rapid Recovery . Cuando agregue un clúster a la protección, debe especificar el nombre de host o dirección IP del clúster, la aplicación del clúster o uno de los nodos o equipos de clúster que incluye el software Rapid Recovery Agent.

NOTA: Se utiliza un repositorio para almacenar las instantáneas de datos que se capturan desde sus nodos protegidos. Para poder empezar a proteger datos en su clúster, debe tener configurado al menos un repositorio que esté asociado al Core de Rapid Recovery.

Para obtener información sobre la configuración de repositorios, consulte [Definición de los repositorios](#).

- 1 Desde la Core Console de Rapid Recovery, haga clic en el menú desplegable del botón **Proteger** y, a continuación, haga clic en **Proteger clúster**.
- 2 En el cuadro de diálogo Conectarse al clúster, introduzca la siguiente información.

Tabla 67. Configuración de Conectarse al clúster

Cuadro de texto	Descripción
Host	El nombre de host o dirección IP del clúster, la aplicación de clúster o uno de los nodos de clúster.
Puerto	El número de puerto del equipo en el que el Core de Rapid Recovery se comunica con el Agent. El puerto predeterminado es 8006.
Nombre de usuario	El nombre de usuario del administrador de dominio utilizado para conectar a este equipo; por ejemplo, domain_name\administrator.

NOTA: El nombre de dominio es obligatorio. No puede conectar con el clúster mediante el nombre de usuario de administrador local.

Contraseña	La contraseña que se utiliza para conectar a ese equipo.

- 3 Haga clic en **Conectar**.
- 4 En el cuadro de diálogo Proteger clúster, seleccione un repositorio para este clúster.
- 5 Si desea asegurar los puntos de recuperación para este clúster utilizando cifrado basado en Core, seleccione una clave de cifrado.
- 6 Si no desea que la protección comience de inmediato tras completar este procedimiento, seleccione **Pausar protección inicialmente**.
- 7 Para proteger el clúster basándose en la configuración predeterminada, seleccione los nodos para la protección predeterminada y, a continuación, vaya al [paso 10](#).

NOTA: La configuración predeterminada programa una instantánea de todos los volúmenes cada 60 minutos.

- 8 Para introducir una configuración personalizada para el clúster (por ejemplo, para personalizar el programa de protección para los volúmenes compartidos), haga una de las siguientes acciones, y, a continuación, consulte [Creación de calendarios de programación de protección personalizados](#).
 - Para personalizar la configuración de un nodo individual, haga clic en **Configuración** junto al nodo que desea personalizar, y, a continuación, haga clic en **Función** al lado del volumen pertinente.
 - Para personalizar la configuración del clúster, haga clic en el botón de configuración en la parte inferior del cuadro de diálogo, y, a continuación, haga clic en **Función** al lado del volumen pertinente.

Para obtener más información sobre cómo personalizar nodos, consulte [Protección de los nodos de un clúster](#).

- 9 Cuando haya hecho todos los cambios necesarios, haga clic en **Guardar**.
- 10 En el cuadro de diálogo Proteger clúster, haga clic en **Proteger**.

Modificación de la configuración del nodo de clúster

Una vez que haya agregado protección para nodos de clúster, puede modificar los valores de configuración básicos (por ejemplo, nombre de pantalla, nombre de host, etc.), la configuración de la protección (por ejemplo, cambiar el programa de protección para volúmenes en la máquina, agregar o eliminar volúmenes y pausar la protección), etc.

Para modificar la configuración del nodo de clúster, debe realizar las tareas siguientes:

- En la Rapid Recovery Core Console, vaya hasta el clúster que contiene el nodo que desee modificar, y seleccione el equipo o el nodo que desea modificar.
- Para modificar y ver los valores de configuración, ver [Configuración de grupos de notificación](#).
- Para configurar los grupos de notificación para eventos del sistema, ver [Visualización y modificación de la configuración de equipos protegidos](#).
- Para personalizar la configuración de la política de retención, ver [Personalización de la configuración de la política de retención de una máquina protegida](#).
- Para modificar el programa de protección, ver [Modificación de los programas de protección](#).
- Para modificar la configuración de transferencia, ver [Modificación de la configuración de las transferencias](#).

Protección de los nodos de un clúster

Esta tarea requiere que primero proteja un clúster. Para obtener más información, consulte [Protección de un clúster](#).

En este tema se describe cómo proteger los datos en un nodo o equipo que tiene un Rapid Recovery Agent instalado. Este procedimiento permite agregar nodos individuales a la protección que haya omitido al proteger un clúster.

- 1 En la Core Console de Rapid Recovery, en Equipo protegido, haga clic en el clúster con los nodos que desea proteger.
- 2 En la página Resumen del clúster, haga clic en los **Nodos protegidos**.
- 3 En la página Nodos protegidos, haga clic en **Proteger nodo de clúster**.

- 4 En el cuadro de diálogo Proteger nodo de clúster, seleccione o introduzca la información siguiente según corresponda.

Tabla 68. Configuración de Proteger nodo de clúster

Cuadro de texto	Descripción
Host	Una lista desplegable de nodos en el clúster disponibles para su protección.
Puerto	El número de puerto por el que el Core de Rapid Recovery se comunica con el Agent en el nodo.
Nombre de usuario	El nombre de usuario del administrador de dominio utilizado para conectar a este nodo; por ejemplo, example_domain \administrator o administrator@example_domain.com.
Contraseña	La contraseña que se utiliza para conectar a ese equipo.

- 5 Para agregar el nodo, haga clic en **Conectar**.
- 6 Para iniciar la protección de este nodo con la configuración de protección predeterminada, vaya al [Paso 13](#).

NOTA: La configuración predeterminada garantiza que todos los volúmenes de este equipo están protegidos con un calendario de programación predeterminado cada 60 minutos.

- 7 En el cuadro de diálogo Proteger [nombre del nodo], si desea utilizar un repositorio que no sea el valor predeterminado, utilice la lista desplegable para seleccionar un repositorio.
- 8 Si desea asegurar los puntos de recuperación para este clúster utilizando cifrado basado en Core, utilice la lista desplegable para seleccionar una clave de cifrado.
- 9 Si no desea que la protección comience de inmediato tras completar este procedimiento, seleccione **Pausar protección inicialmente**.
- 10 Para introducir una configuración personalizada (por ejemplo, para personalizar el programa de protección para los volúmenes compartidos), haga lo siguiente:
 - a Para personalizar la configuración de un volumen individual, haga clic en **Función** junto al volumen que desea personalizar, y, a continuación, haga clic al lado del volumen pertinente.
 - b Consulte [Creación de calendarios de programación de protección personalizados](#).
- 11 Haga clic en **Protect (Proteger)**.

Creación de calendarios de programación de protección personalizados

Realice los pasos que se indican en este procedimiento para crear calendarios de programación personalizados para proteger los datos en los equipos protegidos al definir la protección mediante un asistente.

- 1 En la página **Protección** del asistente de protección (Proteger equipo, Proteger varios equipos, Protecting a Cluster [Proteger un clúster]), seleccione Protección personalizada.
- 2 Haga clic en **Siguiente**.
- 3 En la página **Volúmenes de protección**, seleccione los volúmenes que desee exportar y, a continuación, haga clic en **Siguiente**.
- 4 En la página **Calendario de programación de protección**, para cambiar el intervalo del calendario de programación, haga lo siguiente:
 - a Seleccione **Períodos**.
Aparecerán los períodos existentes, los cuales se podrán modificar. Los campos editables incluyen una hora de inicio, una hora de finalización y un intervalo (cada x minutos) para cada período.
 - b Para cada período, haga clic en el cuadro de texto del intervalo y escriba un intervalo adecuado en minutos.
Por ejemplo, resalte el intervalo predeterminado de 60 y sustitúyalo por el valor 20 para realizar instantáneas cada 20 minutos durante este período.
- 5 Para crear un período de horas pico y fuera de horas pico para los días de la semana, cambie el rango de tiempo para el período de días de la semana para que no incluya un período de 24 horas, establezca un intervalo óptimo para las horas pico, seleccione **Take snapshots for the remaining time** (Realizar instantánea para horas restantes) y establezca un intervalo fuera de horas pico, haciendo lo siguiente:
 - a Seleccione **Períodos**.
Aparecerán los períodos existentes, los cuales se podrán modificar.
 - b Haga clic en el cuadro **De** o utilice el icono del reloj para cambiar la hora de inicio de este período.
 - c Haga clic en el cuadro **To** (A) o utilice el icono del reloj para cambiar la hora de finalización de este período.

- d Haga clic en el cuadro de texto del intervalo y escriba un intervalo adecuado en minutos.
Por ejemplo, resalte el intervalo existente de 60 y sustitúyalo por el valor 20 para realizar instantáneas cada 20 minutos durante el rango de tiempo que seleccionó para este período.
- e Seleccione **Realizar instantáneas durante el resto del tiempo** y, a continuación, especifique un intervalo en minutos.
- 6 Para establecer que se realice a diario una única copia de seguridad a una sola hora del día, seleccione **Hora de protección diaria** y, a continuación, introduzca una hora con el formato HH:MM AM. Por ejemplo, para realizar una copia de seguridad diaria a las 21:00, introduzca 09:00 PM.
- 7 Para definir el calendario de programación sin comenzar copias de seguridad, seleccione **Pausar protección inicialmente**.
Después de que haya realizado una pausa en la protección desde el asistente, permanecerá en pausa hasta que no la reanude de manera explícita. Una vez reanude la protección, las copias de seguridad se realizarán basándose en el calendario de programación que establezca. Para obtener más información sobre reanudar la protección, consulte [Puesta en pausa y reanudación de la protección](#).
- 8 Cuando esté satisfecho con los cambios realizados en su calendario de programación de protección, haga clic en **Finalizar** o **Siguiente**, según sea adecuado. Vuelva al procedimiento para que el asistente adecuado cumpla los requisitos restantes.

Modificación de los programas de protección

El programa de protección define cuándo se transfieren las copias de seguridad desde las máquinas protegidas al Core de Rapid Recovery. Los calendarios de programación de protección se definen inicialmente mediante el Asistente para proteger un equipo o el Asistente para proteger varios equipos.

Puede modificar un calendario de programación de protección existente en cualquier momento desde la ficha Resumen para un equipo Agent específico.

NOTA: Para obtener información sobre los conceptos de los calendarios de programación de protección, consulte [Comprensión del calendario de programación de protección](#). Para obtener información sobre cómo proteger un único equipo, consulte [Cómo proteger una máquina](#). Para obtener información sobre la protección masiva (la protección de varios equipos), consulte [Acerca de la protección de varios equipos](#). Para obtener información sobre cómo personalizar periodos de protección al proteger un Agent mediante uno de estos asistentes, consulte [Creación de calendarios de programación de protección personalizados](#). Para obtener información sobre cómo modificar un calendario de programación de protección existente, consulte [Modificación de los programas de protección](#).

Realice los pasos que se indican en este procedimiento para modificar un calendario de programación de protección existente para volúmenes en un equipo protegido.

- 1 En la Core Console, en la lista de equipos protegidos, haga clic en el equipo protegido que tiene la programación de protección que desea cambiar.
- 2 En la página del equipo que ha seleccionado, seleccione los volúmenes aplicables y, a continuación, haga clic en **Establecer una programación**.
Para seleccionar todos los volúmenes a la vez, haga clic en la casilla de verificación de la fila del encabezado. Inicialmente, todos los volúmenes comparten el mismo calendario de programación de protección.

NOTA: Por lo general, es recomendable proteger, como mínimo, el volumen reservado para el sistema y el volumen con el sistema operativo (normalmente la unidad C).

Se abrirá el cuadro de diálogo Calendario de programación de protección.

- 3 En el cuadro de diálogo Calendario de programación de protección, realice una de las siguientes acciones:
 - Si ha creado previamente una plantilla de calendario de programación de protección y desea aplicarla al equipo protegido, seleccione la plantilla en la lista desplegable y, a continuación, vaya al [paso 7](#).
 - Si desea eliminar un periodo de tiempo de una programación, desmarque la casilla de verificación junto a cada opción de periodo de tiempo y, a continuación, vaya al [paso 7](#). Las opciones incluyen las siguientes:
 - Lun-Vie: este intervalo de tiempo se refiere a una semana laboral típica de cinco días.
 - Sáb-Dom: este intervalo de tiempo indica un fin de semana típico.
 - Si desea guardar un nuevo calendario de programación de protección como una plantilla, vaya al [paso 4](#).
- 4 Cuando las horas de inicio y finalización del día de la semana sean desde las 12:00 hasta las 23:59, solo existe un periodo. Para cambiar la hora de inicio o de finalización de un período definido, haga lo siguiente:

- a Seleccione el período de tiempo adecuado.
 - b Para cambiar la hora de inicio de este periodo, utilice el icono del reloj en **Hora de inicio**.
Por ejemplo, utilice las flechas para mostrar las 08:00.
 - c Para cambiar la hora de finalización de este periodo, utilice el icono del reloj en **Hora de finalización**.
Por ejemplo, utilice las flechas para mostrar las 18:00.
 - d Cambie el intervalo de acuerdo con sus requisitos. Por ejemplo, si define un periodo de hora punta, cambie el intervalo de 60 minutos a 20 minutos para tomar instantáneas tres veces cada hora.
- 5 Si se ha definido un periodo distinto al de las 12:00 a las 23:59 en el [Paso 7](#) y si desea que las copias de seguridad se lleven a cabo en el resto de intervalos de tiempo, deberá agregar períodos adicionales para definir la protección mediante los pasos siguientes:
- a En la categoría adecuada, haga clic en **Agregar periodo**.
 - b Haga clic en el icono del reloj y seleccione la hora de inicio y la hora de finalización deseadas, según corresponda.
Por ejemplo, establezca la hora de inicio a las 12:00 y la hora de finalización a las 07:59.
 - c Cambie el intervalo de acuerdo con sus requisitos. Por ejemplo, si define un periodo fuera de la hora punta, cambie el intervalo de 60 minutos a 120 minutos para tomar instantáneas cada dos horas.
- 6 Si es necesario, siga creando períodos adicionales, estableciendo horas de inicio y finalización e intervalos, según sea adecuado.
- NOTA:** Si desea eliminar un periodo que ha agregado, haga clic en el icono de la papelera del extremo derecho de ese periodo y, a continuación, haga clic en **Sí** para confirmar.
- 7 Para crear una plantilla desde el calendario de programación que ha establecido, haga clic en **Guardar como plantilla**.
 - 8 En el cuadro de diálogo Guardar plantilla, introduzca un nombre para la plantilla y, a continuación, haga clic en **Guardar**.
 - 9 Cuando el programa de protección cumpla sus requisitos, haga clic en **Aplicar**.
El cuadro de diálogo Calendario de programación de protección se cerrará.

Puesta en pausa y reanudación de la protección

Cuando se pausa la protección, se detienen temporalmente todas las transferencias de datos del equipo seleccionado al Core de Rapid Recovery. Cuando reanuda la protección, el Core de Rapid Recovery sigue los requisitos del calendario de programación de protección, creando copias de seguridad de sus datos con regularidad basándose en ese calendario de programación.

Puede pausar la protección para cualquier equipo protegido de Rapid Recovery:

- Al establecer la protección mediante el Asistente para proteger un equipo o el Asistente para proteger varios equipos.
- Desde el menú desplegable Equipos protegidos que se encuentra en el área de navegación izquierda del Core de Rapid Recovery (puesta en pausa de la protección para todos los equipos protegidos).
- Desde la página Equipos protegidos (accesible cuando hace clic en el menú Equipos protegidos).
- Desde un equipo protegido específico del menú desplegable Equipos protegidos.
- Desde la parte superior de cada página para un equipo protegido específico.

Si pausa la protección mediante el Asistente para proteger un equipo o el Asistente para proteger varios equipos, la protección se pausará hasta que se reanude de manera explícita.

Si pausa la protección fuera de un asistente, puede elegir entre pausar la protección hasta que se reanude o pausarla durante una cantidad de tiempo indicada (especificada en cualquier combinación de días, horas y minutos). Si la pausa durante un período de tiempo, cuando venza ese tiempo, el sistema reanudará la protección basándose en el calendario de programación de protección automáticamente.

Puede reanudar la protección para cualquier equipo protegido de Rapid Recovery en pausa:

- Desde el menú desplegable Equipos protegidos que se encuentra en el área de navegación izquierda del Core de Rapid Recovery (reanudación de la protección para todos los equipos protegidos).
- Desde un equipo protegido específico del menú desplegable Equipos protegidos.
- Desde la página Equipos protegidos (accesible cuando hace clic en el menú Equipos protegidos).
- Desde la parte superior de cada página para un equipo protegido específico.

Utilice el procedimiento siguiente para pausar o reanudar la protección, según sea adecuado.

- 1 En la Core Console de Rapid Recovery, para pausar la protección en todos los equipos, haga clic en el menú desplegable Equipos protegidos del área de navegación izquierda y, a continuación, haga lo siguiente:
 - a Seleccione **Pausar la protección**.
Aparecerá el cuadro de diálogo Pausar la protección.
 - b Seleccione el ajuste adecuado utilizando una de las opciones descritas a continuación y, a continuación, haga clic en **Aceptar**.
 - Si desea pausar la protección hasta que la reanude de manera explícita, seleccione **Pausar hasta reanudación**.
 - Si desea pausar la protección durante un período especificado, seleccione **Pausar durante** y, a continuación, en los controles Días, Horas y Minutos, escriba o seleccione el período de pausa que sea adecuado.
- 2 Para reanudar la protección en todos los equipos, haga lo siguiente:
 - a Seleccione **Reanudar la protección**.
Aparecerá el cuadro de diálogo Reanudar la protección.
 - b En el cuadro de diálogo Reanudar la protección, seleccione **Sí**.
El cuadro de diálogo Reanudar la protección se cerrará y la protección se reanudará para todos los equipos.
- 3 Para pausar la protección de un solo equipo, a continuación, en el área de navegación izquierda, haga clic en el menú desplegable que se encuentra a la derecha del equipo cuya protección quiere modificar y haga lo siguiente:
 - a Seleccione **Pausar la protección**.
Aparecerá el cuadro de diálogo Pausar la protección.
 - b Seleccione el ajuste adecuado utilizando una de las opciones descritas a continuación y, a continuación, haga clic en **Aceptar**.
 - Si desea pausar la protección hasta que la reanude de manera explícita, seleccione **Pausar hasta reanudación**.
 - Si desea pausar la protección durante un período especificado, seleccione **Pausar durante** y, a continuación, en los controles Días, Horas y Minutos, escriba o seleccione el período de pausa que sea adecuado.
- 4 Para reanudar la protección de un solo equipo, haga lo siguiente:
 - a Seleccione **Reanudar la protección**.
Aparecerá el cuadro de diálogo Reanudar la protección.
 - b En el cuadro de diálogo Reanudar la protección, seleccione **Sí**.
El cuadro de diálogo Reanudar la protección se cerrará y la protección se reanudará para el equipo seleccionado.
- 5 Para pausar la protección de un único equipo desde la página Equipo, desplácese hasta el equipo cuya protección quiere modificar. Aparecerá la página Resumen para el equipo seleccionado.
 - a En la parte superior de la página, haga clic en **Pausar**.
Aparecerá el cuadro de diálogo Pausar la protección.
 - b Seleccione el ajuste adecuado utilizando una de las opciones descritas a continuación y, a continuación, haga clic en **Aceptar**.
 - Si desea pausar la protección hasta que la reanude de manera explícita, seleccione **Pausar hasta reanudación**.
 - Si desea pausar la protección durante un período especificado, seleccione **Pausar durante** y, a continuación, en los controles Días, Horas y Minutos, escriba o seleccione el período de pausa que sea adecuado.
- 6 Si desea reanudar la protección, haga lo siguiente:
 - a En la parte superior de la página, haga clic en **Reanudar**.
 - b En el cuadro de diálogo Reanudar la protección, haga clic en **Sí**.
El cuadro de diálogo Reanudar la protección se cierra y la protección se reanuda para el equipo seleccionado.

Administración de equipos protegidos

Esta sección describe cómo ver, configurar y administrar los equipos protegidos en su entorno de Rapid Recovery.

Acerca de la administración de equipos protegidos

Las tareas que puede realizar para administrar equipos protegidos se desglosan en algunas categorías.

- Puede ver las máquinas protegidas en el Core de Rapid Recovery utilizando las opciones se describe en el tema [Visualización de equipos protegidos](#).
- Puede configurar los parámetros del equipo, acceder a información del sistema, o bien configurar notificaciones para eventos referentes a un equipo en particular. Para obtener más información, consulte [Configuración de los ajustes de la máquina](#).
- Puede acceder a los diagnósticos de un equipo protegido. Para obtener más información, consulte [Descarga y visualización del archivo de registro de un equipo protegido](#).
- Puede retirar un equipo de la protección, cancelar operaciones que se están realizando, o ver la información de licencia de un equipo protegido. Para obtener más información, consulte [Administración de equipos](#).
- Puede ver y administrar datos guardados en el Core. Para obtener más información, consulte [Administración de instantáneas y puntos de recuperación](#).

Visualización de equipos protegidos

Desde la página **Inicio** de la Core Console de Rapid Recovery, cuando observa la vista Tablas de resumen, puede ver información de resumen de cualquier equipo que proteja el Core en el panel Equipos protegidos.

NOTA: Un agente de software actúa por parte del usuario para realizar acciones específicas. Los equipos protegidos a veces se denominan **Agents**, ya que ejecutan el software **Rapid Recovery Agent** para facilitar las copias de seguridad y la replicación en el Core de Rapid Recovery.

Puede ver el estado, el nombre de visualización de cada equipo, qué repositorio utiliza, la fecha y la hora de la última instantánea, cuántos puntos de recuperación hay en el repositorio para el equipo, así como la cantidad total de espacio de almacenamiento que utilizan las instantáneas en el repositorio.

Para administrar aspectos de cualquier equipo protegido, empiece desplazándose hasta el equipo que desee ver, configurar o administrar. Desde la página Inicio, hay tres maneras de desplazarse hasta un equipo protegido:

- Puede hacer clic en la dirección IP o nombre de visualización de cualquier equipo protegido del panel Equipos protegidos. Esta acción le llevará a la página Resumen del equipo protegido seleccionado.
- En el área de navegación de la izquierda, puede hacer clic en el título del menú **Equipos protegidos**. Aparecerá la página Protected Machines (Máquinas protegidas). En la página Equipos protegidos, puede ver información de resumen sobre cada equipo. Para obtener una descripción detallada de esta página, consulte [Visualización de información de resumen de un equipo protegido](#).
- En el menú Equipos protegidos del área de navegación de la izquierda, puede hacer clic en la dirección IP o en el nombre de visualización de cualquier equipo protegido. Esta acción le llevará a la página Resumen del equipo protegido seleccionado. Para obtener una descripción detallada de esta página, consulte [Visualización de información de resumen de un equipo protegido](#).

Visualización de información de resumen del clúster

Realice los pasos de este procedimiento para ver información de resumen sobre un clúster, incluyendo información sobre el quórum asociado para el clúster.

- 1 En la Core Console de Rapid Recovery, en Equipos protegidos, haga clic en el clúster que desea ver.
Aparece la página Resumen para el equipo.
- 2 En la página Resumen, puede ver información como el nombre del clúster, tipo de clúster, tipo de quórum (si procede) y ruta de acceso de quórum (si procede). En esta página también se muestra información de un vistazo sobre los volúmenes de este clúster, que incluye el tamaño y la programación de protección. Si es aplicable, también puede ver información de SQL Server o Exchange Server para un clúster diferente.
- 3 Para ver la información más actual, haga clic en **Actualizar**.

Para obtener más información sobre la visualización de información de resumen y estado para una máquina o nodo individual del clúster, consulte [Visualización de equipos protegidos](#).

Configuración de los ajustes de la máquina

Una vez que haya agregado máquinas para protegerlas en Rapid Recovery, puede ver y modificar fácilmente la configuración que gestiona el comportamiento de esa máquina protegida. Al modificar la configuración de una máquina específica, esa configuración sustituye el conjunto de comportamientos establecidos en el Core.

Es posible ver y configurar los siguientes ajustes de máquina en la Rapid Recovery Core Console:

- **General.** Los ajustes generales de configuración de la máquina incluyen el nombre de visualización, el nombre de host, el puerto, la clave de cifrado y el repositorio. Para obtener más información sobre la configuración de los ajustes generales de una máquina, consulte [Visualización y modificación de la configuración de equipos protegidos](#).
- **Trabajos nocturnos.** El subconjunto de ajustes de trabajos nocturnos del Core que aparecen para una determinada máquina protegida le permiten sustituir los ajustes de los trabajos nocturnos establecidos a nivel del Core. Este subconjunto incluye la agregación, que le permite administrar la política de retención. Algunos ajustes pueden diferir según el tipo de máquina que esté protegida.
- **Ajustes de las transferencias.** Son los ajustes específicos para la gestión de los procesos de transferencia de datos para la máquina protegida seleccionada. Para obtener información sobre los tipos de transferencia de datos afectados por estos ajustes, consulte [Modificación de la configuración de las transferencias](#).
- **Escritores excluidos.** Estos ajustes le permiten excluir los escritores, que son específicos de la máquina. Un escritor es una API específica publicada por Microsoft que permite que otros componentes del software participen en el uso de Microsoft Volume Shadow Services (VSS). Todos los escritores en Rapid Recovery que participan en las instantáneas del volumen se muestran en los ajustes de los Escritores excluidos. En caso de que un escritor está interfiriendo con la copia de seguridad de las transferencias o impidiendo las transferencias, estas pueden desactivarse una por una. Dell recomienda no modificar estos ajustes, a menos que un representante del servicio de asistencia técnica de Dell indique lo contrario.
- **Detalles de licencia.** Se trata de los detalles específicos de la licencia para la máquina protegida. Estos ajustes notifican la información del Core y la Dell Data Protection | Portal de licencias de Rapid Recovery. Estos ajustes son de sólo lectura. Para cambiar estos ajustes, actualice su información de licencia entre el Core y el portal de licencias. Consulte el administrador de licencias para obtener más detalles. Para obtener más información, consulte la *Dell Dell Data Protection | Portal de licencias de Rapid Recovery User Guide (Guía del usuario de la Protección de datos de Dell | Portal de licencias de Rapid Recovery)*.

El procedimiento para visualizar o cambiar los ajustes de nivel de máquina es idéntico para los ajustes generales, los escritores excluidos y los detalles de licencia. Para obtener más información, consulte [Visualización y modificación de la configuración de equipos protegidos](#).

El procedimiento para modificar los trabajos nocturnos para una máquina es diferente. Para obtener información sobre la configuración de los ajustes de trabajos nocturnos para una máquina, consulte [Personalización de las tareas nocturnas de una máquina protegida](#).

En algunos casos, es posible que desee ajustar la velocidad de transferencia de datos de una máquina protegida. Para obtener más información, consulte [Modificación de la configuración de las transferencias](#).

Visualización y modificación de la configuración de equipos protegidos

La configuración de los equipos ayuda a determinar el comportamiento de un equipo protegido por el Core. Cuando modifica la configuración de un equipo específico, las nuevas opciones de configuración sustituyen el comportamiento establecido a nivel del Core.

Siga los pasos de este procedimiento para ver y modificar la configuración general, la configuración de transferencia, la configuración de escritores excluidos y la configuración de licencias de un equipo protegido.

NOTA: Para ver y modificar la configuración de un trabajo nocturno, consulte [Personalización de las tareas nocturnas de una máquina protegida](#).

Esta tarea es también un paso en [Modificación de la configuración del nodo de clúster](#).

- 1 En la Core Console de Rapid Recovery, bajo el menú Equipos protegidos, haga clic en la dirección IP o en el nombre de equipo del equipo del que desea ver o modificar su configuración.
Aparecerá la página **Resumen** del equipo seleccionado.
- 2 Haga clic en el menú **Configuración**.

Aparecerá la página **Configuración**, que muestra las opciones de configuración del equipo seleccionado. De manera opcional, para ver las categorías de configuración desde cualquier parte de la página, haga clic en el hipervínculo correspondiente del lado izquierdo de la página.

Cuando haga clic en una opción que desee cambiar, ese valor se volverá editable como un campo de texto o un menú desplegable.

Cuando esté satisfecho con los cambios realizados en cada opción, haga clic en  para guardar el cambio y salir del modo edición, o haga clic en  para salir del modo edición sin guardar.

- 3 Para modificar la configuración general de un equipo protegido, haga clic en la opción pertinente y, a continuación, introduzca la información de configuración tal como se describe en la tabla siguiente.

Tabla 69. Configuración general de un equipo protegido

Cuadro de texto	Descripción
Nombre mostrado	Escriba el nombre mostrado del equipo. Es el nombre que aparece para un equipo protegido en la Core Console de Rapid Recovery. Puede introducir hasta 64 caracteres. De manera predeterminada, es el nombre de host del equipo. Si fuera necesario, puede cambiarlo a otro de uso más fácil. No utilice caracteres prohibidos ni frases prohibidas.
Nombre de host	Escriba el nombre de host del equipo.
Puerto	Especifique un número de puerto para el equipo. El puerto lo utiliza el servicio del Core de Rapid Recovery para la comunicación con este equipo. El puerto predeterminado es 8006.
Clave de cifrado	Si desea que se aplique una clave de cifrado que ya esté definida para este Core de Rapid Recovery a los datos de todos los volúmenes de este equipo protegido, puede especificarla aquí. Es necesario desbloquear la clave. Si no hay claves de cifrado, puede agregar una clave de cifrado. Para obtener más información sobre la administración de las claves de cifrado, consulte Administración de las claves de cifrado. Si los volúmenes de este equipo protegido están cifrados, puede cambiar a una clave de cifrado diferente. De forma alternativa, para desasociar una clave de cifrado, seleccione (ninguno) en el menú desplegable Clave de cifrado.  NOTA: Después de aplicar una clave de cifrado, de cambiar una clave de cifrado o de desasociar una clave de cifrado para un equipo protegido, Rapid Recovery realiza una nueva imagen base en la siguiente instantánea programada o forzada.
Repositorio	Seleccione un repositorio para los puntos de recuperación. Muestra el repositorio configurado en el Core de Rapid Recovery donde se almacenarán los datos de este equipo. El volumen del repositorio puede ser local (en almacenamiento conectado al servidor del Core) o encontrarse en un volumen en una ubicación CIFS compartida.  NOTA: La configuración de repositorio en esta página solo se puede cambiar si no hay puntos de recuperación o si falta el repositorio anterior.

- 4 Para modificar la configuración de trabajo nocturno de un equipo protegido, consulte [Personalización de las tareas nocturnas de una máquina protegida](#).
- 5 Para modificar la configuración de Exchange de un servidor Exchange protegido, en la sección Configuración de Exchange Server, haga clic en **Habilitar comprobación de capacidad de montaje automático** y realice lo siguiente:
 - Para activar las comprobaciones de capacidad de montaje automático, marque la casilla de verificación y, a continuación, haga clic en .
 - Para desactivar las comprobaciones de capacidad de montaje automático, desmarque la casilla de verificación y, a continuación, haga clic en .

Para obtener más información sobre comprobaciones automáticas de capacidad de montaje, consulte [Acerca de las comprobaciones de capacidad de montaje de base de datos de Exchange](#).

- 6 Para modificar la configuración de transferencia de un equipo protegido, haga clic en la opción pertinente y, a continuación, introduzca la información de configuración tal como se describe en la tabla siguiente.

NOTA: Para obtener información sobre los conceptos de la configuración de transferencia, consulte [Modificación de la configuración de las transferencias](#).

Tabla 70. Configuración de transferencia de un equipo protegido

Cuadro de texto	Descripción
 Restaurar valores predeterminados	Este control restaura la configuración de transferencia a sus valores predeterminados.
Prioridad	Establece la prioridad de transferencia entre equipos protegidos. Le permite asignar prioridad por comparación con otros equipos protegidos. Seleccione un número del 1 al 10, siendo 1 la mayor prioridad. El valor predeterminado establece una prioridad de 5.
NOTA: La prioridad se aplica a las transferencias que hay en la cola.	
Número máximo de transmisiones simultáneas	Establece el número máximo de enlaces de TCP que se envían al Core para procesarlos en paralelo por equipo protegido, para equipos protegidos en un repositorio DVM.
NOTA: Dell recomienda establecer este valor como 8. Si se descartan paquetes, pruebe a incrementar este valor.	
Número máximo de escrituras simultáneas	Establece el número máximo de acciones de escritura en disco simultáneas por conexión de equipo protegido.
NOTA: Dell recomienda establecer este valor igual que el valor que seleccionó para Número máximo de transmisiones simultáneas. Si se pierden paquetes, establezca un valor ligeramente menor: por ejemplo, si Número máximo de transmisiones simultáneas es 8, establezca este valor como 7.	
Utilizar el número máximo predeterminado de reintentos del Core	Seleccione esta opción para utilizar el número predeterminado de reintentos para cada equipo protegido, si algunas de las operaciones no se pueden completar.
Tamaño máximo del segmento	Especifica la cantidad mayor de datos, en bytes, que un equipo puede recibir en un único segmento TCP. El valor predeterminado es 4194304. No cambie este valor predeterminado a menos que así se lo indique un representante de asistencia técnica de Dell.
Profundidad máxima de la cola de transferencia	Especifica la cantidad de comandos que pueden enviarse simultáneamente. El valor predeterminado es 64. Puede ajustar este valor con un número más alto si su sistema tiene un alto número de operaciones de entrada/salida simultáneas.
Lecturas pendientes por transmisión	Especifica cuántas operaciones de lectura en cola se almacenarán en el back-end. Este parámetro ayuda a controlar la puesta en cola de equipos protegidos. El valor predeterminado es 0.
Puerto de servidor de datos de transferencia	Establece el puerto de las transferencias. El valor predeterminado es 8009.
Tiempo de espera de transferencia	Especifica en minutos y segundos la cantidad de tiempo que se permite a un paquete ser estático sin transferirlo.

Cuadro de texto	Descripción
Tiempo de espera de la instantánea	Especifica en minutos y segundos el tiempo máximo de espera para tomar una instantánea.
Tiempo de espera de limpieza de la instantánea	Especifica en minutos y segundos el tiempo máximo para procesar o eliminar una instantánea de VSS en un equipo protegido.
Tiempo de espera de lectura de red	Especifica en minutos y segundos el tiempo máximo de espera para una conexión de lectura. Si la lectura de red no se puede realizar en ese momento, se volverá a intentar realizar la operación.
Tiempo de espera de escritura de red	Especifica el tiempo máximo en segundos que se esperará para una conexión de escritura. Si la escritura de red no se puede realizar en ese momento, se volverá a intentar realizar la operación.

- 7 Para modificar la configuración de escritores excluidos, haga clic en la opción pertinente y, a continuación, introduzca la información de configuración tal como se describe en la tabla siguiente.

Tabla 71. Configuración de escritores excluidos de un equipo protegido

Cuadro de texto	Descripción
Escritores excluidos	Seleccione un escritor si desea excluirlo. Como los escritores que aparecen en la lista son específicos del equipo que está configurando, no verá a todos los escritores de su lista. Por ejemplo, algunos de los escritores que quizá vea incluyen: • Escritor ASR • Escritor COM+ REGDB • Escritor de contadores de rendimiento • Escritor de registro • Escritor de optimización de servicio de instantáneas • SQLServerWriter • Escritor del sistema • Escritor del Programador de tareas • Escritor del almacén de metadatos de VSS • Escritor WMI

- 8 Los detalles de la licencia de un equipo protegido son de solo lectura. La información de detalles de la licencia se describe en la tabla siguiente.

Tabla 72. Detalles de la licencia de un equipo protegido

Cuadro de texto	Descripción
Fecha de caducidad	Indica la fecha de caducidad de la licencia del equipo protegido seleccionado.
Estado de la licencia	Indica el estado actual de la licencia del equipo protegido seleccionado.
Tipo de licencia	Indica el tipo de licencia del equipo protegido seleccionado.
Tipo de Agent	Indica si el equipo protegido actual es un agente físico o virtual.

Cómo modificar la configuración de un host iHyper-V o nodo

Este procedimiento se aplica a los hosts Hyper-V o nodos que utilizan Rapid Recovery Rapid Snap for Virtual (sin agente protección) para proteger las máquinas virtuales (MV).

Un host Hyper-V que usa Rapid Snap for Virtual (protección sin agente) para proteger las máquinas virtuales se muestra en el área de

navegación de la izquierda, junto al icono del host . La configuración de un host Hyper-V con máquinas virtuales con protección sin agente no es la misma que la de una máquina protegida típica. Todos los cambios efectuados en la configuración de un host se aplican a las máquinas virtuales de dicho host.

- 1 En la Core Console, opción Protected Machines (Máquinas protegidas) en el área de navegación de la izquierda, haga clic en el host Hyper-V cuyos valores desea cambiar.

Se abre la página **Summary (Resumen)**.

- 2 En la barra de menú para el host, haga clic en **Settings (Configuración)**.

Se abre la página **Settings (Configuración)**.

- 3 En **General**, haga clic en el valor que desee cambiar.

El ajuste seleccionado se convierte en editable, como un campo de texto o un menú desplegable.

- 4 Introduzca la información de configuración según se describe en la tabla siguiente.

Tabla 73. Información de la configuración general

Cuadro de texto	Descripción
Display Name (Nombre de visualización)	El nombre que se muestra en una máquina protegida en la Rapid Recovery Core Console. Puede introducir hasta 64 caracteres. De manera predeterminada, es el nombre de host de la máquina, y puede cambiarlo por un nombre más fácil de identificar si lo desea. No utilice caracteres prohibidos ni frases prohibidas .
Host Name (Nombre del host)	El nombre de la máquina protegida tal y como aparece en los metadatos de la máquina. NOTA: No cambie este valor, ya que se podría interrumpir la conexión entre la máquina protegida y el Core.

- 5 Para cambiar el número de trabajos de transferencia que pueden producirse en el host en un momento determinado, en **Transfer Queue (Cola de transferencia)**, haga clic en el ajuste **Maximum Concurrent Transfers (Número máximo de transferencias simultáneas)**.

NOTA: Para obtener un mejor rendimiento, se recomienda que el número máximo de transferencias simultáneas para el host Hyper-V o nodo se establezca en 1, que es el valor predeterminado.

- 6 En **Nightly Jobs (Trabajos nocturnos)**, cambie la configuración de los trabajos nocturnos disponibles. Haga clic en **Change (Cambiar)**.

Aparece la ventana **Nightly Jobs (Trabajos nocturnos)**.

- 7 Introduzca la información de configuración según se describe en la tabla siguiente.

Tabla 74. Información de configuración de los trabajos nocturnos

Cuadro de texto	Descripción
Clear orphaned registry keys on protected Hyper-V host (Borrar las claves de registro huérfanas en el host Hyper-V protegido)	Elimina los archivos innecesarios del registro que se producen como resultado de vincular y desvincular los discos virtuales durante las transferencias de datos.
Check integrity of recovery points (Verificar la integridad de los puntos de recuperación)	Realiza una comprobación de la integridad de cada punto de recuperación creado para las máquinas virtuales en el host Hyper-V.

- 8 Haga clic en **OK (Aceptar)**.

- 9 Para determinar si desea proteger automáticamente las nuevas máquinas virtuales cuando se agregan al host Hyper-V, en **Auto Protection (Protección automática)** haga clic en **Auto protect new virtual machines (Proteger automáticamente las nuevas máquinas virtuales)**.

Cambiar la configuración de una máquina virtual protegida Hyper-V

Este procedimiento se aplica a máquinas virtuales Hyper-V (VM) protegidas mediante la función Rapid Snap for Virtual de Rapid Recovery (protección sin agentes).

Una VM Hyper-V que se protege mediante la función Rapid Snap for Virtual (protección sin agentes) se indica en el área de navegación de la izquierda con el icono de host . La configuración de una VM Hyper-V sin agentes es la misma que la de un equipo protegido normal con la excepción de la sección Hyper-V que se encuentra en la parte inferior de la página **Configuración**. La siguiente tarea proporciona instrucciones solo para la configuración de la sección **Hyper-V**. Para ver la configuración de todos los demás equipos protegidos, consulte [Visualización y modificación de la configuración de equipos protegidos](#).

- 1 En la Core Console, en el área de navegación izquierda en **Equipos protegidos**, haga clic en la VM Hyper-V cuya configuración quiere cambiar.
Se abre la página **Resumen** para la VM.
- 2 En la barra de menú del host, haga clic en **Configuración**.
Aparecerá la página **Configuración**.
- 3 En la lista de la izquierda, haga clic en **Hyper-V**.
La configuración seleccionada se convierte en editable, como un campo de texto o un menú desplegable.
- 4 En **Hyper-V**, haga clic en **Configuración de instantáneas**.
La configuración seleccionada se convierte en un menú desplegable editable.
- 5 En el menú desplegable, seleccione una de las opciones que se describen en la tabla siguiente.

Tabla 75. Información de la configuración de Hyper-V

Cuadro de texto	Descripción
Intente crear una instantánea VSS durante la primera transferencia, si falla, cree un punto de control	Si la instantánea VSS se realiza correctamente, el punto de recuperación estará en un estado coherente con la aplicación. Si la instantánea de VSS falla y se crea un punto de control, el punto de recuperación estará en un estado coherente con bloqueo.
No cree instantáneas VSS durante la transferencia.	Genera un punto de recuperación en un estado coherente con bloqueo.
Utilice únicamente instantáneas VSS durante las transferencias. Si la creación de instantáneas VSS falla, fallará toda la transferencia.	Genera solo puntos de recuperación coherentes con la aplicación. Si la instantánea VSS falla, no se genera ningún punto de recuperación.

Cambiar la configuración de vSphere para una máquina virtual protegida VMware
Este procedimiento se aplica a máquinas virtuales (VM) Workstation o VMware ESXi que están protegidas mediante la función Rapid Snap de Rapid Recovery de Virtual (protección sin agentes).
La configuración de una VM VMware que está protegida sin agentes incluye la misma configuración que se utiliza para una máquina protegida normal, con una excepción. En la sección **vSphere** de la página **Configuración** se incluye la configuración que se aplica solo a las VM VMware protegidas sin agentes. La siguiente tarea proporciona instrucciones solo de la sección **vSphere** de la página **Configuración**. Para ver la configuración de todos los demás equipos protegidos, consulte [Visualización y modificación de la configuración de equipos protegidos](#).

- 1 En la Core Console, en Equipos protegidos en el área de navegación izquierda, haga clic en el host de Hyper-V cuya configuración quiera cambiar.
Se abre la página **Resumen** del host.
- 2 En la barra de menú del host, haga clic en **Configuración**.
Aparecerá la página **Configuración**.
- 3 En la lista de la izquierda, haga clic en **vSphere**.
La configuración seleccionada se convierte en editable, como un campo de texto o un menú desplegable.
- 4 En **vSphere**, haga clic en la configuración que desea cambiar.
La configuración seleccionada se convierte en editable, como un campo de texto o un menú desplegable.
- 5 Introduzca la información de configuración según se describe en la tabla siguiente.

Tabla 76. Información de la configuración de vSphere

Cuadro de texto	Descripción
Permitir a Rapid Recovery eliminar la VMware creada por el usuario	El valor predeterminado es No.
Permitir la transferencia de volúmenes con capacidad utilizada no válida	El valor predeterminado es Sí.
Permitir instantáneas en modo inactivo	El valor predeterminado es Sí.

Modificación de la configuración de las transferencias

En Rapid Recovery, puede modificar la configuración para administrar procesos de transferencia de datos en una máquina protegida. La configuración de transferencia que se describe en esta sección es a nivel de la máquina protegida. Para ver cómo modificar las transferencias a nivel del Core, consulte [Modificación de la configuración de la cola de transferencias](#).

Rapid Recovery admite Windows 8 y Windows Server 2012 para transferencias normales, tanto bases como incrementales, así como restaurar, restauración Bare Metal Restor y exportaciones de máquina virtual.

Hay tres tipos de transferencias en Rapid Recovery:

- **Snapshot (Instantánea):** Crea una copia de seguridad de los datos de la máquina protegida. Hay dos tipos de instantáneas posibles: una imagen base de todos los datos protegidos y una instantánea acumulada de los datos actualizados desde la última instantánea. Este tipo de transferencia crea los puntos de recuperación, que se almacenan en el repositorio asociadas con el Core. Para obtener más información, consulte [Administración de instantáneas y puntos de recuperación](#).
- **Virtual Machine Export (Máquina virtual Exportar):** Crea una máquina virtual (VM) de un punto de recuperación, que contiene todos los de los datos a partir de la copia de seguridad de la máquina protegida, así como del sistema operativo y los controladores y datos asociados para garantizar que la máquina virtual pueda iniciarse. Para obtener más información, consulte [Exportación de VM](#).
- **Restore (Restauración):** Restaura la información de la copia de seguridad a una máquina protegida. Para obtener más información, consulte [Restauración de volúmenes desde un punto de recuperación](#).

NOTA: Todo el volumen siempre se vuelve a escribir durante la restauración de sistemas Windows con particiones del sistema EFI.

La transferencia de datos en Rapid Recovery conlleva la transmisión de un volumen de datos a través de una red desde las máquinas protegidas hasta el Core. En caso de replicación, la transferencia también se puede efectuar desde el Core de origen hasta el de destino.

Además, la transferencia de datos se puede optimizar para el sistema mediante una configuración opcional de rendimiento. Esta configuración controla el uso del ancho de banda de los datos durante los procesos de copia de seguridad de máquinas protegidas, exportaciones de máquina virtual o restauraciones. Estos son algunos de los factores que influyen en el rendimiento de la transferencia de datos:

- Número de transferencias de datos de Agent simultáneas
- Número de flujos de datos simultáneos
- Número de cambios de datos en el disco
- Ancho de banda de red disponible
- Rendimiento del subsistema del disco del repositorio
- Cantidad de memoria disponible para el almacenamiento en búfer de los datos

Puede ajustar las opciones de rendimiento para que mejor se adapten a sus necesidades empresariales y adaptarlas a su entorno. Para obtener más información, consulte [Regulación de la velocidad de transferencia](#).

Regulación de la velocidad de transferencia

Cuando se transfieren datos de copia de seguridad o puntos de recuperación replicados entre equipos protegidos y Cores a través de la red, puede reducir deliberadamente la velocidad de transferencia. Este proceso se denomina regulación.

Cuando regula la velocidad de transferencia, está limitando la cantidad del ancho de banda de la red que dedica a las transferencias de archivos desde Rapid Recovery. Al configurar la replicación, por ejemplo, la regulación puede reducir la probabilidad de que la transferencia de puntos de recuperación anteriores al Core replicado consuma todo el ancho de banda de la red.

⚠ PRECAUCIÓN: No siempre es necesario o recomendable limitar la velocidad de transferencia. Esta información se facilita para indicar una posible solución a los problemas de rendimiento que puedan producirse en el entorno de Rapid Recovery. Por ejemplo, a veces, la regulación puede resolver los problemas relacionados con fallos de transferencia recurrentes o deceleraciones en la red debidos a la transferencia de una cantidad importante de datos a los Cores protegidos o replicados.

Existen varios factores que determinan la mejor forma de abordar la regulación. El tipo de equipos que se protege es un elemento clave. Por ejemplo, un servidor de Microsoft Exchange ocupado tiene una velocidad de cambio mucho más elevada que la de un servidor web heredado que se utiliza poco.

Las capacidades de entrada y salida de los volúmenes de almacenamiento en los equipos protegidos también pueden contribuir a que la eficiencia sea mayor o menor.

La velocidad de la red también es otro factor fundamental, y tiene muchas variables. La red troncal implantada (por ejemplo, de 1 GbE frente a 10 GbE), la arquitectura, la configuración, el uso deliberado de grupos de NIC e incluso el tipo de cables que se utilizan pueden afectar a la velocidad de transferencia de la red. Si su entorno tiene una red de área amplia más lenta y si los trabajos de transferencia fallan para la copia de seguridad o la replicación, plantéese limitar la velocidad de transferencia utilizando algunas de estas opciones de configuración.

Por último, la regulación de la red implica un proceso de prueba y error. Dell recomienda ajustar y probar la configuración de transferencia y volver a examinar estas opciones periódicamente para garantizar que su configuración sigue satisfaciendo sus necesidades.

El ajuste de la velocidad de transferencia debe realizarse de manera individual equipo por equipo. En la Core Console, navegue hasta a un equipo específico, seleccione Configuración y ajuste la velocidad de transferencia. Para obtener información específica sobre cómo ver y cambiar estos valores, consulte [Visualización y modificación de la configuración de equipos protegidos](#). Ese tema también incluye descripciones de cada una de las opciones que se utilizan para la regulación transferencia. Estas descripciones pueden resultar útiles para determinar con qué opciones de configuración debe experimentar primero.

Las cuatro principales opciones que controlan la regulación de la velocidad se describen en la siguiente tabla:

Tabla 77. Configuración del equipo protegido que se utiliza para regular la velocidad de transferencia

Configuración a nivel del equipo	Configuración predeterminada	Configuración de regulación sugerida
Número máximo de transmisiones simultáneas	8	4
Número máximo de escrituras simultáneas	8	4
Tamaño máximo del segmento	4194304	2097152
Lecturas pendientes por transmisión	0	Empiece por 24.

Dell recomienda ajustar y probar el resto de opciones antes de cambiar la configuración predeterminada de las lecturas pendientes por transmisión, a menos que un representante del servicio de asistencia técnica de Dell indique lo contrario. A la hora de calibrar esta opción, empiece por un valor de 24.

Cuando especifique limitaciones para parámetros de transferencia de equipos protegidos, estas limitaciones se aplican por trabajo. Si dos trabajos de transferencia se producen simultáneamente o se superponen, se consume el doble de ancho de banda. Si cuatro trabajos de transferencia por la red se superponen, se usa el cuádruple de ancho de banda; y así sucesivamente.

Personalización de las tareas nocturnas de una máquina protegida

Las tareas nocturnas pueden configurarse a nivel del Core y al de la máquina en la pestaña de Configuración que corresponda. Cuando se establecen los valores de una tarea nocturna a nivel del Core, los cambios se aplicarán a todos los máquinas protegidas por dicho Core. Los

cambios realizados en las tareas nocturnas a nivel de la máquina sustituyen los cambios realizados a nivel del Core, solo para las máquinas especificadas.

Para obtener una lista de todas las tareas nocturnas, incluidas las descripciones y el ámbito disponible de cada una de ellas, consulte el tema [Descripción de los trabajos nocturnos](#).

Complete los pasos del siguiente procedimiento para realizar cambios en las tareas nocturnas de una única máquina protegida.

- 1 En la Core Console de Rapid Recovery, en el menú Protected Machines (Máquinas protegidas), haga clic en la dirección IP o en el nombre de la máquina cuyas tareas nocturnas desea personalizar.
Aparecerá la página **Summary (Resumen)**.
- 2 Haga clic en el menú **Settings (Configuración)**.
Aparecerá la página **Settings (Configuración)**, que muestra los valores de configuración de la máquina seleccionada.
- 3 De manera opcional, también puede hacer clic en el enlace **Nightly Jobs (Tareas nocturnas)** para desplazarse hacia abajo en la página Configuración y ver las tareas nocturnas.
- 4 Debajo del encabezado de Tareas nocturnas, haga clic en  **Change (Cambiar)**.
Aparecerá el cuadro de diálogo **Nightly Jobs (Tareas nocturnas)**.

NOTA: Para obtener más información sobre la configuración de la consolidación, incluida la configuración de una política de retención personalizada, consulte [Personalización de la configuración de la política de retención de una máquina protegida](#).

- 5 En el cuadro de diálogo **Nightly Jobs (Tareas nocturnas)**, seleccione los trabajos que desea incluir para ejecutar todas las noches, o anule la selección de opciones que desea omitir para esta máquina.

NOTA: Las opciones pueden variar en cada máquina. Por ejemplo, una máquina protegida mediante Exchange Server puede incluir Check checksum of Exchange databases (Comprobación de la suma de comprobación de bases de datos de Exchange) y registros de Truncate Exchange.

- 6 Haga clic en **Aceptar**.

NOTA: Los resultados de este procedimiento solo se aplicarán a la máquina protegida seleccionada. Para aplicarlos en otra, repita el procedimiento para cada una de las máquinas que desee personalizar. Para cambiar la configuración de las tareas nocturnas de todas las máquinas protegidas por un Core, consulte [Configuración de trabajos nocturnos para el Core](#).

Visualización de la información del sistema de un equipo protegido

La Core Console de Rapid Recovery le permite acceder fácilmente a la información del sistema sobre los equipos protegidos en el Core.

El panel **General** incluye información general sobre el equipo y el entorno del Core. El panel **Volúmenes** muestra información sobre los volúmenes de almacenamiento en el equipo del Core. El panel **Conexiones del motor de reproducción** muestra los volúmenes de todos los equipos que se están protegiendo.

Realice los pasos de este procedimiento para ver la información detallada del sistema de un equipo protegido.

- 1 Desplácese a la Core Console de Rapid Recovery y, desde el menú de los equipos protegidos en el área de navegación izquierda, haga clic en el nombre de un equipo protegido.
Aparece la página **Resumen** del equipo protegido seleccionado.
- 2 En la página **Resumen**, en la parte inferior del panel **Resumen**, haga clic en  **Información del sistema**.
- 3 En la página **Información del sistema**, puede ver los siguientes detalles del equipo protegido seleccionado.
 - **Información del sistema.** Incluye el Nombre de host, la Versión del sistema operativo, la Arquitectura del sistema operativo, la Memoria (física), el Nombre de visualización, el Nombre de dominio totalmente cualificado, la Ubicación de metadatos de la caché, la Ubicación de la caché principal, la Ubicación de la caché secundaria y el Tipo de máquina virtual (si procede).
 - **Volúmenes.** Incluye el Nombre del volumen, el Id. del dispositivo, el Sistema de archivos, la Capacidad formateada, la Capacidad usada y los Puntos de montaje.
 - **Procesadores.** Incluye la Arquitectura y el Número de núcleos.

- **Adaptadores de red.** Incluye el Tipo de adaptador y la Velocidad.
- **Direcciones IP.** Incluye la Dirección IP y la Familia.

Administración de equipos

Esta sección describe una variedad de tareas que puede realizar para administrar sus equipos. Los temas incluyen:

- [Retirada de un equipo](#)
- [Retirada de un clúster de la protección](#)
- [Visualización de la información de licencia en un equipo](#)
- [Descarga y visualización del archivo de registro de un equipo protegido](#)
- [Conversión de un nodo de clúster protegido en un equipo protegido](#)

Retirada de un equipo

Cuando retira un equipo de la protección en el Core de Rapid Recovery, se le presentan dos opciones: puede mantener los puntos de recuperación guardados hasta ahora en el Core de RR o bien puede eliminarlos. Si mantiene los puntos de recuperación, tendrá lo que se conoce como un “equipo solo con puntos de recuperación”. Utilizando esos puntos de recuperación para el equipo que se ha retirado de la protección actual, podrá seguir restaurando el equipo en el futuro, pero solo hasta el estado capturado en un punto de recuperación guardado.

Si elimina los puntos de recuperación, esta acción elimina todos los datos de instantáneas del equipo que antes estaba protegido del Core de Rapid Recovery.

 **PRECAUCIÓN:** Si elimina los puntos de recuperación, ya no podrá restaurar datos para ese equipo.

Realice los pasos de este procedimiento para quitar un equipo de la protección de su entorno de Rapid Recovery.

- 1 Desde la Core Console de Rapid Recovery, en el panel de navegación de la izquierda en Equipos protegidos, haga clic en el equipo desee quitar.
- 2 En la página Resumen del equipo en cuestión, haga clic en **Quitar equipo**.
- 3 En el cuadro de diálogo, si también desea eliminar todos los puntos de recuperación para este equipo del repositorio, seleccione **Quitar con puntos de recuperación**.
- 4 Para confirmar su decisión de quitar el equipo, haga clic en **Sí**.
Rapid Recovery quitará la protección del equipo y cancelará todas las tareas activas del mismo.

Retirada de un clúster de la protección

Realice los pasos del procedimiento siguiente para quitar un clúster de la protección.

- 1 En la Core Console de Rapid Recovery, en Equipos protegidos, haga clic en el clúster que desea eliminar.
- 2 En la página Resumen del clúster, haga clic en **Quitar clúster**.
- 3 Opcionalmente, en el cuadro de diálogo, para eliminar del repositorio todos los puntos de recuperación de este clúster almacenados actualmente, seleccione **Quitar con puntos de recuperación**.
- 4 En el cuadro de diálogo, haga clic en **Sí** para confirmar.

Retirada de nodos de clúster de la protección

Realice los pasos de los procedimientos siguientes para quitar los nodos de clúster de la protección.

Si solamente desea quitar un nodo del clúster, consulte [Conversión de un nodo de clúster protegido en un equipo protegido](#).

- 1 En la Core Console de Rapid Recovery, en Equipos protegidos, haga clic en el nodo de clúster que desea eliminar.
- 2 En la página Resumen del nodo, haga clic en **Quitar equipo**.
Se abrirá el cuadro de diálogo Quitar nodo.
- 3 Opcionalmente, en el cuadro de diálogo, para eliminar del repositorio todos los puntos de recuperación de este clúster almacenados actualmente, seleccione **Quitar con puntos de recuperación**.

- En el cuadro de diálogo, haga clic en **Sí** para confirmar.

Retirada de todos los nodos de un clúster de la protección

Realice los pasos de este procedimiento para quitar todos los nodos de un clúster de la protección.

⚠ PRECAUCIÓN: Si quita todos los nodos de un clúster, también se quita el clúster.

- En la Core Console de Rapid Recovery, en Equipos protegidos, haga clic en el clúster cuyos nodos desea eliminar.
- En la página Resumen del clúster, haga clic en **Nodos protegidos**.
- En la página Nodos protegidos, seleccione todos los nodos.
- Haga clic en el menú desplegable **Quitar equipos** y, a continuación, seleccione una de las opciones que se describen en la siguiente tabla.

Tabla 78. Opciones de Quitar nodos

Opción	Descripción
Eliminar y mantener puntos de recuperación	Para mantener todos los puntos de recuperación actualmente almacenados para este clúster.
Quitar puntos de recuperación	Para quitar del repositorio todos los puntos de recuperación actualmente almacenados para este clúster.

- En el cuadro de diálogo Eliminar nodos, haga clic en **Sí** para confirmar.

Visualización de la información de licencia en un equipo

Puede ver la información sobre el estado actual de la licencia del software Rapid Recovery Agent instalado en un equipo protegido.

- En la Core Console de Rapid Recovery, en Equipos protegidos, haga clic en el equipo que desea modificar.
Aparecerá la página **Resumen** del equipo seleccionado.
- Haga clic en el menú **Configuración**.
Aparece la página **Configuración**, que muestra los ajustes de configuración del equipo seleccionado.
- Haga clic en el vínculo **Licencias** para desplazarse hasta la página Configuración para visualizar la configuración de licencias específica del equipo.
Aparecerá la pantalla Estado, la cual mostrará detalles sobre las licencias del producto.

Descarga y visualización del archivo de registro de un equipo protegido

Si se produce algún error o problema con un equipo protegido, puede descargar los registros del equipo para verlos o consultarlos con su representante de Dell Support.

- En el área de navegación izquierda de Core Console, bajo el menú Equipos protegidos, haga clic en la fecha para expandir el menú contextual de dicho equipo protegido. Desplácese hasta **Más**, expanda ese menú y, a continuación, seleccione  **Agent Log**.
Aparece la página **Descargar el registro de agentes**.
- En la página **Descargar registro de Agent**, haga clic en  **Haga clic aquí para iniciar la descarga**.
- En el cuadro de diálogo **Apertura de AgentAppRecovery.log**, realice una de las siguientes acciones:
 - Para abrir el archivo de registro, seleccione **Abrir con** y, a continuación, seleccione una aplicación (como Bloc de notas) para visualizar el archivo de registro basado en texto y haga clic en **Aceptar**.
Se abre el archivo AgentAppRecovery.log en la aplicación seleccionada.
 - Para guardar el archivo localmente, seleccione **Guardar archivo** y después haga clic en **Aceptar**.
El archivo AgentAppRecovery.log se guardará en su carpeta Descargas. Se puede abrir con un editor de texto.

Vínculos relacionados

[Descarga y visualización del archivo de registro del Core](#)

Conversión de un nodo de clúster protegido en un equipo protegido

En Rapid Recovery, puede convertir un nodo de clúster protegido en un equipo protegido de forma que aún siga administrado por el Core, pero que ya no sea parte del clúster. Esto es útil en el caso, por ejemplo, de que necesite quitar un nodo del clúster, pero quiera mantenerlo protegido.

- 1 En la Core Console de Rapid Recovery, desplácese hasta el clúster que contenga el equipo que quiera convertir y, a continuación, haga clic en **Nodos protegidos**.
- 2 En la página **Nodos protegidos**, desde el nodo específico que quiera convertir, haga clic en el menú desplegable Acciones y seleccione **Convertir en Agent**.
- 3 Para agregar el equipo nuevamente al clúster, selecciónelo y, a continuación, en la página Resumen, desde el menú Acciones, seleccione **Convertir en nodo de clúster** y, a continuación, haga clic en **Sí** para confirmar la acción.

Comprensión de los grupos personalizados

La Core Console de Rapid Recovery muestra un menú de Equipos protegidos en el área de navegación izquierda. Esto incluye todos los equipos o los clústeres de servidor agregados a la protección del Core de Rapid Recovery. Es posible que debajo aparezcan otros menús, en función de si incluye esos objetos en el Core. De la misma manera, puede crear un grupo personalizado, que se muestra como el último tipo de menú en el área de navegación de la izquierda.

La ventaja principal de un grupo personalizado es la capacidad de agrupar los objetos de Core en un contenedor lógico. Esto puede ayudarle a organizar y gestionar los objetos de Core para un fin específico (por ejemplo, por la organización, el centro de costes, el departamento, la región geográfica, etc.).

El acto de creación de un grupo siempre agrega un miembro del grupo (por ejemplo, un equipo protegido o un clúster de servidor, un equipo replicado o un equipo con solo puntos de recuperación) al nuevo grupo personalizado. El objeto agregado viene determinado por el punto de origen al crear el grupo. Idealmente, debería agregar entonces los miembros adicionales al grupo. De ahí en adelante, puede realizar acciones de grupo que se apliquen a todos los miembros de ese grupo personalizado, según se describe en [Realización de acciones de grupo](#).

Los grupos personalizados pueden incluir equipos protegidos, clústeres de servidor, equipos replicados y equipos con solo puntos de recuperación. Los clústeres de servidor se comportan igual que los equipos protegidos, con la excepción de que un clúster de servidor y sus nodos se comportan como una entidad única. Si intenta agregar un nodo desde un clúster de servidor a un grupo, se agrega todo el clúster.

Un grupo personalizado puede contener miembros similares o no similares. Con grupos de miembros similares, todas las acciones de grupo se aplican a todos los miembros del grupo. Por ejemplo, si fuerza una instantánea de un grupo personalizado de equipos protegidos, se realizará una copia de seguridad de todos los equipos. En los grupos con miembros no similares (por ejemplo, equipos protegidos y replicados), si aplica una acción de grupo, como el forzado de la replicación, esta solo se aplicará en los equipos replicados.

Puede crear uno o varios grupos. Un equipo protegido único o un equipo replicado se pueden incluir en uno o varios grupos. De esta forma, puede agrupar los equipos en su Core de la forma que quiera y puede realizar acciones en ese grupo en concreto.

Todos los grupos personalizados aparecen en el área de navegación izquierda, con la etiqueta que designe. Los grupos que tienen equipos protegidos estándar aparecen en primer lugar en el grupo personalizado y los equipos replicados aparecen debajo de los protegidos, según corresponda. Si hay algún equipo con solo puntos de recuperación, se enumerará debajo de los equipos replicados.

En el área de navegación de la izquierda, los objetos que están protegidos en el Core aparecen cada uno en su propio menú. De estos menús, los grupos personalizados aparecen al final.

Incluir un equipo en un grupo no lo quita de su ubicación original. Por ejemplo, si tiene tres equipos protegidos denominados Agent1, Agent2 y Agent3 y agrega Agent1 a CustomGroup1, el Agent1 aparecerá en ambas ubicaciones.

Para obtener más información, consulte los siguientes temas:

- [Modificación de nombres de grupo personalizados](#)
- [Eliminación de los grupos personalizados](#)

- [Realización de acciones de grupo](#)
- [Visualización de todos los equipos de un grupo personalizado en una página](#)

Creación de grupos personalizados

Cuando desplace el cursor sobre el nombre de cualquier equipo de los menús Equipos protegidos o Equipos replicados, verá una flecha que abre el menú desplegable. En este menú, puede crear una etiqueta personalizada.

Utilice el siguiente procedimiento para crear un grupo personalizado.

- 1 Vaya a la Core Console de Rapid Recovery.
- 2 Desde el menú Equipos protegidos, Equipos replicados o Equipos con puntos de recuperación únicamente, haga lo siguiente:
 - a Coloque el cursor sobre un equipo en el menú.
 - b Haga clic en el menú desplegable para ese equipo.
 - c Desplácese hacia abajo y seleccione **Etiquetar como** y, a continuación, haga clic en **Nueva etiqueta**.

Aparece el cuadro de diálogo **Crear instantánea**.

- 3 En el campo **Nombre**, introduzca una etiqueta adecuada para su grupo personalizado.
 Utilice un nombre descriptivo que comunique el objetivo del grupo. Por ejemplo, para agrupar los equipos protegidos, replicados y con puntos de recuperación únicamente por departamento, escriba `Accounting Department`. Puede cambiar el nombre del grupo más adelante.

NOTA: Las etiquetas deben tener 50 caracteres o menos. Puede incluir un espacio entre las palabras. Debe proporcionar una etiqueta para su grupo personalizado.

- 4 Cuando esté satisfecho con el nombre de la etiqueta, haga clic en **Aceptar**.
 Se cierra el cuadro de diálogo y aparece el grupo personalizado como el último elemento en el área de navegación izquierda.
- 5 De forma opcional, pueden agregar otros equipos protegidos, replicados o con puntos de recuperación únicamente a este grupo. Vaya al nombre del equipo en el menú adecuado, haga clic en su menú desplegable, desplácese hacia abajo y seleccione **Etiquetar como** y, a continuación, haga clic en el nombre del grupo personalizado.
 Ahora puede realizar acciones grupo en este grupo. Para obtener más información, consulte [Realización de acciones de grupo](#).

Modificación de nombres de grupo personalizados

Cuando modifica el nombre de un grupo personalizado, solo cambia la etiqueta. El nombre de equipo permanece igual.

Utilice el siguiente procedimiento para modificar un nombre de grupo personalizado.

- 1 Vaya a la Core Console de Rapid Recovery.
- 2 En el menú Equipos protegidos, desplace el cursor sobre el grupo personalizado que desea modificar.
- 3 Haga clic en el menú desplegable del grupo y, a continuación, haga clic en **Editar**.
 Aparece el cuadro de diálogo **Modificar etiqueta**, que dentro del nombre del grupo personalizado se puede editar.
- 4 En el campo **Nombre**, actualice el texto o elimine el texto de la etiqueta existente y escriba una nueva etiqueta o su grupo personalizado.
 Utilice un nombre descriptivo que comunique el objetivo del grupo. Por ejemplo, para agrupar equipo protegidos, replicados y con puntos de recuperación únicamente por región geográfica, escriba `Tokyo`. Puede cambiar el nombre del grupo más adelante.

NOTA: Las etiquetas deben tener 50 caracteres o menos. Puede incluir un espacio entre las palabras. Debe proporcionar una etiqueta para su grupo personalizado.

- 5 Cuando esté satisfecho con el nombre de la etiqueta, haga clic en **Aceptar**.
 Se cierra el cuadro de diálogo y aparece el grupo personalizado modificado como el último elemento en el área de navegación izquierda.
- 6 De forma opcional, pueden agregar otros equipos protegidos, replicados o con puntos de recuperación únicamente a este grupo. Vaya al nombre del equipo en el menú adecuado, haga clic en su menú desplegable, desplácese hacia abajo y seleccione **Etiquetar como** y, a continuación, haga clic en el nombre del grupo personalizado.

Eliminación de los grupos personalizados

Cuando quita un grupo personalizado, lo elimina del menú Equipos protegidos. Los equipos que estaban en el grupo no se quitan, sino que siguen en el menú estándar correspondiente.

Utilice el siguiente procedimiento para quitar un grupo personalizado.

- 1 Vaya a la Core Console de Rapid Recovery.
- 2 En el menú Equipos protegidos, desplace el cursor sobre el grupo personalizado que desea quitar.
- 3 Haga clic en el menú desplegable del grupo y, a continuación, haga clic en **Quitar etiqueta**.
Ve un mensaje que le pide confirmar que desea quitar el grupo.
- 4 Confirme la eliminación del grupo personalizado.
Se cierra el cuadro de diálogo y el grupo personalizado se quita del área de navegación.

Realización de acciones de grupo

Puede realizar las acciones de grupo en cualquier grupo que aparece en el área de navegación izquierda de la Core Console de Rapid Recovery. Si el grupo contiene miembros no similares (por ejemplo, equipos replicados y equipos con puntos de recuperación únicamente), las acciones que solicite solo se realizarán en los miembros del grupo relevantes.

Utilice el siguiente procedimiento para realizar acciones de grupo en un grupo personalizado.

- 1 Vaya a la Core Console de Rapid Recovery.
- 2 En el menú Equipos protegidos, desplace el cursor sobre el grupo personalizado sobre el que desee realizar una acción de grupo.
- 3 Haga clic en el menú desplegable de ese grupo y, a continuación, seleccione una acción de la siguiente forma:
 - Para forzar una instantánea incremental o una imagen de base para todos los equipos protegidos en el grupo, haga clic en **Forzar instantánea** o **Forzar imagen base**, como corresponda. Para obtener más información, consulte [Cómo forzar una instantánea](#).
 - Para pausar la protección de todos los equipos protegidos en el grupo, haga clic en **Pausar la protección** y, a continuación, especifique los parámetros de reanudación. Para obtener más información, consulte [Pausa y reanudación de la replicación](#).
 - Para reanudar la protección de todos los equipos protegidos en el grupo para el que se ha pausado la protección, haga clic en **Reanudar la protección** y, a continuación, confirme que quiere reanudarla. Para obtener más información, consulte [Pausa y reanudación de la replicación](#).
 - Para actualizar la información de todos los objetos en el grupo, haga clic en **Actualizar los metadatos**.
 - Para pausar la replicación de todos los equipos protegidos en este grupo, debajo de Replicación, haga clic en **Pausar**. Para obtener más información, consulte [Pausa y reanudación de la replicación](#).
 - Para reanudar la replicación de todos los equipos replicados en este grupo para el que se ha puesto en pausa la replicación, debajo de Replicación, haga clic en **Reanudar**. Para obtener más información, consulte [Pausa y reanudación de la replicación](#).
 - Para forzar la replicación de todos los equipos replicados en este grupo, debajo de Replicación, haga clic en **Forzar**. Para obtener más información, consulte [Forzado de la replicación](#).
 - Para eliminar la replicación de todos los equipos replicados en este grupo, debajo de Replicación, haga clic en **Eliminar**. Para obtener más información, consulte [Eliminar la replicación entrante del Core de destino](#).
 - Para eliminar los equipos con puntos de recuperación únicamente de este Core y descartar los puntos de recuperación, debajo de Solo puntos de recuperación, haga clic en **Quitar puntos de recuperación**.
 - Para modificar la etiqueta del grupo personalizado, solo en el caso de los grupos personalizados, seleccione **Editar**. Para obtener más información, consulte [Modificación de nombres de grupo personalizados](#).
 - Para quitar el grupo personalizado del menú de navegación, solo en el caso de los grupos personalizados, seleccione **Quitar etiqueta**. Para obtener más información, consulte [Eliminación de los grupos personalizados](#).

Visualización de todos los equipos de un grupo personalizado en una página

Si hace clic en el nombre de un grupo personalizado, accederá a la página Equipos que muestra todos los equipos de ese grupo personalizado. Ahí puede realizar algunas funciones del menú Acciones en todos los equipos o puede realizar acciones individuales seleccionando comandos de cada equipo concreto.

Acerca de la protección de varios equipos

Puede agregar dos o más equipos con Windows para su protección en el Core de Rapid Recovery simultáneamente mediante el Asistente para proteger varios equipos. Para proteger sus datos mediante Rapid Recovery, debe agregar las estaciones de trabajo y los servidores para la protección en la Core Console de Rapid Recovery; por ejemplo, su Exchange Server, SQL Server, servidor Linux, etc.

Al igual que al proteger equipos individuales, la protección de varios equipos simultáneamente requiere la instalación del software Rapid Recovery Agent en todos los equipos que desee proteger.

NOTA: Como excepción a la regla, si protege máquinas virtuales en VMware o un host ESXi, puede utilizar protección sin agentes. Para obtener más información, incluidas las restricciones para la protección sin agentes, consulte [Descripción Rapid Snap para Virtual](#).

Los equipos protegidos se deben configurar con una política de seguridad que permita que la instalación remota sea posible.

Para conectarse a los equipos, tienen que ser accesibles y estar encendidos.

Hay más de un método para implementar el software de Agent en varios equipos simultáneamente. Por ejemplo:

- Puede instalar el software Rapid Recovery Agent en varios equipos utilizando el Asistente para implementar el software de Agent. Para obtener más información, consulte [Implementación del software Rapid Recovery Agent en uno o más equipos](#).
- Puede implementar el software Rapid Recovery Agent como parte del Asistente para proteger varios equipos.

El proceso de protección de varios equipos incluye pasos opcionales a los que puede acceder si selecciona una configuración avanzada. Las opciones avanzadas incluyen las funciones de repositorio y el cifrado. Por ejemplo, puede especificar un repositorio de Rapid Recovery existente para guardar instantáneas o puede crear un nuevo repositorio. También puede especificar una clave de cifrado existente (o agregar una nueva clave de cifrado) para aplicarla a los datos guardados en el Core para los equipos que protege.

El flujo de trabajo del Asistente para proteger varios equipos puede variar ligeramente según su entorno. Por ejemplo, si el software Rapid Recovery Agent está instalado en los equipos que desea proteger, no se le pedirá que lo instale desde el asistente. Del mismo modo, si ya existe un repositorio en el Core, no se le pedirá que cree uno.

Al proteger varios equipos, siga los procedimientos adecuados en función de su configuración. Consulte las siguientes opciones para proteger varios equipos:

- [Protección de varias máquinas en un dominio de Active Directory](#)
- [Protección de varias máquinas en un host virtual VMware vCenter/ESX\(i\)](#)
- [Protección de varios equipos manualmente](#)

Protección de varias máquinas en un dominio de Active Directory

Utilice este procedimiento para proteger simultáneamente una o varias máquinas en un dominio de Active Directory.

- 1 En la Rapid Recovery Core Console, haga clic en el menú desplegable **Protect (Proteger)** y, a continuación, haga clic en **Protect Multiple Machines (Proteger varias máquinas)**.
Se abre el Protect Multiple Machines Wizard (Asistente de protección de varias máquinas).
- 2 En la página **Welcome (Bienvenido)** del asistente, seleccione una de las opciones siguientes:
 - Typical (Típica)
 - Advanced (show optional steps) (Avanzada [mostrar pasos opcionales])
- 3 Haga clic en **Next (Siguiente)**.
- 4 En la página **Connection (Conexión)** del asistente, lista desplegable **Source (Origen)**, seleccione **Active Directory**.
- 5 Introduzca la información del dominio y las credenciales de inicio de sesión como se describe en la tabla siguiente.

Tabla 79. Información sobre el dominio y las credenciales

Cuadro de texto	Descripción
Host (Host)	El nombre de host o la dirección IP del dominio de Active Directory.
(User name (Nombre de usuario)	El nombre de usuario que se utiliza para conectar al dominio; por ejemplo, Administrador (o, si la máquina está en un dominio, [nombre de dominio]\Administrador).
Password (Contraseña)	La contraseña segura que se utiliza para conectarse al dominio.

6 Haga clic en **Next (Siguiente)**.

7 En la página **Select Machines (Seleccionar máquinas)** del asistente, seleccione las máquinas que desee proteger.

El sistema verifica automáticamente cada máquina seleccionada.

8 Haga clic en **Next (Siguiente)**.

Si la página **Protection (Protección)** aparece en el asistente de protección de varias máquinas, vaya al Paso 11.

Si el software Agent no se ha distribuido en las máquinas que desee proteger, o si una de las máquinas que ha especificado no puede protegerse por otro motivo, las máquinas seleccionadas aparecerán en la página Warnings (Advertencias).

9 Opcionalmente, en la página **Warnings (Advertencias)** del asistente puede verificar cualquier máquina. Para ello, seleccione la máquina y, a continuación, haga clic en **Verify (Verificar)** en la barra de herramientas.

10 Opcionalmente, en la página **Warnings (Advertencias)**, seleccione **After Agent installation, restart the machines automatically (Reiniciar la máquina automáticamente después de la instalación de Agent)**.

NOTA: Dell recomienda esta opción. Debe reiniciar las máquinas de Agent antes de que se puedan proteger.

11 Si el estado indica que es posible acceder a la máquina, haga clic en **Next (Siguiente)** para instalar el software Rapid Recovery Agent. Se muestra la página **Protection (Protección)**.

12 En la página **Protection (Protección)** del asistente, seleccione el programa de protección adecuado tal como se describe a continuación.

- A continuación, para usar el programa de protección predeterminado, en la opción **Schedule Settings (Configuración de programación)**, seleccione Default protection (hourly snapshots of all volumes) (Protección predeterminada [instantáneas cada hora de todos los volúmenes]).
- Si desea definir un programa de protección diferente, en la opción Schedule Settings (Configuración de programación) seleccione **Custom protection (Protección personalizada)**.

13 Continúe con la configuración de la manera siguiente:

- Si en el asistente Protect Machine Wizard (Asistente de protección de máquina) ha seleccionado una configuración típica y ha especificado la protección predeterminada, haga clic en **Finish (Finalizar)** para confirmar la selección, cerrar el asistente y proteger la máquina especificada.

La primera vez que se agrega protección para una máquina, se inicia de inmediato la transferencia de una imagen base (una instantánea de todos los datos de los volúmenes protegidos) al repositorio en el Rapid Recovery Core, salvo que haya especificado pausar la protección inicialmente.

- Si ha seleccionado una configuración típica para el asistente y ha especificado la protección personalizada, haga clic en **Next (Siguiente)**. Consulte [Creación de calendarios de programación de protección personalizados](#).
- Si ha seleccionado Advanced configuration (Configuración avanzada) para el asistente Protect Machine Wizard (Asistente para proteger máquina), haga clic en **Next (Siguiente)** y vaya al [Paso 15](#) para ver las opciones de repositorio y cifrado.
- Si ha seleccionado una configuración típica para el asistente Protect Machine Wizard (Asistente para proteger máquina) y ha especificado una protección personalizada, haga clic en **Next (Siguiente)** para configurar un programa de protección personalizado. Para obtener más información sobre cómo definir un programa de protección, consulte [Creación de calendarios de programación de protección personalizados](#).

14 Haga clic en **Next (Siguiente)**.

15 En la página **Repository (Repositorio)** del asistente, seleccione una de las opciones siguientes:

- Si ya tiene un repositorio y desea guardar los datos de esta máquina para protegerlos en el repositorio existente, realice lo siguiente:
 - 1 Seleccione **Use an existing repository (Usar un repositorio existente)**.

- 2 Seleccione un repositorio existente de la lista.
- 3 Haga clic en **Next (Siguiente)**.

Aparece la página **Encryption (Cifrado)**. Vaya al Paso 19 si desea definir el cifrado opcionalmente.

- Si desea crear un repositorio existente), seleccione **Create a Repository (Crear un repositorio)** y, a continuación, realice los pasos siguientes.

- 1 En la página **Repository (Repositorio)**, introduzca la información que se describe en la tabla siguiente.

Tabla 80. Agregar configuración del nuevo repositorio

Cuadro de texto	Descripción
Repository Name (Nombre del repositorio)	Escriba el nombre de pantalla del repositorio. De manera predeterminada, este cuadro de texto se compone de la palabra Repositorio y un número, que coincide con el número de repositorios que existen para este Core. Por ejemplo, si este es el primer repositorio, el nombre predeterminado es Repositorio 1. Cambie el nombre según sea necesario. Los nombres de repositorio deben contener entre 1 y 40 caracteres alfanuméricos, incluidos espacios. No utilice caracteres prohibidos ni frases prohibidas.
Concurrent Operations (Operaciones simultáneas)	Define el nombre de solicitudes simultáneas que desea que admita el repositorio. De manera predeterminada, el valor es 64.
Comments (Comentarios)	Opcionalmente, introduzca una nota descriptiva sobre este repositorio. Puede introducir hasta 254 caracteres. Por ejemplo, escriba DVM Repositorio 2 .

- 2 Haga clic en **Add Storage Location (Agregar ubicación de almacenamiento)** para definir la ubicación de almacenamiento específica o el volumen del repositorio. Este volumen debe ser la ubicación de almacenamiento principal.

⚠ PRECAUCIÓN: Defina una carpeta específica dentro de la raíz para la ubicación de almacenamiento del repositorio. No especifique la ubicación raíz. Por ejemplo, utilice E:\Repository\, no E:\. Si el repositorio que va a crear en este paso se elimina posteriormente, se eliminarán todos los archivos incluidos en la ubicación de almacenamiento de su repositorio. Si define la ubicación de almacenamiento en la raíz, todos los demás archivos en el volumen (ej., E:\) se eliminan, lo que podría provocar una pérdida de datos catastrófica.

Aparecerá el cuadro de diálogo **Add Storage Location (Agregar ubicación de almacenamiento)**.

- 3 Haga clic en **Add Storage Location (Agregar ubicación de almacenamiento)** para definir la ubicación de almacenamiento específica o el volumen del repositorio. Este volumen debe ser la ubicación de almacenamiento principal.
 - 4 En el área **Storage Location (Ubicación de almacenamiento)**, especifique cómo desea agregar el archivo para la ubicación de almacenamiento. Puede agregar un volumen de almacenamiento conectado localmente (por ejemplo, un almacenamiento de conexión directa, una red de área de almacenamiento o un almacenamiento de red conectado). También puede especificar un volumen de almacenamiento en una ubicación compartida del Common Internet File System (Sistema de archivos de Internet común - CIFS)
- Haga clic en **Add the file on local disk (Agregar el archivo en disco local)** para especificar una máquina local y, a continuación, indique la información según se describe en la tabla siguiente.

Tabla 81. Configuración de disco local

Cuadro de texto	Descripción
Data Path (Ruta de datos)	Introduzca la ubicación para almacenar los datos protegidos. Por ejemplo, escriba X:\Repository\Data. Al especificar la ruta, escriba solo caracteres alfanuméricos, un guión o un punto (para separar los nombres de host y los dominios). Puede utilizar la barra diagonal invertida únicamente para definir los niveles en la ruta. No utilice espacios. No se admite ningún otro símbolo ni caracteres de puntuación.
Metadata path (Ruta de metadatos)	Introduzca la ubicación para almacenar los metadatos protegidos.

Cuadro de texto	Descripción

Por ejemplo, escriba X:\Repository\Metadata.

Al especificar la ruta, escriba solo caracteres alfanuméricos, un guión o un punto (para separar los nombres de host y los dominios). Puede utilizar la barra diagonal invertida únicamente para definir los niveles en la ruta. No utilice espacios. No se admite ningún otro símbolo ni caracteres de puntuación.

- O bien, seleccione **Add file on CIFS share (Agregar archivo en recurso compartido CIFS)** para especificar una ubicación compartida de red y, a continuación, indique la información según se describe en la tabla siguiente.

Tabla 82. Credenciales del recurso compartido CIFS

Cuadro de texto	Descripción

UNC Path (Ruta UNC)

Introduzca la ruta de acceso para la ubicación del recurso compartido de red.
Si la ubicación se encuentra en la raíz, cree un nombre de carpeta específico (por ejemplo, Repository).

La ruta debe empezar por \\. Al especificar la ruta, escriba solo caracteres alfanuméricos, un guión o un punto (para separar los nombres de host y los dominios). Las letras de la "a" a la "z" no distinguen mayúsculas de minúsculas. No utilice espacios. No se admite ningún otro símbolo ni caracteres de puntuación.

(User name (Nombre de usuario)

Especifique un nombre de usuario para el acceso a la ubicación del recurso compartido de red.

Password (Contraseña)

Especifique una contraseña para acceder a la ubicación del recurso compartido de red.

- 5 En el área **Storage Configuration (Configuración de almacenamiento)**, haga clic en **More Details (Más detalles)** e introduzca los detalles de la ubicación de almacenamiento según se describe en la tabla siguiente.

Tabla 83. Detalles de la configuración de almacenamiento

Cuadro de texto	Descripción

Size (Tamaño)

Establezca el tamaño o capacidad de la ubicación de almacenamiento. El tamaño mínimo es 1 GB. El valor predeterminado es 250 GB. Puede elegir entre las opciones siguientes:

- GB
- TB

① | NOTA: El tamaño que especifique no puede superar el tamaño del volumen.

Si la ubicación de almacenamiento es un volumen de sistema de archivos de nueva tecnología (NTFS) que tiene Windows XP o Windows 7 instalado, el límite de tamaño de archivo es 16 TB.

Si la ubicación de almacenamiento es un volumen NTFS que ejecuta Windows 8, 8.1, Windows 10 o Windows Server 2012, 2012 R2, el límite de tamaño de archivo es 256 TB.

① | NOTA: Para que Rapid Recovery pueda validar el sistema operativo, el Instrumental de administración de Windows (WMI) debe estar instalado en la ubicación de almacenamiento deseada.

Write Caching Policy (Política de escritura en caché)

La política de escritura en caché de controla cómo se utiliza el Windows Cache Manager (Administrador de caché de Windows) en el repositorio y ayuda a ajustar el repositorio para un rendimiento óptimo en diferentes configuraciones.

Establezca el valor en una de las opciones siguientes:

- On (Activado)
- Off (Desactivado)
- Sync (Sincronizar)

Cuadro de texto	Descripción
	Si se establece en On (Activado), que es el valor predeterminado, Windows controla el almacenamiento en caché. Esto es adecuado para Windows 10, y para las versiones de Windows Server 2012 y posteriores.
	NOTA: Si se establece la política de escritura en caché en On (Activado), se mejora el rendimiento. Si utiliza Windows Server 2008 SP2 o Windows Server 2008 R2 SP2, el valor recomendado es Off (Desactivado). Si se establece en Off (Desactivado), Rapid Recovery controla el almacenamiento en caché. Si se establece en Sync (Sincronizar), Windows controla el almacenamiento en caché así como la entrada/salida sincrónica.
Bytes per sector (Bytes por sector)	Especifique el número de bytes que desee incluir en cada sector. El valor predeterminado es 512.
Average Bytes per Record (Número promedio de bytes por registro)	Especifique el número promedio de bytes por segundo. El valor predeterminado es 8192.

6 Haga clic en **Next (Siguiente)**.

Si ha seleccionado la opción **Advanced (Avanzado)** en el paso 1, aparece la página **Encryption (Cifrado)**.

- 16 De manera opcional, para **activar** el cifrado en la página de cifrado, seleccione **Enable Encryption (Activar cifrado)**. Aparecerán los campos de clave de cifrado en la página Encryption (Cifrado).

NOTA: Si activa el cifrado, se aplicará a los datos para todos los volúmenes protegidos de esta máquina. Puede cambiar la configuración posteriormente en la pestaña Encryption Keys (Claves de cifrado) de la Rapid Recovery Core Console. Para obtener más información sobre el cifrado, consulte el tema [Descripción de las claves de cifrado](#).

PRECAUCIÓN: Rapid Recovery utiliza cifrado AES de 256 bits en el modo Encadenamiento de bloques de cifrado (CBC) con claves de 256 bits. Mientras el uso de cifrado es opcional, Dell recomienda encarecidamente que establezca una clave de cifrado y que proteja la frase de contraseña que defina. Guarde la frase de contraseña en un lugar seguro, ya que es fundamental para la recuperación de datos. Sin una frase de contraseña, la recuperación de datos no es posible.

- 17 Si desea cifrar estas máquinas protegidas con una clave de cifrado que ya está definida en este Rapid Recovery Core, seleccione **Encrypt data using an existing Encryption key (Cifrar los datos mediante una clave de cifrado existente)** y seleccione la clave apropiada en el menú desplegable.
- Continúe con el Paso 19.
- 18 Si desea agregar una clave de cifrado para el Core y aplicar dicha clave a estas máquinas protegidas, introduzca la información según se describe en la tabla siguiente.

Tabla 84. Configuración de clave de cifrado

Cuadro de texto	Descripción
Name (Nombre)	Introduzca un nombre para la clave de cifrado. Los nombres de la clave de cifrado debe contener entre 1 y 130 caracteres alfanuméricos. No se podrá incluir caracteres especiales, tales como la barra diagonal inversa, barra diagonal, barra vertical, dos puntos, asterisco, comilla, signo de interrogación, paréntesis de apertura o cierre o almohadilla.
Description (Descripción)	Escriba un comentario para la clave de cifrado. Esta información se muestra en el campo de descripción cuando se ven las claves de cifrado desde Core Console.
Passphrase (Frase de contraseña)	Introduzca la frase de contraseña usada para controlar el acceso. Se recomienda evitar el uso de los caracteres especiales mencionados anteriormente.

Cuadro de texto	Descripción
	Registre la frase de contraseña en un lugar seguro. Dell Support no puede recuperar una frase de contraseña. Una vez que haya creado una clave de cifrado y la haya aplicado a una o varias máquinas protegidas, no podrá recuperar los datos si pierde la frase de contraseña.
Confirm Passphrase (Confirmar frase de contraseña)	Vuelva a introducir la frase de contraseña que acaba de introducir.

- 19 Haga clic en **Finish (Finalizar)** para guardar y aplicar la configuración.
El asistente se cerrará.
- 20 Si se ha mostrado la página **Warning (Advertencia)** y está satisfecho con las opciones seleccionadas, haga clic de nuevo en **Finish (Finalizar)**.

Si es necesario, el software Rapid Recovery se implementa en las máquinas especificadas, y se agregan las máquinas para su protección en el Core.

Protección de varias máquinas en un host virtual VMware vCenter/ESX(i)

Utilice este procedimiento para proteger simultáneamente una o varias máquinas en un host virtual VMware vCenter/ESX(i).

⚠ PRECAUCIÓN: Si utiliza protección sin Agent, Dell recomienda que imite la protección sin Agent a no más de 200 máquinas virtuales a la vez. Por ejemplo, no seleccione más de 200 de las máquinas virtuales al usar el asistente Protect Multiple Machines Wizard (Asistente de protección de varias máquinas). Si protege más de 200 máquinas virtuales, reducirá el rendimiento. No hay límite en cuántas máquinas virtuales puede proteger sin Agent un Core a lo largo del tiempo. Por ejemplo, puede proteger 200 máquinas virtuales hoy y otras 200 máquinas virtuales mañana.

- 1 En la Core Console de Rapid Recovery, haga clic en el menú desplegable **Protect (Proteger)** y, a continuación, haga clic en **Protect Multiple Machines (Proteger varias máquinas)**.
Se abrirá el Protect Multiple Machines Wizard (Asistente de protección de varias máquinas).
- 2 En la página Welcome (Bienvenida), seleccione una de las siguientes opciones:
 - Typical (Típica)
 - Advanced (show optional steps) (Avanzada [mostrar pasos opcionales])
- 3 Haga clic en **Siguiente**.
- 4 En la página Connection (Conexión) del asistente, en la lista desplegable **Source (Origen)**, seleccione **vCenter / ESX(i)**.
- 5 Introduzca la información del host y las credenciales de inicio de sesión como se describe en la tabla siguiente.

Tabla 85. Configuración de conexión de VCenter/ESX(i)

Cuadro de texto	Descripción
Host	El nombre o la dirección IP del host virtual de VMware vCenter Server/ESX(i).
Port (Puerto)	El puerto utilizado para conectarse al host virtual. El valor predeterminado es 443.
User name (Nombre de usuario)	El nombre de usuario utilizado para conectarse a la máquina virtual; por ejemplo, Administrador o, si la máquina está en un dominio, [nombre de dominio]\Administrador.
Password (Contraseña)	Introduzca la contraseña que utiliza para conectarse al host virtual.

- Para utilizar protección sin Agent, seleccione **Protect selected VMs Agentlessly (Proteger las máquinas virtuales seleccionadas sin Agent)**, y, a continuación, consulte [Protección de máquinas virtuales vCenter/ESXi sin Rapid Recovery Agent](#).
- 6 En la página Select Machines (Seleccionar página Máquinas), seleccione una de las siguientes opciones del menú desplegable:
 - Hosts and Clusters (Hosts y clústeres)
 - VMs and Templates (VM y plantillas)

- 7 Amplíe la lista de máquinas y seleccione las máquinas virtuales que desea proteger.
Aparece una notificación si Rapid Recovery detecta que hay máquina fuera de línea o no tiene VMware Tools instalado.
- 8 Haga clic en **Siguiente**.
- 9 En la página Adjustments (Ajustes), escriba las credenciales de cada máquina en el siguiente formato:
hostname::username::password.

NOTA: Introduzca una máquina en cada línea.

- 10 Haga clic en **Siguiente**.
Si la página Protection (Protección) se abre a continuación en el Protect Multiple Machines Wizard Asistente de protección de varias máquinas, vaya al [paso 14](#).
Si el software del Agent no se ha distribuido en las máquinas que desea proteger, o si cualquiera de las máquinas que ha especificado no se puede proteger por otro motivo, las máquinas seleccionadas aparecerán en la página Warnings (Avisos).
- 11 De manera opcional, en la página Avisos, puede verificar cualquier máquina. Para ello, seleccione la máquina y, a continuación, haciendo clic en **Verify (Verificar)** en la barra de herramientas.
- 12 De manera opcional, en la página Avisos, seleccione **After Agent installation, restart the machines automatically (Reiniciar las máquinas automáticamente después de la instalación del Agent)**.

NOTA: Dell recomienda esta opción. Debe reiniciar las máquinas del Agent para poder protegerlas.

- 13 Si el estado indica que se puede acceder a la máquina, haga clic en **Next (Siguiente)** para instalar el software del Agent.
Aparecerá la página Protection (Protección).
- 14 En la página Protection (Protección), seleccione el programa de protección que corresponda como se describe a continuación.
 - A continuación, para usar la programación de protección predeterminada, en la opción **Schedule Settings (Configuración de programación)**, seleccione Default protection (hourly snapshots of all volumes) (Protección predeterminada [instantáneas cada hora de todos los volúmenes]).
 - Si desea definir una programación de protección diferente, en la opción Schedule Settings (Configuración de programación), seleccione **Custom protection (Protección personalizada)** y, a continuación, haga clic en Next (Siguiente).
- 15 Continúe con la configuración de la manera siguiente:
 - Si ha seleccionado una configuración Typical (Típica) del Protect Machine Wizard (Asistente para proteger la máquina) y especificado la protección predeterminada, a continuación, haga clic en **Finish (Finalizar)** para confirmar la selección, cierre el asistente y proteja la máquina especificada.
La primera vez que se agrega protección para una máquina, se inicia de inmediato la transferencia de una imagen base (una instantánea de todos los datos de los volúmenes protegidos) al repositorio en el Core de Rapid Recovery, salvo que haya especificado pausar la protección inicialmente.
 - Si ha seleccionado una configuración típica del asistente **Protect Machine Wizard (Asistente de protección de máquinas)** y ha especificado una protección personalizada, haga clic en Next (Siguiente) para configurar una programación de protección personalizada. Para obtener más información sobre cómo definir una programación de protección personalizada, consulte [Creación de calendarios de programación de protección personalizados](#).
 - Si ha seleccionado la configuración avanzada para el Protect Machine Wizard (Asistente de protección de máquina), haga clic en **Next (Siguiente)** y continúe en el [paso 17](#) para ver las opciones de repositorio y cifrado.
 - Si ha seleccionado la configuración típica para el Protect Machine Wizard (Asistente de protección de máquinas) y ha especificado una protección personalizada, haga clic en **Next (Siguiente)** para configurar una programación de protección personalizada. Para obtener más información sobre cómo definir una programación de protección, consulte [Creación de calendarios de programación de protección personalizados](#).
- 16 Haga clic en **Siguiente**.
- 17 En la página **Repository (Repositorio)**, realice una de las acciones siguientes:
 - Si ya tiene un repositorio y desea que se almacenen los datos de esta máquina para protegerlos en la repositorio existente, haga lo siguiente:
 - 1 Seleccione **Use an existing repository (Usar un repositorio existente)**.
 - 2 Seleccione un repositorio existente de la lista.
 - 3 Haga clic en **Siguiente**.
Se abrirá la página **Encryption (Cifrado)**. Vaya al [paso 18](#) para definir el cifrado opcionalmente.
 - Si desea crear un repositorio existente, seleccione **Create a Repository (Crear un repositorio)** y, a continuación, realice los pasos siguientes.

- 1 En la página **Repository (Repositorio)**, introduzca la información que se describe en la tabla siguiente.

Tabla 86. Agregar nueva configuración del repositorio

Cuadro de texto	Descripción
Nombre del repositorio	Escriba el nombre del repositorio. De manera predeterminada, este cuadro de texto se compone de la palabra Repository y un número, que corresponde con el número de repositorios de este Core. Por ejemplo, para el primer repositorio, el nombre sugerido es Repository 1. Cambie el nombre si es necesario. Los nombres de los repositorios deben contener entre 1 y 40 caracteres alfanuméricos, incluidos espacios. No utilice caracteres prohibidos ni frases prohibidas.
Concurrent Operations	Define el nombre de solicitudes concurrentes que desea que admita el repositorio. De manera predeterminada, el valor es 64.
Comments	Opcionalmente, introduzca una nota descriptiva sobre este repositorio. Puede introducir hasta 254 caracteres. Por ejemplo, escriba DVM Repositorio 2 .

- 2 Haga clic en **Add Storage Location (Agregar ubicación de almacenamiento)** para definir la ubicación de almacenamiento específico o el volumen del repositorio. Este volumen debe ser la ubicación principal del almacenamiento..

⚠ PRECAUCIÓN: Defina una carpeta dedicada dentro de la raíz para la ubicación del almacenamiento del repositorio. No especifique la ubicación raíz. Por ejemplo, utilice E:\Repository\, no E:\. Si elimina el repositorio que va a crear en este paso más tarde, se eliminarán todos los archivos de la ubicación del almacenamiento del repositorio se eliminan. Si define la ubicación de almacenamiento en la raíz, todos los demás archivos del volumen (p. ej., E:\) se eliminarán, lo que podría provocar una pérdida de datos enorme.

Aparecerá el cuadro de diálogo **Add Storage Location (Agregar ubicación de almacenamiento)**.

- 3 Haga clic en **Add Storage Location (Agregar ubicación de almacenamiento)** para definir la ubicación de almacenamiento específico o el volumen del repositorio. Este volumen debe ser la ubicación principal del almacenamiento..
- 4 En el área de la **Ubicación de almacenamiento**, especifique cómo se agregará el archivo de la ubicación de almacenamiento. Puede elegir agregar un volumen de almacenamiento conectado de forma local (por ejemplo, como almacenamiento de conexión directa, una red de área de almacenamiento, o almacenamiento conectado a la red). También puede especificar un volumen de almacenamiento en una ubicación compartida Sistema de archivos de Internet común (CIFS).
 - Haga clic en **Add the file on local disk (Agregar el archivo en el disco local)** para especificar una máquina local y, a continuación, introduzca la información descrita en la siguiente tabla.

Tabla 87. Configuración del disco local

Cuadro de texto	Descripción
Ruta de acceso a datos	Introduzca la ubicación para almacenar los datos protegidos. Por ejemplo, escriba X:\Repository\Data. Al especificar la ruta, escriba solo caracteres alfanuméricos, un guion o un punto (para separar los nombres de host de los dominios). Puede utilizar la barra diagonal invertida solo para definir los niveles en la ruta de acceso. No utilice espacios. No se admite ningún otro símbolo o carácter de puntuación.
Ruta de acceso a metadatos	Introduzca la ubicación para almacenar los metadatos protegidos. Por ejemplo, escriba X:\Repository\Metadata. Al especificar la ruta, escriba solo caracteres alfanuméricos, un guion o un punto (para separar los nombres de host de los dominios). Puede utilizar la barra diagonal invertida solo para definir los niveles en la ruta de acceso. No utilice espacios. No se admite ningún otro símbolo o carácter de puntuación.

- También puede hacer clic en **Add file on CIFS share (Agregar archivo en CIFS compartido)** para especificar una ubicación compartida de red y, a continuación, indique la información según se describe en la tabla siguiente.

Tabla 88. Credenciales del CIFS compartido

Cuadro de texto	Descripción
Ruta de acceso UNC	Introduzca la ruta de acceso para la ubicación del recurso compartido de red. Si la ubicación se encuentra en la raíz, cree un nombre de carpeta dedicado (por ejemplo, Repository). La extensión del archivo debe empezar con \\. Al especificar la ruta, escriba solo caracteres alfanuméricos, un guion o un punto (para separar los nombres de host de los dominios). Las letras de la "a" a la "z" no distinguen mayúsculas de minúsculas. No utilice espacios. No se admite ningún otro símbolo o carácter de puntuación.
Nombre de usuario	Especifique un nombre de usuario para el acceso a la ubicación del recurso compartido de red.
Contraseña	Especifique una contraseña para acceder a la ubicación del recurso compartido de red.

- 5 En el área de **Configuración de almacenamiento**, haga clic en **More Details (Obtener más detalles)** e introduzca los detalles para la ubicación de almacenamiento como se describen en la tabla siguiente.

Tabla 89. Detalles de configuración del almacenamiento

Cuadro de texto	Descripción
Tamaño	Establezca el tamaño o capacidad para la ubicación de almacenamiento. El tamaño mínimo es 1 GB. El valor predeterminado es 250 GB. Puede elegir entre las siguientes opciones: - GB - TB NOTA: El tamaño que especifique no puede superar el tamaño del volumen. Si la ubicación de almacenamiento es un volumen de sistema de archivos de nueva tecnología (NTFS) que tiene Windows XP o Windows 7 instalado, el límite de tamaño de archivo es 16 TB. Si la ubicación de almacenamiento es un volumen NTFS con Windows 8, Windows 8.1, Windows 10 o Windows Server 2012, 2012 R2, el límite de tamaño de archivo es 256 TB. NOTA: Para que Rapid Recovery pueda validar el sistema operativo, el instrumental de administración de Windows (WMI) debe estar instalado en la ubicación de almacenamiento deseada.
Política de escritura en caché	La política de escritura en caché de controla cómo se utiliza el Windows Cache Manager (Administrador de caché de Windows) en el repositorio y ayuda a ajustar el repositorio para un rendimiento óptimo en diferentes configuraciones. Establezca el valor en una de las opciones siguientes: - Encendido - Off (Apagado) - Sincronizar Si se establece en Activado, que es el valor predeterminado, Windows controla el almacenamiento en caché. Esto es adecuado para Windows 10, las versiones de Windows Server 2012 y posteriores. NOTA: Si se establece la política de escritura en caché en Activado, se mejora el rendimiento. Si utiliza Windows Server 2008 SP2 o Windows Server 2008 R2 SP2, el valor recomendado es Desactivado. Si se establece en Desactivado, Rapid Recovery controla el almacenamiento en caché. Si se establece en Sync (Sincronizar), Windows controla el almacenamiento en caché así como la entrada/salida sincrónica.
Bytes por sector	Especifique el número de bytes que desee incluir en cada sector. El valor predeterminado es 512.

Cuadro de texto	Descripción

Promedio de bytes por segundo	Especifique el número promedio de bytes por segundo. El valor predeterminado es 8192.

6 Haga clic en **Siguiente**.

Si ha seleccionado la opción **Avanzado** en el paso 1, aparecerá la página **Encryption (Cifrado)**.

18 De manera opcional, en la página Cifrado, seleccione **Enable Encryption (Activar el cifrado)** para activar el cifrado.

Aparecerán los campos de clave de cifrado en la página Encryption (Cifrado).

NOTA: Si activa el cifrado, se aplicará a los datos de todos los volúmenes protegidos de esta máquina de Agent. Puede cambiar la configuración posteriormente en la pestaña Configuration (Configuración) en la Core Console de Rapid Recovery. Para obtener más información sobre el cifrado, consulte el tema [Descripción de las claves de cifrado](#).

PRECAUCIÓN: Rapid Recovery utiliza cifrado AES de 256 bits en el modo Encadenamiento de bloques de cifrado (CBC) con claves de 256 bits. Aunque el uso de cifrado es opcional, Dell recomienda encarecidamente que establezca una clave de cifrado y que proteja la frase de contraseña que defina. Guarde la frase de contraseña en un lugar seguro, ya que es fundamental para la recuperación de datos. Sin una frase de contraseña, la recuperación de datos no es posible.

19 Si desea cifrar estas máquinas protegidas con una clave de cifrado que ya está definida en este Core de Rapid Recovery, seleccione **Encrypt data using an existing Encryption key (Cifrar los datos mediante una clave de cifrado existente)** y seleccione la clave apropiada en el menú desplegable.

Continúe con el [paso 21](#).

20 Si desea agregar una nueva clave de cifrado para el Core y aplicar dicha clave de estas máquinas protegidas, introduzca la información según se describe en la tabla siguiente.

Tabla 90. Configuración de la clave de cifrado

Cuadro de texto	Descripción
Nombre	Introduzca un nombre para la clave de cifrado. Los nombres clave de cifrado debe contener entre 1 y 130 caracteres alfanuméricos. No se podrá incluir caracteres especiales como barra diagonal inversa, barra diagonal, canalización, dos puntos, asterisco, comilla, signo de interrogación, paréntesis y corchetes abiertos o cerrados, & y gato.
Descripción	Escriba un comentario para la clave de cifrado. Esta información se muestra en el campo Descripción al ver las claves de cifrado desde la Core Console.
Passphrase	Introduzca la frase de contraseña usada para controlar el acceso. Se recomienda evitar el uso de caracteres especiales mencionados anteriormente. Guarde la frase de contraseña en un lugar seguro. La Asistencia de Dell no puede recuperar una frase de contraseña. Una vez que haya creado una clave de cifrado y la haya aplicado a una o más máquinas protegidas, no podrá recuperar los datos si pierde la frase de contraseña.
Confirm Passphrase	Vuelva a introducir la frase de contraseña que acaba de introducir.

21 Haga clic en **Finish (Finalizar)** para guardar y aplicar la configuración.

22 Si se muestra la página Warning (Advertencia), pero aún está satisfecho con sus elecciones, haga clic en **Finish (Finalizar)** nuevamente.

El software del Agent de Rapid Recovery se implementa en las máquinas especificadas, si es necesario, y las máquinas se agregan a la lista de máquinas protegidas en el Core.

Protección de varios equipos manualmente

Utilice este procedimiento para introducir manualmente cada uno de los equipos que desea proteger. Se utiliza, por ejemplo, al proteger equipos Linux.

- 1 En la Core Console de Rapid Recovery, haga clic en el menú desplegable **Proteger** y, a continuación, haga clic en **Proteger varios equipos**.
Se abre el Asistente para proteger varios equipos.
 - 2 En la página de **bienvenida**, seleccione una de las opciones siguientes:
 - Típicas
 - Avanzado (mostrar pasos opcionales)
 - 3 Haga clic en **Siguiente**.
 - 4 En la página del asistente **Conexión**, de la lista desplegable **Origen**, seleccione **Manualmente**.
 - 5 Haga clic en **Siguiente**.
 - 6 En la página **Seleccionar equipos**, introduzca los detalles de equipo en el cuadro de diálogo en el formato `hostname::username::password::port`. La configuración de puertos es opcional. Los ejemplos incluyen:
`10.255.255.255::administrator::&11@yYz90z::8006`
`abc-host-00-1::administrator::99!zU$ø83r::168`
 - 7 Haga clic en **Siguiente**.
Si a continuación aparece la página **Protección** en el Asistente para proteger varios equipos, vaya al [paso 11](#).
Si el software Agent todavía no se ha implementado en los equipos que desee proteger o si alguno de los equipos que especificó no puede protegerse por cualquier otro motivo, los equipos seleccionados aparecerán en la página **Advertencias**.
 - 8 Opcionalmente, en la página **Advertencias de equipos**, puede verificar cualquier equipo seleccionando el equipo y, a continuación, haciendo clic en **Verificar** en la barra de herramientas.
 - 9 Opcionalmente, en la página **Advertencias de equipos**, seleccione **Tras la instalación de Agent, reinicie los equipos automáticamente**.
-  **NOTA:** Dell recomienda esta opción. Debe reiniciar los equipos Agent antes de poder protegerlas. Reiniciarlos garantiza que el servicio de Agent esté en ejecución y que el módulo del kernel adecuado se utilice para proteger el equipo, si corresponde.
- 10 Si el estado indica que puede llegarse al equipo, haga clic en **Siguiente** para instalar el software Agent.
Aparecerá la página **Protección**.
 - 11 En la página **Protección**, seleccione la programación de protección adecuada como se describe a continuación.
 - Si desea utilizar el calendario de programación de protección predeterminado, en la opción Configuración de calendario de programación, seleccione **Protección predeterminada (instantáneas de todos los volúmenes cada hora)**.
 - Si desea definir una programación de protección diferente, en la opción Configuración de programa, seleccione **Protección personalizada**.
 - 12 Continúe con su configuración del modo siguiente:
 - Si ha seleccionado una configuración Típica para el Asistente para proteger un equipo y ha especificado una protección predeterminada, haga clic en **Finalizar** para confirmar sus opciones, cierre el asistente y proteja el equipo que ha especificado.
La primera vez que se agrega protección para una máquina, se inicia de inmediato la transferencia de una imagen base (una instantánea de todos los datos de los volúmenes protegidos) al repositorio en el Core de Rapid Recovery, salvo que haya especificado pausar la protección inicialmente.
 - Si ha seleccionado una configuración Típica para el Asistente para proteger un equipo y ha especificado una protección personalizada, haga clic en **Siguiente** para consultar [Creación de calendarios de programación de protección personalizados](#).
 - Si ha seleccionado una configuración avanzada para el Asistente para proteger un equipo, así como la protección predeterminada, haga clic en **Siguiente** y continúe en el [paso 14](#) para ver las opciones de repositorio y cifrado.
 - Si ha seleccionado la configuración avanzada para el Asistente para proteger un equipo y ha especificado una protección personalizada, haga clic en **Siguiente** para configurar un calendario de programación de protección personalizado. Para obtener información detallada sobre cómo definir un calendario de programación de protección personalizado, consulte [Creación de calendarios de programación de protección personalizados](#).
 - 13 En la página **Repositorio**, realice una de las acciones siguientes:

- Si ya tiene un repositorio y desea almacenar los datos de este equipo para la protección del repositorio existente, realice una de las acciones siguientes:
 - 1 Seleccione **Usar un repositorio existente**.
 - 2 Seleccione un repositorio existente de la lista.
 - 3 Haga clic en **Siguiente**.

Se abrirá la página de **Cifrado**. Vaya al [paso 19](#) para definir el cifrado de manera opcional.

- Si desea crear un repositorio, seleccione **Crear un repositorio** y, a continuación, realice los siguientes pasos.
 - 1 En **Repositorio**, introduzca la información que se describe en la tabla siguiente.

Tabla 91. Parámetros de Agregar repositorio nuevo

Cuadro de texto	Descripción
Nombre de repositorio	Introduzca el nombre mostrado del repositorio. De manera predeterminada, este cuadro de texto incluye el término Repositorio y un número, que se corresponde con el número de repositorios de este Core. Por ejemplo, si se trata del primer repositorio, el nombre predeterminado es Repositorio 1. Cambie el nombre según sea necesario. Los nombres del repositorio contienen entre 1 y 40 caracteres alfanuméricos, incluidos los espacios. No utilice caracteres prohibidos ni frases prohibidas.
Operaciones simultáneas	Defina el número de solicitudes simultáneas que desee que admita el repositorio. De manera predeterminada, el valor es 64.
Comentarios	Opcionalmente, escriba una nota descriptiva sobre este repositorio. Puede introducir hasta 254 caracteres. Por ejemplo, escriba Repositorio DVM 2 .

- 2 Haga clic en **Agregar ubicación de almacenamiento** para definir la ubicación de almacenamiento o el volumen específicos para el repositorio. Este volumen debe ser la ubicación de almacenamiento principal.

⚠ PRECAUCIÓN: Defina una carpeta específica en la raíz para la ubicación de almacenamiento del repositorio. No especifique la ubicación raíz. Por ejemplo, utilice E:\Repository\ en lugar de E:\. Si el repositorio que está creando en este paso se elimina más adelante, se eliminarán todos los archivos en la ubicación de almacenamiento de su repositorio. Si define la ubicación de almacenamiento en la raíz, el resto de archivos del volumen (p. ej., E:\) se eliminan, lo que podría derivar en una pérdida grave de datos.

Aparecerá el cuadro de diálogo **Agregar ubicación de almacenamiento**.

- 3 Haga clic en **Agregar ubicación de almacenamiento** para definir la ubicación de almacenamiento o el volumen específicos para el repositorio. Este volumen debe ser la ubicación de almacenamiento principal.
- 4 En el área **Ubicación del almacenamiento**, especifique cómo agregar el archivo para la ubicación de almacenamiento. Puede elegir si desea agregar un volumen de almacenamiento conectado de forma local (como un almacenamiento de conexión directa, una red de área de almacenamiento o un almacenamiento conectado a la red). También podría especificar un volumen de almacenamiento en una ubicación compartida de sistema de archivos de Internet comunes (CIFS).
 - Seleccione **Agregar el archivo en disco local** para especificar un equipo local y, a continuación, introduzca la información según se describe en la siguiente tabla.

Tabla 92. Parámetros de Disco local

Cuadro de texto	Descripción
Ruta de acceso a datos	Introduzca la ubicación para almacenar los datos protegidos. Por ejemplo, introduzca X:\Repository\Data. Quando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guión y el punto (solo para separar nombres de host y dominios). Puede utilizar el carácter de barra invertida solo para definir los niveles de la ruta. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.
Ruta de acceso a metadatos	Introduzca la ubicación para almacenar los metadatos protegidos. Por ejemplo, introduzca X:\Repository\Metadata.

Cuadro de texto	Descripción

Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guión y el punto (solo para separar nombres de host y dominios). Puede utilizar el carácter de barra invertida solo para definir los niveles de la ruta. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.

- O, seleccione **Agregar archivo en recurso compartido CIFS** para especificar una ubicación de uso compartido de red y, a continuación, introduzca la información según se describe en la siguiente tabla.

Tabla 93. Credenciales de recurso compartido CIFS

Cuadro de texto	Descripción

Ruta de acceso a UNC	Introduzca la ruta de acceso de la ubicación de uso compartido de red. Si esta ubicación está en la raíz, defina un nombre de carpeta específico (por ejemplo, Repository). La ruta de acceso debe comenzar por \\. Cuando especifique la ruta de acceso, utilice solo caracteres alfanuméricos, el guión y el punto (solo para separar nombres de host y dominios). Las letras de la a a la z no distinguen entre mayúsculas y minúsculas. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.
Nombre de usuario	Especifique un nombre de usuario para el acceso a la ubicación compartida de red.
Contraseña	Especifique una contraseña para acceder a la ubicación de uso compartido de red.

- 5 En el área **Configuración de almacenamiento**, haga clic en **Más detalles** e introduzca los detalles para la ubicación de almacenamiento según se describen en la siguiente tabla.

Tabla 94. Detalles de configuración de almacenamiento

Cuadro de texto	Descripción
Tamaño	Defina el tamaño o la capacidad de la ubicación del archivo. El tamaño mínimo es de 1 GB. El valor predeterminado es 250 GB. Puede elegir entre las siguientes opciones: • GB • TB ① NOTA: El tamaño que especifique no puede superar el tamaño del volumen. Si la ubicación del almacenamiento es un volumen New Technology File System (NTFS) utilizando Windows XP o Windows 7, el límite de tamaño del archivo es 16 TB. Si la ubicación de almacenamiento es un volumen NTFS que utiliza Windows 8, 8.1, Windows 10 o Windows Server 2012, 2012 R2, el límite de tamaño del archivo es 256 TB. ① NOTA: Para que Rapid Recovery pueda validar el sistema operativo, el Instrumental de administración de Windows (WMI) debe estar instalado en la ubicación de almacenamiento deseada.
Política de almacenamiento en caché de escritura	La política de almacenamiento en caché de escritura controla cómo se utiliza el Administrador de caché de Windows en el repositorio y ayuda a ajustar el repositorio para un rendimiento óptimo en diferentes configuraciones. Establezca el valor en una de las opciones siguientes: • Activado • Desactivado • Sincronización Si se establece como Activado, que es el valor predeterminado, Windows controla el almacenamiento en caché. Es adecuado para Windows 10 y para versiones de Windows Server 2012 y posteriores.

Cuadro de texto	Descripción

NOTA: si se establece la política de escritura en caché en **Activado**, se mejora el rendimiento; no obstante, el valor recomendado es **Desactivada**. Si utiliza Windows Server 2008 SP2 o Windows Server 2008 R2 SP2, la configuración recomendada es **Desactivado**.

Si se establece en **Desactivado**, Rapid Recovery controla el almacenamiento en caché.

Si se establece en **Sincronización**, Windows controla el almacenamiento en caché así como la entrada/salida sincrónica.

Bytes por sector	Especifique el número de bytes que desea que incluya cada sector. El valor predeterminado es 512.

Promedio de bytes por registro	Especifique el promedio del número de bytes por registro. El valor predeterminado es 8192.

6 Haga clic en **Siguiente**.

Si ha seleccionado la opción **Avanzada** en el paso 1, aparece la página **Cifrado**.

- 14 De manera opcional, en la página **Cifrado**, seleccione **Habilitar cifrado** para habilitar el cifrado. Aparecerán los campos de clave de cifrado en la página **Cifrado**.

NOTA: Si habilita el cifrado, se aplicará a los datos de todos los volúmenes protegidos de este equipo. Puede cambiar los ajustes posteriormente desde la página **Claves de cifrado** en la **Rapid Recovery Core Console**. Para obtener más información acerca del cifrado, consulte el tema [Descripción de las claves de cifrado](#).

PRECAUCIÓN: Rapid Recovery utiliza cifrado AES de 256 bits en el modo Encadenamiento de bloques de cifrado (CBC) con claves de 256 bits. Si bien el uso de cifrado es opcional, Dell recomienda encarecidamente que establezca una clave de cifrado y que proteja la frase de contraseña que defina. Almacene la frase de contraseña en una ubicación segura, dado que es clave para la recuperación de datos. Sin una frase de contraseña, la recuperación de datos no es posible.

- 15 Si desea cifrar estos equipos protegidos utilizando una clave de cifrado que ya esté definida en este Core de Rapid Recovery, seleccione **Cifrar datos con una clave de cifrado existente** y seleccione la clave apropiada en el menú desplegable. Continúe en el [paso 17](#).
- 16 Si desea agregar una nueva clave de cifrado al Core y aplicar esa clave a estos equipos protegidos, introduzca la información según se describe en la siguiente tabla:

Tabla 95. Configuración de la clave de cifrado

Cuadro de texto	Descripción
Nombre	Escriba un nombre para la clave de cifrado. Los nombres de las claves de cifrado contienen entre 1 y 130 caracteres alfanuméricos. No incluya caracteres especiales como la barra diagonal, la barra diagonal inversa, la barra vertical, dos puntos, comillas, símbolo de interrogación, paréntesis de apertura o cierre, & o almohadilla.
Descripción	Escriba un comentario para la clave de cifrado. Esta información aparece en el campo Descripción cuando se ven claves de cifrado desde la Core Console.
Frase de contraseña	Introduzca la frase de contraseña usada para controlar el acceso. La práctica recomendada es evitar el uso de los caracteres especiales descritos anteriormente. Registre la frase de contraseña en lugar seguro. Dell Support no puede recuperar frases de contraseña. Una vez cree una clave de cifrado y la aplique a uno o más equipos protegidos no podrá recuperar los datos si pierde la frase de contraseña.
Confirmar frase de contraseña	Vuelva a introducir la frase de contraseña que acaba de introducir.

- 17 Haga clic en **Finalizar** para guardar y aplicar sus ajustes.

El Asistente se cerrará.

18 Si ha aparecido la página **Advertencia** pero está satisfecho con la selección de repositorios, haga clic de nuevo en **Finalizar**.

El software Rapid Recovery Agent se implementa en los equipos especificados y, si es necesario, se añaden los equipos a la protección en el Core.

Supervisión de la protección de varios equipos

Puede supervisar el progreso a medida que Rapid Recovery aplica las políticas y calendarios de programación de protección a los equipos.

En la Core Console de Rapid Recovery, navegue a la página Inicio de Rapid Recovery y, a continuación, haga clic en  (Eventos). Aparece la página **Eventos**, que se compone de los elementos Tareas, Alertas y Eventos. A medida que los volúmenes se transfieren, en el panel Tareas se muestra el estado y las horas de inicio y finalización.

También puede filtrar tareas por estado (activas, en espera, completadas, en cola y fallidas). Para obtener más información, consulte [Visualización de tareas](#).

 **NOTA:** Para ver únicamente las tareas que están a la espera de realizarse, asegúrese de seleccionar el icono Tareas en espera.

A medida que se agrega cada equipo protegido, se registra una alerta, que indica si la operación ha sido correcta o si se han registrado errores. Para obtener más información, consulte [Visualización de alertas](#).

Para obtener información sobre cómo visualizar todos los eventos, consulte [Visualización de todos los eventos](#).

Configuración y funciones en servidores de Exchange protegidos

Si desea proteger un servidor de Microsoft Exchange en su Core, puede configurar parámetros adicionales en la Core Console de Rapid Recovery y realizar funciones adicionales.

Solo hay disponible un parámetro, **Habilitar comprobación de capacidad de montaje automático**, en la Core Console relacionada con Exchange Server. Si está activada, las comprobaciones de capacidad de montaje del Exchange Server se realizan automáticamente. Este parámetro está disponible cuando el estado del equipo protegido es verde (activo) o amarillo (en pausa).

Para obtener más información, consulte [Acerca de las comprobaciones de capacidad de montaje de base de datos de Exchange](#).

También puede realizar una comprobación de la capacidad de montaje a petición, en el panel Puntos de recuperación de un equipo protegido del Exchange Server. Para obtener más información, consulte [Forzado de una comprobación de capacidad de montaje de una base de datos de Exchange](#).

A continuación, se indican las funciones que puede realizar en un Exchange Server protegido por el Core.

- **Especificar las credenciales del servidor de Exchange.** El Core de Rapid Recovery le permite establecer las credenciales para que el Core pueda autenticarse en el Exchange Server y obtener información.
Para obtener más información acerca del establecimiento de credenciales para Exchange Servers, consulte [Establecimiento de las credenciales para un equipo Exchange Server](#).
- **Truncar registros de Exchange.** Cuando fuerza el truncamiento de los registros del Exchange Server, este proceso identifica el espacio disponible y reclama espacio en el servidor protegido de Exchange.
Para obtener más información acerca del truncamiento de los registros del Exchange Server a petición, consulte [Forzado del truncamiento de registros para un equipo Exchange](#). Este proceso también puede llevarse a cabo como parte de los trabajos nocturnos.
- **Forzar una comprobación de la capacidad de montaje de una base de datos de Exchange.** Esta función comprueba que se puedan montar las bases de datos de Exchange, para detectar daños y alertar a los administradores para que todos los datos del servidor de Exchange se puedan recuperar correctamente.
Para obtener más información acerca del forzado de una comprobación de la capacidad de montaje a petición, consulte [Forzado de una comprobación de capacidad de montaje de una base de datos de Exchange](#).

También puede forzar una comprobación de la capacidad de montaje para que se inicie automáticamente después de cada instantánea. Para obtener más información acerca de las comprobaciones de la capacidad de montaje, consulte [Acerca de las comprobaciones de capacidad de montaje de base de datos de Exchange](#).

- **Forzar una comprobación de la suma de comprobación de puntos de recuperación de Exchange Server.** Esta función comprueba la integridad de los puntos de recuperación que contienen los archivos de la base de datos de Exchange. Para obtener más información acerca del forzado de una comprobación de la suma de comprobación a petición, consulte [Forzado de comprobación de suma de comprobación de archivos de bases de datos de Exchange](#).

Puede truncar registros de Exchange y forzar una comprobación de la suma de comprobación como parte de los trabajos nocturnos. Para obtener más información acerca de las tareas que puede programar como trabajos nocturnos, consulte [Descripción de los trabajos nocturnos](#). Para obtener información sobre la configuración de trabajos nocturnos, consulte [Configuración de trabajos nocturnos para el Core](#).

Establecimiento de las credenciales para un equipo Exchange Server

Para establecer las credenciales al iniciar sesión, debe haber un Exchange Server en un volumen protegido. Si Rapid Recovery no detecta la presencia de un Exchange Server, la función Establecer las credenciales no aparece en la Core Console.

Una vez que ha protegido datos en un servidor Microsoft Exchange, puede establecer credenciales de inicio de sesión en la Core Console de Rapid Recovery.

Complete los pasos de este procedimiento para definir las credenciales de cada Exchange Server.

- 1 En el área de navegación izquierda de la Core Console de Rapid Recovery, seleccione el equipo Exchange Server protegido para el que desea establecer las credenciales.
La página **Resumen** se muestra en el Exchange Server protegido.
- 2 En la página **Resumen**, en los vínculos que aparecen en la parte superior de la página, haga clic en la flecha hacia abajo ▼ que se encuentra a la derecha del menú Exchange y, a continuación, en el menú desplegable resultante, seleccione **Establecer las credenciales**.
Aparece el cuadro de diálogo **Editar las credenciales de Exchange** para el Exchange Server.
- 3 En el cuadro de diálogo **Editar las credenciales de Exchange**, introduzca las credenciales, como se indica a continuación:
 - a En el campo de texto **Nombre de usuario**, introduzca el nombre de usuario de un usuario con permisos en el servidor de Exchange; por ejemplo, Administrador (o, si el equipo está en un dominio, [nombre de dominio]\Administrador).
 - b En el campo de texto **Contraseña**, introduzca la contraseña con el nombre que especificó para conectar con el Exchange Server.
 - c Haga clic en **Aceptar** para confirmar los ajustes y cerrar el cuadro de diálogo.

Forzado del truncamiento de registros para un equipo Exchange

Para forzar el truncamiento del log, debe haber una base de datos de Exchange en un volumen protegido. Si Rapid Recovery no detecta la presencia de una base de datos, la comprobación del truncamiento del log no aparece en la Consola de Core.

Cuando se fuerza un truncamiento del log para un servidor de Exchange protegido, el tamaño de los registros se reduce. Complete los pasos de este procedimiento para forzar el truncamiento del log bajo demanda.

- 1 En el área de navegación izquierda de la Core Console de Rapid Recovery, seleccione el servidor de Exchange protegido para el que desea forzar el truncamiento del log.
Aparece la página **Resumen** para el equipo protegido.
- 2 En la parte superior de la página, haga clic en el menú desplegable **Exchange** y seleccione **Forzar truncamiento del log**.
- 3 En el cuadro de diálogo resultante, haga clic para confirmar que desea forzar el truncamiento del log.
El cuadro de diálogo se cierra. El sistema empieza a truncar los registros de servidor de Exchange. Si las alertas del sistema están habilitadas para este tipo de evento, se muestra un mensaje que indica que empieza el proceso de truncamiento del log.

Acerca de las comprobaciones de capacidad de montaje de base de datos de Exchange

Cuando utilice Rapid Recovery para hacer copia de seguridad de archivos de servidores Microsoft Exchange, las comprobaciones de capacidad de montaje se pueden realizar en todas las bases de datos de Exchange tras cada instantánea. Esta función de detección de corrupción avisa a los administradores de posibles errores, y asegura que todos los datos en los servidores de Exchange se recuperarán correctamente en caso de error.

Para habilitar o deshabilitar esta función, vaya al menú **Configuración** del equipo protegido y establezca la opción **Habilitar comprobación de capacidad de montaje automática** en Sí o No, respectivamente. Para obtener más información acerca de la modificación de la configuración de un equipo protegido, consulte [Visualización y modificación de la configuración de equipos protegidos](#).

Las comprobaciones de la capacidad de montaje no forman parte de la configuración nocturna. Sin embargo, si la comprobación de capacidad de montaje automática está habilitada, y si los trabajos nocturnos de Truncar registros de Exchange están habilitados, la comprobación de la capacidad de montaje se activa tras completar el truncamiento del registro.

También puede realizar una comprobación de la capacidad de montaje a petición, en el panel **Puntos de recuperación** de un equipo protegido del servidor de Exchange. Para obtener más información, consulte [Forzado de una comprobación de capacidad de montaje de una base de datos de Exchange](#).

NOTA: Las comprobaciones de capacidad de montaje solo se aplican a Microsoft Exchange 2007, 2010 y 2013. Además, la cuenta de servicio de Rapid Recovery Agent debe estar asignada al rol Administrador organizativo en Exchange.

Forzado de una comprobación de capacidad de montaje de una base de datos de Exchange

Para forzar una comprobación de la capacidad de montaje, debe haber una base de datos de Exchange en un volumen protegido. Si Rapid Recovery no detecta la presencia de una base de datos, la función de comprobación de la capacidad de montaje no aparece en la Core Console.

Complete los pasos de este procedimiento para forzar que el sistema haga una comprobación de la capacidad de montaje para un punto de recuperación del servidor de Exchange a petición.

- 1 En el área de navegación izquierda de la Core Console de Rapid Recovery, seleccione el equipo Exchange Server protegido para el que quiere forzar la comprobación de la capacidad de montaje y, a continuación, haga clic en el menú **Puntos de recuperación**.
- 2 Desplácese hasta el panel **Puntos de recuperación**.
- 3 Navegue por los puntos de recuperación para encontrar el punto de recuperación en cuestión. De manera opcional, también puede hacer clic en la flecha ▶ a la derecha de un punto de recuperación de la lista para expandir la vista.
En la información del punto de recuperación expandido, puede ver los volúmenes incluidos en el punto de recuperación.
- 4 En el panel **Puntos de recuperación**, desde la fila que representa el punto de recuperación correcto, haga clic en , y en el menú desplegable, seleccione **Forzar comprobación de la capacidad de montaje**.
- 5 En el cuadro de diálogo resultante, haga clic para confirmar que desea forzar la comprobación de la capacidad de montaje.
El cuadro de diálogo se cierra. El sistema realiza la comprobación de capacidad de montaje. Si las alertas del sistema están habilitadas para este tipo de evento, se muestra un mensaje que indica que empieza la comprobación de la capacidad de montaje.

Para obtener instrucciones sobre cómo ver el estado de la comprobación de la capacidad de montaje, consulte [Visualización de eventos mediante las tareas, las alertas y el diario](#).

Forzado de comprobación de suma de comprobación de archivos de bases de datos de Exchange

Para forzar una comprobación de suma de comprobación, debe haber una base de datos de Exchange en un volumen protegido. Si Rapid Recovery no detecta la presencia de una base de datos, la función de comprobación de suma de comprobación no aparece en la Core Console.

Complete los pasos de este procedimiento para forzar que el sistema haga una comprobación de suma de comprobación para un punto de recuperación del servidor de Exchange específico.

- 1 En el área de navegación izquierda de Core Console de Rapid Recovery, seleccione el servidor Exchange protegido para el que quiere forzar la comprobación de suma de comprobación y, a continuación, haga clic en el menú **Puntos de recuperación**.
La página **Puntos de recuperación** se muestra en el servidor Exchange protegido.
- 2 Desplácese hacia abajo hasta el panel **Puntos de recuperación**.
- 3 Navegue por los puntos de recuperación para encontrar el punto de recuperación en cuestión. De manera opcional, también puede hacer clic en la flecha ▶ a la derecha de un punto de recuperación de la lista para expandir la vista.
En la información del punto de recuperación expandido, puede ver los volúmenes incluidos en el punto de recuperación.
- 4 En el panel **Puntos de recuperación**, desde la fila que representa el punto de recuperación correcto, haga clic en  y, desde el menú desplegable, seleccione **Forzar comprobación de suma de comprobación**.
- 5 En el cuadro de diálogo resultante, haga clic para confirmar que desea forzar la comprobación de suma de comprobación.
El cuadro de diálogo se cierra. El sistema realiza la comprobación de suma de comprobación. Si las alertas del sistema están habilitadas para este tipo de evento, se muestra un mensaje que indica que empieza la comprobación de suma de comprobación.

Para obtener instrucciones sobre cómo ver el estado de la comprobación de suma de comprobación, consulte [Visualización de eventos mediante las tareas, las alertas y el diario](#).

Configuración y funciones en servidores SQL Server protegidos

Si desea proteger un servidor Microsoft SQL Server en su Core, puede configurar parámetros adicionales en la Core Console de Rapid Recovery y realizar funciones adicionales.

Solo hay disponible un parámetro, **Conectabilidad**, en la Core Console relacionada con SQL Server.

El Core de Rapid Recovery le permite realizar una comprobación de conectabilidad de SQL para comprobar la integridad de los puntos de recuperación que contienen bases de datos de SQL. Esta acción comprueba la coherencia de bases de datos de SQL y garantiza que todos los archivos MDF (datos) y LDF (registro) compatibles están disponibles en la instantánea de copia de seguridad.

En versiones anteriores, las comprobaciones de conectabilidad de SQL requerían una versión con licencia de SQL Server en el equipo del Core. El Core de Rapid Recovery ahora ofrece la posibilidad de realizar las comprobaciones de conectabilidad de SQL desde una instancia de SQL Server en el Core o desde una versión con licencia en un equipo protegido de SQL Server.

Los parámetros de conectabilidad le permiten especificar qué versión con licencia de SQL Server se utiliza para llevar a cabo esta comprobación. Para obtener más información sobre la configuración de los parámetros de conectabilidad, consulte [Administración de la configuración de conectabilidad de SQL del Core](#).

Para obtener más información sobre la conectabilidad de SQL, consulte [Acerca de la conectabilidad de SQL](#).

A continuación, se indican las funciones que puede realizar en un servidor SQL protegido por el Core.

- **Especificar las credenciales de SQL Server.** El Rapid Recovery Core permite establecer las credenciales para que el Core pueda autenticarse en el SQL Server y obtener información. Puede establecer credenciales para un solo equipo protegido de SQL Server o establecer las credenciales predeterminadas para todos los servidores SQL Server protegidos.
Para obtener más información acerca del establecimiento de credenciales para servidores de SQL, consulte [Establecimiento de las credenciales para un equipo SQL Server](#).
- **Truncar registros de SQL.** Cuando fuerza el truncamiento de los registros del servidor de SQL, este proceso identifica el espacio disponible en el servidor protegido. Este proceso no reclama ningún espacio.
Para obtener más información acerca del truncamiento de los registros de SQL Server a petición, consulte [Forzado del truncamiento de registros para un equipo SQL](#).
- **Forzar una comprobación de conectabilidad de un servidor SQL Server.** Esta función comprueba la coherencia de bases de datos de SQL y garantiza que todos los archivos MDF (datos) y LDF (registro) compatibles están disponibles en la instantánea de copia de seguridad.

Para obtener más información acerca del forzado de una comprobación de conectabilidad de servidores SQL Server a petición, consulte [Forzado de una comprobación de conectabilidad de SQL Server](#).

Además de especificar las credenciales, cada una de las funciones descritas en la lista anterior pueden realizarse a petición, y también pueden configurarse para que se produzcan como parte de los trabajos nocturnos realizados para el Core. Para obtener más información acerca de las tareas que puede programar como trabajos nocturnos, consulte [Descripción de los trabajos nocturnos](#). Para obtener información sobre la configuración de trabajos nocturnos, consulte [Configuración de trabajos nocturnos para el Core](#).

Establecimiento de las credenciales para un equipo SQL Server

Debe agregar el equipo SQL Server a la protección en el Core de Rapid Recovery antes de realizar este proceso. Para obtener más información sobre la protección de equipos, consulte [Cómo proteger una máquina](#).

Una vez proteja los datos en un equipo SQL Server de Microsoft, puede definir las credenciales de inicio de sesión para una única instancia o para todos los SQL Server, en la Core Console de Rapid Recovery.

Complete los pasos de este procedimiento para definir las credenciales de cada SQL Server.

- 1 En el área de navegación izquierda de la Core Console de Rapid Recovery, seleccione el equipo SQL Server protegido para el que desea establecer las credenciales.
Aparece la página **Resumen** para el SQL Server protegido.
- 2 En la página **Resumen**, en los vínculos que aparecen en la parte superior de la página, haga clic en la flecha hacia abajo ▼ que se encuentra en la derecha del menú de SQL y, a continuación, desde el menú desplegable resultante, realice una de las siguientes acciones:
 - Si desea establecer credenciales para todas las instancias de bases de datos de SQL Server, haga clic en **Definir credenciales predeterminadas para todas las instancias** y, en el cuadro de diálogo **Editar credenciales predeterminadas**, haga lo siguiente:
 - 1 En el campo de texto **Nombre de usuario**, introduzca el nombre de usuario de un usuario con permisos para todos los servidores SQL asociados; por ejemplo, Administrador (o, si el equipo está en un dominio, [nombre de dominio]\Administrador).
 - 2 En el campo de texto **Contraseña**, introduzca la contraseña con el nombre que especificó para conectar con el SQL Server.
 - 3 Haga clic en **Aceptar** para confirmar los ajustes y cerrar el cuadro de diálogo.
 - Si desea definir unas credenciales para una única instancia de la base de datos de SQL Server, haga clic en el nombre de visualización del equipo SQL Server protegido y, a continuación, en el cuadro de diálogo **Editar credenciales de instancia**, haga lo siguiente:
 - 1 Seleccione el tipo de credencial (Predeterminada, Windows o SQL).
 - 2 En el campo de texto **Nombre de usuario**, introduzca el nombre de usuario de un usuario con permisos en el servidor SQL; por ejemplo, Administrador (o, si el equipo está en un dominio, [nombre de dominio]\Administrador).
 - 3 En el campo de texto **Contraseña**, introduzca la contraseña con el nombre que especificó para conectar con el SQL Server.
 - 4 Haga clic en **Aceptar** para confirmar los ajustes y cerrar el cuadro de diálogo.

Forzado del truncamiento de registros para un equipo SQL

El truncamiento de registros está disponible para equipos que usan SQL Server. Complete los pasos de este procedimiento para forzar el truncamiento del registro.

❗ NOTA: Cuando se realiza para un equipo SQL, el truncamiento identifica el espacio libre en un disco, pero no reduce el tamaño de los registros.

- 1 En el área de navegación izquierda de la Core Console de Rapid Recovery, seleccione el equipo para el que desea forzar el truncamiento del registro.
Aparece la página **Resumen** para el equipo protegido.
- 2 Desde la página **Resumen** (o desde cualquier página de este equipo protegido), en la parte superior de la página, haga clic en el menú desplegable **SQL** y seleccione **Forzar truncamiento del registro**.
- 3 Haga clic en **Sí** para confirmar que desea forzar el truncamiento del registro.

Acerca de la conectabilidad de SQL

La función de conectabilidad de SQL permite que el Core de Rapid Recovery adjunte archivos de base de datos maestras de SQL (archivos .MDF) y archivos de base de datos de registro (archivos .LDF) a una instantánea de un SQL Server protegido. La instantánea se captura mediante una instancia local de Microsoft SQL Server.

Algunas cuestiones de importancia para los usuarios de Rapid Recovery que protejan equipos con SQL Server incluyen qué instancia de SQL Server realiza la conectabilidad y el método para realizar la conectabilidad SQL (a petición o como parte de los trabajos nocturnos).

La comprobación de conectabilidad permite que el Core compruebe la coherencia de las bases de datos de SQL y garantiza que todos los archivos MDF y LDF estén disponibles en la instantánea de copia de seguridad.

Las comprobaciones de conectabilidad se pueden ejecutar para puntos de recuperación específicos a petición, o bien como parte de un trabajo nocturno.

Para realizar la comprobación de conectabilidad de SQL a petición, consulte [Forzado de una comprobación de conectabilidad de SQL Server](#). Para realizar la conectabilidad de SQL una vez al día, a la hora especificada para las operaciones de trabajos nocturnos, active la opción **Comprobar la conectabilidad de las bases de datos SQL** durante los trabajos nocturnos. Para obtener más información acerca de la configuración de los trabajos nocturnos para el Core, consulte [Configuración de trabajos nocturnos para el Core](#). Para obtener más información acerca de la configuración de los trabajos nocturnos en un equipo específico (en este caso, un SQL Server protegido), consulte [Personalización de las tareas nocturnas de una máquina protegida](#).

En versiones anteriores, la conectabilidad de SQL requería instalar y configurar una instancia local de Microsoft SQL Server en el equipo del Core. El Core de Rapid Recovery ahora le permite elegir realizar la comprobación de conectabilidad desde una instancia de SQL Server en el Core, o bien desde una instancia de SQL Server en un equipo protegido de SQL Server. La instancia que seleccione debe ser una versión con licencia completa de SQL Server proporcionada por Microsoft o mediante un distribuidor autorizado. Microsoft no permite el uso de licencias SQL pasivas.

La instancia de SQL Server que especifique se utilizará para todas las comprobaciones de conectabilidad. La conectabilidad se sincroniza entre la configuración del Core y los trabajos nocturnos. Por ejemplo, si especifica el uso de la instancia del Core de SQL Server para los trabajos nocturnos, las comprobaciones de conectabilidad a petición también utilizarán el Core. Por el contrario, si especifica el uso de la instancia de SQL Server en un equipo protegido específico, todas las comprobaciones de conectabilidad nocturna y a petición utilizarán la instancia local en el equipo protegido.

Seleccione la instancia de SQL Server que desea utilizar como parte de la configuración global del Core. Para obtener más información, consulte [Administración de la configuración de conectabilidad de SQL del Core](#).

❗ NOTA: Realizar la comprobación de conectabilidad desde un equipo protegido de SQL Server requiere que el software Rapid Recovery Agent esté instalado en dicho servidor. La protección sin agentes no es compatible con la conectabilidad de SQL.

La conectabilidad del Core de Rapid Recovery es compatible con SQL Server 2005, 2008, 2008 R2, 2012 y 2014. La cuenta que se utiliza para realizar las pruebas debe tener el rol sysadmin en la instancia de SQL Server.

el formato de almacenamiento en disco de SQL Server es el mismo en entornos de 32 y 64 bits, y la conectabilidad funciona entre ambas versiones. Una base de datos que se desconecta de una instancia de servidor que se ejecute en un entorno se puede adjuntar en una instancia de servidor que se ejecute en otro entorno.

❗ NOTA: La versión de SQL Server en el Core tiene que ser igual o superior a la versión de SQL Server de todos los equipos protegidos con SQL Server instalado.

Forzado de una comprobación de conectabilidad de SQL Server

Para forzar una comprobación de capacidad de conexión, debe haber una base de datos de SQL en un volumen protegido. Si Rapid Recovery no detecta la presencia de una base de datos, la función de comprobación de capacidad de conexión no aparece en la Core Console.

Realice los pasos de este procedimiento para forzar que el sistema realice una comprobación de conectabilidad para un punto de recuperación del servidor SQL específico.

- 1 En el área de navegación izquierda de la Core Console de Rapid Recovery, seleccione el equipo SQL Server protegido para el que quiere forzar la comprobación de capacidad de conexión y, a continuación, haga clic en el menú **Puntos de recuperación**.
- 2 Desplácese hasta el panel **Puntos de recuperación**.
- 3 Navegue por los puntos de recuperación para encontrar el punto de recuperación en cuestión. De manera opcional, también puede hacer clic en la flecha ▶ a la derecha de un punto de recuperación de la lista para expandir la vista.
En la información del punto de recuperación expandido, puede ver los volúmenes incluidos en el punto de recuperación.
- 4 En el panel **Puntos de recuperación**, desde la fila que representa el punto de recuperación correcto, haga clic en , y en el menú desplegable, seleccione **Forzar comprobación de conectabilidad**.
- 5 En el cuadro de diálogo resultante, haga clic para confirmar que desea forzar la comprobación de capacidad de conexión.
El cuadro de diálogo se cierra. El sistema realiza la comprobación de conectabilidad.

Para obtener instrucciones sobre cómo ver el estado de las comprobación de capacidad de conexión, consulte [Visualización de eventos mediante las tareas, las alertas y el diario](#).

Descripción Rapid Snap para Virtual

Al instalar el software del Agent de Rapid Recovery, puede proteger máquinas físicas o virtuales en el Core de Rapid Recovery. Los sistemas operativos admitidos se indican en los requisitos del sistema en el tema "Requisitos de software del Agent de Rapid Recovery."

Rapid Recovery ofrece ahora otra forma de proteger máquinas.

La función Rapid Snap for Virtual : también conocida como función de protección sin Agent. Rapid Recovery le permite proteger las máquinas virtuales en un host VMware ESXi o Hyper-V sin instalar el Agent de Rapid Recovery en cada máquina virtual.

⚠ PRECAUCIÓN: Dell recomienda que limite la protección sin agente a no más de 200 máquinas virtuales a la vez. Por ejemplo, no seleccione más de 200 de las máquinas virtuales al usar el asistente Protect Multiple Machines Wizard (Asistente de protección de varias máquinas). Si protege más de 200 máquinas virtuales, reducirá el rendimiento. No hay límite en cuántas máquinas virtuales puede proteger sin Agent un Core a lo largo del tiempo. Por ejemplo, puede proteger 200 máquinas virtuales hoy y otras 200 máquinas virtuales mañana.

Protección de máquinas virtuales vCenter/ESXi

Rapid Recovery le permite proteger máquinas virtuales vCenter/ESXi sin instalar el Agent de la Rapid Recovery en la máquina virtual o un host ESXi, con lo que se consigue proteger sin Agent. Para proteger un entorno ESXi, el Core Rapid Recovery funciona con la tecnología de instantáneas nativa a VMware.

Rapid Recovery sin Agent utiliza el cliente ESXi y la interfaz de programación de aplicaciones (API) para proteger las máquinas virtuales en un solo host seleccionado sin tener que instalar el software del Agent de Rapid Recovery. Después, el Core de Rapid Recovery se comunica con el disco de máquina virtual para determinar las indicaciones necesarias sobre los volúmenes protegidos. Debido a que Rapid Recovery crea los puntos de recuperación basados en volúmenes, y no en discos de máquinas virtuales, cada volumen se puede montar, restaurar y exportar por separado.

❗ NOTA: Rapid Recovery recomienda que se instale VMware Tools en las máquinas virtuales que desea proteger en hosts vSphere o ESXi. Cuando se instala VMware Tools en una máquina virtual mediante un sistema operativo Windows, las copias de seguridad que el Core de Rapid Recovery captura utilizan Microsoft Volume Shadow Services (VSS). Para obtener más información sobre el comportamiento de máquinas virtuales sin Agent con o sin VMware Tools, consulte [Beneficios de instalar herramientas de VMware para la protección sin agentes](#).

La protección sin agente también utiliza VMware Changed Block Tracking (CBT) para reducir el tiempo que necesitan las instantáneas acumuladas. CBT determina qué bloques se han cambiado en el archivo del disco de la máquina virtual, y permite que Rapid Recovery cree

una copia de seguridad de solo las partes del disco que han cambiado desde la última instantánea. Este método de copia frecuentemente crea operaciones de copia más cortas y reduce el consumo de recursos en la red y de los elementos de almacenamiento.

Hay varias ventajas al utilizar protección sin Agent. Algunas de los atributos más útiles incluyen las siguientes características:

- No se requiere software adicional en la máquina host.
- La protección sin agente le permite optar por proteger automáticamente nuevas máquinas virtuales agregadas al host ESXi.
- No es necesario reiniciar durante el proceso de protección.
- Las credenciales no son necesarias para cada una de las máquinas virtuales.
- La protección sin agente le permite proteger una máquina virtual incluso si está apagada.
- La protección sin agente le permite restaurar en los discos.
- La protección sin agente no requiere espacio libre en un volumen durante las transferencias.
- La protección sin agente es compatible con todos los sistemas operativos invitados.
- La protección sin agente le permite exportar los discos dinámicos o volúmenes.

❗ NOTA: Si los volúmenes dinámicos son complejos (seccionados, reflejados, distribuidos o RAID), se exportan como imágenes de disco y se redistribuyen en volúmenes una vez que la operación de exportación se haya completado en la máquina virtual exportada.

Si bien hay muchas razones para utilizar protección sin Agent en máquinas virtuales ESXi, elija el método de protección que mejor se adapte a sus entornos y necesidades empresariales. Además de las ventajas mencionadas anteriormente, también existen las siguientes consideraciones a tener en cuenta cuando al elegir protección sin Agent:

- La protección sin Agent no admite la protección de volúmenes dinámicos (por ejemplo, extendidos, seccionados, reflejados o volúmenes RAID) a nivel de volumen. Se protegen a nivel del disco.
- La protección sin Agent no admite Live Recovery (Recuperación en vivo). Para obtener más información acerca de esta función, consulte [Descripción de Live Recovery](#).
- Después de cada restauración de un único volumen en la máquina virtual protegida, deberá reiniciar la máquina virtual.
- La protección sin Agent no recopila metadatos de Microsoft SQL o Microsoft Exchange.
- No puede realizar comprobaciones de conectabilidad de SQL, truncamientos de registro o comprobaciones de la capacidad de montaje en los puntos de recuperación capturados en máquinas protegidas sin Agent.
- La protección sin Agent no recopila ni muestra las etiquetas de volumen, o letras de unidad.
- La protección sin Agent no muestra la cantidad real de espacio utilizado en una máquina virtual si el tipo de disco virtual se llena con ceros diligentes en aprovisionamiento grueso.

Si elige utilizar protección sin Agent para las máquinas virtuales ESXi, el host debe cumplir con los siguientes requisitos mínimos para que la protección sin Agent sea eficaz.

- La máquina host debe ejecutar la versión 5.0.0 integrada de ESXi 623860 o posterior.
- La máquina host debe cumplir con los requisitos mínimos del sistema que se indican en la *Guía de actualización e instalación Rapid Recovery*.
- Para la protección a nivel de volumen, el disco de máquina virtual debe incluir el registro maestro de arranque (Master Boot Record, MBR) tablas de partición o tablas de partición GUID. Las tablas de partición de los discos de máquinas virtuales se protegen como discos enteros en vez de volúmenes individuales.
- Cada máquina virtual VMware debe tener VMware Tools instalado para garantizar la coherencia de las instantáneas.

Protección de los servidores Hyper-V y clústeres

Para proteger un Hyper-V Server sin Agent, no es necesario que instale el Agent de Rapid Recovery en ninguna de las máquinas virtuales. Solo tiene que instalarlo en la máquina host o nodo de clúster. El Agent protege el disco duro virtual en el host y convierte los cambios en los archivos del disco duro en una imagen de volumen o imagen de disco, según el sistema de archivos. Un nuevo nivel de archivo controlador proporciona compatibilidad para las máquinas virtuales en los hosts y en los volúmenes compartidos de clúster (CSV).

❗ NOTA: Rapid Recovery es compatible con el formato de archivo de disco VHDx. No admite el formato VHD.

Para proteger máquinas virtuales en un CSV, el Agent de Rapid Recovery y el controlador deben estar instalados en cada nodo del clúster mediante la función de implementación automática del asistente Protect Multiple Machines Wizard (Asistente de protección de varias

máquinas). En los nodos, el agente puede proteger todas las máquinas virtuales en CSV mediante la creación dos tipos de cambios para todos los archivos. El primer tipo de cambio se guarda solo antes o después de una instantánea o reinicio limpio del sistema. El segundo tipo de cambio reside en el disco, lo que hace que haya una instantánea acumulada incluso si se produce una interrupción de la alimentación o cierre con errores. El Agent instalado en el nodo combina todos los cambios en uno antes de transferir los datos.

Cuando se está ejecutando un host o nodo, Rapid Recovery crea una copia de seguridad coherente con las aplicaciones. Si el host no se está ejecutando, no se puede crear copia; sin embargo, si uno de los nodos no se está ejecutando, Rapid Recovery puede continuar tomando instantáneas de las máquinas virtuales en el clúster.

NOTA: Para obtener un mejor rendimiento, se recomienda que el número máximo de transferencias para el host Hyper-V o nodo se establezca en 1, que es el valor predeterminado.

La protección sin Agent de Hyper-V tiene muchas de las mismas capacidades que la protección tradicional, en la que el Agent está instalado en cada máquina virtual, incluyendo:

- Archivado
- Comprobación de integridad de los puntos de recuperación
- Montaje de los puntos de recuperación
- Detección automática de las nuevas máquinas virtuales (únicamente protección sin Agent)
- Replicación
- Restauración de máquinas virtuales
- Restauración de CSV
- Restauración en CIFS mediante el formato VHDX
- Restauración de archivos en un formato VHDX invitado
- Consolidación
- Exportación virtual a máquinas virtuales de Hyper-V y otros hipervisores, incluidos ESXi, VMware Workstation y VirtualBox

Sin embargo, existen limitaciones a tener en cuenta al momento de elegir protección sin Agent de Hyper-V. Las capacidades que no se realizan incluyen:

- Comprobación de integridad de montaje de Exchange
- Comprobación de conectabilidad de SQL
- Live Recovery
- Restauración de máquinas virtuales en CIFS mediante formato VHD
- Restauración de archivos en formato VHD invitado

NOTA: Para crear instantáneas coherentes con la aplicación, debe tener el controlador SCSI instalado en cada máquina virtual. Sin este controlador, el resultado es siempre una instantánea coherente de bloqueo.

Beneficios de instalar herramientas de VMware para la protección sin agentes

Al proteger máquinas virtuales (VM) sin utilizar el Rapid Recovery Agent, Dell recomienda instalar las herramientas de VMware en las VM protegidas en hosts ESXi o vSphere para sacar el máximo provecho a las funcionalidades del Servicio de instantáneas de volumen de Microsoft (VSS).

La protección sin agentes utiliza la tecnología de instantáneas nativa a VMware para realizar una copia de seguridad de los datos protegidos. Cuando se instalan las herramientas de VMware en una VM con el sistema operativo (SO) Windows, las copias de seguridad que captura el Core de Rapid Recovery también pueden utilizar VSS. Cuando las herramientas de VMware no se instalan, Rapid Recovery sigue recopilando instantáneas, pero la ausencia de las herramientas de VMware puede afectar de forma negativa al estado de los datos en su VM protegida.

Existen dos posibles estados de datos:

- **Coherente con el bloqueo.** El SO de la VM se inicia y puede leer y entender el sistema de archivos.
- **Coherente con la aplicación.** El SO de la VM se inicia y puede leer y entender el sistema de archivos. Además, los archivos para aplicaciones transaccionales se encuentran en un estado coherente. Por ejemplo, con SQL Server, los registros coinciden con los archivos de base de datos, y la base de datos se abre rápida y fácilmente.

Si recupera una aplicación transaccional a partir de un estado coherente con el bloqueo, la base de datos vuelve al último estado válido. El estado válido más reciente puede ser desde el momento del bloqueo o anterior al bloqueo. Si es anterior al bloqueo, la base de datos debe actualizar algunos trabajos para que los archivos de datos coincidan con la información de los registros. Este proceso tarda un tiempo cuando abre la base de datos por primera vez, lo que provoca un retraso al iniciar el equipo.

Las siguientes condiciones se aplican en función de si las herramientas de VMware están o no instaladas y si la VM está encendida:

Tabla 96. Condiciones del tipo de copia de seguridad para las VM

Herramientas de VMware	VM encendida	Tipo de copia inteligente
No instalado	Sí	Coherentes con el bloqueo
No instalado	No (cierre con errores)	Coherentes con el bloqueo
No instalado	No (cierre correcto)	Coherente con la aplicación
Instalada	Sí	Coherente con la aplicación
Instalada	No (cierre con errores)	Coherentes con el bloqueo
Instalada	No (cierre correcto)	Coherente con la aplicación

Protección de máquinas virtuales vCenter/ESXi sin Rapid Recovery Agent

Lleve a cabo el siguiente procedimiento para proteger máquinas virtuales ESXi sin agente.

NOTA: Rapid Recovery recomienda instalar VMware Tools en máquinas virtuales (MV) que desea proteger en hosts vSphere o ESXi. Cuando VMware Tools esté instalado en una máquina virtual que ejecute un sistema operativo Windows, las copias de seguridad que captura Rapid Recovery Core utilizan Microsoft Volume Shadow Services (VSS). Para obtener más información sobre el comportamiento de máquinas virtuales con o sin VMware Tools, consulte [Beneficios de instalar herramientas de VMware para la protección sin agentes](#).

PRECAUCIÓN: Dell recomienda que limite la protección sin agente a no más de 200 máquinas virtuales a la vez. Por ejemplo, no seleccione más de 200 máquinas virtuales cuando utiliza e mediante el Protect Multiple Machines Wizard (Asistente para proteger varias máquinas). Si se protegen más de 200 máquinas virtuales, se reducirá el rendimiento. No hay límite en el número de máquinas virtuales que puede proteger un Core a lo largo del tiempo. Por ejemplo, puede proteger 200 máquinas virtuales hoy y otras 200 máquinas virtuales mañana.

- 1 En Rapid Recovery Core Console, haga clic en el menú desplegable **Protect (Proteger)** y, a continuación, haga clic en **Protect Multiple Machines (Proteger varias máquinas)**.
Se abre el Protect Multiple Machines Wizard (Asistente para proteger varias máquinas).
- 2 En la página **Welcome (Bienvenida)**, seleccione una de las opciones siguientes:
 - Typical (Típica)
 - Advanced (mostrar pasos opcionales) (Avanzada [mostrar pasos opcionales])
- 3 Haga clic en **Next (Siguiente)**.
- 4 En la página **Connection (Conexión)** del asistente, lista desplegable **Source (Origen)**, seleccione **vCenter / ESX(i)**.
- 5 Introduzca la información del host y las credenciales de inicio de sesión como se describe en la tabla siguiente.

Tabla 97. Configuración de conexión VCenter/ESX(i)

Cuadro de texto	Descripción
Host	El nombre o la dirección IP del host virtual de VMware vCenter Server/ESX(i).
Port (Puerto)	El puerto utilizado para conectarse al host virtual. El valor predeterminado es 443.

Cuadro de texto	Descripción
User name (Nombre de usuario)	El nombre de usuario utilizado para conectarse al host virtual; por ejemplo, Administrador o, si la máquina está en un dominio, [nombre de dominio]\Administrador.
Contraseña	Introduzca la contraseña segura que se utiliza para conectarse al host virtual.

- 6 Confirme que **Protect selected VMs Agentlessly** (Proteger MV sin agente seleccionadas. (Esta opción está seleccionada de manera predeterminada).
- 7 En la página **Select Machines (Máquinas seleccionadas)**, seleccione las máquinas virtuales que desea proteger. Puede utilizar el menú desplegable para mostrar una lista de hosts y clústeres o una lista de máquinas virtuales y plantillas.

NOTA: VMware Changed Block Tracking (CBT) debe estar activado en cada una de las máquinas virtuales que desee proteger. Si no está activado, Rapid Recovery activa automáticamente CBT para garantizar la protección.

- 8 Si desea proteger automáticamente nuevas máquinas virtuales cuando se agregan a el host, seleccione **Auto protect new machines (Protección automática nuevas máquinas)** y, a continuación, realice los pasos siguientes.
 - a Haga clic en **Next (Siguiente)**.
 - b En la página **Auto Protection (Protección automática)**, seleccione el contenedor donde espera agregar nuevas máquinas.
- 9 Haga clic en **Next (Siguiente)**.
- 10 En la página Protection (Protección), seleccione una de los programas de protección siguientes, según corresponda:
 - A continuación, para usar el programa de protección predeterminado, en la opción **Schedule Settings (Configuración de programación)**, seleccione Default protection (hourly snapshots of all volumes) (Protección predeterminada [instantáneas cada hora de todos los volúmenes]).
 - Si desea definir un programa de protección diferente, en la opción Schedule Settings (Configuración de programación) seleccione **Custom protection (Protección personalizada)**.
- 11 Continúe con la configuración de la manera siguiente:
 - Si ha seleccionado una configuración típica y ha especificado la protección predeterminada, haga clic en **Finish (Finalizar)** para confirmar la selección, cerrar el asistente y proteger la máquina especificada.
La primera vez que agregue protección para una máquina, una imagen base (una instantánea de todos los datos de los volúmenes protegidos) pasa al repositorio en Rapid Recovery Core de acuerdo con la programación que haya definido, salvo que haya especificado pausar la protección inicialmente.
 - Si ha seleccionado una configuración típica y ha especificado la protección personalizada, haga clic en **Next (Siguiente)** para configurar un programa de protección personalizado. Para obtener más información sobre cómo definir un programa de protección personalizado, consulte [Creación de calendarios de programación de protección personalizados](#).
 - Si ha seleccionado Advanced configuration (Configuración avanzada) para el asistente Protect Machine Wizard (Asistente para proteger máquina), haga clic en **Next (Siguiente)** y vaya al [Paso 13](#) para ver las opciones de repositorio y cifrado.
 - Si ha seleccionado una configuración típica para el asistente Protect Machine Wizard (Asistente para proteger máquina) y ha especificado una protección personalizada, haga clic en **Next (Siguiente)** para configurar un programa de protección personalizado. Para obtener más información sobre cómo definir un programa de protección, consulte [Creación de calendarios de programación de protección personalizados](#).
- 12 Haga clic en **Next (Siguiente)**.
- 13 En la página **Repository (Repositorio)**:
 - Si ya tiene un repositorio y desea almacenar los datos de esta máquina protegida en la repositorio existente, realice lo siguiente:
 - 1 Seleccione **Use an existing repository (Usar un repositorio existente)**.
 - 2 Seleccione un repositorio existente de la lista.
 - 3 Haga clic en **Next (Siguiente)**.

Aparece la página **Encryption (Cifrado)**. Vaya al [Paso 19](#) si desea definir el cifrado opcionalmente.
 - Si desea crear un repositorio existente), seleccione **Create a Repository (Crear un repositorio)** y, a continuación, realice los pasos siguientes.
 - 1 En la página **Repository (Repositorio)**, introduzca la información que se describe en la tabla siguiente.

Tabla 98. Agregar configuración del nuevo repositorio

Cuadro de texto	Descripción
Repository Name (Nombre del repositorio)	Escriba el nombre de pantalla del repositorio. De manera predeterminada, este cuadro de texto se compone de la palabra Repositorio y un número, que coincide con el número de repositorios que existen para este Core. Por ejemplo, si este es el primer repositorio, el nombre predeterminado es Repositorio 1. Cambie el nombre según sea necesario. Los nombres de repositorio deben contener entre 1 y 40 caracteres alfanuméricos, incluidos espacios. No utilice caracteres prohibidos ni frases prohibidas.
Concurrent Operations (Operaciones simultáneas)	Define el nombre de solicitudes simultáneas que desea que admita el repositorio. De manera predeterminada, el valor es 64.
Comments (Comentarios)	Opcionalmente, introduzca una nota descriptiva sobre este repositorio. Puede introducir hasta 254 caracteres. Por ejemplo, escriba DVM Repositorio 2.

- 2 Haga clic en **Add Storage Location (Agregar ubicación de almacenamiento)** para definir la ubicación de almacenamiento específica o el volumen del repositorio. Este volumen debe ser la ubicación de almacenamiento principal.

⚠ PRECAUCIÓN: Defina una carpeta específica dentro de la raíz para la ubicación de almacenamiento del repositorio. No especifique la ubicación raíz. Por ejemplo, utilice E:\Repository\, no E:\. Si el repositorio que va a crear en este paso se elimina posteriormente, se eliminarán todos los archivos incluidos en la ubicación de almacenamiento de su repositorio. Si define la ubicación de almacenamiento en la raíz, todos los demás archivos en el volumen (ej., E:\) se eliminan, lo que podría provocar una pérdida de datos catastrófica.

Aparecerá el cuadro de diálogo **Add Storage Location (Agregar ubicación de almacenamiento)**.

- 3 Haga clic en **Add Storage Location (Agregar ubicación de almacenamiento)** para definir la ubicación de almacenamiento específica o el volumen del repositorio. Este volumen debe ser la ubicación de almacenamiento principal.
- 4 En el área **Storage Location (Ubicación de almacenamiento)**, especifique cómo desea agregar el archivo para la ubicación de almacenamiento. Puede agregar un volumen de almacenamiento conectado localmente (por ejemplo, un almacenamiento de conexión directa, una red de área de almacenamiento o un almacenamiento de red conectado). También puede especificar un volumen de almacenamiento en una ubicación compartida del Common Internet File System (Sistema de archivos de Internet común - CIFS)
 - Haga clic en **Add the file on local disk (Agregar el archivo en disco local)** para especificar una máquina local y, a continuación, indique la información según se describe en la tabla siguiente.

Tabla 99. Configuración de disco local

Cuadro de texto	Descripción
Data Path (Ruta de datos)	Introduzca la ubicación para almacenar los datos protegidos. Por ejemplo, escriba X:\Repository\Data. Al especificar la ruta, escriba solo caracteres alfanuméricos, un guión o un punto (para separar los nombres de host y los dominios). Puede utilizar la barra diagonal invertida únicamente para definir los niveles en la ruta. No utilice espacios. No se admite ningún otro símbolo ni caracteres de puntuación.
Metadata path (Ruta de metadatos)	Introduzca la ubicación para almacenar los metadatos protegidos. Por ejemplo, escriba X:\Repository\Metadata. Al especificar la ruta, escriba solo caracteres alfanuméricos, un guión o un punto (para separar los nombres de host y los dominios). Puede utilizar la barra diagonal invertida únicamente para definir los niveles en la ruta. No utilice espacios. No se admite ningún otro símbolo ni caracteres de puntuación.

- O bien, seleccione **Add file on CIFS share (Agregar archivo en recurso compartido CIFS)** para especificar una ubicación compartida de red y, a continuación, indique la información según se describe en la tabla siguiente.

Tabla 100. Credenciales del recurso compartido CIFS

Cuadro de texto	Descripción
UNC Path (Ruta UNC)	Introduzca la ruta de acceso para la ubicación del recurso compartido de red. Si la ubicación se encuentra en la raíz, cree un nombre de carpeta específico (por ejemplo, Repository). La ruta debe empezar por \\ . Al especificar la ruta, escriba solo caracteres alfanuméricos, un guión o un punto (para separar los nombres de host y los dominios). Las letras de la "a" a la "z" no distinguen mayúsculas de minúsculas. No utilice espacios. No se admite ningún otro símbolo ni caracteres de puntuación.
User name (Nombre de usuario)	Especifique un nombre de usuario para el acceso a la ubicación del recurso compartido de red.
Password (Contraseña)	Especifique una contraseña para acceder a la ubicación del recurso compartido de red.

- 5 En el área **Storage Configuration (Configuración de almacenamiento)**, haga clic en **More Details (Más detalles)** e introduzca los detalles de la ubicación de almacenamiento según se describe en la tabla siguiente.

Tabla 101. Detalles de la configuración de almacenamiento

Cuadro de texto	Descripción
Size (Tamaño)	Establezca el tamaño o capacidad de la ubicación de almacenamiento. El tamaño mínimo es 1 GB. El valor predeterminado es 250 GB. Puede elegir entre las opciones siguientes: - GB - TB NOTA: El tamaño que especifique no puede superar el tamaño del volumen. Si la ubicación de almacenamiento es un volumen de sistema de archivos de nueva tecnología (NTFS) que tiene Windows XP o Windows 7 instalado, el límite de tamaño de archivo es 16 TB. Si la ubicación de almacenamiento es un volumen NTFS que ejecuta Windows 8, 8.1, Windows 10 o Windows Server 2012, 2012 R2, el límite de tamaño de archivo es 256 TB. NOTA: Para que Rapid Recovery pueda validar el sistema operativo, el Instrumental de administración de Windows (WMI) debe estar instalado en la ubicación de almacenamiento deseada.
Write Caching Policy (Política de escritura en caché)	La política de escritura en caché de controla cómo se utiliza el Windows Cache Manager (Administrador de caché de Windows) en el repositorio y ayuda a ajustar el repositorio para un rendimiento óptimo en diferentes configuraciones. Establezca el valor en una de las opciones siguientes: - On (Activado) - Off (Desactivado) - Sync (Sincronizar) Si se establece en On (Activado), que es el valor predeterminado, Windows controla el almacenamiento en caché. Esto es adecuado para Windows 10, y para las versiones de Windows Server 2012 y posteriores. NOTA: Si se establece la política de escritura en caché en On (Activado), se mejora el rendimiento. Si utiliza Windows Server 2008 SP2 o Windows Server 2008 R2 SP2, el valor recomendado es Off (Desactivado). Si se establece en Off (Desactivado), Rapid Recovery controla el almacenamiento en caché. Si se establece en Sync (Sincronizar), Windows controla el almacenamiento en caché así como la entrada/salida sincrónica.

Cuadro de texto	Descripción
Bytes per sector (Bytes por sector)	Especifique el número de bytes que desee incluir en cada sector. El valor predeterminado es 512.
Average Bytes per Record (Número promedio de bytes por registro)	Especifique el número promedio de bytes por registro. El valor predeterminado es 8192.

6 Haga clic en **Next (Siguiente)**.

Si ha seleccionado la opción **Advanced (Avanzado)** en el paso 1, aparece la página **Encryption (Cifrado)**.

14 De manera opcional, para activar el cifrado en la página de cifrado, seleccione **Enable Encryption (Activar cifrado)**.

Aparecerán los campos de clave de cifrado en la página Encryption (Cifrado).

NOTA: Si activa el cifrado, se aplicará a los datos para todos los volúmenes protegidos de esta máquina de Agent. puede cambiar la configuración posteriormente en la pestaña Configuration (Configuración) de la Rapid Recovery Core Console. Para obtener más información sobre el cifrado, consulte el tema [Descripción de las claves de cifrado](#).

PRECAUCIÓN: Rapid Recovery utiliza cifrado AES de 256 bits en el modo Encadenamiento de bloques de cifrado (CBC) con claves de 256 bits. Mientras el uso de cifrado es opcional, Dell recomienda encarecidamente que establezca una clave de cifrado y que proteja la frase de contraseña que defina. Guarde la frase de contraseña en un lugar seguro, ya que es fundamental para la recuperación de datos. Sin una frase de contraseña, la recuperación de datos no es posible.

15 Si desea cifrar estas máquinas protegidas con una clave de cifrado que ya está definida en este Rapid Recovery Core, seleccione **Encrypt data using an existing Encryption key** (Cifrar los datos mediante una clave de cifrado existente) y seleccione la clave apropiada en el menú desplegable.

Continúe con el [paso 17](#).

16 Si desea agregar una clave de cifrado para el Core y aplicar dicha clave a estas máquinas protegidas, Introduzca la información según se describe en la tabla siguiente.

Tabla 102. Configuración de clave de cifrado

Cuadro de texto	Descripción
Name (Nombre)	Introduzca un nombre para la clave de cifrado. Los nombres de la clave de cifrado debe contener entre 1 y 130 caracteres alfanuméricos. No se podrá incluir caracteres especiales, tales como la barra diagonal inversa, barra diagonal, barra vertical, dos puntos, asterisco, comilla, signo de interrogación, paréntesis de apertura o cierre o almohadilla.
Description (Descripción)	Escriba un comentario para la clave de cifrado. Esta información se muestra en el campo Description (Descripción) cuando se visualizan las claves de cifrado desde Core Console.
Passphrase (Frase de contraseña)	Introduzca la frase de contraseña usada para controlar el acceso. Se recomienda evitar el uso de los caracteres especiales indicados en la descripción de nombre de esta tabla. Registre la frase de contraseña en un lugar seguro. Dell Support no puede recuperar una frase de contraseña. Una vez que haya creado una clave de cifrado y la haya aplicado a una o varias máquinas protegidas, no podrá recuperar los datos si pierde la frase de contraseña.
Confirm Passphrase (Confirmar frase de contraseña)	Vuelva a introducir la frase de contraseña que acaba de introducir.

17 Haga clic en **Finish (Finalizar)**

Rapid Recovery agrega las máquinas virtuales seleccionadas y sus host en la lista de máquinas protegidas.

Acceso a los diagnósticos de equipos protegidos

En Rapid Recovery, puede descargar y ver información de diagnósticos para equipos protegidos individuales. Además, Rapid Recovery le permite descargar y ver los datos de registro del Core.

Para acceder a los registros, consulte los siguientes procedimientos:

- [Descarga y visualización del archivo de registro del Core](#)
- [Descarga y visualización del archivo de registro de un equipo protegido](#)

Descarga y visualización del archivo de registro de un equipo protegido

Si se produce algún error o problema con un equipo protegido, puede descargar los registros del equipo para verlos o consultarlos con su representante de Dell Support.

- 1 En el área de navegación izquierda de Core Console, bajo el menú Equipos protegidos, haga clic en la fecha para expandir el menú contextual de dicho equipo protegido. Desplácese hasta **Más**, expanda ese menú y, a continuación, seleccione  **Agent Log** (Registro de agentes).
Aparece la página **Download Agent Log** (Descargar el registro de agentes).
- 2 En la página **Download Agent Log** (Descargar el registro de agentes), haga clic en  **Haga clic aquí para iniciar la descarga.**
- 3 En el cuadro de diálogo **Opening AgentAppRecovery.log** (Apertura de AgentAppRecovery.log), realice una de las siguientes acciones:
 - Para abrir el archivo de registro, seleccione **Abrir con** y, a continuación, seleccione una aplicación (como Bloc de notas) para visualizar el archivo de registro basado en texto y haga clic en **Aceptar**.
Se abre el archivo AgentAppRecovery.log en la aplicación seleccionada.
 - Para guardar el archivo localmente, seleccione **Guardar archivo** y después haga clic en **Aceptar**.
El archivo AgentAppRecovery.log se guardará en su carpeta Descargas. Se puede abrir con un editor de texto.

Descarga y visualización del archivo de registro de un equipo protegido

Si se produce algún error o problema con un equipo protegido, puede descargar los registros del equipo para verlos o consultarlos con su representante de Dell Support.

- 1 En el área de navegación izquierda de Core Console, bajo el menú Equipos protegidos, haga clic en la fecha para expandir el menú contextual de dicho equipo protegido. Desplácese hasta **Más**, expanda ese menú y, a continuación, seleccione  **Agent Log**.
Aparece la página **Descargar el registro de agentes**.
- 2 En la página **Descargar registro de Agent**, haga clic en  **Haga clic aquí para iniciar la descarga.**
- 3 En el cuadro de diálogo **Apertura de AgentAppRecovery.log**, realice una de las siguientes acciones:
 - Para abrir el archivo de registro, seleccione **Abrir con** y, a continuación, seleccione una aplicación (como Bloc de notas) para visualizar el archivo de registro basado en texto y haga clic en **Aceptar**.
Se abre el archivo AgentAppRecovery.log en la aplicación seleccionada.
 - Para guardar el archivo localmente, seleccione **Guardar archivo** y después haga clic en **Aceptar**.
El archivo AgentAppRecovery.log se guardará en su carpeta Descargas. Se puede abrir con un editor de texto.

Vínculos relacionados

[Descarga y visualización del archivo de registro del Core](#)

Visualización del estado de la máquina y otros detalles

Siga los pasos de este procedimiento para ver el estado y otros detalles de una máquina.

En la Core Console de Rapid Recovery, navegue hasta la máquina protegida que desea ver.

La información sobre la máquina se muestra en la página Summary (Resumen). A continuación, se describen los detalles que se incluyen:

- Nombre del host
- Last Snapshot (Última instantánea tomada)
- Next Snapshot (Siguiente instantánea programada)
- Encryption status (Estado de cifrado)
- Version number (Número de versión)

Si Exchange Server está instalado en la máquina, también se muestra información detallada sobre el servidor, como por ejemplo:

- Last successful Mountability check performed (Última comprobación de la capacidad de montaje exitosa)
- Last successful Checksum check performed (Última comprobación de la suma de comprobación exitosa)
- Last Log Truncation (Último truncamiento del registro realizado)

También se muestra información sobre los volúmenes contenidos en esta máquina, que incluye:

- Volume Name (Nombre del volumen)
- Schedule (Programación)
- Current Schedule (Programa actual)
- Next Snapshot (Próxima instantánea)
- File System Type (Tipo de sistema de archivos)
- Space Usage out of total size (Uso del espacio de tamaño total)
- Si SQL Server está instalado en la máquina, también se muestra información detallada sobre el servidor, como por ejemplo:

Estado en línea

- Nombre
- Install Path (Ruta de instalación)
- Versión

Si Exchange Server está instalado en la máquina, también se muestra información detallada sobre el servidor y los almacenes de correo, como por ejemplo:

- Versión
- Install Path (Ruta de instalación)
- Data Path (Ruta de acceso a datos)
- Database Name (Nombre de base de datos)
- Exchange Databases Path (Ruta de bases de datos de Exchange)
- Log File Path (Ruta de acceso al archivo de registro)
- Log Prefix (Prefijo de registro)
- System Path (Ruta de acceso al sistema)
- MailStore Type (Tipo de almacén de correo)

Administración de equipos

Esta sección describe una variedad de tareas que puede realizar para administrar sus equipos. Los temas incluyen:

- [Retirada de un equipo](#)
- [Retirada de un clúster de la protección](#)

- [Visualización de la información de licencia en un equipo](#)
- [Descarga y visualización del archivo de registro de un equipo protegido](#)
- [Conversión de un nodo de clúster protegido en un equipo protegido](#)

Retirada de un equipo

Cuando retira un equipo de la protección en el Core de Rapid Recovery, se le presentan dos opciones: puede mantener los puntos de recuperación guardados hasta ahora en el Core de RR o bien puede eliminarlos. Si mantiene los puntos de recuperación, tendrá lo que se conoce como un “equipo solo con puntos de recuperación”. Utilizando esos puntos de recuperación para el equipo que se ha retirado de la protección actual, podrá seguir restaurando el equipo en el futuro, pero solo hasta el estado capturado en un punto de recuperación guardado.

Si elimina los puntos de recuperación, esta acción elimina todos los datos de instantáneas del equipo que antes estaba protegido del Core de Rapid Recovery.

 **PRECAUCIÓN:** Si elimina los puntos de recuperación, ya no podrá restaurar datos para ese equipo.

Realice los pasos de este procedimiento para quitar un equipo de la protección de su entorno de Rapid Recovery.

- 1 Desde la Core Console de Rapid Recovery, en el panel de navegación de la izquierda en Equipos protegidos, haga clic en el equipo desee quitar.
- 2 En la página Resumen del equipo en cuestión, haga clic en **Quitar equipo**.
- 3 En el cuadro de diálogo, si también desea eliminar todos los puntos de recuperación para este equipo del repositorio, seleccione **Quitar con puntos de recuperación**.
- 4 Para confirmar su decisión de quitar el equipo, haga clic en **Sí**.
Rapid Recovery quitará la protección del equipo y cancelará todas las tareas activas del mismo.

Cancelación de operaciones en un equipo

Puede cancelar las operaciones que se estén ejecutando actualmente en un equipo. Puede especificar la cancelación de la instantánea actual o cancelar todas las operaciones actuales, que incluye exportaciones, replicaciones, etc.

- 1 En la Core Console de Rapid Recovery, en el área de navegación izquierda debajo de Equipos protegidos, haga clic en el equipo para el que desea cancelar las operaciones.
- 2 Haga clic en **Eventos**.
- 3 Haga clic en el icono Detalles del trabajo en el extremo derecho para cancelar la operación o el evento en curso que desee.
- 4 En el cuadro de diálogo Supervisar tarea activa, haga clic en **Cancelar**.

Visualización de la información de licencia en un equipo

Puede ver la información sobre el estado actual de la licencia del software Rapid Recovery Agent instalado en un equipo protegido.

- 1 En la Core Console de Rapid Recovery, en Equipos protegidos, haga clic en el equipo que desea modificar.
Aparecerá la página **Resumen** del equipo seleccionado.
- 2 Haga clic en el menú **Configuración**.
Aparece la página **Configuración**, que muestra los ajustes de configuración del equipo seleccionado.
- 3 Haga clic en el vínculo **Licencias** para desplazarse hasta la página Configuración para visualizar la configuración de licencias específica del equipo.
Aparecerá la pantalla Estado, la cual mostrará detalles sobre las licencias del producto.

Exportación de VM

Este capítulo describe cómo exportar un punto de recuperación para crear una máquina virtual.

Información sobre la exportación a máquinas virtuales con Rapid Recovery

Desde el Core de Rapid Recovery, puede exportar un punto de recuperación de un repositorio a una máquina virtual. Este proceso (denominado en ocasiones exportación virtual) es un proceso físico a virtual (FaV) que crea una máquina virtual a partir de un punto de recuperación. La máquina virtual es un clon de inicio de un equipo protegido.

NOTA: El punto de recuperación utilizado debe formar parte de una cadena de puntos de recuperación completa. Para obtener más información sobre las cadenas de puntos de recuperación, consulte el tema [Cadenas del punto de recuperación y huérfanos](#).

Puede realizar una exportación virtual desde la página Servidor virtual en espera en la Core Console o seleccionando **Exportación de la MV**



desde el menú desplegable **Restaurar** en la barra de botones.

Cuando realiza una exportación virtual desde el Core de Rapid Recovery, tiene dos opciones:

- Puede realizar una **única exportación virtual**, que representa una instantánea única en el tiempo de la información en el punto de recuperación.
- Puede crear un **servidor virtual en espera**. Con el servidor virtual en espera, el Core actualiza continuamente la instantánea de máquina virtual que se crea del punto de recuperación seleccionado después de cada instantánea programada o forzada capturada en la máquina de origen. Esto genera un recurso de alta disponibilidad para la recuperación de datos. Si el equipo protegido falla, puede arrancar la máquina virtual para sustituirlo rápidamente de manera temporal, lo que permite recuperar el equipo protegido original sin un tiempo de inactividad importante.

El siguiente diagrama muestra una implementación típica para exportar datos a una máquina virtual.

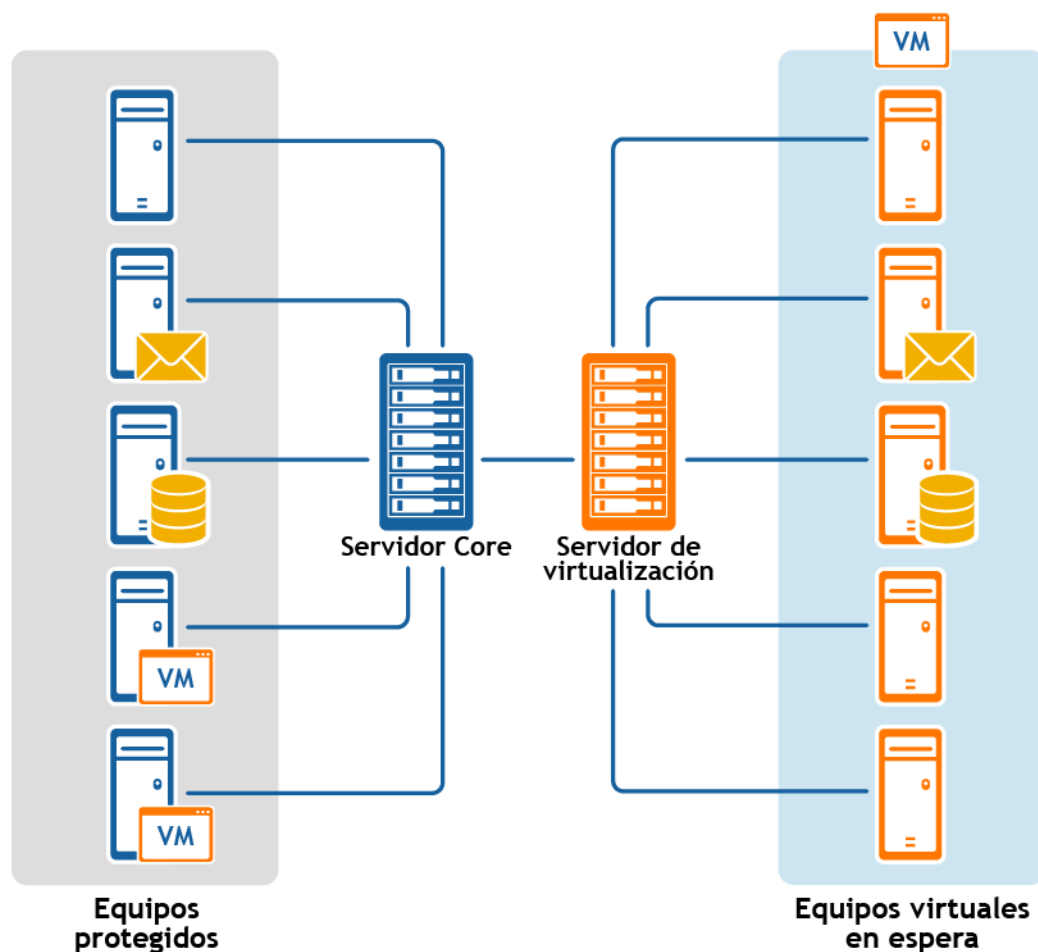


Ilustración 8. Implementación en espera virtual

NOTA: En una configuración que implica replicación, el Core mostrado representa el Core de destino.

Cuando se exporta a una máquina virtual, también se exporta la siguiente información:

- Todos los datos de copia de seguridad desde un punto de recuperación
- El sistema operativo y la configuración del equipo protegido original

Puede realizar una exportación virtual de los puntos de recuperación de sus equipos Windows o Linux protegidos en VMware, ESXi, Hyper-V y VirtualBox.

NOTA: Para ESXi, VMware Workstation o Hyper-V, la versión de la máquina virtual debe ser una versión con licencia de estas máquinas virtuales; no una versión de prueba o gratuita.

Si ha configurado la replicación entre dos Cores (origen y destino), solo podrá exportar datos del Core de destino después de que la replicación inicial se haya completado.

Cómo realizar una exportación de ESXi puntual

Realice los pasos de este procedimiento para realizar una exportación puntual a ESXi.

- 1 En la Core Console de Rapid Recovery, en la barra de botones, haga clic en el menú desplegable **Restaurar** y, a continuación, haga clic en **Exportación de la MV**.
- 2 En el Asistente de exportación de máquinas virtuales, seleccione **Exportación única**.
- 3 Haga clic en **Siguiente**.
- 4 En la página Equipos, seleccione el equipo protegido que desea exportar.
- 5 Haga clic en **Siguiente**.
- 6 En la página Puntos de recuperación, seleccione el punto de recuperación que desea utilizar para la exportación.
- 7 Haga clic en **Siguiente**.
- 8 En la página Destino del Asistente de exportación, en el menú desplegable Recuperar en máquina virtual, seleccione **ESXi(i)**.
- 9 Introduzca los parámetros para acceder a la máquina virtual según se describen en la tabla siguiente y, a continuación, haga clic en **Siguiente**.

Tabla 103. Parámetros de la máquina virtual

Opciones	Descripción
Nombre de host	Escriba un nombre para el equipo host.
Puerto	Escriba el puerto para el equipo host. El valor predeterminado es 443.
Nombre de usuario	Introduzca el nombre de usuario para iniciar sesión en el equipo host.
Contraseña	Introduzca la contraseña para iniciar sesión en el equipo host.

- 10 En la página Opciones de máquina virtual, introduzca la información como se describe en la tabla siguiente.

Tabla 104. Opciones de máquina virtual

Opción	Descripción
Grupo de recursos	Seleccione un bloque de recursos de la lista desplegable.
Almacenamiento de configuración de la máquina virtual	Seleccione un almacén de datos de la lista desplegable.
Nombre de la máquina virtual	Introduzca un nombre para la máquina virtual.
Memoria	Especifique el uso de memoria de la máquina virtual haciendo clic en una de las opciones siguientes: • Utilizar la misma cantidad de RAM que el equipo de origen • Utilizar una cantidad de RAM específica y, a continuación, especificar la cantidad en MB La cantidad mínima es 1024 MB y el máximo permitido por la aplicación es 65536 MB. La cantidad máxima de uso de memoria está limitada por la cantidad de RAM disponible para el equipo host.
Número de procesadores	El número de procesadores (CPU) que desea para la máquina virtual exportada. El valor mínimo es 1.
Cores por procesador	El número de núcleos que desea que tenga cada procesador. El valor mínimo es 1.
Aprovisionamiento de discos	Seleccione el tipo de aprovisionamiento de discos a partir de las siguientes opciones:

Opción	Descripción
	- Compacto. El aprovisionamiento compacto crea un disco virtual con el tamaño del espacio utilizado en los volúmenes originales, en lugar de con el tamaño de todo el volumen. Por ejemplo, si el volumen original es de 1 TB, pero contiene solo 2 GB de espacio utilizado, Rapid Recovery crea un disco virtual de 2 GB. - Grueso. El aprovisionamiento grueso crea un nuevo disco o volumen del mismo tamaño que el volumen original del servidor protegido, incluso si solo se está utilizando una parte del volumen original. Por ejemplo, si el volumen es de 1 TB pero contiene solo 2 GB de espacio utilizado, Rapid Recovery crea un disco virtual de 1 TB.
Asignación de discos	Especifique el tipo de asignación de discos a partir de las siguientes opciones: - Automático - Manual - Con VM
Versión	En la lista desplegable, seleccione la versión de ESXi que se vaya a utilizar para crear la máquina virtual.

11 Haga clic en **Siguiente**.

12 En la página Volúmenes, seleccione los volúmenes que desee exportar y, a continuación, haga clic en **Siguiente**.

13 En la página Resumen, haga clic en **Finalizar** para completar el asistente e iniciar la exportación.

 **NOTA:** Puede supervisar el estado y el progreso de la exportación visualizando las páginas **En espera virtual** y **Eventos**.

Cómo realizar una exportación de ESXi continua (En espera virtual)

Complete los pasos de este procedimiento para realizar una exportación continua a una máquina virtual ESXi (VM) mediante Rapid Recovery.

1 En la Core Console de Rapid Recovery, realice una de las acciones siguientes:

- Desde la Consola de Core, en la barra de botones, haga clic en el menú desplegable  **Restaurar** y después seleccione **Exportación de la MV**.

1 En el Asistente de exportación de máquinas virtuales, seleccione **Continuo (servidor virtual en espera)**.

2 Haga clic en **Siguiente**.

- En Core Console, en la barra de iconos, haga clic en  (En espera virtual).

- En la página **En espera virtual**, haga clic en **Agregar** para iniciar el Asistente de exportación de máquinas virtuales.

2 En la página **Equipos** del Asistente de exportación de máquinas virtuales, seleccione el equipo protegido que quiere exportar.

3 Haga clic en **Siguiente**.

4 En la página **Puntos de recuperación**, seleccione el punto de recuperación que desea utilizar para la exportación.

5 Haga clic en **Siguiente**.

6 En la página **Destino** del Asistente de exportación, en el menú desplegable Recuperar en una máquina virtual, seleccione **ESXi**.

7 Introduzca la información para acceder a la máquina virtual según se describe en la tabla siguiente y, a continuación, haga clic en **Siguiente**.

Tabla 105. Credenciales de ESXi

Opción	Descripción
Nombre de host	Escriba un nombre para el equipo host.
Puerto	Escriba el puerto para el equipo host. El valor predeterminado es 443.
Nombre de usuario	Escriba las credenciales de inicio de sesión para el equipo host.

Opción	Descripción
Contraseña	Escriba las credenciales de inicio de sesión para el equipo host.

- 8 En la página **Opciones de máquina virtual**, introduzca la información que se describe en la tabla siguiente.

Tabla 106. Opciones de máquina virtual

Opción	Descripción
Bloque de recursos	Seleccione un bloque de recursos de la lista desplegable.
Almacén de datos	Seleccione un almacén de datos de la lista desplegable.
Nombre de la máquina virtual	Introduzca un nombre para la máquina virtual.
Memoria	Especifique el uso de memoria de la máquina virtual haciendo clic en una de las opciones siguientes: - Utilizar la misma cantidad de RAM que el equipo de origen - Utilizar una cantidad de RAM específica y, a continuación, especificar la cantidad en MB La cantidad mínima es 1024 MB y el máximo permitido por la aplicación es 65536 MB. La cantidad máxima de uso de memoria está limitada por la cantidad de RAM disponible para el equipo host.
Número de procesadores	El número de procesadores (CPU) que desea para la máquina virtual exportada. El mínimo es 1.
Núcleos por procesador	El número de núcleos que desea tener para cada procesador. El mínimo es 1.
Aprovisionamiento de discos	Seleccione el tipo de aprovisionamiento de discos a partir de las siguientes opciones: - Compacto. El aprovisionamiento compacto crea un disco virtual del tamaño del espacio utilizado en los volúmenes originales, en lugar de el tamaño de todo el volumen. Por ejemplo, si el volumen original es 1 TB, pero contiene solo 2 GB de espacio utilizado, Rapid Recovery crea un disco virtual de 2 GB. - Grueso. El aprovisionamiento grueso crea un disco o volumen nuevo que sea del mismo tamaño que el volumen original del servidor protegido, aunque solo se utilice una parte del volumen original. Por ejemplo, si el volumen es de 1 TB, pero contiene 2 GB de espacio utilizado, Rapid Recovery crea un disco virtual de 1 TB.
Asignación de discos	Especifique el tipo de asignación de discos apropiado (Automática, Manual o con VM).
Versión	Seleccione la versión de la máquina virtual.
Realizar exportación única inicial	Seleccione para realizar la exportación virtual inmediatamente en lugar de hacerlo después de la próxima instantánea programada (opcional).

- 9 Haga clic en **Siguiente**.
- 10 En la página **Volúmenes**, seleccione los volúmenes que quiere exportar y, a continuación, haga clic en **Siguiente**.
- 11 En la página **Resumen**, haga clic en **Finalizar** para completar el asistente e iniciar la exportación.

NOTA: Puede supervisar el estado y el progreso de la exportación visualizando las páginas **En espera virtual** o **Eventos**.

Cómo realizar una exportación de VMWare Workstation puntual

Realice los pasos de este procedimiento para realizar una exportación puntual a VMware Workstation.

- En la Core Console de Rapid Recovery, en la barra de botones, haga clic en el menú desplegable **Restaurar** y, a continuación, haga clic en **Exportación de la MV**.
- En el Asistente de exportación de máquinas virtuales, seleccione **Exportación única**.
- Haga clic en **Siguiente**.
- En la página Equipos, seleccione el equipo protegido que desea exportar.

- 5 Haga clic en **Siguiente**.
- 6 En la página Puntos de recuperación, seleccione el punto de recuperación que desea utilizar para la exportación.
- 7 Haga clic en **Siguiente**.
- 8 En la página Destino del Asistente de exportación, en el menú desplegable Recuperar en máquina virtual, seleccione **VMware Workstation** y, a continuación, haga clic en **Siguiente**.
- 9 En la página Opciones de máquina virtual, introduzca los parámetros para acceder a la máquina virtual como se describen en la tabla siguiente.

Tabla 107. Parámetros de la máquina virtual

Opción	Descripción
VM Machine Location (Ubicación de VM)	Especifique la ruta de acceso de la carpeta local o recurso compartido de red en el que crear la máquina virtual. NOTA: Si ha especificado una ruta de acceso compartida de red, tendrá que escribir credenciales de inicio de sesión válidas para una cuenta registrada en el equipo de destino. La cuenta debe tener permisos de lectura y escritura en el recurso compartido de red.
Nombre de usuario	Introduzca las credenciales de inicio de sesión de la ubicación de red de la exportación. - Si ha especificado una ruta de acceso compartida de red, debe especificar un nombre de usuario válido para una cuenta registrada en el equipo de destino. - Si ha especificado una ruta de acceso local, no hace falta nombre de usuario.
Contraseña	Introduzca las credenciales de inicio de sesión de la ubicación de red de la exportación. - Si ha especificado una ruta de acceso compartida de red, tendrá que especificar una contraseña válida para una cuenta registrada en el equipo de destino. - Si ha especificado una ruta de acceso local, no hace falta contraseña.
Nombre de VM	Escriba un nombre para la máquina virtual que se está creando; por ejemplo, VM-0A1B2C3D4. NOTA: el nombre predeterminado es el nombre del equipo de origen.
Versión	Especifique la versión de VMware Workstation para la máquina virtual. Puede elegir entre: - VMware Workstation 7.0 - VMware Workstation 8.0 - VMware Workstation 9.0 - VMware Workstation 10.0 - VMware Workstation 11.0 - VMware Workstation 12.0
Cantidad de RAM (MB)	Especifique el uso de memoria de la máquina virtual haciendo clic en una de las opciones siguientes: - Utilizar la misma cantidad de RAM que el equipo de origen - Utilizar una cantidad de RAM específica y, a continuación, especificar la cantidad en MB La cantidad mínima es 1024 MB y el máximo permitido por la aplicación es 65536 MB. La cantidad máxima de uso de memoria está limitada por la cantidad de RAM disponible para el equipo host.
Número de procesadores	El número de procesadores (CPU) que desea para la máquina virtual exportada. El valor mínimo es 1.
Núcleos por procesador	El número de núcleos que desea que tenga cada procesador. El valor mínimo es 1.

- 10 Haga clic en **Siguiente**.
- 11 En la página Volúmenes, seleccione los volúmenes que desee exportar, por ejemplo, C:\ y D:\, y, a continuación, haga clic en **Siguiente**.

12 En la página Resumen, haga clic en **Finalizar** para completar el asistente e iniciar la exportación.

 **NOTA:** Puede supervisar el estado y el progreso de la exportación visualizando la ficha **En espera virtual** o **Eventos**.

Cómo realizar una exportación de VMWare Workstation continua (En espera virtual)

Complete los pasos de este procedimiento para realizar una exportación continua a una máquina virtual (VM) VMware Workstation con Rapid Recovery.

1 En la Core Console de Rapid Recovery, realice una de las acciones siguientes:

- Desde la Consola de Core, en la barra de botones, haga clic en el menú desplegable  **Restaurar** y, a continuación, seleccione **Exportación de la VM**.

1 En el Asistente de exportación de máquinas virtuales, seleccione **Continuo (servidor virtual en espera)**.

2 Haga clic en **Siguiente**.

- Desde la Consola de Core, en la barra de iconos, haga clic en  (En espera virtual).
 - En la página **En espera virtual**, haga clic en **Agregar** para iniciar el Asistente de exportación de máquinas virtuales.

2 En la página **Equipos** del Asistente de exportación de máquinas virtuales, seleccione el equipo protegido que quiere exportar.

3 Haga clic en **Siguiente**.

4 En la página **Puntos de recuperación**, seleccione el punto de recuperación que quiere utilizar para la exportación.

5 Haga clic en **Siguiente**.

6 En la página **Destino** del Asistente de exportación de máquinas virtuales, en el menú desplegable Recuperar en una máquina virtual, seleccione **VMware Workstation** y, a continuación, haga clic en **Siguiente**.

7 En la página **Opciones de máquina virtual**, introduzca los parámetros para acceder a la máquina virtual tal como se describen en la tabla siguiente.

Tabla 108. Parámetros de la máquina virtual

Opción	Descripción
Ruta de acceso de destino	Especifique la ruta de acceso de la carpeta local o recurso compartido de red en el que crear la máquina virtual.  NOTA: Si ha especificado una ruta de acceso compartida de red, tendrá que escribir credenciales de inicio de sesión válidas para una cuenta registrada en el equipo de destino. La cuenta debe tener permisos de lectura y escritura en el recurso compartido de red.
Nombre de usuario	Introduzca las credenciales de inicio de sesión de la ubicación de red de la exportación. - Si ha especificado una ruta de acceso compartida de red, debe especificar un nombre de usuario válido para una cuenta registrada en el equipo de destino. - Si ha especificado una ruta de acceso local, no hace falta nombre de usuario.
Contraseña	Introduzca las credenciales de inicio de sesión de la ubicación de red de la exportación. - Si ha especificado una ruta de acceso compartida de red, tendrá que especificar una contraseña válida para una cuenta registrada en el equipo de destino. - Si ha especificado una ruta de acceso local, no hace falta contraseña.
Máquina virtual	Escriba un nombre para la máquina virtual que se está creando; por ejemplo, VM-0A1B2C3D4.  NOTA: el nombre predeterminado es el nombre del equipo de origen.

Opción	Descripción
Versión	Especifique la versión de VMware Workstation para la máquina virtual. Puede elegir entre: • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0 • VMware Workstation 10.0 • VMware Workstation 11.0 • VMware Workstation 12.0
Memoria	Especifique el uso de memoria de la máquina virtual haciendo clic en una de las opciones siguientes: • Utilizar la misma cantidad de RAM que el equipo de origen • Utilizar una cantidad de RAM específica y, a continuación, especificar la cantidad en MB La cantidad mínima es 1024 MB y el máximo permitido por la aplicación es 65536 MB. La cantidad máxima de uso de memoria está limitada por la cantidad de RAM disponible para el equipo host.
Número de procesadores	El número de procesadores (CPU) que desea para la máquina virtual exportada. El mínimo es 1.
Núcleos por procesador	El número de núcleos que desea tener para cada procesador. El mínimo es 1.

- 8 Seleccione **Realizar exportación única inicial** para realizar la exportación virtual inmediatamente en lugar de hacerlo después de la próxima instantánea programada.
- 9 Haga clic en **Siguiente**.
- 10 En la página **Volúmenes**, seleccione los volúmenes que desee exportar, por ejemplo, C:\ y D:\, y, a continuación, haga clic en **Siguiente**.
- 11 En la página **Resumen**, haga clic en **Finalizar** para completar el asistente y para iniciar la exportación.

 **NOTA:** Puede supervisar el estado y el progreso de la exportación visualizando las páginas **En espera virtual** o **Eventos**.

Cómo realizar una exportación de Hyper-V puntual

Realice los pasos de este procedimiento para realizar una exportación puntual a Hyper-V.

- 1 En la Core Console de Rapid Recovery, en la barra de botones, haga clic en el menú desplegable **Restaurar**, haga clic en **Exportación de la VM**.
- 2 En el Asistente de exportación de máquinas virtuales, seleccione **Exportación única**.
- 3 Haga clic en **Siguiente**.
- 4 En la página **Equipos**, seleccione el equipo protegido que quiere importar.
- 5 Haga clic en **Siguiente**.
- 6 En la página **Puntos de recuperación**, seleccione el punto de recuperación que desea utilizar para la exportación.
- 7 Haga clic en **Siguiente**.
- 8 En la página **Destino**, en el menú desplegable Exportar a máquina virtual, seleccione **Hyper-V**.
- 9 Para exportar a un equipo local con el rol Hyper-V asignado, haga clic en **Utilizar equipo local**.
- 10 Para indicar que el servidor Hyper-V se encuentra en un equipo remoto, haga clic en **Host remoto** y, a continuación, introduzca la información del host remoto como se describe en la tabla siguiente.

Tabla 109. Información de host remoto

Cuadro de texto	Descripción
Nombre de host	Especifique la dirección IP o el nombre de host para el servidor Hyper-V. Representa la dirección IP o nombre de host del servidor Hyper-V remoto.
Puerto	Especifique un número de puerto para el equipo. Representa el puerto por el que el Core se comunica con este equipo.
Nombre de usuario	Especifique el nombre de usuario para el usuario con permisos administrativos para la estación de trabajo con el servidor Hyper-V. Se utiliza para especificar las credenciales de inicio de sesión para la máquina virtual.
Contraseña	Especifique la contraseña para la cuenta de usuario con permisos administrativos en la estación de trabajo con el servidor Hyper-V. Se utiliza para especificar las credenciales de inicio de sesión para la máquina virtual.

11 Haga clic en **Siguiente**.

12 En la página **Opciones de máquinas virtuales** del cuadro de texto **Ubicación de la máquina virtual**, introduzca la ruta de acceso de la máquina virtual; por ejemplo, **D:\export**. Esto se utiliza para identificar la ubicación de la máquina virtual.

NOTA: Debe especificar la ubicación de la máquina virtual tanto para los servidores locales como remotos de Hyper-V. La ruta de acceso debe ser una ruta de acceso local válida para el servidor Hyper-V. Los directorios que no existan se crean automáticamente. No debería intentar crearlos manualmente. La exportación a carpetas compartidas (por ejemplo a \\datos\compartición) no está permitida.

13 En el cuadro de texto **Nombre de la máquina virtual**, introduzca un nombre para la máquina virtual.

El nombre que especifique aparecerá en la lista de máquinas virtuales en la consola Administrador de Hyper-V.

14 Para especificar el uso de la memoria, haga clic en una de las opciones siguientes:

- **Utilizar la misma cantidad de RAM que el equipo de origen.** Seleccione esta opción para identificar que el uso de RAM es idéntico entre la máquina virtual y la de origen.
- **Utilizar una cantidad específica de RAM.** Seleccione esta opción si desea especificar la cantidad de RAM en MB. La cantidad mínima es 1024 MB y el máximo permitido por la aplicación es 65536 MB. La cantidad máxima de uso de memoria está limitada por la cantidad de RAM disponible para el equipo host.

15 Para especificar el formato de disco, junto a Formato de disco, haga clic en una de las siguientes opciones:

- VHDX
- VHD

NOTA: La exportación de Hyper-V admite formatos de disco VHDX si el equipo de destino ejecuta Windows 8 (Windows Server 2012) o posterior. Si VHDX no se admite para su entorno, la opción está desactivada. Si está exportando a Hyper-V de segunda generación, solo se admite la operación de formato de disco VHDX.

16 Para especificar la generación de Hyper-V que hay que emplear para la exportación, haga clic en uno de los siguientes elementos:

- Generación 1
- Generación 2

NOTA: Solo la segunda generación admite la opción de inicio seguro.

17 Especifique el adaptador de red apropiado para la VM exportada.

18 En la página **Volúmenes**, seleccione los volúmenes que se van a exportar, por ejemplo, C:\.

NOTA: Si los volúmenes seleccionados tienen mayor capacidad que las asignaciones máximas apropiadas admitidas por la aplicación como se indica a continuación, o bien superan la cantidad de espacio disponible, aparecerá un error.

- Para el formato de disco VHDX, sus volúmenes seleccionados no deben tener un tamaño superior a 64 TB.
- Para el formato de disco VHD, sus volúmenes seleccionados no deben tener un tamaño superior a 2040 GB.

19 En la página **Volúmenes**, haga clic en **Finalizar** para completar el asistente e iniciar la exportación.

NOTA: Para supervisar el estado y el progreso de la exportación, visualice **En espera virtual** o las páginas **Eventos**.

Complete los pasos de este procedimiento para realizar una exportación continua a una máquina virtual Hyper-V (VM) utilizando Rapid Recovery.

- Desde la Core Console, en la barra de botones, haga clic en el menú desplegable  **Restaurar** y después seleccione **Exportación de la MV**.



- 1 En el Asistente de exportación de máquinas virtuales, seleccione **Continuo (servidor virtual en espera)**.
- 2 Haga clic en **Siguiente**.

- En Core Console, en la barra de iconos, haga clic en  (En espera virtual).
- En la página **En espera virtual**, haga clic en **Agregar** para iniciar el Asistente de exportación de máquinas virtuales.

- 3 Haga clic en **Siguiente**.

- 5 Haga clic en **Siguiente**.

- 6 En la página **Destino**, en el menú desplegable Exportar a una máquina virtual, seleccione **Hyper-V** y después realice una de las siguientes opciones:

- Para exportar a un equipo local con el rol Hyper-V asignado, haga clic en **Utilizar equipo local**.
- Para indicar que el servidor Hyper-V se encuentra en un equipo remoto, haga clic en **Host remoto** y, a continuación, introduzca los parámetros del host remoto como se describe en la tabla siguiente.

Cuadro de texto	Descripción
Nombre de host	Especifique la dirección IP o el nombre de host para el servidor Hyper-V. Representa la dirección IP o nombre de host del servidor Hyper-V remoto.
Puerto	Especifique un número de puerto para el equipo. Representa el puerto por el que el Core se comunica con este equipo.
Nombre de usuario	Especifique el nombre de usuario para el usuario con permisos administrativos para la estación de trabajo con el servidor Hyper-V. Se utiliza para especificar las credenciales de inicio de sesión para la máquina virtual.
Contraseña	Especifique la contraseña para la cuenta de usuario con permisos administrativos en la estación de trabajo con el servidor Hyper-V. Se utiliza para especificar las credenciales de inicio de sesión para la máquina virtual.

- 8 En la página **Virtual Machines Options** (Opciones de máquinas virtuales) del cuadro de texto **Ubicación de la máquina virtual**, introduzca la ruta de acceso de la máquina virtual; por ejemplo, **D:\export**. Esto se utiliza para identificar la ubicación de la máquina virtual.

NOTA: Debe especificar la ubicación de la máquina virtual tanto para los servidores locales como remotos de Hyper-V. La ruta de acceso debe ser una ruta de acceso local válida para el servidor Hyper-V. Los directorios que no existan se crean automáticamente. No debería intentar crearlos manualmente. La exportación a carpetas compartidas (por ejemplo a \\data\share) no está permitida.

- El nombre que especifique aparecerá en la lista de máquinas virtuales en la consola Administrador de Hyper-V.

- **Utilizar la misma cantidad de RAM que el equipo de origen.** Seleccione esta opción para identificar que el uso de RAM es idéntico entre los equipos virtuales y de origen.

- **Utilizar una cantidad específica de RAM.** Seleccione esta opción si desea especificar la cantidad de RAM en MB. La cantidad mínima es 1024 MB y el máximo permitido por la aplicación es 65536 MB. La cantidad máxima de uso de memoria está limitada por la cantidad de RAM disponible para el equipo host.

11 Para especificar el formato de disco, junto a Formato de disco, haga clic en una de las siguientes opciones:

- VHDX
- VHD

NOTA: La exportación de Hyper-V admite formatos de disco VHDX si el equipo de destino ejecuta Windows 8 (Windows Server 2012) o posterior. Si VHDX no se admite para su entorno, la opción está desactivada. Si está exportando a Hyper-V de segunda generación, solo se admite la operación de formato de disco VHDX.

12 Para especificar la generación de Hyper-V que hay que emplear para la exportación, haga clic en uno de los siguientes elementos:

- Generación 1
- Generación 2

NOTA: Solo la segunda generación admite la opción de inicio seguro.

13 Especifique el adaptador de red apropiado para la VM exportada.

14 En la página **Volumes (Volúmenes)**, seleccione los volúmenes que se van a exportar, por ejemplo, C:\.

NOTA: Si los volúmenes seleccionados tienen mayor capacidad que las asignaciones máximas apropiadas admitidas por la aplicación como se indica a continuación, o bien superan la cantidad de espacio disponible, aparecerá un error.

- Para el formato de disco VHDX, sus volúmenes seleccionados no deben tener un tamaño superior a 64 TB.
- Para el formato de disco VHD, sus volúmenes seleccionados no deben tener un tamaño superior a 2040 GB.

15 Seleccione **Realizar exportación única inicial** para realizar la exportación virtual inmediatamente en lugar de hacerlo después de la próxima instantánea programada.

16 En la página **Volúmenes**, haga clic en **Finalizar** para completar el asistente y para iniciar la exportación.

NOTA: Puede supervisar el estado y el progreso de la exportación visualizando las páginas **En espera virtual** o **Eventos**.

Cómo realizar una exportación de VirtualBox puntual

Realice los pasos de este procedimiento para realizar una exportación puntual a VirtualBox.

- 1 En la Core Console de Rapid Recovery, en la barra de botones, haga clic en el menú desplegable **Restaurar** y, a continuación, haga clic en **Exportación de la MV**.
- 2 En el Asistente de exportación de máquinas virtuales, seleccione **Exportación única**.
- 3 Haga clic en **Siguiente**.
- 4 En la página Equipos, seleccione el equipo protegido que desea exportar.
- 5 Haga clic en **Siguiente**.
- 6 En la página Puntos de recuperación, seleccione el punto de recuperación que desea utilizar para la exportación.
- 7 Haga clic en **Siguiente**.
- 8 En la página Destino del Asistente de exportación, en el menú desplegable Recuperar en máquina virtual, seleccione **VirtualBox** y, a continuación, haga clic en **Siguiente**.
- 9 En la página Opciones de máquina virtual, seleccione **Utilizar equipo con Windows**.
- 10 Especifique los parámetros para acceder a la máquina virtual, según se describe en la tabla siguiente.

Tabla 111. Parámetros de la máquina virtual

Opción	Descripción
Nombre de la máquina virtual	Introduzca un nombre para la máquina virtual que se está creando.

Opción	Descripción
 NOTA: el nombre predeterminado es el nombre del equipo de origen.	
Ruta de acceso de destino	Especifique una ruta de acceso de destino local o remota para crear la máquina virtual.  NOTA: La ruta de acceso de destino no debería ser un directorio raíz. Si especifica una ruta de acceso compartida de red, tendrá que especificar credenciales de inicio de sesión válidas (nombre de usuario y contraseña) para una cuenta registrada en el equipo de destino. La cuenta debe tener permisos de lectura y escritura en el recurso compartido de red.
Memoria	Especifique el uso de memoria de la máquina virtual haciendo clic en una de las opciones siguientes: - Utilizar la misma cantidad de RAM que el equipo de origen - Utilizar una cantidad de RAM específica y, a continuación, especificar la cantidad en MB La cantidad mínima es 1024 MB y el máximo permitido por la aplicación es 65536 MB. La cantidad máxima de uso de memoria está limitada por la cantidad de RAM disponible para el equipo host.
11	Para especificar una cuenta de usuario para la máquina virtual, seleccione Especificar la cuenta de usuario para la máquina virtual exportada y, a continuación, introduzca la información siguiente. Esto hace referencia a una cuenta de usuario específica para la que se registrará la máquina virtual en el caso de que haya varias cuentas de usuario en la máquina virtual. Cuando esta cuenta de usuario esté registrada, solamente este usuario verá esta máquina virtual en el administrador de VirtualBox. Si no se especifica una cuenta, la máquina virtual se registrará para todos los usuarios existentes en el equipo con Windows con VirtualBox. - Nombre de usuario: Introduzca el nombre de usuario para el que está registrada la máquina virtual. - Contraseña: Introduzca la contraseña para esta cuenta de usuario.
12	Haga clic en Siguiente .
13	En la página Volúmenes, seleccione los volúmenes que desee exportar, por ejemplo, C:\ y D:\, y, a continuación, haga clic en Siguiente .
14	En la página Resumen, haga clic en Finalizar para completar el asistente e iniciar la exportación.
 NOTA: Puede supervisar el estado y el progreso de la exportación visualizando la ficha En espera virtual o Eventos.	

Cómo realizar una exportación de VirtualBox continua (En espera virtual)

Para realizar este paso, VirtualBox debe estar instalado en el equipo del Core.

Complete los pasos de este procedimiento para realizar una exportación continua a una máquina virtual (VM) de VirtualBox mediante Rapid Recovery.

- En la Core Console de Rapid Recovery, realice una de las acciones siguientes:

- Desde la Consola de Core, en la barra de botones, haga clic en el menú desplegable  **Restaurar** y, a continuación, seleccione **Exportación de la VM**.

- En el Asistente de exportación de máquinas virtuales, seleccione **Continuo (servidor virtual en espera)**.

- Haga clic en **Siguiente**.

- Desde la Consola de Core, en la barra de iconos, haga clic en  (En espera virtual).
 - En la página **En espera virtual**, haga clic en **Agregar** para iniciar el Asistente de exportación de máquinas virtuales.

- En la página **Equipos** del Asistente de exportación de máquinas virtuales, seleccione el equipo protegido que quiere exportar.

- Haga clic en **Siguiente**.

- En la página **Puntos de recuperación**, seleccione el punto de recuperación que desea utilizar para la exportación.

- Haga clic en **Siguiente**.

- En la página **Destino** del Asistente de exportación, en el menú desplegable **Recuperar en una máquina virtual**, seleccione **VirtualBox**.

- 7 En la página **Opciones de máquina virtual**, seleccione **Equipo remoto Linux**.
- 8 Introduzca información sobre la máquina virtual según se describe en la tabla siguiente.

Tabla 112. Configuración del equipo Linux remoto

Opción	Descripción
Nombre de host de VirtualBox	Introduzca una dirección IP o un nombre de host para el servidor VirtualBox. Este campo representa la dirección IP o el nombre de host del servidor VirtualBox remoto.
Puerto	Especifique un número de puerto para el equipo. Este número representa el puerto por el que el Core se comunica con este equipo.
Nombre de la máquina virtual	Introduzca un nombre para la máquina virtual que se está creando. NOTA: el nombre predeterminado es el nombre del equipo de origen.
Ruta de acceso de destino	Especifique una ruta de acceso de destino para crear la máquina virtual. NOTA: Se recomienda que cree una carpeta raíz desde la raíz para que la máquina virtual se ejecute desde la raíz. Si no utiliza la raíz, deberá crear la carpeta de destino manualmente en el equipo de destino antes de configurar la exportación. También deberá vincular o cargar manualmente la máquina virtual después de la exportación.
Nombre de usuario	Nombre de usuario de la cuenta del equipo de destino, por ejemplo, raíz.
Contraseña	Contraseña de la cuenta de usuario del equipo de destino.
Memoria	Especifique el uso de memoria de la máquina virtual haciendo clic en una de las opciones siguientes: - Utilizar la misma cantidad de RAM que el equipo de origen - Utilizar una cantidad de RAM específica y, a continuación, especificar la cantidad en MB La cantidad mínima es 1024 MB y el máximo permitido por la aplicación es 65536 MB. La cantidad máxima de uso de memoria está limitada por la cantidad de RAM disponible para el equipo host.

- 9 Seleccione **Realizar exportación única inicial** para realizar la exportación virtual inmediatamente en lugar de hacerlo después de la próxima instantánea programada.
- 10 Haga clic en **Siguiente**.
- 11 En la página **Volúmenes**, seleccione los volúmenes de datos que desea exportar y, a continuación, haga clic en **Siguiente**.
- 12 En la página **Resumen**, haga clic en **Finalizar** para completar el asistente y para iniciar la exportación.

NOTA: Puede supervisar el estado y el progreso de la exportación visualizando las páginas **En espera virtual** o **Eventos**.

Administración de exportaciones

Si el Core tiene la exportación virtual establecida, los parámetros de configuración de cada exportación virtual aparecen como una fila en la página **En espera virtual**. Desde aquí puede ver el estado de las exportaciones que ha configurado actualmente y gestionar sus equipos en espera virtual. Puede agregar una espera virtual, forzar la exportación, pausar o reanudar la espera virtual o eliminar los requisitos de la exportación continua.

Cuando se lleva a cabo una exportación única, el trabajo se incluye en la cola de exportación en la página **En espera virtual**. Durante este tiempo, puede pausar, reanudar o cancelar la operación de exportación.

NOTA: Rapid Recovery admite la exportación de Hyper-V a Windows 8, Windows 8.1, Windows Server 2012 y 2012 R2.

La exportación virtual a una VM en espera virtual no se produce si la VM está encendida.

Complete los pasos de este procedimiento para gestionar las exportaciones virtuales.

- 1 En la Consola de Core, en la barra de iconos, haga clic en  (En espera virtual). Aparece la página **En espera virtual**. Aquí puede ver dos tablas de la configuración guardada de la exportación. Incluyen la información que se describe en la tabla siguiente.

Tabla 113. Información de espera virtual

Columna	Descripción
Select item (Seleccionar elemento)	En cada fila de la tabla de resumen, puede seleccionar la casilla de verificación para llevar a cabo acciones de la lista de opciones de menú anterior a la tabla.
Indicador de estado	Las esferas de colores de la columna Estado muestran el estado de la espera virtual. Si pasa el cursor sobre el círculo coloreado, se muestra la condición de estado. • Verde. La espera virtual se ha configurado correctamente, está activa y no está en pausa. La exportación siguiente se lleva a cabo inmediatamente después de que se haya completado la instantánea siguiente. • Amarillo. Se pausa la espera virtual, pero los parámetros aún están definidos y guardados en el Core. Sin embargo, tras una nueva transferencia, el trabajo de exportación no se iniciará automáticamente y no habrá nuevas exportaciones para este equipo protegido hasta que cambie el estado.
Nombre del equipo	Nombre del equipo de origen.
Destino	Máquina virtual y ruta de acceso a la que los datos se están exportando.
Tipo de exportación	El tipo de plataforma de máquina virtual para la exportación, como ESXi, VMware, Hyper-V o VirtualBox.
Última exportación	Fecha y hora de la última exportación Si se acaba de agregar una exportación, pero no se ha completado, se muestra un mensaje que indica que la exportación todavía no se ha realizado. Si una exportación ha fallado o se canceló, también se muestra el mensaje correspondiente.
Configuración	El menú desplegable  permite realizar las siguientes funciones: • Editar. Permite editar la configuración de la espera virtual. • Forzar. Fuerza una exportación virtual. • Pausar. Pausa la exportación virtual. Solo está disponible cuando el estado está activo. • Reanudar. Reanuda la exportación virtual. Sólo está disponible cuando el estado está en pausa. • Quitar. Elimina el requisito de una exportación continua. No elimina la VM exportada actualizada más recientemente.

Tabla 114. Información de la cola de exportación

Columna	Descripción
Select item (Seleccionar elemento)	En cada fila de la tabla de resumen, puede seleccionar la casilla de verificación para llevar a cabo acciones de la lista de opciones de menú anterior a la tabla.
Destino	Máquina virtual y ruta de acceso a la que los datos se están exportando.
Tipo de exportación	El tipo de plataforma de máquina virtual para la exportación, como ESXi, VMware, Hyper-V o VirtualBox.
Tipo de calendario de programación	Tipo de exportación, ya sea Puntual o Continua.

Columna	Descripción
Estado	Progreso de la exportación, mostrado como porcentaje en una barra de progreso.
2	Para gestionar los ajustes de exportación guardados, seleccione una exportación y, a continuación, haga clic en una de las siguientes opciones: • Editar. Se abre el Asistente de exportación de máquinas virtuales en la página Opciones de VM. Desde aquí puede cambiar la ubicación de la VM exportada, cambiar la versión del tipo de VM o especificar la RAM o los procesadores para la exportación. Para iniciar inmediatamente la exportación de VM, seleccione Realizar exportación única inicial. • Forzar. Fuerza una nueva exportación. Esta opción podría ser de utilidad cuando el estado en espera virtual esté pausado y luego se reanuda, lo que significa que el trabajo de exportación se reiniciará solamente después de una nueva transferencia. Si no desea esperar a la nueva transferencia, puede forzar una exportación. • Pausar. Pausa una exportación activa. • Reanudar. Se reanuda el requisito de la exportación continua en la próxima instantánea forzada o programada.
3	Para eliminar una exportación del sistema, seleccione el exportar y, a continuación, haga clic en Quitar. La configuración de exportación se elimina de manera permanente del sistema. Al eliminar la configuración de espera virtual no se eliminan las máquinas virtuales exportadas como resultado de la configuración.
4	Para gestionar el número de exportaciones que se ejecutan al mismo tiempo, haga lo siguiente: • Debajo de Cola de exportación, haga clic en Configuración. • En el cuadro de diálogo N.º máximo de exportaciones simultáneas, introduzca el número de exportaciones que quiere ejecutar de forma simultánea. El número predeterminado es 5. • Haga clic en Guardar.
5	Para cancelar una exportación única o continua que se incluye actualmente en la cola de exportación, seleccione la exportación y, a continuación, haga clic en Cancelar.
6	Para agregar una nueva exportación en espera virtual, puede hacer clic en Agregar para iniciar el Asistente de exportación. Para obtener más información sobre cómo configurar el estado en espera virtual para una máquina virtual específica, consulte uno de los temas siguientes: • Exportación de datos a una máquina virtual ESXi • Exportación de datos a una máquina virtual VMWare Workstation • Exportación de datos a una máquina virtual Hyper-V • Exportación de datos a una máquina virtual VirtualBox

Exportación de datos a una máquina virtual ESXi

En Rapid Recovery, puede decidir exportar datos a ESXi realizando una exportación única o estableciendo una exportación continua (para el estado en espera virtual). Realice los pasos de los procedimientos siguientes para el tipo de exportación adecuado.

Cómo realizar una exportación de ESXi puntual

Realice los pasos de este procedimiento para realizar una exportación puntual a ESXi.

- 1 En la Core Console de Rapid Recovery, en la barra de botones, haga clic en el menú desplegable **Restaurar** y, a continuación, haga clic en **Exportación de la MV**.
- 2 En el Asistente de exportación de máquinas virtuales, seleccione **Exportación única**.
- 3 Haga clic en **Siguiente**.
- 4 En la página Equipos, seleccione el equipo protegido que desea exportar.
- 5 Haga clic en **Siguiente**.
- 6 En la página Puntos de recuperación, seleccione el punto de recuperación que desea utilizar para la exportación.
- 7 Haga clic en **Siguiente**.
- 8 En la página Destino del Asistente de exportación, en el menú desplegable Recuperar en máquina virtual, seleccione **ESX(i)**.

- 9 Introduzca los parámetros para acceder a la máquina virtual según se describen en la tabla siguiente y, a continuación, haga clic en **Siguiente**.

Tabla 115. Parámetros de la máquina virtual

Opciones	Descripción
Nombre de host	Escriba un nombre para el equipo host.
Puerto	Escriba el puerto para el equipo host. El valor predeterminado es 443.
Nombre de usuario	Introduzca el nombre de usuario para iniciar sesión en el equipo host.
Contraseña	Introduzca la contraseña para iniciar sesión en el equipo host.

- 10 En la página Opciones de máquina virtual, introduzca la información como se describe en la tabla siguiente.

Tabla 116. Opciones de máquina virtual

Opción	Descripción
Grupo de recursos	Seleccione un bloque de recursos de la lista desplegable.
Almacenamiento de configuración de la máquina virtual	Seleccione un almacén de datos de la lista desplegable.
Nombre de la máquina virtual	Introduzca un nombre para la máquina virtual.
Memoria	Especifique el uso de memoria de la máquina virtual haciendo clic en una de las opciones siguientes: - Utilizar la misma cantidad de RAM que el equipo de origen - Utilizar una cantidad de RAM específica y, a continuación, especificar la cantidad en MB La cantidad mínima es 1024 MB y el máximo permitido por la aplicación es 65536 MB. La cantidad máxima de uso de memoria está limitada por la cantidad de RAM disponible para el equipo host.
Número de procesadores	El número de procesadores (CPU) que desea para la máquina virtual exportada. El valor mínimo es 1.
Cores por procesador	El número de núcleos que desea que tenga cada procesador. El valor mínimo es 1.
Aprovisionamiento de discos	Seleccione el tipo de aprovisionamiento de discos a partir de las siguientes opciones: - Compacto. El aprovisionamiento compacto crea un disco virtual con el tamaño del espacio utilizado en los volúmenes originales, en lugar de con el tamaño de todo el volumen. Por ejemplo, si el volumen original es de 1 TB, pero contiene solo 2 GB de espacio utilizado, Rapid Recovery crea un disco virtual de 2 GB. - Grueso. El aprovisionamiento grueso crea un nuevo disco o volumen del mismo tamaño que el volumen original del servidor protegido, incluso si solo se está utilizando una parte del volumen original. Por ejemplo, si el volumen es de 1 TB pero contiene solo 2 GB de espacio utilizado, Rapid Recovery crea un disco virtual de 1 TB.
Asignación de discos	Especifique el tipo de asignación de discos a partir de las siguientes opciones: - Automático - Manual - Con VM
Versión	En la lista desplegable, seleccione la versión de ESXi que se vaya a utilizar para crear la máquina virtual.

- 11 Haga clic en **Siguiente**.
- 12 En la página Volúmenes, seleccione los volúmenes que desee exportar y, a continuación, haga clic en **Siguiente**.
- 13 En la página Resumen, haga clic en **Finalizar** para completar el asistente e iniciar la exportación.

 **NOTA:** Puede supervisar el estado y el progreso de la exportación visualizando las páginas En espera virtual y Eventos.

Cómo realizar una exportación de ESXi continua (En espera virtual)

Complete los pasos de este procedimiento para realizar una exportación continua a una máquina virtual ESXi (VM) mediante Rapid Recovery.

1 En la Core Console de Rapid Recovery, realice una de las acciones siguientes:

- Desde la Consola de Core, en la barra de botones, haga clic en el menú desplegable  **Restaurar** y después seleccione **Exportación de la MV**.

1 En el Asistente de exportación de máquinas virtuales, seleccione **Continuo (servidor virtual en espera)**.

2 Haga clic en **Siguiente**.

- En Core Console, en la barra de iconos, haga clic en  (En espera virtual).

- En la página **En espera virtual**, haga clic en **Agregar** para iniciar el Asistente de exportación de máquinas virtuales.

2 En la página **Equipos** del Asistente de exportación de máquinas virtuales, seleccione el equipo protegido que quiere exportar.

3 Haga clic en **Siguiente**.

4 En la página **Puntos de recuperación**, seleccione el punto de recuperación que desea utilizar para la exportación.

5 Haga clic en **Siguiente**.

6 En la página **Destino** del Asistente de exportación, en el menú desplegable Recuperar en una máquina virtual, seleccione **ESXi**.

7 Introduzca la información para acceder a la máquina virtual según se describe en la tabla siguiente y, a continuación, haga clic en **Siguiente**.

Tabla 117. Credenciales de ESXi

Opción	Descripción
Nombre de host	Escriba un nombre para el equipo host.
Puerto	Escriba el puerto para el equipo host. El valor predeterminado es 443.
Nombre de usuario	Escriba las credenciales de inicio de sesión para el equipo host.
Contraseña	Escriba las credenciales de inicio de sesión para el equipo host.

8 En la página **Opciones de máquina virtual**, introduzca la información que se describe en la tabla siguiente.

Tabla 118. Opciones de máquina virtual

Opción	Descripción
Bloque de recursos	Seleccione un bloque de recursos de la lista desplegable.
Almacén de datos	Seleccione un almacén de datos de la lista desplegable.
Nombre de la máquina virtual	Introduzca un nombre para la máquina virtual.
Memoria	Especifique el uso de memoria de la máquina virtual haciendo clic en una de las opciones siguientes: - Utilizar la misma cantidad de RAM que el equipo de origen - Utilizar una cantidad de RAM específica y, a continuación, especificar la cantidad en MB La cantidad mínima es 1024 MB y el máximo permitido por la aplicación es 65536 MB. La cantidad máxima de uso de memoria está limitada por la cantidad de RAM disponible para el equipo host.

Opción	Descripción
Número de procesadores	El número de procesadores (CPU) que desea para la máquina virtual exportada. El mínimo es 1.
Núcleos por procesador	El número de núcleos que desea tener para cada procesador. El mínimo es 1.
Aprovisionamiento de discos	Seleccione el tipo de aprovisionamiento de discos a partir de las siguientes opciones: - Compacto. El aprovisionamiento compacto crea un disco virtual del tamaño del espacio utilizado en los volúmenes originales, en lugar de el tamaño de todo el volumen. Por ejemplo, si el volumen original es 1 TB, pero contiene solo 2 GB de espacio utilizado, Rapid Recovery crea un disco virtual de 2 GB. - Grueso. El aprovisionamiento grueso crea un disco o volumen nuevo que sea del mismo tamaño que el volumen original del servidor protegido, aunque solo se utilice una parte del volumen original. Por ejemplo, si el volumen es de 1 TB, pero contiene 2 GB de espacio utilizado, Rapid Recovery crea un disco virtual de 1 TB.
Asignación de discos	Especifique el tipo de asignación de discos apropiado (Automática, Manual o con VM).
Versión	Seleccione la versión de la máquina virtual.
Realizar exportación única inicial	Seleccione para realizar la exportación virtual inmediatamente en lugar de hacerlo después de la próxima instantánea programada (opcional).

9 Haga clic en **Siguiente**.

10 En la página **Volúmenes**, seleccione los volúmenes que quiere exportar y, a continuación, haga clic en **Siguiente**.

11 En la página **Resumen**, haga clic en **Finalizar** para completar el asistente e iniciar la exportación.

 **NOTA:** Puede supervisar el estado y el progreso de la exportación visualizando las páginas **En espera virtual** o **Eventos**.

Exportación de datos a una máquina virtual VirtualBox

En Rapid Recovery, puede exportar datos a una exportación de VirtualBox mediante una exportación única o estableciendo una exportación continua (para el servidor virtual en espera).

 **NOTA:** La exportación de VirtualBox de un equipo protegido de Windows 10 no es compatible actualmente.

Realice los pasos de los procedimientos siguientes para el tipo de exportación adecuado.

 **NOTA:** Para realizar este tipo de exportación, debería tener VirtualBox instalado en el equipo Core. Se admite VirtualBox versión 4.2.18 o posterior para hosts Windows.

Cómo realizar una exportación de VirtualBox puntual

Realice los pasos de este procedimiento para realizar una exportación puntual a VirtualBox.

- 1 En la Core Console de Rapid Recovery, en la barra de botones, haga clic en el menú desplegable **Restaurar** y, a continuación, haga clic en **Exportación de la MV**.
- 2 En el Asistente de exportación de máquinas virtuales, seleccione **Exportación única**.
- 3 Haga clic en **Siguiente**.
- 4 En la página Equipos, seleccione el equipo protegido que desea exportar.
- 5 Haga clic en **Siguiente**.
- 6 En la página Puntos de recuperación, seleccione el punto de recuperación que desea utilizar para la exportación.
- 7 Haga clic en **Siguiente**.
- 8 En la página Destino del Asistente de exportación, en el menú desplegable Recuperar en máquina virtual, seleccione **VirtualBox** y, a continuación, haga clic en **Siguiente**.
- 9 En la página Opciones de máquina virtual, seleccione **Utilizar equipo con Windows**.

- 10 Especifique los parámetros para acceder a la máquina virtual, según se describe en la tabla siguiente.

Tabla 119. Parámetros de la máquina virtual

Opción	Descripción
Nombre de la máquina virtual	Introduzca un nombre para la máquina virtual que se está creando.  NOTA: el nombre predeterminado es el nombre del equipo de origen.
Ruta de acceso de destino	Especifique una ruta de acceso de destino local o remota para crear la máquina virtual.  NOTA: La ruta de acceso de destino no debería ser un directorio raíz. Si especifica una ruta de acceso compartida de red, tendrá que especificar credenciales de inicio de sesión válidas (nombre de usuario y contraseña) para una cuenta registrada en el equipo de destino. La cuenta debe tener permisos de lectura y escritura en el recurso compartido de red.
Memoria	Especifique el uso de memoria de la máquina virtual haciendo clic en una de las opciones siguientes: - Utilizar la misma cantidad de RAM que el equipo de origen - Utilizar una cantidad de RAM específica y, a continuación, especificar la cantidad en MB La cantidad mínima es 1024 MB y el máximo permitido por la aplicación es 65536 MB. La cantidad máxima de uso de memoria está limitada por la cantidad de RAM disponible para el equipo host.

- 11 Para especificar una cuenta de usuario para la máquina virtual, seleccione **Especificar la cuenta de usuario para la máquina virtual exportada** y, a continuación, introduzca la información siguiente. Esto hace referencia a una cuenta de usuario específica para la que se registrará la máquina virtual en el caso de que haya varias cuentas de usuario en la máquina virtual. Cuando esta cuenta de usuario esté registrada, solamente este usuario verá esta máquina virtual en el administrador de VirtualBox. Si no se especifica una cuenta, la máquina virtual se registrará para todos los usuarios existentes en el equipo con Windows con VirtualBox.
- Nombre de usuario: Introduzca el nombre de usuario para el que está registrada la máquina virtual.
 - Contraseña: Introduzca la contraseña para esta cuenta de usuario.
- 12 Haga clic en **Siguiente**.
- 13 En la página Volúmenes, seleccione los volúmenes que desee exportar, por ejemplo, C:\ y D:\, y, a continuación, haga clic en **Siguiente**.
- 14 En la página Resumen, haga clic en **Finalizar** para completar el asistente e iniciar la exportación.

 **NOTA:** Puede supervisar el estado y el progreso de la exportación visualizando la ficha **En espera virtual** o **Eventos**.

Cómo realizar una exportación de VirtualBox continua (En espera virtual)

Para realizar este paso, VirtualBox debe estar instalado en el equipo del Core.

Complete los pasos de este procedimiento para realizar una exportación continua a una máquina virtual (VM) de VirtualBox mediante Rapid Recovery.

- 1 En la Core Console de Rapid Recovery, realice una de las acciones siguientes:

- Desde la Consola de Core, en la barra de botones, haga clic en el menú desplegable  **Restaurar** y, a continuación, seleccione **Exportación de la VM**.

- 1 En el Asistente de exportación de máquinas virtuales, seleccione **Continuo (servidor virtual en espera)**.

- 2 Haga clic en **Siguiente**.

- Desde la Consola de Core, en la barra de iconos, haga clic en  (En espera virtual).
 - En la página **En espera virtual**, haga clic en **Agregar** para iniciar el Asistente de exportación de máquinas virtuales.

- 2 En la página **Equipos** del Asistente de exportación de máquinas virtuales, seleccione el equipo protegido que quiere exportar.
- 3 Haga clic en **Siguiente**.

- 4 En la página **Puntos de recuperación**, seleccione el punto de recuperación que desea utilizar para la exportación.
- 5 Haga clic en **Siguiente**.
- 6 En la página **Destino** del Asistente de exportación, en el menú desplegable **Recuperar en una máquina virtual**, seleccione **VirtualBox**.
- 7 En la página **Opciones de máquina virtual**, seleccione **Equipo remoto Linux**.
- 8 Introduzca información sobre la máquina virtual según se describe en la tabla siguiente.

Tabla 120. Configuración del equipo Linux remoto

Opción	Descripción
Nombre de host de VirtualBox	Introduzca una dirección IP o un nombre de host para el servidor VirtualBox. Este campo representa la dirección IP o el nombre de host del servidor VirtualBox remoto.
Puerto	Especifique un número de puerto para el equipo. Este número representa el puerto por el que el Core se comunica con este equipo.
Nombre de la máquina virtual	Introduzca un nombre para la máquina virtual que se está creando. NOTA: el nombre predeterminado es el nombre del equipo de origen.
Ruta de acceso de destino	Especifique una ruta de acceso de destino para crear la máquina virtual. NOTA: Se recomienda que cree una carpeta raíz desde la raíz para que la máquina virtual se ejecute desde la raíz. Si no utiliza la raíz, deberá crear la carpeta de destino manualmente en el equipo de destino antes de configurar la exportación. También deberá vincular o cargar manualmente la máquina virtual después de la exportación.
Nombre de usuario	Nombre de usuario de la cuenta del equipo de destino, por ejemplo, raíz.
Contraseña	Contraseña de la cuenta de usuario del equipo de destino.
Memoria	Especifique el uso de memoria de la máquina virtual haciendo clic en una de las opciones siguientes: - Utilizar la misma cantidad de RAM que el equipo de origen - Utilizar una cantidad de RAM específica y, a continuación, especificar la cantidad en MB La cantidad mínima es 1024 MB y el máximo permitido por la aplicación es 65536 MB. La cantidad máxima de uso de memoria está limitada por la cantidad de RAM disponible para el equipo host.

- 9 Seleccione **Realizar exportación única inicial** para realizar la exportación virtual inmediatamente en lugar de hacerlo después de la próxima instantánea programada.
- 10 Haga clic en **Siguiente**.
- 11 En la página **Volúmenes**, seleccione los volúmenes de datos que desea exportar y, a continuación, haga clic en **Siguiente**.
- 12 En la página **Resumen**, haga clic en **Finalizar** para completar el asistente y para iniciar la exportación.

NOTA: Puede supervisar el estado y el progreso de la exportación visualizando las páginas **En espera virtual** o **Eventos**.

Exportación de datos a una máquina virtual VMWare Workstation

En Rapid Recovery puede exportar datos a VMware Workstation realizando una exportación puntual o estableciendo una exportación continua (para el estado en espera virtual). Realice los pasos de los procedimientos siguientes para el tipo de exportación adecuado.

Cómo realizar una exportación de VMWare Workstation puntual

Realice los pasos de este procedimiento para realizar una exportación puntual a VMware Workstation.

- 1 En la Core Console de Rapid Recovery, en la barra de botones, haga clic en el menú desplegable **Restaurar** y, a continuación, haga clic en **Exportación de la MV**.
- 2 En el Asistente de exportación de máquinas virtuales, seleccione **Exportación única**.

- 3 Haga clic en **Siguiente**.
- 4 En la página Equipos, seleccione el equipo protegido que desea exportar.
- 5 Haga clic en **Siguiente**.
- 6 En la página Puntos de recuperación, seleccione el punto de recuperación que desea utilizar para la exportación.
- 7 Haga clic en **Siguiente**.
- 8 En la página Destino del Asistente de exportación, en el menú desplegable Recuperar en máquina virtual, seleccione **VMware Workstation** y, a continuación, haga clic en **Siguiente**.
- 9 En la página Opciones de máquina virtual, introduzca los parámetros para acceder a la máquina virtual como se describen en la tabla siguiente.

Tabla 121. Parámetros de la máquina virtual

Opción	Descripción
VM Machine Location (Ubicación de VM)	Especifique la ruta de acceso de la carpeta local o recurso compartido de red en el que crear la máquina virtual. NOTA: Si ha especificado una ruta de acceso compartida de red, tendrá que escribir credenciales de inicio de sesión válidas para una cuenta registrada en el equipo de destino. La cuenta debe tener permisos de lectura y escritura en el recurso compartido de red.
Nombre de usuario	Introduzca las credenciales de inicio de sesión de la ubicación de red de la exportación. - Si ha especificado una ruta de acceso compartida de red, debe especificar un nombre de usuario válido para una cuenta registrada en el equipo de destino. - Si ha especificado una ruta de acceso local, no hace falta nombre de usuario.
Contraseña	Introduzca las credenciales de inicio de sesión de la ubicación de red de la exportación. - Si ha especificado una ruta de acceso compartida de red, tendrá que especificar una contraseña válida para una cuenta registrada en el equipo de destino. - Si ha especificado una ruta de acceso local, no hace falta contraseña.
Nombre de VM	Escriba un nombre para la máquina virtual que se está creando; por ejemplo, VM-0A1B2C3D4. NOTA: el nombre predeterminado es el nombre del equipo de origen.
Versión	Especifique la versión de VMware Workstation para la máquina virtual. Puede elegir entre: - VMware Workstation 7.0 - VMware Workstation 8.0 - VMware Workstation 9.0 - VMware Workstation 10.0 - VMware Workstation 11.0 - VMware Workstation 12.0
Cantidad de RAM (MB)	Especifique el uso de memoria de la máquina virtual haciendo clic en una de las opciones siguientes: - Utilizar la misma cantidad de RAM que el equipo de origen - Utilizar una cantidad de RAM específica y, a continuación, especificar la cantidad en MB La cantidad mínima es 1024 MB y el máximo permitido por la aplicación es 65536 MB. La cantidad máxima de uso de memoria está limitada por la cantidad de RAM disponible para el equipo host.
Número de procesadores	El número de procesadores (CPU) que desea para la máquina virtual exportada. El valor mínimo es 1.
Núcleos por procesador	El número de núcleos que desea que tenga cada procesador. El valor mínimo es 1.

- 10 Haga clic en **Siguiente**.

- 11 En la página Volúmenes, seleccione los volúmenes que desee exportar, por ejemplo, C:\ y D:\, y, a continuación, haga clic en **Siguiente**.
- 12 En la página Resumen, haga clic en **Finalizar** para completar el asistente e iniciar la exportación.

 **NOTA:** Puede supervisar el estado y el progreso de la exportación visualizando la ficha **En espera virtual** o **Eventos**.

Cómo realizar una exportación de VMWare Workstation continua (En espera virtual)

Complete los pasos de este procedimiento para realizar una exportación continua a una máquina virtual (VM) VMware Workstation con Rapid Recovery.

- 1 En la Core Console de Rapid Recovery, realice una de las acciones siguientes:

- Desde la Consola de Core, en la barra de botones, haga clic en el menú desplegable  **Restaurar** y, a continuación, seleccione **Exportación de la VM**.

- 1 En el Asistente de exportación de máquinas virtuales, seleccione **Continuo (servidor virtual en espera)**.
- 2 Haga clic en **Siguiente**.

- Desde la Consola de Core, en la barra de iconos, haga clic en  (En espera virtual).
 - En la página **En espera virtual**, haga clic en **Agregar** para iniciar el Asistente de exportación de máquinas virtuales.

- 2 En la página **Equipos** del Asistente de exportación de máquinas virtuales, seleccione el equipo protegido que quiere exportar.
- 3 Haga clic en **Siguiente**.
- 4 En la página **Puntos de recuperación**, seleccione el punto de recuperación que quiere utilizar para la exportación.
- 5 Haga clic en **Siguiente**.
- 6 En la página **Destino** del Asistente de exportación de máquinas virtuales, en el menú desplegable Recuperar en una máquina virtual, seleccione **VMware Workstation** y, a continuación, haga clic en **Siguiente**.
- 7 En la página **Opciones de máquina virtual**, introduzca los parámetros para acceder a la máquina virtual tal como se describen en la tabla siguiente.

Tabla 122. Parámetros de la máquina virtual

Opción	Descripción
Ruta de acceso de destino	Especifique la ruta de acceso de la carpeta local o recurso compartido de red en el que crear la máquina virtual.
 NOTA: Si ha especificado una ruta de acceso compartida de red, tendrá que escribir credenciales de inicio de sesión válidas para una cuenta registrada en el equipo de destino. La cuenta debe tener permisos de lectura y escritura en el recurso compartido de red.	
Nombre de usuario	Introduzca las credenciales de inicio de sesión de la ubicación de red de la exportación. • Si ha especificado una ruta de acceso compartida de red, debe especificar un nombre de usuario válido para una cuenta registrada en el equipo de destino. • Si ha especificado una ruta de acceso local, no hace falta nombre de usuario.
Contraseña	Introduzca las credenciales de inicio de sesión de la ubicación de red de la exportación. • Si ha especificado una ruta de acceso compartida de red, tendrá que especificar una contraseña válida para una cuenta registrada en el equipo de destino. • Si ha especificado una ruta de acceso local, no hace falta contraseña.
Máquina virtual	Escriba un nombre para la máquina virtual que se está creando; por ejemplo, VM-0A1B2C3D4.
 NOTA: el nombre predeterminado es el nombre del equipo de origen.	

Opción	Descripción
Versión	Especifique la versión de VMware Workstation para la máquina virtual. Puede elegir entre: • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0 • VMware Workstation 10.0 • VMware Workstation 11.0 • VMware Workstation 12.0
Memoria	Especifique el uso de memoria de la máquina virtual haciendo clic en una de las opciones siguientes: • Utilizar la misma cantidad de RAM que el equipo de origen • Utilizar una cantidad de RAM específica y, a continuación, especificar la cantidad en MB La cantidad mínima es 1024 MB y el máximo permitido por la aplicación es 65536 MB. La cantidad máxima de uso de memoria está limitada por la cantidad de RAM disponible para el equipo host.
Número de procesadores	El número de procesadores (CPU) que desea para la máquina virtual exportada. El mínimo es 1.
Núcleos por procesador	El número de núcleos que desea tener para cada procesador. El mínimo es 1.

- 8 Seleccione **Realizar exportación única inicial** para realizar la exportación virtual inmediatamente en lugar de hacerlo después de la próxima instantánea programada.
- 9 Haga clic en **Siguiente**.
- 10 En la página **Volúmenes**, seleccione los volúmenes que desee exportar, por ejemplo, C:\ y D:\, y, a continuación, haga clic en **Siguiente**.
- 11 En la página **Resumen**, haga clic en **Finalizar** para completar el asistente y para iniciar la exportación.

NOTA: Puede supervisar el estado y el progreso de la exportación visualizando las páginas **En espera virtual** o **Eventos**.

Exportación de datos a una máquina virtual Hyper-V

En Rapid Recovery, puede exportar datos a una exportación de Hyper-V realizando una exportación puntual o estableciendo una exportación continua (para el estado en espera virtual).

Rapid Recovery es compatible con la exportación de Hyper-V de primera generación en los siguientes hosts:

- Windows 8
- Windows 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Rapid Recovery es compatible con la exportación de Hyper-V de segunda generación en los siguientes hosts:

- Windows 8.1
- Windows Server 2012 R2

NOTA: No es posible exportar todos los equipos virtuales a equipos host Hyper-V de segunda generación.

Solo los equipos protegidos con los siguientes sistemas operativos con Extensible Firmware Interface (UEFI) admiten la exportación virtual a equipos host Hyper-V de segunda generación:

- Windows 8 (UEFI)

- Windows 8.1 (UEFI)
- Windows Server 2012 (UEFI)
- Windows Server 2012 R2 (UEFI)

1 **NOTA:** La exportación de Hyper-V a una VM de segunda generación puede fallar si el host Hyper-V no dispone de RAM suficiente asignada para realizar la exportación.

Realice los pasos de los procedimientos siguientes para el tipo de exportación adecuado.

Cómo realizar una exportación de Hyper-V puntual

Realice los pasos de este procedimiento para realizar una exportación puntual a Hyper-V.

- 1 En la Core Console de Rapid Recovery, en la barra de botones, haga clic en el menú desplegable **Restaurar**, haga clic en **Exportación de la VM**.
- 2 En el Asistente de exportación de máquinas virtuales, seleccione **Exportación única**.
- 3 Haga clic en **Siguiente**.
- 4 En la página **Equipos**, seleccione el equipo protegido que quiere importar.
- 5 Haga clic en **Siguiente**.
- 6 En la página **Puntos de recuperación**, seleccione el punto de recuperación que desea utilizar para la exportación.
- 7 Haga clic en **Siguiente**.
- 8 En la página **Destino**, en el menú desplegable Exportar a máquina virtual, seleccione **Hyper-V**.
- 9 Para exportar a un equipo local con el rol Hyper-V asignado, haga clic en **Utilizar equipo local**.
- 10 Para indicar que el servidor Hyper-V se encuentra en un equipo remoto, haga clic en **Host remoto** y, a continuación, introduzca la información del host remoto como se describe en la tabla siguiente.

Tabla 123. Información de host remoto

Cuadro de texto	Descripción
Nombre de host	Especifique la dirección IP o el nombre de host para el servidor Hyper-V. Representa la dirección IP o nombre de host del servidor Hyper-V remoto.
Puerto	Especifique un número de puerto para el equipo. Representa el puerto por el que el Core se comunica con este equipo.
Nombre de usuario	Especifique el nombre de usuario para el usuario con permisos administrativos para la estación de trabajo con el servidor Hyper-V. Se utiliza para especificar las credenciales de inicio de sesión para la máquina virtual.
Contraseña	Especifique la contraseña para la cuenta de usuario con permisos administrativos en la estación de trabajo con el servidor Hyper-V. Se utiliza para especificar las credenciales de inicio de sesión para la máquina virtual.

- 11 Haga clic en **Siguiente**.
- 12 En la página **Opciones de máquinas virtuales** del cuadro de texto **Ubicación de la máquina virtual**, introduzca la ruta de acceso de la máquina virtual; por ejemplo, **D:\export**. Esto se utiliza para identificar la ubicación de la máquina virtual.

1 **NOTA:** Debe especificar la ubicación de la máquina virtual tanto para los servidores locales como remotos de Hyper-V. La ruta de acceso debe ser una ruta de acceso local válida para el servidor Hyper-V. Los directorios que no existan se crean automáticamente. No debería intentar crearlos manualmente. La exportación a carpetas compartidas (por ejemplo a \\datos \compartición) no está permitida.

- 13 En el cuadro de texto **Nombre de la máquina virtual**, introduzca un nombre para la máquina virtual.
El nombre que especifique aparecerá en la lista de máquinas virtuales en la consola Administrador de Hyper-V.
- 14 Para especificar el uso de la memoria, haga clic en una de las opciones siguientes:
 - **Utilizar la misma cantidad de RAM que el equipo de origen.** Seleccione esta opción para identificar que el uso de RAM es idéntico entre la máquina virtual y la de origen.
 - **Utilizar una cantidad específica de RAM.** Seleccione esta opción si desea especificar la cantidad de RAM en MB.

La cantidad mínima es 1024 MB y el máximo permitido por la aplicación es 65536 MB. La cantidad máxima de uso de memoria está limitada por la cantidad de RAM disponible para el equipo host.

15 Para especificar el formato de disco, junto a Formato de disco, haga clic en una de las siguientes opciones:

- VHDX
- VHD

NOTA: La exportación de Hyper-V admite formatos de disco VHDX si el equipo de destino ejecuta Windows 8 (Windows Server 2012) o posterior. Si VHDX no se admite para su entorno, la opción está desactivada.

Si está exportando a Hyper-V de segunda generación, solo se admite la operación de formato de disco VHDX.

16 Para especificar la generación de Hyper-V que hay que emplear para la exportación, haga clic en uno de los siguientes elementos:

- Generación 1
- Generación 2

NOTA: Solo la segunda generación admite la opción de inicio seguro.

17 Especifique el adaptador de red apropiado para la VM exportada.

18 En la página **Volúmenes**, seleccione los volúmenes que se van a exportar, por ejemplo, C:\.

NOTA: Si los volúmenes seleccionados tienen mayor capacidad que las asignaciones máximas apropiadas admitidas por la aplicación como se indica a continuación, o bien superan la cantidad de espacio disponible, aparecerá un error.

- Para el formato de disco VHDX, sus volúmenes seleccionados no deben tener un tamaño superior a 64 TB.
- Para el formato de disco VHD, sus volúmenes seleccionados no deben tener un tamaño superior a 2040 GB.

19 En la página **Volúmenes**, haga clic en **Finalizar** para completar el asistente e iniciar la exportación.

NOTA: Para supervisar el estado y el progreso de la exportación, visualice **En espera virtual** o las páginas **Eventos**.

Cómo realizar una exportación de Hyper-V continua (En espera virtual)

Complete los pasos de este procedimiento para realizar una exportación continua a una máquina virtual Hyper-V (VM) utilizando Rapid Recovery.

1 En la Core Console de Rapid Recovery, realice una de las acciones siguientes:

- Desde la Core Console, en la barra de botones, haga clic en el menú desplegable  **Restaurar** y después seleccione **Exportación de la MV**.

1 En el Asistente de exportación de máquinas virtuales, seleccione **Continuo (servidor virtual en espera)**.

2 Haga clic en **Siguiente**.

- En Core Console, en la barra de iconos, haga clic en  (En espera virtual).
 - En la página **En espera virtual**, haga clic en **Agregar** para iniciar el Asistente de exportación de máquinas virtuales.

2 En la página **Equipos** del Asistente de exportación de máquinas virtuales, seleccione el equipo protegido que quiere exportar.

3 Haga clic en **Siguiente**.

4 En la página **Puntos de recuperación**, seleccione el punto de recuperación que desea utilizar para la exportación.

5 Haga clic en **Siguiente**.

6 En la página **Destino**, en el menú desplegable Exportar a una máquina virtual, seleccione **Hyper-V** y después realice una de las siguientes opciones:

- Para exportar a un equipo local con el rol Hyper-V asignado, haga clic en **Utilizar equipo local**.
- Para indicar que el servidor Hyper-V se encuentra en un equipo remoto, haga clic en **Host remoto** y, a continuación, introduzca los parámetros del host remoto como se describe en la tabla siguiente.

Tabla 124. Información de host remoto

Cuadro de texto	Descripción
Nombre de host	Especifique la dirección IP o el nombre de host para el servidor Hyper-V. Representa la dirección IP o nombre de host del servidor Hyper-V remoto.
Puerto	Especifique un número de puerto para el equipo. Representa el puerto por el que el Core se comunica con este equipo.
Nombre de usuario	Especifique el nombre de usuario para el usuario con permisos administrativos para la estación de trabajo con el servidor Hyper-V. Se utiliza para especificar las credenciales de inicio de sesión para la máquina virtual.
Contraseña	Especifique la contraseña para la cuenta de usuario con permisos administrativos en la estación de trabajo con el servidor Hyper-V. Se utiliza para especificar las credenciales de inicio de sesión para la máquina virtual.

7 Haga clic en **Siguiente**.

8 En la página **Virtual Machines Options** (Opciones de máquinas virtuales) del cuadro de texto **Ubicación de la máquina virtual**, introduzca la ruta de acceso de la máquina virtual; por ejemplo, **D:\export**. Esto se utiliza para identificar la ubicación de la máquina virtual.

NOTA: Debe especificar la ubicación de la máquina virtual tanto para los servidores locales como remotos de Hyper-V. La ruta de acceso debe ser una ruta de acceso local válida para el servidor Hyper-V. Los directorios que no existan se crean automáticamente. No debería intentar crearlos manualmente. La exportación a carpetas compartidas (por ejemplo a \\data\share) no está permitida.

9 En el cuadro de texto **Nombre de la máquina virtual**, introduzca el nombre de la máquina virtual.

El nombre que especifique aparecerá en la lista de máquinas virtuales en la consola Administrador de Hyper-V.

10 Para especificar el uso de la memoria, haga clic en una de las opciones siguientes:

- **Utilizar la misma cantidad de RAM que el equipo de origen.** Seleccione esta opción para identificar que el uso de RAM es idéntico entre los equipos virtuales y de origen.
- **Utilizar una cantidad específica de RAM.** Seleccione esta opción si desea especificar la cantidad de RAM en MB. La cantidad mínima es 1024 MB y el máximo permitido por la aplicación es 65536 MB. La cantidad máxima de uso de memoria está limitada por la cantidad de RAM disponible para el equipo host.

11 Para especificar el formato de disco, junto a Formato de disco, haga clic en una de las siguientes opciones:

- VHDX
- VHD

NOTA: La exportación de Hyper-V admite formatos de disco VHDX si el equipo de destino ejecuta Windows 8 (Windows Server 2012) o posterior. Si VHDX no se admite para su entorno, la opción está desactivada. Si está exportando a Hyper-V de segunda generación, solo se admite la operación de formato de disco VHDX.

12 Para especificar la generación de Hyper-V que hay que emplear para la exportación, haga clic en uno de los siguientes elementos:

- Generación 1
- Generación 2

NOTA: Solo la segunda generación admite la opción de inicio seguro.

13 Especifique el adaptador de red apropiado para la VM exportada.

14 En la página **Volumes (Volúmenes)**, seleccione los volúmenes que se van a exportar, por ejemplo, C:\.

NOTA: Si los volúmenes seleccionados tienen mayor capacidad que las asignaciones máximas apropiadas admitidas por la aplicación como se indica a continuación, o bien superan la cantidad de espacio disponible, aparecerá un error.

- Para el formato de disco VHDX, sus volúmenes seleccionados no deben tener un tamaño superior a 64 TB.
- Para el formato de disco VHD, sus volúmenes seleccionados no deben tener un tamaño superior a 2040 GB.

15 Seleccione **Realizar exportación única inicial** para realizar la exportación virtual inmediatamente en lugar de hacerlo después de la próxima instantánea programada.

16 En la página **Volúmenes**, haga clic en **Finalizar** para completar el asistente y para iniciar la exportación.

 **NOTA:** Puede supervisar el estado y el progreso de la exportación visualizando las páginas **En espera virtual** o **Eventos**.

Administración de datos anteriores

En esta sección se describe cómo administrar los datos de las instantáneas de vencimientos guardados en su repositorio. Incluye información sobre la conservación de puntos de recuperación en su repositorio, las políticas de retención y el proceso resultado de consolidar puntos de recuperación para conservar espacio. Describe la nueva capacidad de reubicar puntos de recuperación de su repositorio en una copia seguridad de DR de Dell y a un servidor de deduplicación.

En esta sección también se describe cómo archivar datos para el almacenamiento a largo plazo que no están sujetos a consolidación y cómo acceder a los puntos de recuperación que se han archivado.

Acerca de la retención y el archivado de datos de Rapid Recovery

Cada vez que su Core captura una instantánea, los datos se guardan como punto de recuperación en su repositorio. Los puntos de recuperación se van acumulando sistemáticamente a lo largo del tiempo. El Core utiliza una política de retención para determinar el tiempo durante el que se conservan los datos de instantáneas en el repositorio. Durante la parte de consolidación del trabajo nocturno, el Core aplica la política de retención para reducir la cantidad de espacio de almacenamiento consumido. Durante la consolidación, se compara la fecha de cada punto de recuperación con la fecha del punto de recuperación más reciente. A continuación, el Core combina o "consolida" los puntos de recuperación más antiguos. Con el tiempo, los puntos de recuperación más antiguos van siendo sustituidos por los más recientes conforme los más antiguos van quedándose "obsoletos" una vez superado el periodo de retención más antiguo.

Para conservar puntos de recuperación que, de otro modo, se combinarían y, finalmente, eliminarían, puede crear un archivo comprimido desde Core Console. Un archivo comprimido es un archivo que contiene el conjunto completo de puntos de recuperación de equipos protegidos en su Core en el punto temporal en el que se crearon.

Puede almacenar un archivo comprimido en un sistema de archivos o en una cuenta de almacenamiento en la nube.

Si necesita acceder a los datos de un punto de recuperación, posteriormente puede adjuntar (en Rapid Recovery 6.x y posteriores) o importar el archivo comprimido, para restaurar dichos puntos de recuperación en su repositorio. A continuación, puede realizar las mismas acciones en tales datos al igual que con cualquier otro punto de recuperación ubicado actualmente en su Core.

 **NOTA:** Dado que el Core reconoce las fechas originales de los puntos de recuperación de un archivo comprimido, los puntos de recuperación importados pueden volverse a consolidar o eliminar durante el siguiente periodo de trabajo nocturno. Si desea conservar los puntos de recuperación más antiguos, puede deshabilitar la consolidación en los equipos correspondientes o ampliar el periodo de retención.

Administración de políticas de retención

Una política de retención es un conjunto de reglas que determina la duración en que el Core conservará los puntos de recuperación antes de empezar a consolidarlos. Las políticas de retención se pueden establecer para que se realice una consolidación basada en horas, días, semanas, meses y años. Puede configurar un máximo de seis reglas (la política predeterminada establece cinco reglas).

Gracias a que puede realizar copias de seguridad cada 5 minutos, la primera regla en la política de retención, por lo general, establece la duración de la conservación de todos los puntos de recuperación. Por ejemplo, si realiza una copia de seguridad de una máquina cada quince minutos, se guardarán 96 puntos de recuperación en el repositorio de esa máquina por día hasta que comience la consolidación. Si no administra la política de retención, la cantidad de datos puede llenar rápidamente un dispositivo.

NOTA: Los administradores deben tener en cuenta que realizar copias de seguridad frecuentemente puede afectar el tráfico de la red. Otros factores que afectan el tráfico de la red son otras transferencias (como la replicación), la velocidad de cambio de los datos y el hardware de red, cables y conmutadores.

De manera predeterminada, el Core tiene configurada una política de retención predeterminada. Las tareas de la política predeterminada conservan:

- Todos los puntos de recuperación durante tres días
- Un punto de recuperación por hora durante dos días
- Un punto de recuperación por día durante cuatro días
- Un punto de recuperación por semana durante tres semanas
- Un punto de recuperación por mes durante dos meses
- Un punto de recuperación al año durante X años (opción deshabilitada en la política predeterminada)

De acuerdo con esta política predeterminada, el punto de recuperación más antiguo tiene, por lo general, 92 días. Los datos posteriores a esa fecha de origen se eliminarán con la política predeterminada.

Si configura la política de retención a nivel del Core, se aplica automáticamente a todas las máquinas que el Core protege. Puede cambiar la política predeterminada a fin de que se adapte a sus necesidades.

En todas las máquinas, también puede crear una política de retención personalizada. Si configura la política a nivel de la máquina, podrá especificar una política de retención diferente a la política predeterminada del Core. Para obtener más información sobre la configuración de las políticas de retención, consulte [Configuración de los valores predeterminados de la política de retención del Core](#) y [Personalización de la configuración de la política de retención de una máquina protegida](#).

Configuración de los valores predeterminados de la política de retención del Core

La política de retención del Core especifica el tiempo que los puntos de recuperación de una máquina protegida se almacenan en el repositorio.

La política de retención del Core se ejecuta mediante un proceso de consolidación que se realiza como un componente de ejecución de tareas nocturnas. Después, los puntos de recuperación que hayan superado la edad especificada en la política de retención se "acumulan" (se combinan) en menos puntos de recuperación que cubren un periodo de tiempo menos específico. Al aplicar la política de retención durante las noches, se acumulan copias de seguridad que envejecen de forma continua. Con el tiempo, se eliminan así los puntos de recuperación más antiguos de acuerdo con los requisitos especificados en dicha política de retención.

Se pueden configurar valores distintos para los Cores de origen y de destino.

NOTA: Este tema trata específicamente sobre la personalización de la configuración de la política de retención del Core de Rapid Recovery. Al guardar los valores personalizados de la política de retención en el Core, establece los valores predeterminados de la política de retención que se pueden aplicar a todas las máquinas protegidas por este Core. Para obtener más información sobre cómo personalizar la configuración de la política de retención de máquinas protegidas individuales, consulte [Personalización de la configuración de la política de retención de una máquina protegida](#).

1 Vaya a la Core Console de Rapid Recovery.

2 En la barra de íconos, haga clic en  (Configuración), y a continuación, realice una de las acciones siguientes:

- En la lista de configuración del Core en el lado izquierdo de la página Configuración, haga clic en **Nightly Jobs (Tareas nocturnas)**.
- Desplácese hacia abajo en el lado derecho de la página Configuración hasta que vea el encabezado **Nightly Jobs (Tareas nocturnas)**.

Aparecerá la configuración del Core de tareas nocturnas.

3 En **Nightly Jobs (Tareas nocturnas)**, haga clic en  **Change (Cambiar)**.

Aparecerá el cuadro de diálogo **Nightly Jobs (Tareas nocturnas)**.

- 4 Para especificar los intervalos de tiempo de la retención de datos de copia de seguridad según sea necesario, en el área Nightly Jobs (Tareas nocturnas), seleccione **Rollup (Consolidación)** y, a continuación, haga clic en **Settings (Configuración)**.

Aparecerá el cuadro de diálogo **Configuration (Configuración)** de la política de retención predeterminada del Core.

- 5 Para restaurar los valores predeterminados de la política de retención del Core en cualquier momento, en la parte inferior del cuadro de diálogo Configuración, haga clic en **Restore Defaults (Restaurar los valores predeterminados)** y, a continuación, haga clic en **Yes (Sí)** para confirmar.

Todos los valores predeterminados se restauran como se describe en la tabla que aparece en el [paso 6](#).

- 6 Para definir una política de retención, especifique primero el tiempo que se conservan las instantáneas de copia de seguridad iniciales. Después, defina un conjunto de requisitos de consolidación en cascada que determine los intervalos en los que se deben consolidar los puntos de recuperación.

Las opciones de la política de retención se describen en la tabla siguiente.

Tabla 125. Opciones de programación de la política de retención predeterminada

Cuadro de texto	Descripción
Keep all recovery points for n [retention time period] (Conservar todos los puntos de recuperación durante n [duración de retención])	Especifica la duración de la retención de los puntos de recuperación. Introduzca el número que represente la duración de la retención y seleccione la duración. El valor predeterminado es 3 días. Puede elegir días, semanas, meses o años.
...and then keep one recovery point per hour for n [retention time period] (...y luego conservar un punto de recuperación cada hora durante n [duración de retención])	Proporciona un nivel de retención más específico. Se utiliza como bloque de construcción con la configuración primaria para definir con más detalle durante cuánto tiempo se mantienen los puntos de recuperación. Introduzca el número que represente la duración de la retención y seleccione la duración. El valor predeterminado es 2 días. Puede elegir días, semanas, meses o años.
..and then keep one recovery point per day for n [retention time period] (...y luego conservar un punto de recuperación por día durante n [duración de retención])	Proporciona un nivel de retención más específico. Se utiliza como bloque de construcción para definir con más detalle durante cuánto tiempo se mantienen los puntos de recuperación. Introduzca el número que represente la duración de la retención y seleccione la duración. El valor predeterminado es 4 días. Puede elegir días, semanas, meses o años.
...and then keep one recovery point per week for n [retention time period] (...y luego conservar un punto de recuperación por semana durante n [duración de retención])	Proporciona un nivel de retención más específico. Se utiliza como bloque de construcción para definir con más detalle durante cuánto tiempo se mantienen los puntos de recuperación. Introduzca el número que represente la duración de la retención y seleccione la duración. El valor predeterminado es 3 semanas. Puede elegir semanas, meses o años.
..and then keep one recovery point per month for n [retention time period] (...y luego conservar un punto de recuperación por mes durante n [duración de retención])	Proporciona un nivel de retención más específico. Se utiliza como bloque de construcción para definir con más detalle durante cuánto tiempo se mantienen los puntos de recuperación. Introduzca el número que represente la duración de la retención y seleccione la duración. El valor predeterminado es 2 meses. Puede elegir meses o años.
...and then keep one recovery point per year for n [retention time period] (...y luego conservar un punto de recuperación por año durante n [duración de retención])	Introduzca el número que represente la duración de la retención y seleccione la duración. Puede elegir años.

Cuadro de texto	Descripción
time period] (...y luego conservar un punto de recuperación por año durante n [duración de retención])	

El punto de recuperación más antiguo se determina mediante la configuración de la política de retención.

En el ejemplo siguiente se explica cómo se calcula el periodo de retención.

Conservar todos los puntos de recuperación durante tres días.

...y luego conservar un punto de recuperación por hora durante tres días

...y luego conservar un punto de recuperación por día durante cuatro días

...y luego conservar un punto de recuperación por semana durante tres semanas

...y luego conservar un punto de recuperación por mes durante dos meses

...y luego conservar un punto de recuperación por mes durante un año

En este ejemplo, el punto de recuperación más antiguo tendría 1 año, 4 meses y 6 días de antigüedad.

- 7 Cuando esté satisfecho con la configuración de la política de retención, haga clic en **Save (Guardar)**.

Se cerrará el cuadro de diálogo de **Configuración**.

- 8 En el cuadro de diálogo **Tareas nocturnas**, haga clic en **OK (Aceptar)**.

Se cerrará el cuadro de diálogo **Tareas nocturnas**. La política de retención definida se aplica durante la consolidación nocturna.

También puede aplicar esta configuración al especificar la política de retención de cualquier máquina individual protegida. Para obtener más información sobre la configuración de políticas de retención de máquinas protegidas, consulte [Personalización de la configuración de la política de retención de una máquina protegida](#).

Personalización de la configuración de la política de retención de una máquina protegida

La política de retención de una máquina protegida especifica durante cuánto tiempo se almacenan los puntos de recuperación en el repositorio. Normalmente, cada máquina protegida utiliza el valor predeterminado de la política de retención establecido para el Core, a menos de que especifique una política de retención personalizada, como se describe en este procedimiento.

Utilice este procedimiento para definir una política de retención personalizada de una máquina protegida, incluida una máquina replicada.

- 1 En el menú Protected Machines (Máquinas protegidas) de la Core Console de Rapid Recovery, haga clic en el nombre de la máquina que desea modificar.
Aparecerá página **Summary (Resumen)** con información de la máquina seleccionada.
- 2 Haga clic en el menú **Settings (Configuración)**.
Aparecerá la página **Settings (Configuración)**, que muestra los valores de configuración de la máquina seleccionada.
- 3 De manera opcional, también puede hacer clic en el enlace **Nightly Jobs (Tareas nocturnas)** para desplazarse hacia abajo en la página Configuración y ver las tareas nocturnas.
- 4 Debajo del encabezado de Tareas nocturnas, haga clic en  **Change (Cambiar)**.
Aparecerá el cuadro de diálogo **Nightly Jobs (Tareas nocturnas)**.
- 5 Para especificar los intervalos de tiempo para retener los datos de copia de seguridad según sea necesario, seleccione **Roll up (Consolidación)** y, a continuación, haga clic en **Settings (Configuración)**.

Aparecerá el cuadro de diálogo de **Configuration (Configuración)** de la política de retención.

- 6 Si configura valores personalizados de las políticas de retención de una máquina replicada y si ve un mensaje de precaución que le notifica que realice una Integrity Check (comprobación de integridad) del repositorio, continúe con este paso. De lo contrario, vaya al siguiente paso.
 - a Si está listo para ejecutar la tarea, haga clic en **Check Integrity (Comprobar integridad)**.
 - b Haga clic en **Yes (Sí)** para confirmar la tarea de comprobación de integridad.

NOTA: La ejecución de este trabajo puede tardar un considerablemente según el tamaño de su repositorio. Durante este tiempo, puede realizar otras acciones (instantáneas, replicación, exportación virtual, etc.) en el repositorio. Para obtener más información sobre esta tarea, consulte [Comprobación de la integridad de los repositorios de DVM](#).

- Una vez que la tarea de comprobación de integridad termine todas las tareas secundarias con éxito, vuelva a este procedimiento y continúe con el paso siguiente.

- 7 En el cuadro de diálogo **Configuration (Configuración)**, realice una de las siguientes acciones:
 - Para utilizar la política de retención predeterminada de esta máquina protegida, seleccione **Use Core default retention policy (Utilizar la política de retención predeterminada del Core)** y, a continuación, haga clic en **Save (Guardar)**. La política predeterminada se aplicará a este Agent.
 - Para definir una política de retención personalizada para este Agent, seleccione **Use custom retention policy (Utilizar política de retención personalizada)** y, a continuación, continúe con el paso siguiente.

Se ampliará el cuadro de diálogo **Configuration (Configuración)** para ver la información de la política de retención personalizada.

- 8 Introduzca la programación personalizada de la retención de los puntos de recuperación como se describe en la tabla siguiente.

Tabla 126. Opciones de programación de la política de retención personalizada.

Cuadro de texto	Descripción
Keep all recovery points for n [retention time period] (Conservar todos los puntos de recuperación durante n [duración de retención])	Especifica la duración de la retención de los puntos de recuperación. Introduzca el número que represente la duración de la retención y seleccione la duración. El valor predeterminado es 3 días. Puede elegir días, semanas, meses o años.
...and then keep one recovery point per hour for n [retention time period] (...y luego conservar un punto de recuperación cada hora durante n [duración de retención])	Proporciona un nivel de retención más específico. Se utiliza como bloque de construcción con la configuración primaria para definir con más detalle durante cuánto tiempo se mantienen los puntos de recuperación. Introduzca el número que represente la duración de la retención y seleccione la duración. El valor predeterminado es 2 días. Puede elegir días, semanas, meses o años.
..and then keep one recovery point per day for n [retention time period] (...y luego conservar un punto de recuperación por día durante n [duración de retención])	Proporciona un nivel de retención más específico. Se utiliza como bloque de construcción para definir con más detalle durante cuánto tiempo se mantienen los puntos de recuperación. Introduzca el número que represente la duración de la retención y seleccione la duración. El valor predeterminado es 4 días. Puede elegir días, semanas, meses o años.
...and then keep one recovery point per week for n [retention time period] (...y luego conservar un punto de recuperación por semana durante n [duración de retención])	Proporciona un nivel de retención más específico. Se utiliza como bloque de construcción para definir con más detalle durante cuánto tiempo se mantienen los puntos de recuperación. Introduzca el número que represente la duración de la retención y seleccione la duración. El valor predeterminado es 3 semanas. Puede elegir semanas, meses o años.

Cuadro de texto	Descripción
..and then keep one recovery point per month for n [retention time period] (...y luego conservar un punto de recuperación por mes durante n [duración de retención])	Proporciona un nivel de retención más específico. Se utiliza como bloque de construcción para definir con más detalle durante cuánto tiempo se mantienen los puntos de recuperación. Introduzca el número que represente la duración de la retención y seleccione la duración. El valor predeterminado es 2 meses. Puede elegir meses o años.
...and then keep one recovery point per year for n [retention time period] (...y luego conservar un punto de recuperación por año durante n [duración de retención])	Introduzca el número que represente la duración de la retención y seleccione la duración. Puede elegir años.

En el ejemplo siguiente se explica cómo se calcula el periodo de retención.

Conservar todos los puntos de recuperación durante tres días.

...y luego conservar un punto de recuperación por hora durante tres días

...y luego conservar un punto de recuperación por día durante cuatro días

...y luego conservar un punto de recuperación por semana durante tres semanas

...y luego conservar un punto de recuperación por mes durante dos meses

...y luego conservar un punto de recuperación por mes durante un año

En este ejemplo, el punto de recuperación más antiguo tendría un año con 3 meses.

- 9 Si desea conservar todos los puntos de recuperación en el repositorio principal, deje en blanco la opción **Relocate outdated recovery points to an R3 repository (Reubicar puntos de recuperación desactualizados a un repositorio R3)** y omita el paso siguiente.
- 10 Si desea reubicar los puntos de recuperación desde el repositorio principal a un repositorio R3 almacenado en un dispositivo de copia de seguridad de la serie DR de Dell DR, haga lo siguiente:
 - a Seleccione la opción **Relocate outdated recovery points to an R3 repository (Reubicar puntos de recuperación desactualizados a un repositorio R3)**.
 - b Especifique la edad de los puntos de recuperación que desea reubicar desde el repositorio principal al repositorio R3. Puede especificar la edad por semanas, meses o años. El periodo más corto que puede definir es 1 semana.
 - c Desde el menú desplegable **Select a repository (Seleccione un repositorio)**, seleccione el repositorio R3 en el que desea apilar los puntos de recuperación.

NOTA: Independientemente de dónde se encuentran los puntos de recuperación (repositorio DVM local o repositorio R3 remoto en un dispositivo de copia de seguridad DR), estos se mantienen sujetos a la política de retención, que se mantendrá consolidada. Si necesita conservar puntos de recuperación más antiguos, puede archivarlos. Otra forma de conservarlos es desactivando la consolidación o ampliar el periodo de retención de las máquinas protegidas que correspondan.

- 11 Haga clic en **Guardar**.

Forzar la consolidación en todos los equipos protegidos

Puede omitir la política de retención programada al forzar los puntos de recuperación para consolidar el nivel del equipo protegido.

- 1 A partir del menú de los equipos protegidos de la Core Console de Rapid Recovery, haga clic en el nombre de un equipo protegido específico.

Aparece la página **Resumen** para el equipo seleccionado.

- 2 Haga clic en el menú desplegable **Más** en la parte superior de la vista del equipo protegido y, a continuación, seleccione **Política de retención**.

Aparece la página **Política de retención** del equipo especificado.

- 3 Haga clic en **Force Rollup** (Forzar consolidación).

- 4 En el cuadro de diálogo, haga clic en **Sí** para confirmar.

Rapid Recovery inicia la consolidación para este equipo, independientemente del calendario de programación de la política de retención.

Replicación

Esta sección describe cómo configurar y administrar la replicación de datos protegidos desde un Core de origen de Rapid Recovery en un Core de destino de Rapid Recovery para la recuperación de desastres.

Replicación con Rapid Recovery

En esta sección se proporciona información de conceptos y procedimientos que le ayudará a entender y configurar la replicación en Rapid Recovery.

La replicación es el proceso de copia de puntos de recuperación del Core de Rapid Recovery y su transferencia a otro Core de Rapid Recovery con fines de recuperación tras desastres. El proceso requiere la existencia de una relación de emparejamiento origen-destino entre dos o más Cores.

El Core de origen copia los puntos de recuperación de los equipos protegidos seleccionados y, a continuación, transmite de forma asíncrona y continua los datos de la instantánea al Core de destino.

A menos que haya cambiado el comportamiento predeterminado al establecer un calendario de programación de replicación, el Core inicia un trabajo de replicación inmediatamente después de completar las instantáneas de las copias de seguridad, la comprobación de suma de comprobación, la comprobación de conectabilidad y los trabajos nocturnos. Para obtener más información, consulte [Programación de la replicación](#).

Para lograr una seguridad de los datos óptima, los administradores por lo general utilizan un Core de destino en un sitio de recuperación tras desastres remoto. Puede configurar la replicación de salida en un centro de datos de propiedad de la empresa o en un sitio de recuperación tras desastres remoto (es decir, un Core de destino administrado automáticamente). Otra opción es configurar la replicación de salida en un proveedor de servicio gestionado por terceros (MSP) o proveedor de Nube que aloja copias de seguridad y servicios de recuperación de desastres en una ubicación externa. Al replicar en un Core de destino de terceros, puede utilizar flujos de trabajo integrados que le permiten solicitar conexiones y recibir notificaciones de comentarios automáticas.

La replicación está gestionada por equipos protegidos. Se puede configurar cualquier equipo (o todos los equipos) protegido o replicado en un Core de origen para replicar en un Core de destino.

Estos son algunos de los posibles escenarios para replicación:

- **Replicación a una ubicación local.** El Core de destino está en un centro de datos local o una ubicación in situ, y la replicación se mantiene en todo momento. En esta configuración, la pérdida del Core no impediría una recuperación.
- **Replicación a una ubicación externa.** El Core de destino se ubica en un lugar externo de recuperación tras desastres remoto, en caso de pérdida.
- **Replicación mutua.** Dos centros de datos en dos ubicaciones distintas, cada una de ellas con un Core, y que son equipos de protección y sirven como copia de seguridad de recuperación externa entre sí, en caso de desastre. En este caso, cada Core replica los equipos protegidos en el Core que se encuentra en el otro centro de datos.
- **Replicación alojada y en nube.** Los socios de MSP de Rapid Recovery mantienen varios Cores de destino en un centro de datos o en una nube pública. En cada uno de estos Cores, el socio MSP permite a uno o más de sus clientes replicar puntos de recuperación desde un Core de origen del sitio del cliente en el Core del destino del MSP, siendo un servicio de pago.

① | **NOTA:** En esta situación, los clientes solo tienen acceso a sus propios datos.

Estas son algunas de las configuraciones posibles de replicación:

- **Replicación de punto a punto.** Replica uno o más equipos protegidos desde un Core de origen único a un Core de destino único.

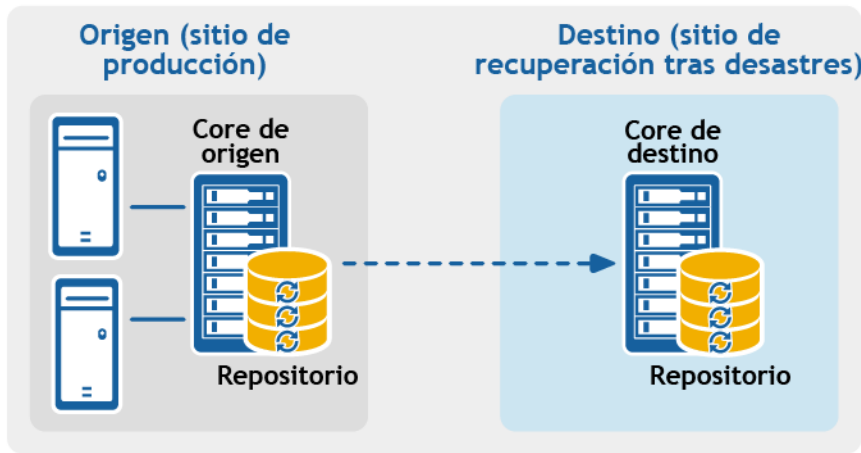


Ilustración 9. Configuración de la replicación de punto a punto

- **Replicación de multipunto a punto.** Replica los equipos protegidos de varios Cores de origen en un único Core de destino.

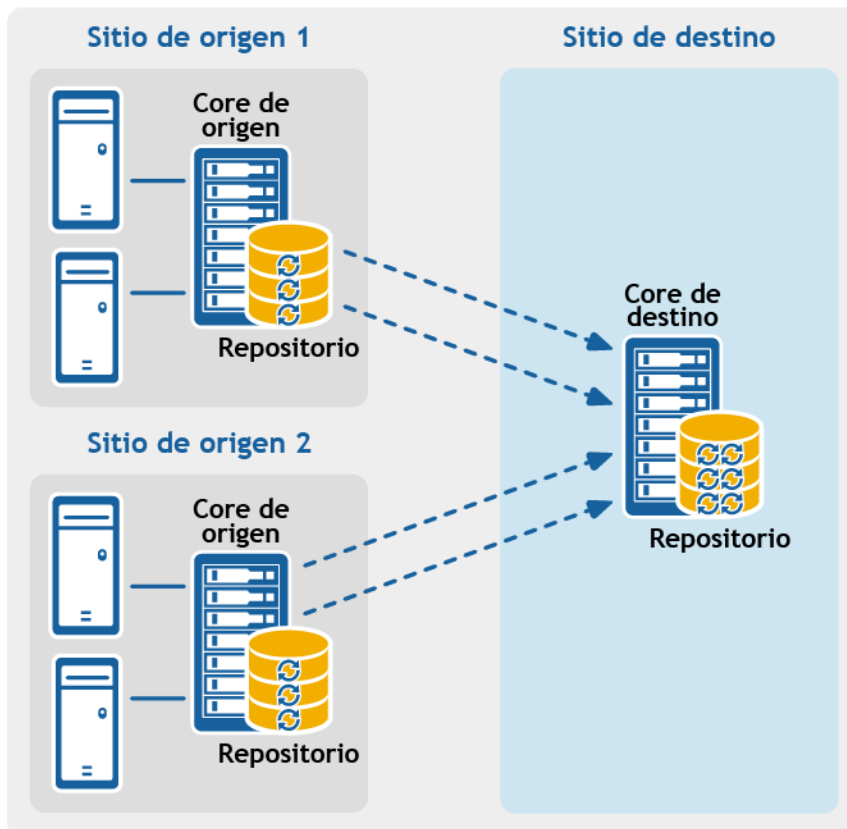


Ilustración 10. Configuración de la replicación de multipunto a punto.

- **Replicación de punto a multipunto.** Replica uno o más equipos protegidos desde un Core de origen único a más de un Core de destino.

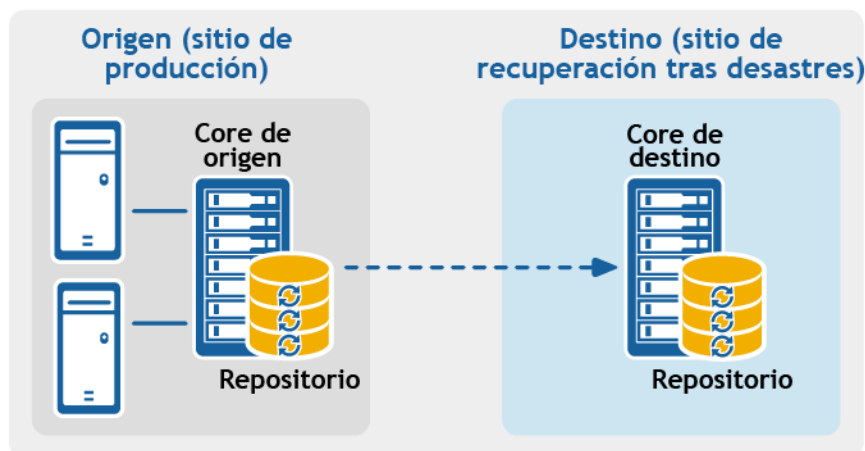


Ilustración 11. Configuración de la replicación de punto a multipunto

- **Replicación de salto múltiple.** Replica uno o más equipos protegidos desde un Core de destino a otro Core de destino, lo que produce opciones de conmutación por error o recuperación adicionales en el Core replicado.

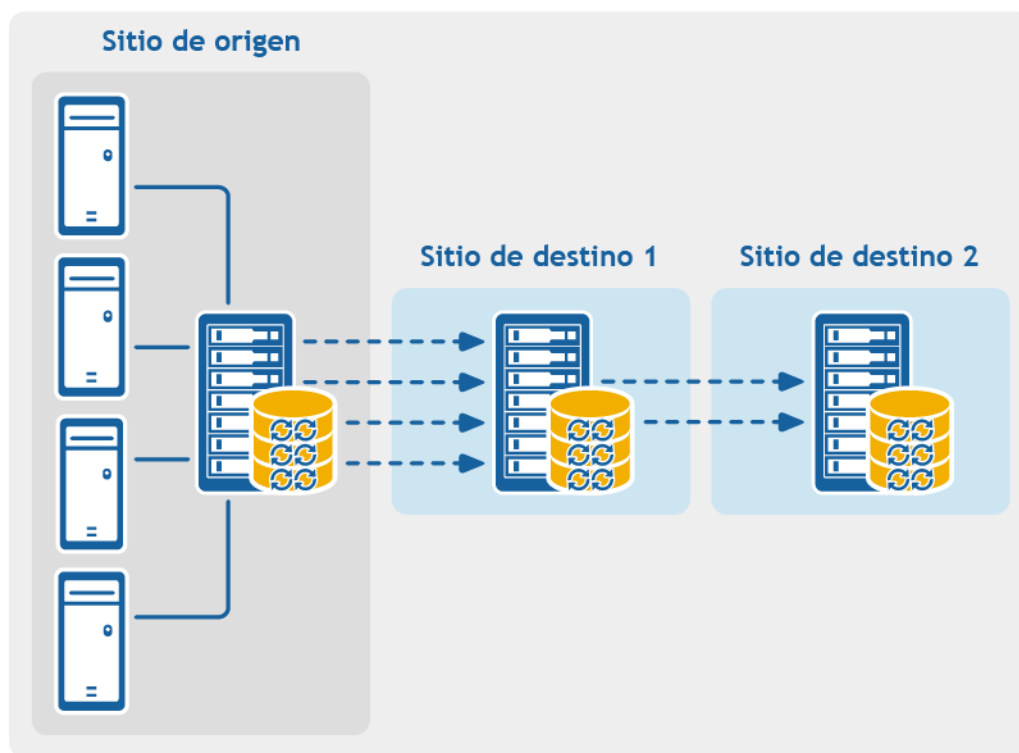


Ilustración 12. Configuración de replicación de salto múltiple

Si utiliza dispositivos de copia de seguridad de Dell Data Protection, como los de la serie DL1x00 o DL4x00, el Core de destino al que replique debe tener una licencia de software válida configurada. Estos dispositivos de hardware incluyen una licencia de destino de replicación con la compra. Compruebe la clave de licencia en el mensaje de correo electrónico de bienvenida que recibió cuando adquirió el

dispositivo. Para obtener ayuda, visite el sitio web de Asistencia con las licencias en <https://support.software.dell.com/licensing-assistance> o envíe un correo electrónico a license@software.dell.com.

Cadenas del punto de recuperación y huérfanos

Rapid Recovery captura instantáneas de un equipo protegido y guarda los datos en un repositorio como *punto de recuperación*. El primer punto de recuperación guardado en el Core se denomina imagen base. La imagen base incluye el sistema operativo, las aplicaciones y las configuraciones de cada volumen que elija proteger, así como todos los datos de dichos volúmenes. Las copias de seguridad posteriores son *instantáneas incrementales*, que constan solo de datos modificados en los volúmenes protegidos desde la realización de la última copia de seguridad. La imagen base más todas las instantáneas incrementales forman una *cadena de puntos de recuperación* completa.

Desde una cadena de puntos de recuperación completa, podrá restaurar los datos con facilidad y confianza, mediante la utilización de la gama completa de opciones de recuperación disponible para Rapid Recovery. Estas opciones incluyen la restauración a nivel de archivos, a nivel de volumen y la restauración bare metal restore.

Debido a que lógicamente no puede realizar una restauración de datos que no existen, en el caso de una cadena de puntos de recuperación incompleta, no podrá restaurar los datos a nivel de volumen ni realizar una restauración bare metal restore. En tales casos, todavía podrá restaurar todos los datos que haya en un punto de recuperación a nivel de archivos.

Si la información que desea restaurar desde un punto de recuperación se encuentra en una copia de seguridad anterior que no está disponible en el Core (una instantánea incremental anterior o la imagen base), se dice que el punto de recuperación es *huérfano*. Los puntos de recuperación huérfanos son los típicos de algunos escenarios de replicación.

Por ejemplo, la primera vez que establece la replicación, las opciones para la restauración de datos desde los puntos de recuperación replicados son limitadas. Hasta que todos los datos de la copia de seguridad del Core de origen se transmitan al Core de destino, mediante la creación de cadenas de puntos de recuperación completas de los huérfanos, solo podrá realizar restauración a nivel de archivos.

Cuando comienza una replicación

De forma predeterminada, el Core pone automáticamente a los trabajos de transferencia de replicación en cola inmediatamente después de que se complete cada transferencia de copias de seguridad programadas con regularidad. Por lo tanto, a menos que el calendario de programación de replicación de un equipo protegido esté personalizado, se basará en su calendario de programación de instantáneas de copias de seguridad estándar.

La primera vez que configure la replicación, si hay uno o más puntos de recuperación en el Core de origen, el proceso de replicación se iniciará inmediatamente, a menos que:

- Seleccione la opción para pausar la replicación inicialmente o
- Seleccione la opción para utilizar una unidad de inicialización para realizar la transferencia inicial.

Si pausa la replicación inicialmente, esta se iniciará al reanudar explícitamente la replicación.

Si configura la replicación y especifica el uso de una unidad de inicialización, la replicación en el Core de destino se iniciará con la siguiente instantánea de copias de seguridad programadas con regularidad.

❗ NOTA: Puede forzar una copia de seguridad del equipo protegido tras establecer la replicación. Esto hace que se inicie la replicación inmediatamente después de completarse la instantánea del equipo protegido.

Si especifica una unidad de inicialización al configurar la replicación, solo se replicarán las transferencias de copias de seguridad futuras. Si desea que haya puntos de recuperación existentes del equipo protegido en el Core de destino, deberá inicializar los datos desde el equipo protegido. Para inicializar datos, cree una unidad de inicialización desde el Core de origen y, a continuación, consuma la unidad de inicialización en el Core de destino.

También puede personalizar el calendario de programación de replicación de un equipo protegido. Por ejemplo, si utiliza el calendario de programación de protección predeterminado de una copia de seguridad por hora, podrá especificar que el Core de origen replique en el Core de destino en un calendario de programación diferente (por ejemplo, una vez al día a las 02:00).

Determinación de la estrategia y necesidades de inicialización

Los temas siguientes analizan la restauración a partir de datos replicados y la necesidad de inicializar datos del punto de recuperación desde el Core de origen.

Cuando es necesaria la inicialización de datos

La primera vez que establezca la replicación, a menos que especifique el uso de una unidad de inicialización, el Core de origen empezará a transmitir todos los puntos de recuperación de los equipos seleccionados al Core de destino. La transmisión de datos a través de la red puede tardar mucho tiempo. Los factores que intervienen incluyen la velocidad de la red, la solidez de la arquitectura de red y la cantidad de datos que se transmiten al Core de destino. Por ejemplo, si los datos de la copia de seguridad son 10 GB y el enlace WAN transfiere a 24 Mbps, la transferencia podría tardar más de una hora en completarse.

En función de la cantidad de información que desee copiar en el Core de destino, la unidad de inicialización podría llegar a agregar hasta cientos o miles de gigabytes de datos. Muchas empresas deciden no consumir el ancho de banda de la red necesario y optan por definir y consumir una unidad de inicialización. Para obtener más información, consulte [Consideraciones de rendimiento para la transferencia de datos replicados](#).

Si especifica el uso de una unidad de inicialización al definir la replicación, solo los puntos de recuperación guardados en el Core de origen después de haber establecido la replicación se replicarán en el Core de destino. Las copias de seguridad guardadas en el Core de origen *antes* de que se estableciera la replicación no estarán presentes en el Core de destino hasta que inicialice de forma explícita los datos, mediante el proceso siguiente.

Para evitar la ralentización de la red a causa de una transferencia intensiva de datos históricos, inicialice los datos de la copia de seguridad previa en el Core de destino mediante una **unidad de inicialización**. Una unidad de inicialización es un archivo de archivos comprimidos que **copia** un conjunto de imágenes base desduplicadas e instantáneas incrementales desde el Core de origen. El archivo de la unidad de inicialización contiene el conjunto completo de puntos de recuperación previos de los equipos protegidos que desee replicar desde el Core de origen al Core de destino.

Mueva el archivo de la unidad de inicialización a un volumen de almacenamiento que, posteriormente, pueda poner a disposición del Core de destino. A continuación, **consume** la información de la unidad de inicialización. Para ello, es necesario adjuntar el volumen con imagen de la unidad de inicialización en el Core de destino e importar los datos en el repositorio de la Core Console. En este proceso se reparan los huérfanos mediante la unión de instantáneas incrementales replicadas al Core de destino con sus imágenes base, para formar una o más cadenas de puntos de recuperación completas. Este proceso a veces se denomina copiar-consumir.

Los datos de inicialización del Core de origen no siempre son necesarios. Por ejemplo:

- Si va a configurar la replicación para un nuevo Core de Rapid Recovery, no es necesaria la inicialización.
- Si los datos de instantáneas anteriores no son críticos para los datos replicados y solo necesita recuperar los datos guardados después de la configuración de la replicación, la inicialización no será necesaria.

① NOTA: En este caso, Dell recomienda capturar una nueva imagen base inmediatamente antes o después de configurar la replicación. Este paso asegura que haya una cadena de puntos de recuperación completa en el Core de destino desde el que poder restaurar los datos en el futuro.

- Si capturó una imagen base inmediatamente antes de configurar la replicación y solo tiene la necesidad de restaurar a partir de los datos capturados después de dicha fecha, no será necesaria la inicialización.
- Si configuró la replicación sin especificar una unidad de inicialización, los datos de la instantánea se transmitirán a través de la red desde el Core de origen al Core de destino.

Si se da alguna de estas situaciones, la inicialización de datos no será necesaria. En tales casos, la replicación se puede completar en su totalidad desde el Core de origen.

Si configuró la replicación de un Core con puntos de recuperación existentes y es posible que sea necesario restaurarla en el nivel del volumen, que desee realizar una restauración BMR o que desee restaurar los datos desde una imagen base o instantánea incremental anterior, la inicialización será necesaria. En estos casos, tenga en cuenta las necesidades de inicialización y la estrategia. Revise la información incluida en este tema y decida si va a inicializar en el Core de destino y qué método utilizará.

Métodos de inicialización de datos

Si desea que los equipos replicados en un Core de destino tengan acceso a los datos guardados previamente en el Core de origen, inicialice el Core de destino mediante uno de los métodos siguientes:

- 1 **Inicialización en el Core de destino a través de una conexión de red.** Especifique el uso de una unidad de inicialización cuando defina la replicación. A continuación, podrá compartir la carpeta que contiene la unidad de inicialización con el Core de destino y consumir el archivo de unidad de inicialización a través de la red. Para transferir grandes cantidades de datos o para conexiones lentas, este método de inicialización podría tardar una cantidad considerable de tiempo y consumir una cantidad importante de ancho de banda de la red.
NOTA: Dell no recomienda la inicialización de grandes cantidades de datos a través de una conexión de red. La primera inicialización puede llegar a implicar cantidades de datos muy grandes, que saturan una conexión WAN típica.
- 2 **Transferencia de datos de la copia de seguridad desde el Core de origen mediante medios de almacenamiento físicos.** Transfiera el archivo de unidad de inicialización a un dispositivo portátil, externo y extraíble de almacenamiento. Normalmente, este método es útil para grandes conjuntos de datos o lugares con conexiones de red lentas. La inicialización mediante este método requiere que se realicen los pasos siguientes:
 - a Crear un archivo de inicialización desde el Core de origen y guardarlo en los medios extraíbles.
 - b Transportar la unidad de inicialización a la ubicación física del Core de destino.
 - c Adjuntar la unidad al Core de destino.
 - d Consumir los datos de la unidad de inicialización en el repositorio del Core de destino.

Si se replica en un Core de terceros, una vez el MSP haya recibido su medio, por lo general, un representante del centro de datos adjuntará dicho medio y le notificará cuando esté listo para que pueda consumir (o importar) los datos de inicialización en el Core.

- NOTA:** Como hay que copiar grandes cantidades de datos al dispositivo de almacenamiento, se recomienda usar una conexión eSATA, USB 3.0 u otra de alta velocidad. Si el tamaño total del archivo de datos de inicialización es mayor que el espacio disponible en el medio extraíble, el archivo podrá exportarse a través de varios dispositivos.
 - 3 **Transferencia de datos de una copia de seguridad mediante disco duro virtual en Cores de origen y de destino almacenados en hosts virtuales.** Si el Core de origen y de destino se encuentran en un host virtual, podrá definir y consumir una unidad de inicialización en un medio de almacenamiento virtual. La inicialización mediante este método requiere que se realicen los pasos siguientes:
 - a Cree un archivo de unidad de inicialización desde el Core de origen y guárdelo en un volumen de almacenamiento virtual.
 - b Desconecte el volumen del Core de origen y adjúntelo al Core de destino.
 - c Consumir los datos de la unidad de inicialización en el repositorio del Core de destino.
- NOTA:** Aunque se puede producir la replicación de instantáneas incrementales entre los Cores de origen y destino antes de que se complete la inicialización, las instantáneas replicadas que se transmiten del origen al destino quedarán huérfanas hasta que se consuman los datos iniciales y se combinen con las imágenes base replicadas.

Enlaces relacionados

- Para obtener información detallada sobre el proceso de consumo de la unidad de inicialización, consulte el tema [Consumo de la unidad de inicialización en un Core de destino](#).
- Para obtener más información sobre los puntos de recuperación huérfanos, consulte [Eliminación de una cadena de puntos de recuperación huérfanos](#).
- Para obtener más información sobre cómo preparar una unidad de inicialización, consulte [Comprensión de unidades de inicialización y Consumo de la unidad de inicialización en un Core de destino](#).

Vínculos relacionados

- [Consumo de la unidad de inicialización en un Core de destino](#)
- [Eliminación de una cadena de puntos de recuperación huérfanos](#)

Consideraciones de rendimiento para la transferencia de datos replicados

Si el ancho de banda entre los Cores de origen y destino no puede dar servicio a la transferencia de puntos de recuperación almacenados, configure la replicación y especifique el uso de una unidad de inicialización. Este proceso inicia el Core de destino con imágenes base y puntos de recuperación de los servidores seleccionados protegidos en el Core de origen. El proceso de inicialización se puede realizar en cualquier momento. La inicialización se puede realizar como parte de la transferencia inicial de datos, que sirve como base para la replicación programada regularmente. También puede inicializar datos para un equipo replicado anteriormente si la replicación se ha pausado o eliminado. En este caso, la opción "Crear cadenas de puntos de recuperación" permite copiar puntos de recuperación no replicados aún en una unidad de inicialización.

Cuando se prepare para la replicación, tenga en cuenta los factores siguientes:

- **Velocidad de cambio.** La velocidad de cambio es la velocidad a la que se acumula la cantidad de datos protegidos. La velocidad depende de la cantidad de datos que cambian en los volúmenes protegidos y el intervalo de protección de los volúmenes. Algunos tipos de máquinas, por lo general, tienen una mayor velocidad de cambio, como un servidor de correo electrónico Exchange. Una forma de reducir la velocidad de cambio es reducir el intervalo de protección.
- **Ancho de banda.** El ancho de banda es la velocidad de transferencia disponible entre el Core de origen y el Core de destino. Es fundamental que el ancho de banda sea mayor que la velocidad de cambio, para que la replicación pueda ajustarse a los puntos de recuperación creados por las instantáneas. En el caso de las transferencias de datos grandes de Core a Core, podrían ser necesarias varias secuencias en paralelo para que el rendimiento en velocidad pueda alcanzar la conexión Ethernet de 1GB Ethernet.

NOTA: El ancho de banda que los ISP especifican es, por lo general, el ancho de banda disponible total. Todos los dispositivos en la red comparten el ancho de banda saliente. Asegúrese de que hay libre ancho de banda suficiente para que la replicación pueda dar servicio a la velocidad de cambios.

- **Número de equipos protegidos.** Es importante tener en cuenta el número de equipos protegidos por Core de origen, y cuántos tiene pensado replicar en el destino. No es obligatorio que se replique cada equipo protegido en el Core de origen; Rapid Recovery permite replicar según equipos protegidos, así que puede elegir replicar solo algunos equipos, si así lo desea. Si todos los equipos protegidos en un Core de origen se deben replicar, la velocidad de cambio es, por lo general, superior. Este factor es relevante si el ancho de banda entre los Cores de origen y destino no es suficiente para la cantidad y el tamaño de los puntos de recuperación que se están replicando.

La opción velocidad de cambios máxima para tipos de conexión WAN aparece en la tabla siguiente, con ejemplos del ancho de banda necesario por gigabyte para una velocidad de cambios razonable.

Tabla 127. Ejemplos de ancho de banda por gigabyte

Banda ancha	Ancho de banda	Velocidad máxima de cambios
DSL	768 Kbps y superior	330MB por hora
Cable	1 Mbps y superior	429MB por hora
T1	1,5 Mbps y superior	644MB por hora
Fibra	20 Mbps y superior	8,38GB por hora

NOTA: Cumpla las recomendaciones que se enumeran en la tabla anterior para obtener resultados óptimos.

Si un enlace falla durante la transferencia de datos, la replicación se reanuda desde el punto de fallo anterior de la transferencia (una vez que se restaura el enlace funcionalmente).

Según su configuración de red, la replicación puede ser un proceso muy largo. Asegúrese de que cuenta con suficiente ancho de banda para alojar la replicación, otras transferencias de Rapid Recovery como las copias de seguridad y cualquiera otra de las aplicaciones importantes que debe ejecutar.

Si experimenta problemas al transferir correctamente datos a través de la red, sobre todo en algunos equipos protegidos o replicados, tenga en cuenta el ajuste de la velocidad de transferencia de datos en esos equipos. Para obtener más información, consulte [Modificación de la configuración de las transferencias](#) y [Regulación de la velocidad de transferencia](#).

Acerca de la replicación y los puntos de recuperación cifrados

Aunque la unidad de inicialización no contiene copias de seguridad del registro de Core de origen y certificados, la unidad de inicialización no contiene claves de cifrado del Core de origen si los puntos de recuperación que se replican del origen al destino están cifrados. Los puntos de recuperación replicados permanecerán cifrados después de su transmisión al Core de destino. Los propietarios o administradores del Core de destino necesitan la frase de contraseña para recuperar los datos cifrados.

Acerca de las políticas de retención para replicación

Las políticas de retención en los Cores de destino y origen no están sincronizadas. La recuperación o eliminación a petición se realizan de forma independiente en cada Core con la acción inicial, así como durante la ejecución de los trabajos nocturnos.

Para obtener más información sobre las políticas de retención, consulte [Administración de políticas de retención](#).

Replicación a un Core de destino administrado automáticamente

Esta configuración se aplica a la replicación en una ubicación externa y a la replicación mutua. Los pasos siguientes son requisito previo:

- Rapid Recovery Core debe estar instalado en todas las máquinas del Core de origen y de destino.
- Si va a configurar Rapid Recovery para la replicación multipunto a punto, debe realizar esta tarea en todos los Cores de origen y en el Core de destino. Para obtener las descripciones de estas configuraciones de replicación, consulte [Replicación](#).
- Si necesita crear una unidad de inicialización y transferirla a un volumen de almacenamiento extraíble físico para realizar la transferencia inicial de puntos de recuperación existentes, debe tener un dispositivo de almacenamiento portátil adecuado. También debe tener acceso físico a la máquina Core de origen para conectar la unidad con el fin de copiar el archivo de la unidad de inicialización.
- Si utiliza una unidad de inicialización en un Core de destino administrado automáticamente, usted o un administrador de confianza debe tener acceso físico al Core de destino.

Un Core de destino administrado automáticamente es aquel al que tiene acceso. Por ejemplo, su compañía puede administrar frecuentemente un Core administrado automáticamente en una ubicación exterior, o bien puede residir en una ubicación geográfica distinta a la del Core de origen. La replicación puede configurarse en su totalidad en el Core de origen, a menos que decida inicializar los datos mediante una unidad de inicialización. En estos casos, deberá crear una unidad de inicialización mediante este procedimiento y, posteriormente, conectar la unidad al Core de destino para consumir los datos de punto de recuperación archivados. Para obtener más información, consulte [Determinación de la estrategia y necesidades de inicialización](#).

Complete los pasos del siguiente procedimiento para configurar el Core de origen con el fin de replicar un Core de destino administrado automáticamente.

- 1 Vaya a la **Rapid Recovery Core Console** del Core de origen.
- 2 En la barra de botones, haga clic en  **Replicate (Replicar)**.
Se abrirá el **Replication Wizard** (Asistente de replicación).
- 3 En la página **Target Core (Core de destino)** del asistente de replicación, y si establece la replicación con un Core de destino que se haya emparejado anteriormente con este Core de origen, seleccione **Use an existing target core (Utiliza un Core de destino existente)** y, a continuación, seleccione el Core de destino en la lista desplegable. Vaya al paso 5.

- 4 En el **Target Core (Core de destino)** del asistente de replicación, y si establece la replicación con un Core de destino desde este Core de origen por primera vez, seleccione **I have my own Target Core (Tengo mi propio Core de destino)** y, a continuación, introduzca la información según se describe en la tabla siguiente.

Tabla 128. Información del Core de destino

Cuadro de texto	Descripción
Host Name (Nombre del host)	Introduzca el nombre de host o dirección IP de la máquina del Core en la que esté replicando.
Port (Puerto)	El número de puerto por el que el Rapid Recovery Core se comunicará con la máquina. El número de puerto predeterminado es 8006.
Username (Nombre del usuario)	Introduzca el nombre de usuario para acceder al servidor proxy.
Password (Contraseña)	Introduzca la contraseña para acceder a la máquina.

- 5 Haga clic en **Next (Siguiente)**.

NOTA: Si no hay ningún repositorio en el Core de destino, aparece un aviso que indica que puede emparejar el Core de origen con el Core de destino, pero que no puede replicar los agentes (máquinas protegidas) en esta ubicación hasta que se establezca un repositorio. Para obtener más información sobre cómo configurar un repositorio para un Core, consulte [Creación de un repositorio DVM](#).

- 6 En la página **Request (Solicitud)**, introduzca un nombre para esta configuración de replicación; por ejemplo, SourceCore1. Este es el nombre que se utiliza para el panel de Replicación entrante en la página de replicación del Core de destino.

- 7 Haga clic en **Next (Siguiente)**.

- 8 En la página **Protected Machines (Máquinas protegidas)**, seleccione las máquinas protegidas que desee replicar y, a continuación, utilice las listas desplegables de la columna Repository (Repositorio) y seleccione un repositorio para cada máquina protegida.

- 9 Si tiene pensado realizar el proceso de inicialización para la transferencia de los datos principales, realice los pasos siguientes:

NOTA: Ya que es necesario copiar grandes cantidades de datos al dispositivo de almacenamiento portátil, Dell recomienda usar una conexión eSATA, USB 3.0 u otra conexión de alta velocidad con el dispositivo de almacenamiento portátil.

- En la página **Protected Machines (Máquinas protegidas)** del asistente de replicación, seleccione **Use a seed drive to perform the initial transfer** (Usar una unidad de inicialización para realizar la transferencia inicial).
 - Si actualmente tiene una o más máquinas protegidas que se replican en un Core de destino, puede incluir estas máquinas protegidas en la unidad de inicialización. Para ello, seleccione **Include already replicated recovery points in the seed drive** (Incluir los puntos de recuperación replicados en la unidad de inicialización).
- Haga clic en **Next (Siguiente)**.
- En la página **Seed Drive Location (Ubicación de la unidad de inicialización)**, utilice la lista desplegable **Location type (Tipo de ubicación)** para seleccionar de entre los tipos de destino siguientes:
 - Local (Local)
 - Network (Red)
 - Cloud (Nube)
- En función del tipo de ubicación que haya seleccionado en el paso c, introduzca los detalles del archivo de la unidad de inicialización según se describen en la tabla siguiente.

Tabla 129. Detalles del archivo

Opción	Cuadro de texto	Descripción
Local (Local)	Ubicación de salida	Especifique la ubicación de salida, que se utiliza para definir la ruta de acceso a la ubicación en la que desea que resida el archivo de la unidad de inicialización; por ejemplo, <code>D:\work\archive</code> .
Network (Red)	Ubicación de salida	Especifique la ubicación de salida, que se utiliza para definir la ruta de acceso a la ubicación en la que desea que resida el archivo; por ejemplo, <code>\\servername\sharename</code> .
	User Name (Nombre de usuario)	Introduzca un nombre de usuario. Se utiliza para establecer las credenciales de inicio de sesión para el recurso compartido de red.
	Password (Contraseña)	Introduzca una contraseña para la ruta de acceso de red. Se utiliza para establecer las credenciales de inicio de sesión para el recurso compartido de red.
Cloud	Account (Cuenta en la nube)	<i>i</i> NOTA: Para seleccionar una cuenta en la nube, debe haberla agregado primero en la Core Console. Para obtener más información, consulte Incorporación de una cuenta de nube.
	Container (Contenedor)	En el menú desplegable, seleccione un contenedor asociado con la cuenta.
	Folder Name (Nombre de carpeta)	Escriba un nombre para la carpeta en la que se vayan a guardar los datos archivados. El nombre predeterminado es Rapid-Recovery-Archive-[FECHA DE CREACIÓN]-[HORA DE CREACIÓN]

e Haga clic en **Next (Siguiente)**.

f En la página **Seed Drive Options (Opciones de la unidad de inicialización)** del asistente de replicación, introduzca la información según se describe en la tabla siguiente.

Tabla 130. Opciones de la unidad de inicialización

Elemento	Descripción
Maximum Size (Tamaño máximo)	Los grandes archivos de datos pueden dividirse en múltiples segmentos. Seleccione el tamaño máximo del segmento que desea reservar para crear la unidad de inicialización mediante una de las acciones siguientes: • Seleccione Entire Target (Todo el destino) para reservar todo el espacio disponible en la ruta de acceso proporcionada en la página Seed Drive Location (Ubicación de la unidad de inicialización) para su uso en el futuro (por ejemplo, si la ubicación es <code>D:\work\archive</code>, se reservará todo el espacio disponible en la unidad D: por si es necesario para copiar la unidad de inicialización, pero no se reserva inmediatamente después de iniciar el proceso de copia. • Seleccione el cuadro de texto, introduzca una cantidad y, a continuación, seleccione una unidad de medida en la lista desplegable para personalizar el espacio máximo que desea reservar.
Recycle action (Acción de reciclado)	En el caso de que la ruta de acceso ya contenga una unidad de inicialización, seleccione una de las opciones siguientes: • Do not reuse (No reutilizar): no sobrescribe ni borra los datos existentes de la ubicación. Si la ubicación no está vacía, fallará la escritura de la unidad de inicialización. • Replace this Core (Reemplazar este Core): sobrescribe los datos de inicialización que ya existen y que pertenecen a este Core, pero deja intactos los datos de los otros Cores. • Erase completely (Borrar completamente): borra todos los datos del directorio antes de escribir la unidad de inicialización.

Elemento	Descripción
Comment (Comentario)	Introduzca un comentario que describa la unidad de inicialización.
Add all Agents to Seed Drive (Agregar todos los agentes a la unidad de inicialización)	Seleccione esta opción para replicar todas las máquinas protegidas en el Core de origen usando la unidad de inicialización. Esta opción está seleccionada de forma predeterminada.
Build recovery point chains (fix orphans) (Crear cadenas de punto de recuperación [fijar huérfanos])	Seleccione esta opción para replicar toda la cadena de puntos de recuperación (PR) en la unidad de inicialización. Esta opción está seleccionada de manera predeterminada. NOTA: En AppAssure 5.4, la inicialización típica replica solo el último punto de recuperación a la unidad de inicialización, lo que reduce la cantidad de tiempo y el espacio necesario para crear la unidad de inicialización. La opción para crear cadenas de punto de recuperación para la unidad de inicialización requiere el espacio suficiente en esa unidad para almacenar los puntos de recuperación más recientes desde la máquina o máquinas protegidas especificadas, lo cual puede llevar un tiempo adicional para completar la tarea.

- g Realice uno de los siguientes pasos:
- Si desactiva la casilla **Add all Agents to Seed Drive (Agregar todos los Agentes a la unidad de inicialización)**, haga clic en **Next (Siguiente)**.
 - Si ha seleccionado **Add all Agents to Seed Drive (Agregar todos los Agentes a la unidad de inicialización)**, vaya al Paso 10.
- h En la página **Protected Machines (Máquinas protegidas)** del asistente de replicación, seleccione las máquinas protegidas que desea replicar en el Core de destino usando la unidad de inicialización.
- 10 Haga clic en **Finish (Finalizar)**.
- 11 Si ha creado una unidad de inicialización, envíela al Core de destino.
El emparejamiento del Core de origen con el Core de destino ha finalizado.

A menos que haya seleccionado la opción para poner en pausa inicialmente la replicación, el proceso de replicación se inicia inmediatamente.

- 1 Si ha seleccionado la opción de usar una unidad de inicialización, la replicación produce puntos de recuperación huérfanos en el Core de destino hasta que la unidad de inicialización se consume y proporciona las imágenes base necesarias.
- 2 Si ha especificado el uso de la unidad a, transfiera el archivo de la unidad de inicialización a un volumen (una carpeta compartida, un disco virtual o un medio de almacenamiento extraíble). A continuación, consuma la unidad de inicialización.

Visualización de la replicación entrante y saliente

Si hace clic en el icono **Replicación**  de la barra de iconos, aparece la página **Replicación**. Esta página le proporciona una comprensión de la replicación desde el ámbito de este Core. Incluye dos paneles:

- En el panel **Replicación saliente** se muestran los equipos protegidos en este Core que se replican en otro Core.
- En el panel **Replicación entrante** se muestran los equipos replicados en este Core y el Core de origen del que se replican dichos equipos.

En esta sección se describe la información que se muestra en los paneles.

La información sobre la replicación saliente del Core de Rapid Recovery se describe en la tabla siguiente.

Tabla 131. Información sobre replicación saliente

Elemento de la IU	Descripción
Seleccionar elemento	Para cada fila de la tabla de resumen, puede seleccionar la casilla de verificación para realizar acciones de la lista de opciones del menú situada encima de la tabla.
Tipo	Muestra el tipo de protección. Puede expandir un Core de destino para mostrar equipos replicados individuales.
Indicador de estado	El estado de la replicación. Los círculos coloreados de la columna Estado muestran si un equipo replicado dispone de conexión o no está accesible. Si pasa el cursor sobre el círculo coloreado, se muestra la condición de estado. Las condiciones de estado incluyen los colores verde (replicación establecida y con conexión), amarillo (replicación en pausa), rojo (error de autenticación) y gris (sin conexión o no accesible).
Nombre de replicación	El nombre mostrado del equipo de Core a los que los equipos de este Core de origen se replican.
Equipos	Muestra el número de equipos replicados en el Core de destino seleccionado.
Sincronización	La fecha y hora de la última transferencia de replicación al Core de destino.
	Al hacer clic en el menú desplegable de acciones de esta columna, verá una lista de acciones que podrá realizar para modificar la relación de replicación específica.

Puede realizar acciones sobre dos o más de los Cores enumerados en la cuadrícula de replicación saliente. Para realizar acciones en diversos Cores de destino, seleccione la casilla de verificación de cada Core en la cuadrícula y, a continuación, desde el menú de encima de dicha cuadrícula, puede seleccionar la acción que desee realizar. Puede realizar las acciones que se describen en la tabla siguiente.

Tabla 132. Acciones globales disponibles en el panel de replicación saliente

Elemento de la IU	Descripción
Agregar Core de destino	Le permite definir otro Core de destino para replicar equipos protegidos en este Core de origen.
Actualizar	Se actualiza la información mostrada en la tabla.
Forzar	Fuerza la replicación.
Realizar pausa	Se pausa la replicación establecida.
Reanudar	Se reanuda la replicación en pausa.
Copiar	Se abre el Asistente para replicación, que le permite copiar puntos de recuperación existentes de equipos protegidos seleccionados en una unidad de inicialización.
Eliminar	Se elimina la replicación saliente.
Unidades de inicialización	Esta opción de menú aparece si los datos se copiaron en una unidad de inicialización cuando se configuró la replicación. Se muestra la información sobre el archivo de unidad de inicialización, que incluye la fecha y hora en la que se guardó la unidad de inicialización. Los menús que pueden contraerse indican el Core de destino y los equipos protegidos desde los que se generaron los archivos de unidad de inicialización.
	Al hacer clic en el menú desplegable de acciones de esta columna, verá una lista de acciones que podrá realizar para modificar la relación de replicación específica.

La información sobre la replicación entrante desde otro Core se describe en la tabla siguiente.

Tabla 133. Información sobre la replicación entrante

Elemento de la IU	Descripción
Seleccionar elemento	Para cada fila de la tabla de resumen, puede seleccionar la casilla de verificación para realizar acciones de la lista de opciones del menú situada encima de la tabla.
Tipo	Muestra el tipo de protección. Puede expandir un Core de origen para mostrar equipos replicados individuales.
Indicador de estado	El estado de la replicación. Los círculos coloreados de la columna Estado muestran si un equipo replicado dispone de conexión o no está accesible. Si pasa el cursor sobre el círculo coloreado, se muestra la condición de estado. Las condiciones de estado incluyen los colores verde (replicación establecida y con conexión), amarillo (replicación en pausa), rojo (error de autenticación) y gris (sin conexión o no accesible).
Nombre de replicación	El nombre de visualización del equipo del Core de origen que contiene los equipos protegidos que se replican en este Core de destino. Este nombre se podrá especificar de manera opcional al establecer la replicación en el Core de origen mediante el Asistente para replicación.
Equipos	Se muestran el número de equipos protegidos en el Core de origen que se replican en este Core de destino.
Sincronización	La fecha y hora de la última transferencia de replicación del Core de origen.
	Al hacer clic en el menú desplegable de acciones de esta columna, verá una lista de acciones que podrá realizar para modificar la relación de replicación específica.

Puede realizar acciones sobre dos o más de los Cores de origen enumerados en la cuadrícula de replicación entrante. Para realizar acciones en diversos Cores de origen, seleccione la casilla de verificación de cada Core en la cuadrícula y, a continuación, desde el menú de encima de dicha cuadrícula, puede seleccionar la acción que desee realizar. Puede realizar las acciones que se describen en la tabla siguiente.

Tabla 134. Acciones globales disponibles en el panel replicación entrante

Elemento de la IU	Descripción
Actualizar	Se actualiza la información mostrada en la tabla.
Forzar	Fuerza la replicación.
Realizar pausa	Se pausa la replicación establecida.
Reanudar	Se reanuda la replicación en pausa.
Eliminar	Se elimina la replicación entrante.

Configuración de la replicación

Para replicar los datos mediante Rapid Recovery, debe configurar los Cores de origen y de destino para la replicación. Después de configurar la replicación, puede replicar los datos del Agent, supervisar y administrar la replicación y realizar la recuperación.

Para realizar replicación en Rapid Recovery, tendrá que hacer las operaciones siguientes:

- Configure un repositorio en el Core de destino. Para obtener más información sobre cómo agregar un repositorio en el Core de destino, consulte [Creación de un repositorio DVM](#).
- Configure la replicación administrada automáticamente. Para obtener más información acerca de cómo replicar a un Core de destino administrado automáticamente, consulte [Replicación a un Core de destino administrado automáticamente](#).
- Configure la replicación de terceros. Para obtener más información acerca de cómo replicar a un Core de destino de terceros, consulte [Replicación en un Core de destino externo](#).
- Replique una máquina protegida existente. Para obtener más información sobre la replicación de una máquina que ya esté protegido por el Core de origen, consulte [Cómo agregar un equipo a una replicación existente](#).

- Consuma la unidad de inicialización. Para obtener más información sobre general sobre los datos de la unidad de inicialización en el Core de destino, consulte [Consumo de la unidad de inicialización en un Core de destino](#).
- Establezca la prioridad de replicación para una máquina protegida. Para obtener más información sobre cómo priorizar la replicación de máquinas protegidas, consulte [Cómo establecer la prioridad de replicación para un equipo protegido](#).
- Configure un programa de replicación para una máquina protegida. Para obtener más información sobre la configuración de una programación de replicación, consulte [Programación de la replicación](#).
- Supervise la replicación según sea necesario. Para obtener más información sobre cómo supervisar la replicación, consulte [Visualización de la replicación entrante y saliente](#).
- Administre la configuración de replicación según convenga. Para obtener más información acerca de cómo administrar la configuración de replicación, consulte [Administración de configuraciones de replicación](#).
- Recupere los datos replicados ante situaciones de desastre o de pérdida de datos. Para obtener más información acerca de cómo recuperar datos replicados, consulte [Recuperación de datos replicados](#).

Replicación en un Core de destino externo

Un Core de terceros es un Core de destino administrado y mantenido por un proveedor de servicios administrados (MSP). La replicación en un Core administrado por un tercero no exige que el cliente tenga acceso al Core de destino.

El proceso de replicación en un Core de terceros implica que el cliente lleve a cabo algunas tareas, así como la otra empresa. Después de que un cliente envíe una solicitud para la replicación del Core o Cores de origen, el proveedor de servicios administrados (MSP) debe completar la configuración en el Core de destino revisando la solicitud.

NOTA: Esta configuración se aplica a replicación alojada y en nube. El Core de Rapid Recovery debe estar instalado en todos los equipos de origen. Si configura Rapid Recovery para la replicación multipunto a punto, debe realizar esta tarea en todos los Cores de origen.

Para replicar en un Core de destino administrado por un tercero, complete las siguientes tareas:

- [Envío de una solicitud de replicación a un proveedor de servicios de terceros](#)
- [Revisión de una solicitud de replicación de un cliente](#)
- [Cómo ignorar una solicitud de replicación de un cliente](#)

Envío de una solicitud de replicación a un proveedor de servicios de terceros

Si usted es un usuario final que se suscribe a un Core administrado por un tercero, como un proveedor de servicios administrados (MSP), complete los pasos de este procedimiento para enviar una solicitud de replicación a su proveedor de servicios de terceros.

- 1 Navegue al Core de Rapid Recovery.
- 2 En barra de botones de iconos, haga clic en  **Replicar**. Aparece el **Asistente para replicación**.
- 3 En la página **Target Core** (Core de destino) del Asistente para replicación, seleccione **Tengo una suscripción a un tercero que proporciona servicios de copia de seguridad y recuperación tras desastres remotos** y, a continuación, introduzca la información según se describe en la tabla siguiente.

Tabla 135. Información del Core de destino externo

Cuadro de texto	Descripción
Nombre de host	Escriba el nombre de host, dirección IP o FQDN para el equipo del Core de terceros.
Puerto	Escriba el número de puerto que le indicó el proveedor de servicios de terceros.

Cuadro de texto	Descripción
	El número de puerto predeterminado es 8006.

• Si el Core que desea agregar se ha emparejado con este Core de origen anteriormente, puede hacer lo siguiente:

- 1 Seleccione **Utilizar un Core de destino existente**.
- 2 Seleccione el Core de destino de la lista desplegable.
- 3 Haga clic en **Siguiente**.
- 4 Vaya al [Paso 7](#).

4 Haga clic en **Siguiente**.

5 En la página **Solicitud** del Asistente para replicación, introduzca la información según se describe en la tabla siguiente.

Tabla 136. Detalles del Core de destino externo

Cuadro de texto	Descripción
Dirección de correo electrónico	Introduzca la dirección de correo electrónico asociada con su suscripción de servicios de terceros.
Id. de cliente (opcional)	Escriba la dirección de correo electrónico de la suscripción y la Id. de cliente que le proporcionó el proveedor de servicios.

6 Haga clic en **Siguiente**.

7 En la página **Equipos protegidos** del Asistente para replicación, seleccione los equipos protegidos que desea replicar en el Core de terceros.

8 Si desea realizar el proceso de inicialización para la transferencia de los datos de base, realice los siguientes pasos.

NOTA: Como hay que copiar grandes cantidades de datos al dispositivo de almacenamiento portátil, se recomienda usar una conexión eSATA, USB 3.0 y otra de alta velocidad con el dispositivo de almacenamiento portátil.

- En la página **Equipos protegidos** del Asistente para replicación, seleccione **Use a seed drive to perform initial transfer** (Utilizar una unidad de inicialización para realizar la transferencia inicial).
 - Si actualmente tiene uno o varios equipos protegidos replicando en un core de destino, puede incluirlos en la unidad de inicialización seleccionando la opción **Incluya los puntos de recuperación ya replicados en la unidad de inicialización**.
- Haga clic en **Siguiente**.
- En la página **Ubicación de la unidad de inicialización** del Asistente para replicación, utilice la lista desplegable tipo de **Ubicación** para seleccionar los tipos de destino siguientes:
 - Local
 - Red
 - Nube
- En función del tipo de ubicación que haya seleccionado en el [Paso c](#), introduzca los detalles del archivo comprimido según se describe en la tabla siguiente.

Tabla 137. Detalles de archivación

Opción	Cuadro de texto	Descripción
Local	Ubicación de salida	Escriba la ubicación de la salida. Se utiliza para definir la ruta de acceso de la ubicación en la que desea que resida el archivo comprimido de la unidad de inicialización; por ejemplo, D:\trabajo\archivación .
Red	Ubicación de salida	Escriba la ubicación de la salida. Se utiliza para definir la ruta de acceso de la ubicación en la que desea que resida el archivo comprimido; por ejemplo, \nombreservidor\nombrecursocompartido .
	Nombre de usuario	Escriba un nombre de usuario. Se utiliza para establecer las credenciales de inicio de la sesión del recurso compartido de red.

Opción	Cuadro de texto	Descripción
	Contraseña	Escriba una contraseña para la ruta de acceso de red. Se utiliza para establecer las credenciales de inicio de la sesión del recurso compartido de red.
Nube	Cuenta	Seleccione una cuenta de la lista desplegable. <i>i</i> NOTA: Para seleccionar una cuenta de nube, debe añadirla primero en Core Console. Para obtener más información, consulte Incorporación de una cuenta de nube .
	Contenedor	Seleccione un contenedor asociado con su cuenta en el menú desplegable.
	Nombre de la carpeta	Introduzca un nombre para la carpeta en la que hay que guardar los datos archivados. El nombre predeterminado es Rapid-Recovery-Archive-[FECHA CREACIÓN]-[HORA CREACIÓN]

e Haga clic en **Siguiente**.

f En la página **Opciones de la unidad de inicialización** del Asistente de replicación, introduzca la información según se describe en la tabla siguiente.

Tabla 138. Opciones de la unidad de inicialización

Elemento	Descripción
Tamaño máximo	Los grandes archivos de datos se pueden dividir en varios segmentos. Seleccione el tamaño máximo de espacio que desea reservar para crear la unidad de inicialización realizando una de las siguientes acciones: • Seleccione Todo el destino para reservar todo el espacio disponible en la ruta de acceso proporcionada en la página Ubicación de unidad de inicialización (por ejemplo, si la ubicación es D: \trabajo\archivo, se reserva todo el espacio disponible en la unidad D:). • Seleccione el cuadro de texto en blanco, introduzca una cantidad y, a continuación, seleccione una unidad de medida en la lista desplegable para personalizar el espacio que desea reservar.
Acción de reciclaje	En el caso de que la ruta de acceso ya contenga una unidad de inicialización, seleccione una de las opciones siguientes: • No reutilizar. No sobrescribe ni borra datos de inicialización existentes de la ubicación. Si la ubicación no está vacía, la escritura en la unidad de inicialización fallará. • Reemplazar este Core. Sobrescribe los datos de inicialización que ya existan y que pertenezcan a este Core, pero deja intactos los datos del resto de Cores. • Borrar completamente. Borra todos los datos de inicialización del directorio antes de escribir en la unidad de inicialización.
Comentario	Introduzca un comentario que describa la unidad de inicialización.
Agregar todos los Agents a la unidad de inicialización	Seleccione esta opción para replicar todos los equipos protegidos en el Core de origen usando la unidad de inicialización. Esta opción se selecciona de forma predeterminada.
Crear cadenas de puntos de recuperación (reparar huérfanos)	Seleccione esta opción para replicar toda la cadena de puntos de recuperación en la unidad de inicialización. Esta opción se selecciona de forma predeterminada. <i>i</i> NOTA: La inicialización típica en AppAssure 5.4 replicaba únicamente el último punto de recuperación en la unidad de inicialización, lo que reducía la cantidad de tiempo y espacio necesarios para crear la unidad de inicialización. La opción para crear las cadenas del punto de recuperación (RP) en la unidad de inicialización necesita suficiente espacio en la unidad de inicialización como para almacenar los últimos puntos de recuperación desde los equipos protegidos especificados y puede llevar más tiempo.

g Realice una de las siguientes acciones:

- Si ha desactivado la casilla de verificación **Agregar todos los Agents a la unidad de inicialización**, haga clic en **Siguiente**.

- Si ha seleccionado **Agregar todos los Agents a la unidad de inicialización**, vaya al [Paso 9](#).
 - h En la página **Equipos** del Asistente para replicación, seleccione los equipos protegidos que desea replicar en el Core de destino usando la unidad de inicialización.
- 9 Haga clic en **Finalizar**.
 - 10 Si ha creado una unidad de inicialización, envíela tal y como se lo indique su proveedor de servicios de terceros.

Revisión de una solicitud de replicación de un cliente

Después de que un usuario complete el procedimiento [Envío de una solicitud de replicación a un proveedor de servicios de terceros](#), se envía una solicitud de replicación desde el Core de origen al Core de destino de terceros. Como tercero, puede revisar la solicitud y, a continuación, aprobarla para iniciar la replicación para su cliente. También puede denegarla para evitar que se produzca.

Elija entre las siguientes opciones:

- [Aprobación de una solicitud de replicación](#)
- [Denegación de una solicitud de replicación](#)

Aprobación de una solicitud de replicación

Complete el siguiente procedimiento para aprobar una solicitud de replicación en un Core de destino de terceros.

- 1 En el Core de destino, vaya a la Core Console de Rapid Recovery.
- 2 Desde la barra de iconos, haga clic en  (Replicación).
Aparece la página **Replicación**.
- 3 En la página **Replicación**, haga clic en **Solicitud (#)**.
Aparece la sección **Pending Replication Requests (Solicitudes de replicación pendientes)**.
- 4 En Solicitudes de replicación pendientes, haga clic en el menú desplegable junto a la solicitud que desea revisar y, a continuación, haga clic en **Revisar**.
Aparecerá la ventana **Review Replication Request (Revisar solicitud de replicación)**.

NOTA: La información que aparece en la sección **Identidad** del Core de origen de esta ventana viene determinada por la solicitud completada por el cliente.

- 5 En Identidad del Core de origen, realice una de las acciones siguientes:
 - Seleccione **Replace an existing replicated Core (Reemplazar un Core replicado existente)** y, a continuación, seleccione un Core en la lista desplegable.
 - Seleccione **Crear un nuevo Core de origen** y, a continuación, confirme que el nombre del Core, la dirección de correo electrónico y la Id. del cliente proporcionados son correctos. Edite la información como sea necesario.
- 6 En Agents, seleccione los equipos a los que se aplica la aprobación y, a continuación, utilice las listas desplegables de la columna Repositorio para seleccionar el repositorio correspondiente a cada equipo.
- 7 De forma optativa, en el cuadro de texto **Comentario**, introduzca una descripción o mensaje que se debe incluir en la respuesta al cliente.
- 8 Haga clic en **Enviar respuesta**.
Se acepta la replicación.

Denegación de una solicitud de replicación

Complete los pasos en el siguiente procedimiento para denegar una solicitud de replicación a un Core de terceros de un cliente.

Para denegar una solicitud sin revisarla, consulte [Cómo ignorar una solicitud de replicación de un cliente](#).

- 1 En el Core de destino, vaya a la Core Console de Rapid Recovery.
- 2 Desde la barra de iconos, haga clic en  (Replicación).
Aparece la página **Replicación**.
- 3 En la página **Replicación**, haga clic en **Solicitud (#)**.
Aparece la sección **Pending Replication Requests (Solicitudes de replicación pendientes)**.
- 4 En Solicitudes de replicación pendientes, haga clic en el menú desplegable junto a la solicitud que desea revisar y, a continuación, haga clic en **Revisar**.
Aparecerá la ventana **Review Replication Request (Revisar solicitud de replicación)**.
- 5 Haga clic en **Denegar**.
Se deniega la replicación. Aparece una notificación de denegación en Alertas en la pestaña Eventos del Core de origen.

Cómo ignorar una solicitud de replicación de un cliente

Como proveedor de servicios de terceros de un Core de destino, tiene la opción de ignorar una solicitud de replicación enviada por un cliente. Esta opción se puede utilizar si se ha enviado una solicitud por error o si desea denegar una solicitud sin revisarla.

Para obtener más información acerca de las solicitudes de replicación, consulte [Revisión de una solicitud de replicación de un cliente](#).

Complete el siguiente procedimiento para ignorar una solicitud de replicación de un cliente.

- 1 En el Core de destino, vaya a la Core Console de Rapid Recovery.
- 2 Desde la barra de iconos, haga clic en  (Replicación).
Aparece la página **Replicación**.
- 3 En la página **Replicación**, haga clic en **Solicitud (#)**.
Aparece la sección **Pending Replication Requests (Solicitudes de replicación pendientes)**.
- 4 En Solicitudes de replicación pendientes, haga clic en el menú desplegable junto a la solicitud que desea ignorar y, a continuación, haga clic en **Omitir**.
- 5 En el cuadro de diálogo **Ignorando solicitud**, haga clic en **Sí** para confirmar el comando.
Se envía la notificación de la omisión de la solicitud al Core de origen y la solicitud se quita de la pestaña Replicación en la pestaña Core.

Cómo agregar un equipo a una replicación existente

Después de que la replicación se haya establecido entre un Core de origen y otro de destino, es posible agregar nuevos equipos protegidos al destino. Complete los pasos del siguiente procedimiento en el Core de origen para agregar un nuevo equipo protegido a un Core de destino emparejado para la replicación.

Para obtener más información sobre la replicación, consulte [Replicación](#) y [Replicación a un Core de destino administrado automáticamente](#).

- 1 Vaya a la Core Console de Rapid Recovery del Core de origen.
- 2 En la barra de botones, haga clic en  **Replicar**.
Se abre el Asistente para replicación en la página **Equipos protegidos**.
- 3 En la página **Equipos protegidos**, seleccione los equipos protegidos que desea replicar y, a continuación, utilice las listas desplegables de la columna Repositorio para seleccionar un repositorio para cada equipo protegido.
- 4 Si desea realizar el proceso de inicialización para la transferencia de los datos de base, realice los siguientes pasos:

NOTA: Como hay que copiar grandes cantidades de datos al dispositivo de almacenamiento portátil, se recomienda usar una conexión eSATA, USB 3.0 y otra de alta velocidad con el dispositivo de almacenamiento portátil.

- En la página **Equipos protegidos** del asistente para replicación, seleccione **Utilizar una unidad de inicialización para realizar la transferencia inicial**.
 - Si actualmente tiene uno o varios equipos protegidos replicando en un Core de destino, puede incluirlos en la unidad de inicialización seleccionando la opción **Incluya los puntos de recuperación ya replicados en la unidad de inicialización**.
- Haga clic en **Siguiente**.
- En la página **Ubicación de unidad de inicialización** del asistente, utilice la lista desplegable Tipo de **ubicación** para seleccionar los siguientes tipos de destino:
 - Local
 - Red
 - Nube
- En función del tipo de ubicación que haya seleccionado en el [Paso c](#), introduzca los detalles para el archivo según se describen en la tabla siguiente.

Tabla 139. Detalles de archivación

Opción	Cuadro de texto	Descripción
Local	Ubicación de salida	Escriba la ubicación de la salida. Se utiliza para definir la ruta de acceso de la ubicación en la que desea que resida el archivo; por ejemplo, d:\trabajo\archivación.
Red	Ubicación de salida	Escriba la ubicación de la salida. Se utiliza para definir la ruta de acceso de la ubicación en la que desea que resida el archivo; por ejemplo, \nombreservidor\nombrecursocompartido.
	Nombre de usuario	Escriba un nombre de usuario. Se utiliza para establecer las credenciales de inicio de la sesión del recurso compartido de red.
	Contraseña	Escriba una contraseña para la ruta de acceso de red. Se utiliza para establecer las credenciales de inicio de la sesión del recurso compartido de red.
Nube	Cuenta	<i>i</i> NOTA: Para seleccionar una cuenta de nube, debe añadirla primero en Core Console. Para obtener más información, consulte Incorporación de una cuenta de nube. Seleccione una cuenta de la lista desplegable.
	Contenedor	Seleccione un contenedor asociado con su cuenta en el menú desplegable.
	Nombre de la carpeta	Introduzca un nombre para la carpeta en la que hay que guardar los datos archivados. El nombre predeterminado es Rapid-Recovery-Archive-[FECHA CREACIÓN]-[HORA CREACIÓN]

- Haga clic en **Siguiente**.
- En la página **Opciones de unidad de inicialización** del asistente, introduzca la información según lo descrito en la siguiente tabla.

Tabla 140. Opciones de la unidad de inicialización

Elemento	Descripción
Tamaño máximo	Los grandes archivos de datos se pueden dividir en varios segmentos. Seleccione el tamaño máximo de espacio que desea reservar para crear la unidad de inicialización realizando una de las siguientes acciones: Seleccione Todo el destino para reservar todo el espacio disponible en la ruta de acceso proporcionada en la página Ubicación de unidad de inicialización (por ejemplo, si la ubicación es D:\trabajo\archivo, se reserva todo el espacio disponible en la unidad D:).

Elemento	Descripción
	• Seleccione el cuadro de texto en blanco, introduzca una cantidad y, a continuación, seleccione una unidad de medida en la lista desplegable para personalizar el espacio que desea reservar.
Acción de reciclaje	En el caso de que la ruta de acceso ya contenga una unidad de inicialización, seleccione una de las opciones siguientes: • No reutilizar. No sobrescribe ni borra datos de inicialización existentes de la ubicación. Si la ubicación no está vacía, la escritura en la unidad de inicialización fallará. • Reemplazar este Core. Sobrescribe los datos de inicialización que ya existan y que pertenezcan a este Core, pero deja intactos los datos del resto de Cores. • Borrar completamente. Borra todos los datos de inicialización del directorio antes de escribir en la unidad de inicialización.
Comentario	Introduzca un comentario que describa la unidad de inicialización.
Agregar todos los Agents a la unidad de inicialización	Seleccione esta opción para replicar todos los equipos protegidos en el Core de origen usando la unidad de inicialización. Esta opción se selecciona de forma predeterminada.
Crear cadenas de puntos de recuperación (reparar huérfanos)	Seleccione esta opción para replicar toda la cadena de puntos de recuperación en la unidad de inicialización. Esta opción se selecciona de forma predeterminada. NOTA: La inicialización típica de Rapid Recovery 5.4 solo replica el último punto de recuperación en la unidad de inicialización, lo que reduce la cantidad de tiempo y espacio necesarios para crear la unidad de inicialización. La opción para crear las cadenas del punto de recuperación (RP) en la unidad de inicialización necesita suficiente espacio en la unidad de inicialización como para almacenar los últimos puntos de recuperación desde los equipos protegidos especificados y puede llevar más tiempo.

- g Realice una de las siguientes acciones:
- Si ha desactivado la casilla de verificación **Agregar todos los Agents a la unidad de inicialización**, haga clic en **Siguiente**.
 - Si ha seleccionado **Agregar todos los Agents a la unidad de inicialización**, vaya al [Paso 5](#).
- h En la página **Equipos protegidos** del asistente, seleccione los equipos protegidos que desea replicar en el Core de destino usando la unidad de inicialización.
- 5 Haga clic en **Finalizar**.

Consumo de la unidad de inicialización en un Core de destino

Complete el siguiente procedimiento para consumir los datos del archivo de la unidad de inicialización en el Core de destino.

NOTA: Este procedimiento solo es necesario si se ha creado una unidad de inicialización como parte de las secciones [Replicación a un Core de destino administrado automáticamente](#) o [Replicación en un Core de destino externo](#).

- 1 Si el archivo de la unidad de inicialización se ha guardado en un dispositivo de almacenamiento portátil, como una unidad USB, conecte la unidad al Core de destino.
- 2 En el Core de destino, abra la Rapid Recovery Core Console y, en la barra de iconos, haga clic en  (Replicación). Aparece la página **Replicación**.
- 3 En la página **Replicación**, en Replicación entrante, haga clic en el menú desplegable para el Core de origen correcto y, a continuación, seleccione **Consumir**. Aparecerá el cuadro de diálogo **Consumir**.
- 4 En el campo **Tipo de ubicación**, seleccione una de las siguientes opciones de la lista desplegable:
 - Local
 - Red

- Nube

- Introduzca los detalles para el archivo comprimido de la unidad de inicialización según se describen en la tabla siguiente en función del tipo de ubicación que haya seleccionado en el [paso 4](#).

Tabla 141. Detalles de archivación

Opción	Cuadro de texto	Descripción
Local	Ubicación	Introduzca la ruta de acceso para el archivo.
Red	Ubicación	Introduzca la ruta de acceso para el archivo.
	Nombre de usuario	Escriba el nombre de usuario. Se utiliza para establecer las credenciales de inicio de la sesión del recurso compartido de red.
	Contraseña	Escriba una contraseña para la ruta de acceso de red. Se utiliza para establecer las credenciales de inicio de la sesión del recurso compartido de red.
Nube	Cuenta	Seleccione una cuenta de la lista desplegable.
 NOTA: Para seleccionar una cuenta de nube, debe añadirla primero en Core Console. Para obtener más información, consulte Incorporación de una cuenta de nube.		
	Contenedor	Seleccione un contenedor asociado con su cuenta en el menú desplegable.
	Nombre de la carpeta	Introduzca el nombre de la carpeta en la que se guardan los datos archivados; por ejemplo, Archivo-Rapid-Recovery-[FECHA CREACIÓN]-[HORA CREACIÓN]

- Haga clic en **Comprobar archivo**.

El Core busca el archivo.

Después de encontrar el archivo, aparecen los siguientes cuadros de texto en la ventana Consumir prerrellenados con los datos recogidos del [paso 4](#), [paso 5](#), y el archivo. En Rango de fechas aparecen las fechas del punto de recuperación más reciente y más antiguo contenido en la unidad de inicialización. Cualquier comentario introducido al crear la unidad de inicialización se importa automáticamente.

- En el cuadro de diálogo **Consumir**, en Agents, seleccione los equipos en los que desea consumir datos.

- Haga clic en **Consumir**.

- Para supervisar el progreso del consumo de datos, vea la página  Eventos.

Abandono de una unidad de inicialización

Si crea una unidad de inicialización con la intención de consumirla en el Core de destino, pero más tarde opta por no consumirla, puede abandonar la unidad de inicialización.

Hasta que abandona la unidad de inicialización o la consume, un vínculo a dicha unidad de inicialización pendiente permanecerá en el panel Replicación saliente en el Core de origen.

Hasta que transmita información de la unidad de inicialización, los puntos de recuperación huérfanos (que existen en el equipo protegido original, pero no en el Core de destino) no se pueden utilizar para restaurar los datos.

⚠ PRECAUCIÓN: Si abandona la unidad de inicialización, los puntos de recuperación originales (definidos en el archivo de la unidad de inicialización) se transmiten por la red hasta el Core de destino durante el siguiente trabajo de replicación. La transmisión de los puntos de recuperación antiguos a través de la red podría ralentizar la red considerablemente, sobre todo si hay muchos puntos de recuperación.

Complete los pasos del procedimiento siguiente para abandonar una unidad de inicialización pendiente.

NOTA: El abandono de la unidad de inicialización en la Core Console no afecta al archivo de la unidad de inicialización desde su ubicación de almacenamiento.

- 1 En el Core de origen, abra la Core Console de Rapid Recovery y, desde la barra de iconos, haga clic en  (Replicación). Aparece la página **Replicación**.
- 2 En la página **Replicación**, en el panel Replicación saliente, haga clic en **Unidades de inicialización (#)**.
En el panel Replicación saliente, una sección aparece con información acerca de las unidades de inicialización pendientes.
- 3 De manera opcional, también puede hacer clic en la flecha hacia abajo ▼ para expandir el menú contraíble.
Aparecerá la información acerca de las unidades de inicialización pendientes, incluido el Core de destino y el rango de fechas de los puntos de recuperación incluidos en la unidad de inicialización.
- 4 Haga clic en  para abrir el menú desplegable del archivo de la unidad de inicialización que desea abandonar y elija **Abandonar**.
- 5 En la ventana de confirmación, confirme que desea abandonar la unidad de inicialización.
Se quita la unidad de inicialización.

Si no existen más unidades de inicialización en el Core de origen, el enlace Unidades de inicialización (#) y la sección del mismo nombre se quitan del panel Replicación saliente.

Administración de configuraciones de replicación

Rapid Recovery le permite monitorizar, programar y ajustar la replicación en los niveles general, de Core y de equipo protegido.

Puede editar la siguiente configuración de replicación:

- Para configurar los siguientes trabajos de replicación, consulte [Programación de la replicación](#).
- Para crear una unidad de inicialización de un equipo protegido que ya está emparejado para la replicación, consulte [Uso de la función de copia para crear una unidad de inicialización](#).
- Para supervisar el progreso de un trabajo de replicación, consulte [Visualización de la replicación entrante y saliente](#).
- Para pausar o reanudar un trabajo de replicación, consulte [Pausa y reanudación de la replicación](#).
- Para forzar la replicación de un equipo protegido saliente o entrante, consulte [Forzado de la replicación](#).
- Para administrar la configuración de todos los Cores de destino y los procedimientos de replicación, consulte [Administración de configuración para la replicación saliente](#).
- Para administrar la configuración de un Core de destino individual, consulte [Cambio de la configuración del Core de destino](#).
- Para administrar la configuración de prioridad para un equipo protegido en concreto replicado en un Core de destino, consulte [Cómo establecer la prioridad de replicación para un equipo protegido](#).

Programación de la replicación

A menos que cambie el comportamiento predeterminado al configurar una programación de replicación, el Core debe iniciar un trabajo de replicación inmediatamente después de la finalización de cada copia de seguridad de la instantánea, comprobación de suma de comprobación, comprobación de capacidad de conexión y los trabajos nocturnos. Para obtener más información, consulte [Programación de la replicación](#).

Puede realizar cambios en el calendario de programación de replicación para reducir la carga de la red.

Complete los pasos del procedimiento siguiente para establecer un calendario de programación de replicación para cualquier equipo replicado.

- 1 En el Core de destino, abra la Core Console de Rapid Recovery y, desde la barra de iconos, haga clic en  (Replicación).

Aparece la página **Replicación**.

- 2 En el panel Replicación saliente, haga clic en  para abrir el menú desplegable junto al Core para que desee establecer la programación de replicación y haga clic en **Calendario de programación**.
Se abrirá el cuadro de diálogo **Calendario de programación de replicación de [NombreCore]**.
- 3 Seleccione una de las tres opciones siguientes:
 - **En todo momento**. Se replica después de cada nueva instantánea, de la comprobación de suma de comprobación y de la comprobación de conectabilidad y después de que se completen los trabajos nocturnos.
 - **Diario (solo inicia la replicación durante el periodo de tiempo especificado)**. Comienza a replicar únicamente durante el rango de tiempo proporcionado.
 - 1 En el cuadro de texto **Desde**, introduzca la hora más reciente en la que se puede producir la replicación.
 - 2 En el cuadro de texto **Hasta**, introduzca la hora más tardía en la que se puede producir la replicación.
 - **Personalizado**. La replicación solo se inicia en el intervalo de tiempo proporcionado, lo que le permite establecer un intervalo de tiempo para los días laborables y otro para los fines de semana.
 - 1 Junto a Días de la semana, en el cuadro de texto **Desde**, introduzca la hora más reciente en la que se puede realizar la replicación entre semana y, a continuación, en el cuadro de texto **Hasta**, introduzca la hora más tardía en la que se puede realizar la replicación entre semana.
 - 2 Junto a Días de la semana, en el cuadro de texto **Desde**, introduzca la hora más reciente en la que se debe producir la replicación durante los fines de semana; a continuación, en el cuadro de texto **Hasta**, introduzca la hora más tardía en la que se debe producir la replicación durante los fines de semana.
- 4 Haga clic en **Guardar**.
El calendario de programación se aplica a todas las replicaciones del Core de destino seleccionado.

 **NOTA:** Si la replicación está en curso cuando termine el tiempo programado, el trabajo de replicación se completará tras el periodo de tiempo asignado.

Uso de la función de copia para crear una unidad de inicialización

Si seleccionó no crear una unidad de inicialización cuando configuró la replicación, puede crear una unidad de inicialización utilizando la función de copia en el menú desplegable del equipo protegido.

- 1 En el Core de origen, abra la Core Console de Rapid Recovery y, desde la barra de iconos, haga clic en  (Replicación).
Aparece la página **Replicación**.
- 2 En la página **Replicación**, en el panel Replicación saliente, haga clic en  para expandir el Core que protege el equipo para el que desea crear una unidad de inicialización.
La selección se expande para mostrar cada equipo protegido especificado en el Core.
- 3 Haga clic en la primera fila de la tabla para seleccionar cada una de las máquinas para las que desea crear una unidad de inicialización.
- 4 En el menú del panel Replicación saliente, haga clic en **Copiar**.
Aparece el **Asistente para replicación**.
- 5 En la página **Ubicación de unidad de inicialización** del asistente, utilice la lista desplegable **Ubicación** para seleccionar los siguientes tipos de destino:
 - Local
 - Red
 - Nube
- 6 Introduzca los detalles para el archivo comprimido de la unidad de inicialización según se describen en la tabla siguiente en función del tipo de ubicación que haya seleccionado en el paso anterior.

Tabla 142. Detalles de archivación

Opción	Cuadro de texto	Descripción
Local	Ubicación de salida	Escriba la ubicación de la salida. Se utiliza para definir la ruta de acceso de la ubicación en la que desea que resida el archivo; por ejemplo, d:\trabajo\archivación.
Red	Ubicación de salida	Escriba la ubicación de la salida. Se utiliza para definir la ruta de acceso de la ubicación en la que desea que resida el archivo; por ejemplo, \\nombreservidor\nombrerecursocompartido.
	Nombre de usuario	Escriba un nombre de usuario. Se utiliza para establecer las credenciales de inicio de la sesión del recurso compartido de red.
	Contraseña	Escriba una contraseña para la ruta de acceso de red. Se utiliza para establecer las credenciales de inicio de la sesión del recurso compartido de red.
Nube	Cuenta	Seleccione una cuenta de la lista desplegable.
		NOTA: Para seleccionar una cuenta de nube, debe añadirla primero en Core Console. Para obtener más información, consulte Incorporación de una cuenta de nube .
	Contenedor	Seleccione un contenedor asociado con su cuenta en el menú desplegable.
	Nombre de la carpeta	Introduzca un nombre para la carpeta en la que hay que guardar los datos archivados. El nombre predeterminado es Rapid-Recovery-Archive-[FECHA CREACIÓN]-[HORA CREACIÓN]

7 Haga clic en **Siguiente**.

8 En la página Opciones de unidad de inicialización, introduzca la información según lo descrito en la siguiente tabla.

Tabla 143. Opciones de la unidad de inicialización

Elemento	Descripción
Tamaño máximo	Los grandes archivos de datos se pueden dividir en varios segmentos. Seleccione el tamaño máximo de espacio que desea reservar para crear la unidad de inicialización realizando una de las siguientes acciones: • Seleccione Todo el destino para reservar todo el espacio disponible en la ruta de acceso proporcionada en la página Ubicación de unidad de inicialización (por ejemplo, si la ubicación es D:\trabajo\archivo, se reserva todo el espacio disponible en la unidad D:). • Seleccione el cuadro de texto en blanco, introduzca una cantidad y, a continuación, seleccione una unidad de medida en la lista desplegable para personalizar el espacio que desea reservar.
Acción de reciclaje	En el caso de que la ruta de acceso ya contenga una unidad de inicialización, seleccione una de las opciones siguientes: • No reutilizar. No sobrescribe ni borra datos de inicialización existentes de la ubicación. Si la ubicación no está vacía, la escritura en la unidad de inicialización fallará. • Reemplazar este Core. Sobrescribe los datos de inicialización que ya existan y que pertenezcan a este Core, pero deja intactos los datos del resto de Cores. • Borrar completamente. Borra todos los datos de inicialización del directorio antes de escribir en la unidad de inicialización.
Comentario	Introduzca un comentario que describa la unidad de inicialización.
Agregar todos los Agents a la unidad de inicialización	Seleccione esta opción para replicar todos los equipos protegidos en el Core de origen usando la unidad de inicialización. Esta opción se selecciona de forma predeterminada.
Crear cadenas de puntos de	Seleccione esta opción para replicar toda la cadena de puntos de recuperación en la unidad de inicialización. Esta opción se selecciona de forma predeterminada.

Elemento	Descripción
recuperación (reparar huérfanos)	NOTA: La inicialización típica de Rapid Recovery 5.4 solo replicaba el último punto de recuperación en la unidad de inicialización, lo que reducía la cantidad de tiempo y espacio necesarios para crear la unidad de inicialización. La opción para crear las cadenas del punto de recuperación en la unidad de inicialización necesita suficiente espacio en la unidad de inicialización como para almacenar los últimos puntos de recuperación desde los equipos protegidos especificados y puede llevar más tiempo.
9	Realice una de las siguientes acciones: - Si ha desactivado la casilla de verificación Agregar todos los Agents a la unidad de inicialización, haga clic en Siguiente. - Si ha seleccionado Agregar todos los Agents a la unidad de inicialización, vaya al Paso 10.
10	En la página Equipos protegidos del asistente, seleccione los equipos protegidos para los que desea crear una unidad de inicialización.
11	Haga clic en Finalizar .

Supervisión de la replicación

Cuando la replicación está configurada, puede supervisar el estado de las tareas de replicación para los Cores de origen y destino. Puede actualizar la información de estado, ver los detalles de replicación, etc.

- En el Core de origen, abra la Core Console de Rapid Recovery y, desde la barra de iconos, haga clic en  (Replicación). Aparece la página **Replicación**.
- En esta página, puede ver información y supervisar el estado de las tareas de replicación según se describen en la tabla siguiente.

Tabla 144. Tareas de replicación

Sección	Descripción	Acciones disponibles
Unidades de inicialización (#)	Después de especificar el uso de una unidad de inicialización al definir la replicación, hasta que la abandone o consuma, el vínculo Unidades de inicialización (#) aparecerá en el panel Replicación saliente en el Core de origen. El número que se muestra indica cuántas unidades de inicialización están pendientes. NOTA: Este vínculo no aparecerá a menos que haya una unidad de inicialización pendiente. Haga clic en este vínculo para enumerar las unidades de inicialización que se han escrito pero aún no han sido consumidas por el Core de destino. Expandir aún más el menú contraíble para mostrar la información acerca de las unidades de inicialización pendientes, incluido el Core de destino y el rango de fechas de los puntos de recuperación incluidos en la unidad de inicialización.	En el menú desplegable, haga clic en Abandonar para abandonar o cancelar el proceso de inicialización. Menú wn
Replicación saliente	Enumera todos los Cores de destino en los que el Core de origen se está replicando. Incluye el nombre de indicador de estado, el nombre del Core de destino, el número de equipos que se replican y el progreso de una transmisión de replicación.	En un Core de origen, en el menú desplegable , puede seleccionar las opciones siguientes: Detalles: muestra Id., URL, nombre para mostrar, estado, Id. de cliente, dirección de correo electrónico y comentarios del Core replicado. Cambiar configuración. Enumera el nombre mostrado y le permite editar el host y puerto para el Core de destino.

Sección	Descripción	Acciones disponibles
		• Calendario de programación. Le permite establecer un calendario de programación personalizado para la replicación en este Core de destino. • Agregar equipos. Le permite elegir un host de una lista desplegable, seleccionar equipos protegidos para replicación y crear una unidad de inicialización para la transferencia inicial del equipo protegido nuevo. Opcionalmente, puede elegir incluir los puntos de recuperación para los equipos de recuperación que ya ha agregado a la replicación. • Eliminar. Permite eliminar la relación de replicación entre los Cores de origen y destino. Si lo hace, cesa cualquier replicación en este Core.
Replicación entrante	Lista todos los equipos de origen desde los que el destino recibe datos replicados. Incluye el nombre, estado, equipos y progreso del Core remoto. Lista todos los Cores de origen desde los que el destino recibe datos replicados. El nombre de visualización para los Cores de origen que se enumeran se ocupan desde el valor en el Asistente para replicación al definir la replicación. Incluye el nombre de indicador de estado, el nombre del Core remoto y el progreso de una transmisión de replicación.	En un Core de destino, en el menú desplegable , puede seleccionar las opciones siguientes: • Detalles. Enumera la Id., nombre de host, Id. de cliente, dirección de correo electrónico y comentarios para el Core replicado. • Consumir. Consume los datos iniciales de la unidad de inicialización y los guarda en el repositorio local. • Eliminar. Permite eliminar la relación de replicación entre los Cores de destino y origen. Si lo hace, cesa cualquier replicación de este Core.
Solicitudes de replicación pendientes	Esta información se aplica a los proveedores de servicios administrados solamente. Cuando un cliente hace clic en el vínculo Solicitudes en el panel Replicación entrante, la sección de una tabla de resumen aparece con una clasificación de los Id. de cliente, la dirección de correo electrónico y el nombre de host para la solicitud.	En el menú desplegable, haga clic en Ignorar para ignorar o rechazar la solicitud, o Revisar para revisar la solicitud pendiente.

Pausa y reanudación de la replicación

Puede realizar una pausa en la replicación de forma temporal para los Cores de origen (salida) o destino (entrada).

La opción para pausar la replicación solo está disponible si la replicación está activa. La opción para reanudar la replicación solo está disponible si la replicación está en pausa.

Realice los pasos del procedimiento siguiente para pausar o reanudar la replicación.

- 1 Abra la Core Console de Rapid Recovery, y en la barra de iconos, haga clic en  (Replicación). Aparece la página **Replicación**.
- 2 Para pausar la replicación en todos los equipos replicados, haga lo siguiente:
 - a Haga clic en la casilla de verificación en la parte superior de la tabla de resumen para seleccionar el Core de origen y de destino.
 - b Haga clic en **Pausar** en el menú anterior a la tabla de resumen.

La replicación de todos los equipos protegidos en el Core seleccionado está en pausa.
- 3 Para pausar la replicación de algunos equipos, haga lo siguiente:
 - a Haga clic en la flecha ▼ situada a la derecha de cualquier Core.

La vista se expande para mostrar cada uno de los equipos protegidos del Core que se han replicado en el Core seleccionado.

- b Haga clic en la primera columna para seleccionar cada máquina para la que desea pausar la replicación. Haga clic de nuevo en cualquier selección para borrar la casilla de verificación de los equipos que no desea pausar.
- c Haga clic en **Pausar** en el menú anterior a la tabla de resumen.
La replicación para los equipos protegidos seleccionados está en pausa.
- 4 Para reanudar la replicación en todos los equipos replicados, haga lo siguiente:
 - a Haga clic en la casilla de verificación en la parte superior de la tabla de resumen para seleccionar el Core de origen y de destino.
 - b Haga clic en **Reanudar** desde el menú de la parte superior de la tabla de resumen.
La replicación de todos los equipos protegidos en el Core seleccionado se reanuda.
- 5 Para reanudar la replicación de algunos equipos, haga lo siguiente:
 - a Haga clic en la flecha ▼ situada a la derecha de cualquier Core.
La vista se expande para mostrar cada uno de los equipos protegidos del Core que se han replicado en el Core seleccionado.
 - b Haga clic en la primera columna para seleccionar cada máquina para la que desea reanudar la replicación. Haga clic de nuevo en cualquier selección para borrar la casilla de verificación de los equipos que no desea reanudar.
 - c Haga clic en **Reanudar** desde el menú de la parte superior de la tabla de resumen.
Se reanuda la replicación para los equipos protegidos seleccionados.

Forzado de la replicación

Desde el Core de origen, puede forzar la replicación en cualquier momento, en lugar de esperar que un trabajo de replicación haga cola después de un evento específico, como una copia de seguridad o comprobación de capacidad de conexión.

Complete los pasos del siguiente procedimiento para forzar la replicación en el Core de origen o de destino.

- 1 En el Core de origen, abra la Core Console de Rapid Recovery y, desde la barra de iconos, haga clic en  (Replicación).
Aparece la página **Replicación**.
- 2 Realice una de las siguientes acciones:
 - Para forzar la replicación en un Core de origen, desde el panel **Replicación saliente**, seleccione un Core y desde el menú de la parte superior de la tabla de resumen, haga clic en  **Forzar**.
 - Para forzar la replicación en un Core de destino, desde el panel **Replicación entrante**, seleccione un Core y desde el menú de la parte superior de la tabla de resumen, haga clic en  **Forzar**.
Se abre el cuadro de diálogo Forzar replicación.
- 3 De manera opcional, si desea reparar cualquier de las cadenas huérfanas de los puntos de recuperación, seleccione **Restaurar cadenas de punto de recuperación huérfanas**.
- 4 Para confirmarlo, en el cuadro de diálogo Forzar la replicación, haga clic en **Sí**.
El cuadro de diálogo se cierra y la replicación se fuerza.

Administración de configuración para la replicación saliente

Los cambios realizados en esta configuración afectan a la transferencia de datos a todos los Cores de destino asociados con este Core de origen.

- 1 En el Core de origen, abra la Core Console de Rapid Recovery y, desde la barra de iconos, haga clic en  (Replicación).
Aparece la página **Replicación**.
- 2 En el panel **Replicación saliente**, en la parte superior de la tabla de resumen, haga clic en  (Configuración).
Se muestra el cuadro de diálogo **Configuración de replicación**.

- 3 En el cuadro de diálogo **Configuración de replicación**, edite la configuración de replicación según se describe en la tabla siguiente.

Tabla 145. Configuración de replicación

Opción	Descripción
Duración de la caché (segundos)	Especifica el tiempo entre las solicitudes de estado de Core de destino realizadas por el Core de origen.
Tiempo de espera de la sesión de imagen del volumen (minutos)	Especifica el tiempo que el Core de origen tarda en intentar transferir una imagen de volumen al Core de destino.
Número máximo de secuencias paralelas	Especifica el número de conexiones de red permitidas para su uso por parte de un equipo protegido único para la replicación de los datos de dicho equipo de una vez.
Velocidad máxima de transferencia (MB/s)	Especifique el límite de velocidad para la transferencia de los datos replicados.
Tamaño máximo de datos de transferencia (GB)	Especifique el tamaño máximo en GB para transferir los bloques de datos replicados.
Restore Defaults	Seleccione esta opción para cambiar toda la configuración de replicación a los valores predeterminados del sistema.

 **NOTA:** Tome nota de cualquier configuración personalizada antes de seleccionar esta opción. No se le solicitará que confirme esta acción

- 4 Cuando esté satisfecho, haga clic en **Guardar** para guardar la configuración de replicación y cerrar el cuadro de diálogo.

Cambio de la configuración del Core de destino

Puede cambiar el host y la configuración de puertos en Cores de destino individuales desde el Core de origen.

- 1 En el Core de origen, abra la Core Console de Rapid Recovery y, desde la barra de iconos, haga clic en  (Replicación). Aparece la página **Replicación**.

En el panel **Replicación saliente**, la tabla de resumen incluye una fila para cada Core de destino que se ha configurado para replicar puntos de recuperación desde este Core de origen.

- 2 Haga clic en la flecha  (Configuración) en el Core de destino que desea modificar y, a continuación, seleccione **Cambiar configuración**.

Aparecerá el cuadro de diálogo **Settings (Configuración)**.

- 3 Edite cualquiera de las opciones que se describen en la siguiente tabla.

Tabla 146. Configuración del Core de destino

Opción	Descripción
Host	Introduzca el host para el Core de destino.
Puerto	Introduzca un puerto para que el Core de destino lo utilice para la comunicación con el Core de origen.

 **NOTA:** El puerto predeterminado es 8006.

- 4 Haga clic en **Guardar**.

Cómo establecer la prioridad de replicación para un equipo protegido

La prioridad de replicación determina qué trabajos de replicación se envían en primer lugar al Core. La priorización se establece de manera ordinal, en una escala del 1 al 10, donde 1 es la primera prioridad y 10 la última. La primera vez que establezca la replicación de cualquier equipo, la prioridad se establece en 5. Puede ver y cambiar la prioridad en el nivel de equipo protegido del Core de origen.

En algunos casos, es posible que se abandonen algunos trabajos de replicación. Por ejemplo, los trabajos de replicación pueden abandonarse si el entorno está experimentando altas velocidades de cambios de manera excepcional o si la red no tiene suficiente ancho de banda. Es probable que se produzca esta situación si establece calendarios de programación que limitan las horas al realizarse la replicación en su entorno. Para obtener más información acerca de la configuración de la replicación de calendarios de programación, consulte [Programación de la replicación](#).

Para garantizar la realización de la replicación de los equipos importantes primero, establezca una prioridad con un número bajo (entre 1 y 5) en los servidores críticos. Establezca una prioridad con un número alto (entre 6 y 10) en los equipos menos importantes.

La configuración del valor de prioridad de replicación de número 4 de cualquier equipo protegido garantiza que el trabajo de replicación se inicie antes que en un equipo con el valor de la prioridad de replicación predeterminada de 5. Los trabajos de replicación de equipos con un valor de prioridad de 3 se ponen en cola antes de los de 4 y así sucesivamente. Cuanto menor es el número de prioridad, antes se envían los trabajos de replicación. Es fácil de recordar que la prioridad 1 es la más importante. Los equipos con una prioridad de replicación de 1 se encuentran los primeros en la cola de replicación.

Complete los pasos siguientes para editar la configuración que será prioridad cuando un equipo protegido se replique.

- 1 En el Core de origen, abra la Core Console de Rapid Recovery y, desde la barra de iconos, haga clic en  (Replicación). Aparece la página **Replicación**.
- 2 En el panel **Replicación saliente**, haga clic en la flecha ▼ a la derecha de cualquier Core de origen. La vista se expande para mostrar cada uno de los equipos protegidos del Core de destino que se han replicado en el Core de destino designado.
- 3 Haga clic en el menú desplegable  (Configuración) en el equipo protegido al que quiere dar prioridad y, a continuación, haga clic en **Configuración**. Se muestra un cuadro de diálogo.
- 4 Haga clic en la lista desplegable **Prioridad** y seleccione la prioridad, desde **1 (más alto)** a **10 (más bajo)**, en función de sus necesidades.
- 5 Haga clic en **Guardar**. Se cerrará el cuadro de diálogo y la prioridad de replicación de las actualizaciones de los equipos seleccionados.

Eliminación de replicación

La replicación es la duplicación intencional de puntos de recuperación para un equipo protegido de un Core de Rapid Recovery (el Core de origen) a un segundo Core (el destino).

El objetivo de la replicación es mantener una alta disponibilidad de duplicación de datos para el equipo protegido original. Para lograr una seguridad de datos óptima, Dell recomienda la ubicación de la Core de destino en una ubicación geográfica independiente.

A menos que cambie el comportamiento predeterminado al configurar una programación de replicación, el Core debe iniciar un trabajo de replicación inmediatamente después de la finalización de cada copia de seguridad de la instantánea, comprobación de suma de comprobación, comprobación de capacidad de conexión y los trabajos nocturnos. Para obtener más información, consulte [Programación de la replicación](#).

Al eliminar la replicación, interrumpe la copia de puntos de recuperación adicionales desde el origen al Core de destino. La eliminación de la replicación nunca afecta a los datos guardados en el Core original (de origen).

Además, al quitar la replicación, tiene la opción de dejar los puntos de recuperación replicados del equipo original en el Core de destino o de eliminarlos. Si mantiene los puntos de recuperación de un equipo replicado que ha quitado, los puntos de recuperación de ese equipo, a su vez, se representa en el Core como un equipo con puntos de recuperación únicamente. Puede examinar los datos de los puntos de recuperación retenidos o restaurar los archivos en el nivel de archivo, mientras que persisten en el Core de destino.

Puede quitar la replicación mediante cualquiera de las siguientes aproximaciones:

- [Eliminar la replicación saliente del Core de inicio](#)
- [Eliminar la replicación entrante del Core de destino](#)

Eliminar la replicación saliente del Core de inicio

Complete los pasos de este procedimiento para eliminar uno o más equipos protegidos de la replicación en el Core de inicio.

- 1 En el Core de origen, abra la Core Console de Rapid Recovery y, desde la barra de iconos, haga clic en  (Replicación). Aparece la página **Replicación**.

En el panel **Replicación saliente**, la tabla de resumen incluye una fila para cada Core de destino que se ha configurado para replicar puntos de recuperación desde este Core de origen.

De manera opcional, también puede hacer clic en la flecha ▼ situada a la derecha de cualquier Core de destino. La vista se expande para mostrar cada uno de los equipos protegidos del Core de destino que se han replicado en el Core de destino designado.
- 3 Seleccione los equipos protegidos que desea eliminar de replicación saliente como se indica a continuación:
 - Para quitar completamente la relación de replicación existente entre este Core de origen y cualquier Core de destino, haga clic en el menú desplegable  (Configuración) para cualquier Core de destino y, a continuación, seleccione **Eliminar**.
 - Para eliminar replicación saliente de un subconjunto de equipos en el Core de destino especificado, amplíe la vista para mostrar todas las máquinas que se están replicando, y seleccione la casilla de verificación para cada equipo replicado que desea quitar. Borre la casilla de verificación de cualquier equipo que desee continuar replicando. A continuación, desde el menú anterior a la tabla de resumen, haga clic en  **Eliminar**.

Aparecerá un mensaje de confirmación que le preguntará si desea quitar las relaciones de replicación.
- 4 En el cuadro de diálogo resultante, haga clic en **Sí** para confirmar la eliminación.

Eliminar la replicación entrante del Core de destino

Complete los pasos de este procedimiento para eliminar uno o más equipos protegidos de la replicación en el Core de destino.

NOTA: También puede eliminar la replicación de equipos protegidos del panel **Replicación saliente** en la página **Replicación del Core de origen**. Para obtener más información, consulte [Eliminar la replicación saliente del Core de inicio](#)

- 1 En el Core de destino, abra la Core Console de Rapid Recovery y, desde la barra de iconos, haga clic en  (Replicación). Aparece la página **Replicación**. En el panel **Replicación entrante**, la tabla de resumen incluye una fila para cada Core de origen con los equipos protegidos que replica ese Core de destino.
- 2 Seleccione los equipos replicados para eliminarlos de la siguiente manera:
 - Para eliminar todos los equipos replicados del Core de origen al Core de destino, en el panel **Replicación entrante**, seleccione la casilla de verificación de ese Core.
 - Para eliminar un subconjunto más pequeño de equipos del mismo Core de origen, haga lo siguiente:

- a Haga clic en la flecha ▼ situada a la derecha del Core de origen.
La vista se expande para mostrar cada uno de los equipos del Core de origen que se han replicado en el Core de destino.
- b Seleccione la casilla de verificación de cada equipo replicado que desea quitar.
- c Desde la fila principal del Core de origen seleccionado, haga clic en el menú desplegable  (Configuración) y, a continuación, seleccione **Eliminar**.

Se abre el cuadro de diálogo **Quitar replicación**.

- 3 En el cuadro de diálogo **Quitar replicación**, haga lo siguiente:
 - Si desea dejar los puntos de recuperación replicados en el Core de destino, desmarque la opción **Eliminar puntos de recuperación existentes**.
 - Si desea eliminar todos los puntos de recuperación replicados recibidos de ese equipo, así como quitar el Core de origen de la replicación, seleccione **Eliminar puntos de recuperación existentes**.
- 4 Haga clic en **Sí** para confirmar la eliminación.

 **AVISO:** Si selecciona esta opción, se eliminarán todos los puntos de recuperación replicados en este Core.

Los equipos protegidos seleccionados en el Core de origen se eliminan de la replicación en este Core de destino. De manera opcional, si ha seleccionado la opción para los eliminar puntos de recuperación, se eliminan del repositorio de este Core.

Recuperación de datos replicados

La funcionalidad de replicación Día a día se mantiene en el Core de origen, mientras que solo el Core de destino es capaz de completar las funciones necesarias para la recuperación tras desastre.

Para la recuperación de desastres, el Core de destino puede utilizar los puntos de recuperación replicados para recuperar los equipos protegidos. Puede realizar las opciones de recuperación siguientes desde el Core de destino:

- **Puntos de recuperación de montaje.** Para obtener más información, consulte [Montaje de un punto de recuperación](#).
- **Revertir a puntos de recuperación.** Para obtener más información, consulte [Restauración de volúmenes desde un punto de recuperación](#) o [Restauración de volúmenes para un equipo Linux mediante la línea de comandos](#).
- **Realizar una exportación de máquina virtual (VM).** Para obtener más información, consulte [Información sobre la exportación a máquinas virtuales con Rapid Recovery](#).
- **Realizar una bare metal restore (BMR).** Para obtener más información, consulte [Restauración Bare Metal Restore en máquinas Windows](#).

Datos de recuperación

Administración de la recuperación

El Core de Rapid Recovery puede restaurar datos o recuperar máquinas en máquinas físicas o virtuales instantáneamente desde puntos de recuperación. Los puntos de recuperación contienen instantáneas de volúmenes de Agent capturadas a nivel de bloque. Estas instantáneas son sensibles a las aplicaciones, lo que implica que se completen todas las transacciones abiertas y registros de transacciones en movimiento y que las cachés se despejen a disco antes de crear la instantánea. El uso de instantáneas sensibles a las aplicaciones junto con Verified Recovery permite al Core realizar varios tipos de recuperaciones, que pueden ser:

- Recuperación de archivos y carpetas
- Recuperación de volúmenes de datos, mediante Live Recovery
- Recuperación de volúmenes de datos para Microsoft Exchange Server y Microsoft SQL Server, mediante Live Recovery
- Restauración desde cero, mediante Universal Recovery
- Recuperación desde cero de hardware diferente, mediante Universal Recovery
- Exportación ad-hoc y continua a máquinas virtuales

Instantáneas y puntos de recuperación

En esta sección se describe cómo utilizar y administrar las instantáneas y los puntos de recuperación generados mediante Rapid Recovery. Incluye información acerca del montaje, la visualización y el forzado, así como la migración y la eliminación de puntos de recuperación.

Administración de instantáneas y puntos de recuperación

Un punto de recuperación es un conjunto de instantáneas tomadas de volúmenes de discos individuales y almacenadas en el repositorio. Las instantáneas capturan y almacenan el estado de un volumen de disco en un punto determinado del tiempo mientras que las aplicaciones que generan los datos siguen utilizándose. En Rapid Recovery, puede forzar una instantánea, pausar temporalmente instantáneas y ver listas de puntos de recuperación actuales en el repositorio, así como eliminarlos si es necesario. Los puntos de recuperación se utilizan para restaurar equipos protegidos o para montar en un sistema de archivo local.

Las instantáneas que captura Rapid Recovery se realizan en el nivel del bloque y ofrecen reconocimiento de la aplicación. Esto significa que todos los registros de transacciones abiertas y transacciones en marcha se completan y que las memorias caché se vacían antes de crear la instantánea.

Rapid Recovery utiliza un controlador de filtro de volúmenes de bajo nivel que se adjunta a los volúmenes montados y, a continuación, realiza el seguimiento de todos los cambios de nivel de bloque para la próxima instantánea inminente. Los Microsoft Volume Shadow Services (VSS) (Servicios de instantáneas de volumen de Microsoft) se utilizan para facilitar instantáneas de la aplicación en estado coherente tras la interrupción.

Visualización de la página de puntos de recuperación de un equipo protegido

Realice los pasos del procedimiento siguiente para ver la lista completa de los puntos de recuperación para un equipo protegido.

NOTA: Si está protegiendo datos desde un clúster de servidor DAG o CCR, los puntos de recuperación asociados no aparecen a nivel de clúster. Sólo están visibles a nivel de nodo o de equipo.

- 1 En la Core Console de Rapid Recovery, desplácese hasta el equipo protegido cuyos puntos de recuperación desee visualizar.
- 2 En el menú de la parte superior de la página, haga clic en **Puntos de recuperación**.
Aparece la página Puntos de recuperación que muestra un panel de resumen los puntos de recuperación y un panel de puntos de recuperación.

Puede ver la información resumida sobre los puntos de recuperación del equipo como se describe en la tabla siguiente.

Tabla 147. Resumen de la información de punto de recuperación

Información	Descripción
Total de puntos de recuperación	Muestra el número total de puntos de recuperación guardados en el repositorio para este equipo.
Total de datos protegidos	Indica la cantidad de espacio de almacenamiento utilizado en el repositorio para estos puntos de recuperación.
Repositorio DVM	Muestra el nombre del repositorio en el que se almacenan estos puntos de recuperación.
Estado del repositorio DVM	Muestra de manera gráfica la cantidad de espacio consumido por los puntos de recuperación. Muestra el porcentaje del repositorio que se usa, la cantidad de espacio, y el espacio total del repositorio. Haga clic en el gráfico para ver la cantidad de espacio restante.

Puede ver la información sobre los puntos de recuperación del equipo como se describe en la tabla siguiente.

Tabla 148. Información de punto de recuperación

Información	Descripción
Icono	Representación gráfica de un punto de recuperación  o, si se expande, un volumen en el punto de recuperación  . Los puntos de recuperación muestran una flecha derecha  que indica que se puede ampliar el detalle.
Cifrado	Indica si el punto de recuperación está cifrado.
Estado	Indica el estado actual del punto de recuperación.
Contenido	Lista los volúmenes incluidos en el punto de recuperación. Haga clic en  (Información) para ver el uso del espacio y el sistema de archivos.
Tipo	Define un punto de recuperación como una imagen base o una instantánea incremental (diferencial).
Fecha de creación	Muestra la fecha de creación del punto de recuperación.
Tamaño	Muestra la cantidad de espacio que el punto de recuperación consume en el repositorio.
	El menú desplegable Configuración le permite realizar ciertas funciones para el punto de recuperación seleccionado.

- 3 De manera opcional, expanda un punto de recuperación para ver los volúmenes protegidos.

Vínculos relacionados

[Visualización de los puntos de recuperación para un equipo](#)

Comprensión de los indicadores de estado de puntos de recuperación

Una vez que se obtiene un punto de recuperación para un Exchange Server o SQL Server protegido, la aplicación muestra un indicador de estado en color correspondiente en la tabla Puntos de recuperación. Esta tabla aparece en el panel **Puntos de recuperación** cuando se visualizan los puntos de recuperación de un equipo determinado. El color que muestra se basa en la configuración de comprobación del equipo protegido y en el éxito o fallo de esas comprobaciones, como se describe en las tablas siguientes.

NOTA: Para obtener más información sobre la visualización de los puntos de recuperación, consulte [Visualización de la página de puntos de recuperación de un equipo protegido](#).

Colores de punto de estado de recuperación para bases de datos Exchange

En la siguiente tabla aparece una lista de los indicadores de estado que se muestran para las bases de datos Exchange.

Tabla 149. Indicadores de estado de bases de datos Exchange

Color de estado	Descripción
Blanco	Indica que no se detecta una base de datos de Exchange dentro del punto de recuperación, volumen o grupo de volúmenes.
Amarillo	Indica que las comprobaciones de capacidad de montaje de base de datos de Exchange aún no se han ejecutado.
Rojo	Indica que las comprobaciones de capacidad de montaje o de suma de comprobación han sido erróneas en al menos una base de datos.
Verde	Indica que el punto de recuperación contiene una o varias bases de datos, que las comprobaciones de capacidad están activadas y que la comprobación de capacidad o la comprobación de la suma de comprobación fueron correctas.

Colores de punto de estado de recuperación para bases de datos SQL

En la siguiente tabla aparece una lista de los indicadores de estado que se muestran para las bases de datos SQL.

Tabla 150. Indicadores de estado de bases de datos SQL

Color de estado	Descripción
Blanco	Indica que no se detecta una base de datos de SQL dentro del punto de recuperación, volumen o grupo de volúmenes.
Amarillo	La base de datos de SQL estaba fuera de línea, indicando que no fueron posibles las comprobaciones de conectabilidad y no se han ejecutado.
Rojo	Indica que la comprobación de conectabilidad ha fallado o que la base de datos de SQL está sin conexión.
Verde	Indica que la comprobación de conectabilidad ha sido correcta.

NOTA: Los puntos de recuperación que no tienen una base de datos de SQL o Exchange asociadas aparecen con un indicador de estado en blanco. En las situaciones en las que existan tanto base de datos de Exchange como SQL para el punto de recuperación, se mostrarán los indicadores de estado más graves para el punto de recuperación.

Montaje de un punto de recuperación

En Rapid Recovery puede montar un punto de recuperación para una máquina Windows para acceder a los datos almacenados a través de un sistema de archivos local.

NOTA: Para montar un punto de recuperación de Linux con la utilidad `local_mount`, consulte [Montaje de un volumen de punto de recuperación en un equipo Linux](#).

NOTA: Al montar puntos de recuperación desde datos restaurados desde un equipo que tiene activada la deduplicación de datos, deberá activar también la deduplicación en el servidor de Core.

- 1 En la Core Console de Rapid Recovery, desplácese hasta el equipo que quiera montar en un sistema de archivos local. Aparece la página **Resumen** del equipo protegido seleccionado.
- 2 Haga clic en el menú **Puntos de recuperación**. Aparecerá la página **Puntos de recuperación** del equipo seleccionado.
- 3 De manera opcional, en el panel **Puntos de recuperación**, en la lista de puntos de recuperación, haga clic en el símbolo de la flecha derecha ▶ para expandir los detalles del punto de recuperación y ver los volúmenes que incluye.
- 4 En la fila del punto de recuperación que desee montar, haga clic en  y en el menú desplegable, seleccione **Montar**. Aparecerá el **Asistente de montaje** y podrá ver la página **Volúmenes**.
- 5 En la página **Volúmenes**, seleccione cada volumen del punto de recuperación que desee montar y, a continuación, haga clic en **Siguiente**. Se mostrará la página **Opciones de montaje** del Asistente de montaje.
- 6 En la página **Opciones de montaje**, edite la configuración para montar un punto de recuperación como se describe en la tabla siguiente.

Tabla 151. Configuración de Opciones de montaje

Opción	Descripción
Carpeta local	Especifica la ruta de acceso que se utiliza para acceder al punto de recuperación montado. Por ejemplo, seleccione <code>C:\ProgramData\AppRecovery\MountPoints\MountPoint1</code> .
Tipo de montaje	Especifica la forma para acceder a los datos para el punto de recuperación montado. • Solo lectura • Solo lectura con escrituras anteriores • Editable
Crear un recurso compartido de Windows para este montaje	De manera opcional, seleccione esta casilla para especificar si el punto de recuperación montado se puede compartir y, en ese caso, configurar los derechos de acceso, incluidos el nombre compartido y los grupos permitidos.

- 7 Haga clic en **Finalizar** para montar el punto de recuperación.

NOTA: Si quiere copiar directorios o archivos desde un punto de recuperación montado a otro equipo con Windows, puede utilizar Windows Explorer para copiarlos con permisos predeterminados o permisos de acceso de archivo original. Para obtener información detallada, consulte desde [Restauración de un directorio o archivo mediante Windows Explorer](#) hasta [Restauración de un directorio o archivo y conservación de permisos mediante Windows Explorer](#).

- 8 Opcionalmente, mientras la tarea está en curso, puede ver su progreso desde el menú desplegable **Tareas en ejecución** en la Core Console, o bien puede ver información detallada en la página **Eventos**. Para obtener más información sobre cómo supervisar eventos de Rapid Recovery, consulte [Visualización de eventos mediante las tareas, las alertas y el diario](#).

Desmontaje de puntos de recuperación

Realice los pasos de este procedimiento para desmontar los puntos de recuperación que están montados localmente en el Core.

NOTA: Cuando desmonte un punto de recuperación montado de forma remota, esta acción se denomina *desconexión*.

- 1 En la Core Console de Rapid Recovery, en la barra de iconos, haga clic en  (Más) y después seleccione  **Montajes**.
Aparecerá la página **Montajes**. Hay un panel para Montajes locales (puntos de recuperación montados en el Core) y otro para Montajes remotos (puntos de recuperación montados con Local Mount Utility). En cada panel, los puntos de recuperación montados correspondientes aparecen en una lista.
- 2 Para desmontar los montajes locales, en el panel **Montajes locales**, haga lo siguiente:
 - a Seleccione el punto o puntos de montaje local que desea desmontar.
 - Para desmontar todos los puntos de recuperación, haga clic en la casilla de verificación de la barra de título de la tabla Montajes locales para seleccionar todos los puntos de montaje.
 - Para desmontar uno o varios puntos de recuperación, haga clic en la casilla de verificación en la primera columna de cada fila que represente el punto de montaje que desea desconectar.
 - b Haga clic en  **Desmontar**.
Aparece un cuadro de diálogo de confirmación.
 - c Haga clic para confirmar que desea desmontar los puntos de recuperación seleccionados.
Los puntos de recuperación locales se desmontan.

NOTA: Si las alertas del sistema están habilitadas, podría ver una alerta sobre que los puntos de montaje adecuados se están desmontando.

- 3 Para desconectar los puntos de recuperación montados de forma remota, haga lo siguiente en el panel **Montajes remotos**:
 - a Seleccione el punto o puntos de montaje remotos que desea desconectar.
 - Para desconectar todos los puntos de recuperación, haga clic en la casilla de verificación de la barra de título de la tabla Montajes remotos para seleccionar todos los puntos de montaje.
 - Para desconectar uno o varios puntos de recuperación, haga clic en la casilla de verificación en la primera columna de cada fila que represente el punto de montaje que desea desconectar.
 - b Haga clic en  **Desconectar**.
Aparece un cuadro de diálogo de confirmación.
 - c Haga clic para confirmar que desea desconectar los puntos de recuperación seleccionados.
Los puntos de recuperación locales se desconectan.

NOTA: Si las alertas del sistema están habilitadas, podría ver una alerta sobre que los puntos de montaje adecuados se están desconectando.

- 4 Confirme que los puntos de recuperación montados anteriormente ya no aparecen en las listas Montajes locales o Montajes remotos, según proceda.

Trabajo con puntos de recuperación de Linux

El método admitido y recomendado para montar y desmontar puntos de recuperación desde un equipo protegido con Linux es emplear la utilidad `local_mount`.

Estos procedimientos se dirigen específicamente al uso de `local_mount` para montar y desmontar puntos de recuperación de Linux.

NOTA: Para administrar los puntos de recuperación de Linux de cualquier otra forma, consulte [Administración de instantáneas y puntos de recuperación](#), ya que cualquier otro tipo de administración se puede realizar desde la Core Console.

Montaje de un volumen de punto de recuperación en un equipo Linux

Mediante la utilidad `local_mount` de Rapid Recovery, puede montar un volumen de forma remota desde un punto de recuperación como volumen local, en un equipo con Linux.

NOTA: Al realizar este procedimiento, no intente montar puntos de recuperación en la carpeta `/tmp`, que contiene los archivos `aavdisk`.

- 1 Cree un nuevo directorio para montar el punto de recuperación (por ejemplo, puede utilizar el comando `mkdir`).
- 2 Verifique que el directorio existe (por ejemplo, utilizando el comando `ls`).
- 3 Ejecute la utilidad `local_mount` de Rapid Recovery como raíz, o como superusuario, por ejemplo:

```
sudo local_mount
```
- 4 En la solicitud de montaje de Rapid Recovery, introduzca el siguiente comando para enumerar las máquinas protegidas.

```
lm
```
- 5 Cuando se le solicite, introduzca la dirección IP o nombre del host del servidor Rapid Recovery Core.
- 6 Introduzca las credenciales de inicio de sesión para el servidor de Core, es decir, el nombre de usuario y la contraseña.
Se mostrará una lista de los equipos protegidos por el servidor de Rapid Recovery. Cada equipo se identifica con lo siguiente: número de elemento de línea, host/dirección IP y número de ID del equipo.

Por ejemplo: 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba

- 7 Introduzca el siguiente comando para enumerar los puntos de recuperación disponibles actualmente para un equipo especificado:

```
lr <line_number_of_machine>
```

NOTA: Tenga en cuenta que también puede introducir el número de ID del equipo en este comando en lugar del número de elemento de línea.

Aparecerá una lista con los puntos de recuperación base e incrementales de ese equipo. Esta lista incluye un número de elemento de línea, fecha y marca de tiempo, ubicación del volumen, tamaño del punto de recuperación y número de ID del volumen que incluye un número secuencial al final, que identifica al punto de recuperación.

Por ejemplo, 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba:2

- 8 Introduzca el comando siguiente para seleccionar y montar el punto de recuperación especificado en el punto o la ruta de acceso de montaje que especifique.

```
m <volume_recovery_point_ID_number> <volume-letter> [flag] <path>
```

El indicador en el comando determina cómo montar el punto de recuperación. Puede utilizar una de las siguientes opciones:

- `[r]` - montar como solo lectura (predeterminado). Este indicador le permite montar un punto de recuperación pero no le permite realizar cambios en él.
- `[w]` - montar como de lectura. Este indicador le permite montar el punto de recuperación y le permite realizar cambios en él.
- `[v]` - montar con escrituras anteriores. Al montar con el indicador "v" le permite montar el punto de recuperación e incluir cualquier cambio que se realizara durante el anterior montaje de escritura pero que no están presentes en el punto de recuperación.
- `[n]` - no montar nbd en `<ruta_de_acceso>`. Un nbd (dispositivo de bloque de red) realiza una conexión de socket entre el Core y el equipo protegido cuando realizar un montaje local. Este indicador le permite montar el punto de recuperación sin montar el nbd, lo que resulta útil si desea comprobar manualmente el sistema de archivos del punto de recuperación.

❗ **NOTA:** También puede especificar un número de línea en el comando en lugar del número de ID del punto de recuperación para identificar al punto de recuperación. En ese caso, utilizaría el número de línea del equipo (desde la salida `lm`), seguido por el número de línea del punto de recuperación y la letra del volumen, seguido por la ruta de acceso, de este modo: `m <número_de_línea_del_equipo> <número_de_línea_del_punto_de_recuperación> <letra_del_volumen> <ruta_de_acceso>`. Por ejemplo, si la salida de `lm` enumera tres equipos protegidos, y especifica el comando `lr` para el número 2 y monta el volumen `b` del punto de recuperación número veintitrés en `/tmp/mount_dir`, el comando sería:

```
m 2 23 b /tmp/mount_dir
```

❗ **NOTA:** Si desea montar un volumen BTRFS desde un sistema operativo compatible (consulte el tema "Matriz de compatibilidad e instalación del sistema operativo para la versión 6.1 de Rapid Recovery" en la *Guía de instalación y actualización de Dell Data Protection | Rapid Recovery*), a continuación, debe incluir los parámetros siguientes:

```
mount -o nodatasum,device=/dev/xxx /dev/xxx /mnt/yyy
```

- 9 Para verificar que el montaje se ha realizado correctamente, introduzca el siguiente comando, que debería enumerar el volumen remoto adjunto:

```
l
```

Desmontaje de un volumen de punto de recuperación en un equipo Linux

Realice los pasos de este procedimiento para ver la información detallada del sistema de un equipo Linux.

- 1 Ejecute la utilidad `local_mount` de Rapid Recovery como raíz, o como superusuario, por ejemplo:

```
sudo local_mount
```
- 2 En la solicitud de montaje de Rapid Recovery, introduzca el siguiente comando para enumerar las máquinas protegidas.

```
lm
```
- 3 Cuando se le solicite, introduzca la dirección IP o nombre del host del servidor Rapid Recovery Core.
- 4 Introduzca las credenciales de inicio de sesión, es decir, el nombre de usuario y la contraseña, para este servidor Core. Se mostrará una lista de los equipos protegidos por el servidor de Rapid Recovery.
- 5 Introduzca el siguiente comando para enumerar los puntos de recuperación disponibles actualmente para un equipo especificado:

```
lr <line_number_of_machine>
```

❗ **NOTA:** Tenga en cuenta que también puede introducir el número de ID del equipo en este comando en lugar del número de elemento de línea.

Aparecerá una lista con los puntos de recuperación base e incrementales de ese equipo. Esta lista incluye: número de elemento de línea, fecha/marca de tiempo, ubicación del volumen, tamaño del punto de recuperación y número de identificación del volumen que incluye un número secuencial al final, que identifica al punto de recuperación.

Por ejemplo: `7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba:2`

- 6 Ejecute el comando `l or list` para obtener una lista de dispositivos NBD (Network Block Device, dispositivo de bloque de red) montados. Si monta cualquier punto de recuperación, obtendrá una ruta de acceso a un dispositivo NBD después de ejecutar el comando `l or list`.
- 7 Introduzca el siguiente comando para desmontar un punto de recuperación.

```
umount <path_of_nbd-device>
```
- 8 Ejecute el comando `l or list` para comprobar que el desmontaje del punto de recuperación se realizó con éxito.

Cómo forzar una instantánea

Forzar una instantánea permite forzar una transferencia de datos para el equipo protegido actual. Cuando se fuerza una instantánea, la transferencia se inicia inmediatamente o se agrega a la cola si se están ejecutando otros trabajos.

Puede elegir entre dos tipos de instantáneas.

Si selecciona una instantánea incremental y no existe ningún punto de recuperación anterior, se captura una imagen base. Forzar una instantánea no cambia el calendario de las instantáneas de programación.

NOTA: Rapid Recovery admite Windows 8, Windows 8.1, Windows Server 2012 y Windows Server 2012 R2 tanto para transferencias base como para transferencias incrementales.

- Una imagen base es una instantánea de todos los datos en los volúmenes seleccionados del equipo.
 - Una instantánea incremental captura todos los datos que se han modificado desde la última instantánea.
- 1 En la Core Console de Rapid Recovery, desplácese hasta el equipo o el clúster con el punto de recuperación para el que quiera forzar una instantánea.
 - 2 En la página Resumen, haga clic en **Forzar instantánea**.
Aparecerá el cuadro de diálogo Forzar instantánea.
 - 3 En el cuadro de diálogo Forzar instantánea, en la casilla de verificación, haga clic en uno o más volúmenes, o grupos de protección.
 - 4 Haga clic en **Forzar instantánea** o en Forzar imagen base, respectivamente.
 - 5 Si ha seleccionado una imagen base, haga clic para confirmar que desea tomar una imagen base.
Una imagen base puede tardar un tiempo considerable, en función de la cantidad de datos en los volúmenes de los que desea realizar una copia de seguridad.

La instantánea que ha seleccionado se pone en cola y comienza en cuanto finalizan otros trabajos.

Eliminación de puntos de recuperación

Puede quitar fácilmente del repositorio los puntos de recuperación de un equipo concreto. Cuando elimine puntos de recuperación de Rapid Recovery, puede especificar una de las opciones siguientes.

- **Eliminar todos los puntos de recuperación.** Quita todos los puntos de recuperación para el equipo protegido del repositorio.
- **Eliminar un rango de puntos de recuperación.** Quita todos los puntos de recuperación de un rango especificado antes del actual, hasta e incluida la imagen base, que son todos los datos del equipo, así como todos los puntos de recuperación después del actual hasta la imagen base siguiente.

NOTA: No puede recuperar los puntos de recuperación que haya eliminado. Si necesita los datos almacenados en los puntos de recuperación, considere archivar primero los datos.

- 1 En la Core Console de Rapid Recovery, bajo el menú **Equipos protegidos**, haga clic en el nombre o dirección IP del equipo del que desea ver y quitar los puntos de recuperación.
Aparecerá la vista Resumen para el equipo protegido seleccionado.
- 2 Junto al nombre del equipo o la dirección IP, haga clic en el menú **Puntos de recuperación**.
Aparece la página **Puntos de recuperación** para el equipo seleccionado.
- 3 Desplácese hasta el panel **Puntos de recuperación**.
Las opciones aparecen bajo el título del panel, incluidas Actualizar, Eliminar rango y Eliminar todo.
- 4 Para eliminar todos los puntos de recuperación almacenados actualmente, bajo el título del panel Puntos de recuperación, haga clic en **Eliminar todo** y, en el cuadro de diálogo de confirmación, haga clic en Confirmar eliminación.
- 5 Para eliminar un conjunto de puntos de recuperación en un rango de datos específico, haga lo siguiente:
 - a Bajo el título del panel Puntos de recuperación, haga clic en **Eliminar rango**.
Aparece el cuadro de diálogo **Eliminar puntos de recuperación dentro del rango**.
 - b En el cuadro de diálogo **Eliminar puntos de recuperación dentro del rango**, seleccione en el campo **Desde** la fecha y la hora desde las que desea empezar a eliminar puntos de recuperación.
 - c En el campo **Hasta**, seleccione la fecha y la hora que definan el último punto de recuperación que desea eliminar.
 - d Haga clic en **Eliminar**.
 - e Haga clic en el cuadro de diálogo de confirmación para confirmar la eliminación.

Eliminación de una cadena de puntos de recuperación huérfanos

Un punto de recuperación huérfano es una instantánea incremental que no está asociada a una imagen base. Las instantáneas posteriores siguen generándose en este punto de recuperación; sin embargo, sin la imagen base, los puntos de recuperación resultantes están incompletos y es poco probable que contengan los datos necesarios para completar una recuperación. Estos puntos de recuperación se consideran parte de la cadena de puntos de recuperación huérfanos. Si se produce esta situación, la mejor solución es eliminar la cadena y crear una nueva imagen base.

Para obtener más información sobre cómo forzar una imagen base, consulte [Cómo forzar una instantánea](#).

- 1 En la Rapid Recovery Core Console, desplácese hasta el equipo protegido cuya cadena de puntos de recuperación huérfanos quiera eliminar.
- 2 En el menú de la parte superior de la página, haga clic en **Puntos de recuperación**.
- 3 En el panel de Puntos de recuperación, amplíe el punto de recuperación huérfano. Este punto de recuperación está etiquetado en la columna Tipo como “Incremental, huérfano”.
- 4 Junto a Acciones, haga clic en **Eliminar**. Aparecerá la ventana Eliminar puntos de recuperación.
- 5 En la ventana Eliminar puntos de recuperación, haga clic en **Sí**.

⚠ PRECAUCIÓN: Al eliminar este punto de recuperación se elimina toda la cadena de puntos de recuperación, incluidos los puntos de recuperación incrementales que se produzcan antes o después del mismo, hasta la siguiente imagen base. Esta operación no puede deshacerse.

La cadena de puntos de recuperación huérfanos se eliminará.

Migración de puntos de recuperación manual a un repositorio diferente

Si desea retirar los puntos de recuperación de un equipo protegido desde un repositorio sin eliminarlos, puede migrarlos a un repositorio diferente manualmente mediante este procedimiento. Este proceso implica archivar puntos de recuperación del repositorio de origen e importar el archivo al repositorio de destino.

Por ejemplo, puede realizar este procedimiento si su repositorio existente está completo o si sus necesidades cambian y quiere proteger un equipo con un Core y un repositorio diferentes.

⚠ PRECAUCIÓN: Si su repositorio se actualizó anteriormente desde AppAssure 5.3 o 5.4 y utilizó la replicación, Dell recomienda realizar el trabajo de comprobación de repositorio en cada repositorio en el Core de destino antes de la migración. Realizar este trabajo impedirá copiar las irregularidades de los datos al nuevo repositorio de destino. El trabajo de comprobación de repositorio solo está disponible en la UI si se puede aplicar a su Core y podría tardar una cantidad sustancial de tiempo en ejecutarse. Para obtener información sobre este trabajo, consulte [Comprobación de la integridad de los repositorios de DVM](#). Para obtener información sobre cómo realizar este trabajo, consulte [Ejecución de un trabajo de comprobación de repositorio en un repositorio DVM](#).

- 1 En la Core Console de Rapid Recovery, pause la protección de los equipos protegidos cuyos puntos de recuperación quiere migrar. Para obtener más información, consulte [Puesta en pausa y reanudación de la protección](#).
- 2 Cancele todas las operaciones en curso en los equipos protegidos cuyos puntos de recuperación quiere migrar o espere a que se hayan completado totalmente.
- 3 Archive los puntos de recuperación del equipo o equipos en los que ha realizado una pausa. Para obtener más información, consulte [Creación de una archivación](#).

- 4 Tras archivar y verificar el archivo, elimine los puntos de recuperación existentes del equipo protegido que quiere migrar. Para obtener más información, consulte [Eliminación de puntos de recuperación](#).

NOTA: Si no elimina los puntos de recuperación existentes, no puede cambiar los repositorios de un equipo protegido.

- 5 Cree un repositorio nuevo para los puntos de recuperación migrados o asegúrese de que existe un nuevo repositorio de destino. Para obtener más información, consulte [Creación de un repositorio DVM](#).
 - Si desea utilizar un repositorio existente, vaya al [paso 6](#).
- 6 Cambie el repositorio de cada equipo en el que realizó una pausa completando los siguientes pasos:
 - a En la Core Console, haga clic en el equipo protegido en el árbol de navegación.
 - b En la página **Resumen** del equipo protegido, haga clic en **Configuración**.
 - c En la página **Configuración**, en el panel **General**, haga clic en la lista desplegable **Repositorio** y, a continuación, seleccione el nombre del repositorio que creó en el [paso 4](#).
 - Si desea utilizar un repositorio existente, seleccione el nombre de un repositorio existente.

NOTA: Cuando migre puntos de recuperación a un repositorio existente, asegúrese de que el repositorio existente tiene espacio libre suficiente para contener los puntos de recuperación migrados.

- d Haga clic en **Aceptar**.
- 7 Reanude la protección del equipo o equipos en los que realizó una pausa. Para obtener más información, consulte [Puesta en pausa y reanudación de la protección](#).
- 8 Tome una nueva imagen base para cada equipo protegido que haya trasladado. Para obtener más información, consulte [Cómo forzar una instantánea](#) y utilice la opción Forzar imagen base.
- 9 Importe los datos archivados para los equipos que desee migrar. Para obtener más información, consulte [Importación de un archivo](#).

Restauración de datos

En esta sección se describe cómo restaurar datos de las copias de seguridad.

Acerca de la restauración de datos con Rapid Recovery

El Rapid Recovery Core puede restaurar datos al instante o realizar la recuperación de equipos en máquinas físicas o virtuales desde puntos de recuperación. Los puntos de recuperación contienen instantáneas del volumen del Agent capturadas en el nivel del bloque. Esas instantáneas ofrecen reconocimiento por parte de la aplicación, lo cual significa que todos los registros de transacciones abiertas y transacciones en marcha se completan y que las memorias caché se vacían antes de crear la instantánea. Mediante instantáneas con reconocimiento por parte de la aplicación, y junto con Verified Recovery, el Core puede realizar varios tipos de recuperaciones, que incluyen:

- Recuperación de archivos y carpetas
- Recuperación de volúmenes de datos, mediante Live Recovery
- Recuperación de volúmenes de datos para Microsoft Exchange Server y Microsoft SQL Server, mediante Live Recovery
- Restauración bare-metal, mediante Universal Recovery
- Recuperación bare-metal de hardware diferente, mediante Universal Recovery
- Exportación ad-hoc y continua a máquinas virtuales

NOTA: Al restaurar datos o realizar una exportación virtual, el punto de recuperación utilizado debe formar parte de una cadena de puntos de recuperación completa. Para obtener más información acerca de las cadenas de puntos de recuperación, consulte el tema [Cadenas del punto de recuperación y huérfanos](#).

Descripción de Live Recovery

Live Recovery es una función de restauración de datos del Rapid Recovery Core. Si la máquina protegida experimenta fallos de datos de un volumen de Windows que no sea del sistema, puede restaurar datos a partir de un punto de recuperación del Rapid Recovery Core. Al

seleccionar Live Recovery en Restore Wizard, permite a los usuarios continuar de inmediato las operaciones empresariales casi sin tiempo de inactividad. Live Recovery durante la restauración proporciona acceso inmediato a los datos, incluso aunque Rapid Recovery continúe restaurando datos en segundo plano. Esta función le permite un tiempo de recuperación prácticamente inexistente, incluso si la restauración implica terabytes de datos.

El Rapid Recovery Core utiliza la exclusiva tecnología de recuperación y copias de seguridad basada en bloques que le permite acceso completo de usuario a los servidores de destino durante el proceso de recuperación. Los bloques solicitados se restauran a petición para una recuperación sencilla.

Live Recovery se aplica a las máquinas físicas y virtuales protegidas por el Rapid Recovery Core, con las siguientes exclusiones:

- Live Recovery está accesible para volúmenes de Windows que no son del sistema. La unidad C:\ y la partición reservada al sistema no se pueden restaurar con Live Recovery.
- Live Recovery es accesible para volúmenes basados en Windows que utilizan Rapid Recovery Agent. Los volúmenes sin agentes o los volúmenes de Linux no pueden aprovecharse de Live Recovery.

Live Recovery le permite restaurar inmediatamente los servidores físicos o virtuales directamente desde el archivo de copia de seguridad. Cuando un volumen sin sistema está siendo restaurado, Rapid Recovery presenta los metadatos de volumen para el sistema operativo al instante, lo que hace que los datos estén disponibles a petición. Por ejemplo, si el volumen de la base de datos de Microsoft Exchange está dañado, Live Recovery puede restaurar el volumen, la base de datos y los servicios de Exchange en minutos.

Esta función proporciona el método más rápido para recuperar grandes cantidades de datos con un tiempo de inactividad mínimo. Los usuarios pueden continuar inmediatamente las operaciones empresariales.

Una vez que Live Recovery se inicia, el volumen restaurado y su contenido vuelven a estar disponibles al instante. El Rapid Recovery Core continúa restaurando los datos en segundo plano, aunque el volumen, sus datos, aplicaciones y servicios estén ya en producción. Si se solicitan datos específicos, el proceso en segundo plano da preferencia a la restauración de dichos datos inmediatamente. Esta poderosa funcionalidad permite también cumplir los acuerdos de servicio más exigentes.

Una vez que ha iniciado Live Recovery, los metadatos (estructura del directorio, descriptores de seguridad, atributos de archivo NTFS, mapa de espacio libre, etc.) del volumen de destino se restauran rápidamente en la máquina protegida. A partir de entonces, el volumen y su contenido pasan a estar disponibles para el sistema. Rapid Recovery Agent comienza la restauración de los bloques de datos desde el servidor del Rapid Recovery Core, escribiendo los bloques en el volumen de destino.

Se responde de inmediato a las solicitudes de datos que todavía no se ha restaurado, con el programa de solicitud o sistema que ignoran que los bloques ya se han restaurado.

Restauración de datos desde puntos de recuperación

Rapid Recovery protege sus datos en equipos Windows y Linux. Las copias de seguridad de los equipos Agent protegidos se guardan en el Rapid Recovery Core como puntos de recuperación. Desde estos puntos de recuperación, puede restaurar los datos uno de tres métodos posibles.

En la Rapid Recovery Core Console, puede restaurar volúmenes completos desde un punto de recuperación de un volumen sin sistema, reemplazando los volúmenes en el equipo de destino. Esto se puede hacer solo para equipos con Windows. Para obtener más información, consulte [Restauración de volúmenes desde un punto de recuperación](#).

No puede restaurar un volumen que contenga el sistema operativo directamente desde un punto de recuperación, dado que el equipo en el que está realizando la restauración está utilizando el sistema operativo y controladores que se incluyen en el proceso de restauración. Si desea restaurar desde un punto de recuperación a un volumen del sistema (por ejemplo, la unidad C del equipo Agent), deberá realizar una restauración Bare Metal Restore (BMR). Esto implica crear una imagen de inicio desde el punto de recuperación, que incluye archivos del sistema operativo y de configuración, así como datos, tras lo que debe iniciarse el equipo de destino desde esa imagen de inicio para completar la restauración. La imagen de inicio es diferente si el equipo que quiere restaurar utiliza un sistema operativo Windows o Linux. Si quiere restaurar desde un punto de recuperación en un volumen del sistema en un equipo con Windows, consulte [Restauración Bare Metal Restore en máquinas Windows](#). Si quiere restaurar desde un punto de recuperación en un volumen del sistema en un equipo con Linux, consulte [Restauración Bare Metal Restore en máquinas Linux](#).

Por último, en contraste con la restauración de volúmenes enteros, puede montar un punto de recuperación desde un equipo con Windows y examinar las carpetas y los archivos individuales para recuperar únicamente un conjunto específico de archivos. Para obtener más información, consulte [Restauración de un directorio o archivo mediante Windows Explorer](#). Si necesita realizar esta acción mientras conserva los permisos de archivo original (por ejemplo, al restaurar la carpeta de un usuario en un servidor de archivos), consulte [Restauración de un directorio o archivo y conservación de permisos mediante Windows Explorer](#).

Los temas de esta sección describen información sobre cómo restaurar datos en equipos físicos. Para obtener más información sobre cómo exportar datos protegidos desde equipos con Windows a máquinas virtuales, consulte [Exportación de VM](#).

NOTA: Al recuperar datos en equipos con Windows, si el volumen que está restaurando tiene activada la deduplicación de datos de Windows, deberá asegurarse de que la deduplicación también está activada en el servidor del Core. Rapid Recovery admite Windows 8, Windows 8.1, Windows 10, Windows Server 2012 y Windows Server 2012 R2 para transferencias normales (tanto base como incrementales), así como con datos de restauración, restauración Bare Metal Restore y exportaciones virtuales. Para obtener más información sobre los tipos de volúmenes admitidos y no admitidos para la copia de seguridad y la recuperación, consulte [Compatibilidad con volúmenes básicos y dinámicos](#).

Restauración de volúmenes desde un punto de recuperación

Puede restaurar los volúmenes de una máquina protegida desde los puntos de recuperación almacenados en el Core de Rapid Recovery.

NOTA: En versiones anteriores, este proceso se conocía como Realizar una reversión.

NOTA: Rapid Recovery es compatible con la protección y recuperación de máquinas configuradas con particiones EISA. Asimismo, es compatible con máquinas con Windows 8, Windows 8.1, Windows Server 2012 y Windows Server 2012 R2 que usan Entorno de recuperación de Windows (Windows RE).

Puede empezar una restauración desde cualquier ubicación de la Core Console de Rapid Recovery haciendo clic en el icono Restaurar en la barra de botones de Rapid Recovery. Cuando se inicia una operación de restauración de esta manera, se deben especificar las máquinas que desea proteger en el Core que desea restaurar y, a continuación, indique el volumen que desea restaurar.

O bien, puede ir a la página Puntos de recuperación de una máquina específica, haga clic en el menú desplegable de un punto de recuperación específico y, a continuación, seleccione **Restaurar**. Si comienza una restauración de esta manera, siga este procedimiento empezando por el [paso 5](#).

Si desea realizar una restauración a partir de un punto de recuperación en un volumen del sistema, o realizar una restauración a partir de un punto de recuperación utilizando un CD de arranque, debe llevar a cabo una restauración Bare Metal Restore (BMR). Para obtener más información sobre BMR, consulte [Comprensión de la restauración Bare Metal Restore para equipos Windows](#), y para obtener información sobre los prerrequisitos de los sistemas operativos Windows o Linux, consulte [Requisitos previos para realizar una restauración Bare Metal Restore para un equipo con Windows](#) y [Requisitos previos para realizar una restauración Bare Metal Restore para un equipo Linux](#), respectivamente. Puede acceder a las funciones de BMR desde la Core Console como se indica en el plan de cada sistema operativo. También puede realizar una restauración Bare Metal Restore mediante el Restore Machines Wizard (Asistente de protección de máquinas). Este procedimiento lo llevará al punto adecuado del asistente para llevar a cabo el procedimiento [Restauración Bare Metal Restore con el Asistente para restaurar un equipo](#).

Restauración de volúmenes desde un punto de recuperación

El equipo protegido debe tener el software Agent instalado y puntos de recuperación desde los que realizar la operación de restauración.

Realice el procedimiento siguiente para restaurar volúmenes desde un punto de recuperación.

- 1 Para restaurar un volumen en un equipo protegido desde el icono Restaurar, desplácese hasta la Core Console y haga clic en **Restaurar** desde la barra de botones de Rapid Recovery.
Aparecerá el Asistente para restaurar un equipo.
- 2 Desde la página Equipos protegidos, seleccione el equipo protegido para el que desee restaurar datos y, a continuación, haga clic en **Siguiente**.

Aparecerá la página Puntos de recuperación.

- 3 Desde la lista de puntos de recuperación, busque la instantánea que quiera restaurar en el equipo Agent.
 - Si es necesario, utilice los botones de la parte inferior de la página para mostrar más páginas de puntos de recuperación.
 - Opcionalmente, para limitar la cantidad de puntos de recuperación que aparecen en la página Puntos de recuperación del asistente, puede filtrar por volúmenes (si está definido) o por fecha de creación del punto de recuperación.
 - 4 Haga clic en cualquier punto de recuperación para seleccionarlo y, a continuación, haga clic en **Siguiente**.

Aparecerá la página Destino.
 - 5 En la página Destino, seleccione el equipo en el que quiera restaurar datos de la manera siguiente:
 - Para restaurar datos desde el punto de recuperación seleccionado al mismo equipo y si los volúmenes que quiere restaurar no incluyen el volumen del sistema, seleccione **Recuperar en un equipo protegido (solamente volúmenes que no sean del sistema)**, verifique que el equipo de destino está seleccionado y, a continuación, haga clic en **Siguiente**.

Aparecerá la página Asignación de volúmenes. Continúe en el [paso 9](#).
 - Para restaurar datos desde el punto de recuperación seleccionado a un equipo protegido diferente (por ejemplo, sustituir el contenido de Equipo2 por datos de Equipo1), seleccione **Recuperar en un equipo protegido (solamente volúmenes que no sean del sistema)**, seleccione el equipo de destino en la lista y, a continuación, haga clic en **Siguiente**.

Aparecerá la página Asignación de volúmenes. Continúe en el [paso 9](#).
 - Si desea restaurar desde un punto de recuperación al mismo equipo o a un equipo diferente utilizando un CD de inicio, este proceso se considera una restauración Bare Metal Restore (BMR). Para obtener información acerca de la restauración BMR, consulte [Comprensión de la restauración Bare Metal Restore para equipos Windows](#).
- NOTA:** La realización de una BMR tiene requisitos específicos, en base al sistema operativo del equipo agente que desea restaurar. Para conocer los requisitos previos, consulte [Requisitos previos para realizar una restauración Bare Metal Restore para un equipo con Windows](#) y [Requisitos previos para realizar una restauración Bare Metal Restore para un equipo Linux](#), respectivamente.

Si los volúmenes que desea restaurar incluyen el volumen del sistema, seleccione **Recupere en cualquier máquina de destino usando un CD de inicio**. Esta opción le pide que cree un CD de inicio.

 - Para continuar y crear el CD de inicio con información del punto de recuperación seleccionado empleando el Asistente para restaurar un equipo, haga clic en **Siguiente** y vaya al [Restauración Bare Metal Restore en máquinas Windows](#).
 - Si ya ha creado el CD de inicio y el equipo de destino se ha iniciado con el CD de inicio, vaya al [paso 8](#) del tema [Restauración Bare Metal Restore en máquinas Windows](#).
- Si desea restaurar desde un punto de recuperación a un volumen del sistema (por ejemplo, la unidad C del equipo Agent llamado Equipo1), este proceso también se considera una BMR. Seleccione **Recuperar en cualquier equipo de destino mediante un CD de inicio**. Esta opción le pide que cree un CD de inicio.
 - Para continuar y crear el CD de inicio con información del punto de recuperación seleccionado empleando el Asistente para restaurar un equipo, haga clic en **Siguiente** y vaya a [Restauración Bare Metal Restore en máquinas Windows](#).
 - Si ya ha creado el CD de inicio, continúe en el [paso 6](#).
 - 6 Inicie el equipo que desea restaurar empleando el CD de inicio. Para obtener más información sobre BMR en un equipo con Windows, consulte [Carga del CD de inicio e inicio del equipo de destino](#) y para BMR en un equipo con Linux, consulte [Carga del Live DVD e inicio del equipo de destino](#).
 - 7 En el servidor Core, en la página Destino del Asistente para restaurar un equipo, seleccione **Ya tengo un CD de inicio ejecutándose en el equipo de destino** y, a continuación, introduzca la información sobre el equipo con el que desea conectar que está descrita en la siguiente tabla.

Tabla 152. Información del equipo

Cuadro de texto	Descripción
Dirección IP	Dirección IP del equipo que desea restaurar. Esta es idéntica a la dirección IP mostrada en la URC.
Clave de autenticación	Contraseña específica con la que conectarse al servidor seleccionado. Esta es idéntica a la clave de autenticación mostrada en la URC.

- 8 Haga clic en **Siguiente**.

Si la información de conexión que introdujo coincide con la URC y si el Core y el servidor de destino pueden identificarse entre sí adecuadamente en la red, se cargarán los volúmenes para el punto de recuperación seleccionado. Aparecerá la página Asignación de discos.

Para completar la restauración BMR desde el Asistente para restaurar un equipo, continúe en el [paso 9](#) del tema [Restauración Bare Metal Restore en máquinas Windows](#).

NOTA: Rapid Recovery es compatible con las particiones FAT32 y ReFS. Solo se admite la restauración completa y el BMR puesto que hay una limitación de controladores con el ReFS. La restauración se implementa en el modo usuario, exportación VM, etc. Si un Core está protegiendo al menos un volumen agente con el sistema de archivos ReFS, debería instalarse en equipos con Windows 8/2012 ya que proporciona compatibilidad nativa con ReFS. Si no es así, las funciones están limitadas y las operaciones de tipo montaje de una imagen de volumen no funcionan. La Core Console de Rapid Recovery presenta los mensajes de error pertinentes en estas apariciones.

La restauración Bare Metal Restore de la configuración de discos de espacios de almacenamiento (una función de Windows 8.1) tampoco se admite en esta versión. Para obtener detalles, consulte la Guía de instalación y actualización de Rapid Recovery.

- 9 En la página Asignación de volúmenes, para cada volumen del punto de recuperación que quiera restaurar, seleccione el volumen de destino adecuado. Si no quiere restaurar un volumen, en la columna Volúmenes de destino, seleccione **No restaurar**.
- 10 Seleccione **Mostrar opciones avanzadas** y, a continuación, haga lo siguiente:
 - Para restaurar en máquinas con Windows, si desea utilizar Live Recovery, seleccione **Live Recovery**.
Al utilizar la tecnología de recuperación instantánea de Live Recovery en Rapid Recovery, puede recuperar o restaurar datos instantáneamente en sus máquinas físicas o en máquinas virtuales desde puntos de recuperación almacenados de equipos Windows, lo cual incluye espacios de almacenamiento de Microsoft Windows. Live Recovery no está disponible para equipos con Linux ni máquinas virtuales que utilicen protección sin agentes.
 - Si desea forzar los volúmenes seleccionados para desmontar antes de que empiece la restauración, seleccione **Forzar desmontaje**.
PRECAUCIÓN: Si no fuerza un desmontaje antes de restaurar datos, puede que la restauración falle con un error que diga que el volumen está en uso.
- 11 Haga clic en **Siguiente**.
- 12 En la página Desmontar bases de datos, si los volúmenes que desea restaurar contienen bases de datos SQL o Microsoft Exchange, se le solicitará que las desmonte.
Si desea volver a montar estas bases de datos después de que la restauración se haya completado, seleccione **Volver a montar todas las bases de datos automáticamente después de que se haya restaurado el punto de recuperación**.
- 13 Haga clic en **Siguiente**.
Es posible que aparezca la página Advertencia y le indique que cierre todos los programas en los volúmenes que desea restaurar. Si lo hace, haga clic en **Siguiente** de nuevo.
- 14 En la página Resumen, seleccione la opción **IMPORTANTE. Entiendo que esta operación sobrescribirá los volúmenes seleccionados con los datos del punto de recuperación seleccionado** para confirmar que entiende las consecuencias de una restauración de volúmenes.
AVISO: Esta opción hace hincapié en la consecuencia de que los datos que se hayan guardado en el volumen seleccionado después de la fecha y la hora del punto de recuperación seleccionado se perderán después de la restauración.
- 15 Haga clic en **Finalizar**.

Restauración de un directorio o archivo mediante Windows Explorer

Puede utilizar Windows Explorer para copiar y pegar directorios y archivos desde un punto de recuperación montado en cualquier equipo con Windows. Esto puede ser de utilidad cuando solamente quiere distribuir una parte de un punto de recuperación a sus usuarios.

Cuando copie directorios y archivos, los permisos de acceso del usuario que esté realizando la operación de copia se utilizarán y aplicarán en los directorios y archivos pegados. Si quiere restaurar directorios y archivos para sus usuarios conservando los permisos de archivo

original (por ejemplo, al restaurar la carpeta de un usuario en un servidor de archivos), consulte [Restauración de un directorio o archivo y conservación de permisos mediante Windows Explorer](#).

- 1 Monte el punto de recuperación que contenga los datos que quiera restaurar. Para obtener información detallada, consulte [Montaje de un punto de recuperación](#).
- 2 En Windows Explorer, desplácese hasta el punto de recuperación montado y seleccione los directorios y archivos que quiera restaurar. Haga clic con el botón secundario y seleccione **Copiar**.
- 3 En Windows Explorer, desplácese hasta la ubicación del equipo en el que quiera restaurar los datos. Haga clic con el botón secundario y seleccione **Pegar**.

Restauración de un directorio o archivo y conservación de permisos mediante Windows Explorer

Puede utilizar Windows Explorer para copiar y pegar directorios y archivos desde un punto de recuperación montado en cualquier equipo con Windows conservando los permisos de acceso de archivo.

Por ejemplo, si necesita restaurar una carpeta a la que solamente accedan usuarios específicos de un servidor de archivos, puede utilizar los comandos Copiar y Pegar con permisos para garantizar que los archivos restaurados conservan los permisos que restringen el acceso. De este modo, puede evitar tener que aplicar permisos manualmente a los directorios y archivos restaurados.

❗ NOTA: El comando Pegar con permisos se instala con el software Rapid Recovery Core y Agent. No está disponible en Local Mount Utility.

- 1 Monte el punto de recuperación que contenga los datos que quiera restaurar. Para obtener información detallada, consulte [Montaje de un punto de recuperación](#).
- 2 En Windows Explorer, desplácese hasta el punto de recuperación montado y seleccione los directorios y archivos que quiera restaurar. Haga clic con el botón secundario y seleccione **Copiar**.
- 3 En Windows Explorer, desplácese hasta la ubicación del equipo en el que quiera restaurar los datos. Haga clic con el botón secundario y seleccione **Pegar con permisos**.

❗ NOTA: En este paso, si el comando Pegar con permisos está desactivado en el menú secundario, Windows Explorer no detecta los archivos que quiere copiar. Repita el [Paso 2](#) para activar el comando Pegar con permisos en el menú secundario.

Restauración de clústeres y nodos de clúster

Una restauración es el proceso de restaurar los volúmenes en una máquina desde puntos de recuperación. Para los clústeres de servidor, se realiza una restauración a nivel de nodo o de máquina. Esta sección proporciona directrices para realizar una restauración de volúmenes de clúster.

Restauración de clústeres CCR y DAG (Exchange)

Realice los pasos de este procedimiento para efectuar una restauración de clústeres CCR y DAG (Exchange).

- 1 Apague todos los nodos excepto uno.
- 2 Realice una restauración utilizando el procedimiento estándar de Rapid Recovery para la máquina, según se describe en [Restauración de volúmenes desde un punto de recuperación](#) y en [Restauración de volúmenes para un equipo Linux mediante la línea de comandos](#).
- 3 Cuando finalice la restauración, monte todas las bases de datos de los volúmenes de clúster.
- 4 Encienda el resto de nodos.
- 5 Para Exchange, acceda a la Exchange Management Console (Consola de administración de Exchange) y, para cada base de datos, realice la operación Update Database Copy (Actualizar copia de base de datos).

Restauración de clústeres SCC (Exchange y SQL)

Realice los pasos de este procedimiento para efectuar una restauración de clústeres de SCC (Exchange y SQL).

- 1 Apague todos los nodos excepto uno.
- 2 Realice una restauración utilizando el procedimiento estándar de Rapid Recovery para la máquina, según se describe en [Restauración de volúmenes desde un punto de recuperación](#) y en [Restauración de volúmenes para un equipo Linux mediante la línea de comandos](#).
- 3 Una vez terminada la restauración, monte todas las bases de datos a partir de los volúmenes de clúster.
- 4 Encienda el resto de nodos, de uno en uno.

NOTA: No es necesario revertir el disco de quórum. Puede regenerarse automáticamente o mediante la función de servicio de clúster.

Restauración a partir de un archivo conectado

Hay dos maneras de restaurar datos a partir de un archivo: puede utilizar un archivo como fuente para una restauración Bare Metal Restor (BMR), o puede conectar un archivo, montar un punto de recuperación desde el archivo y, a continuación, restaurar los datos archivados.

Al conectar un archivo, aparecerá en Attached Archives (Archivos conectados) en la página Archives (Archivos) de la Core Console; se podrá acceder al contenido de los archivos desde el área de navegación de la parte izquierda. El contenido aparecerá debajo del nombre del archivo. Las máquinas que fueron archivadas aparecerán como máquinas de solo puntos de recuperación para que pueda acceder a los puntos de recuperación de la misma forma que lo haría en una máquina protegida: montando un punto de recuperación, ubicando el elemento que desea recuperar y usando Explorador de Windows para copiar y pegar el elemento a su destino.

Existen ventajas con respecto a restaurar a partir de un archivo conectado en lugar de importar un archivo a un repositorio.

- La restauración a partir de un archivo conectado le permite ahorrar el tiempo que pasaría importando un archivo entero a un repositorio.
- Además, cuando importa un archivo, los puntos de recuperación archivados se agregan al repositorio. Debido a que estos puntos de recuperación archivados son probablemente los elementos más antiguos del repositorio, es posible que estén organizados de acuerdo con su política de retención durante la siguiente tarea nocturna. (Sin embargo, con esta acción no se borrarán desde el archivo; tendrá la opción de volver a importarlos al día siguiente).
- Por último, el Core recuerda la relación de la conexión con los archivos, incluso después de desconectar un archivo, lo que facilita y agiliza volver a conectar un archivo más adelante. Puede eliminar la relación mediante eliminando el archivo conectado.

Para restaurar datos desde un archivo conectado, realice los pasos siguientes utilizando los enlaces que correspondan:

NOTA: Con el procedimiento de restauración a partir de un archivo conectado se asume que ya tiene un archivo puntos de recuperación consolidados.

- 1 Conecte el archivo.
- 2 Monte el punto de recuperación que contiene los datos que desea recuperar.
- 3 Restaure los datos mediante cualquiera de los métodos siguientes:
 - Restaure los datos, como archivos o carpetas, desde el punto de recuperación.
 - Restaure todo el punto de recuperación.
 - Exporte el punto de recuperación a una máquina virtual.

Vínculos relacionados

- [Adición de un archivo comprimido](#)
- [Montaje de un punto de recuperación](#)
- [Restauración de un directorio o archivo mediante Windows Explorer](#)
- [Información sobre la exportación a máquinas virtuales con Rapid Recovery](#)
- [Copia de seguridad de Windows](#)
- [Cómo funciona la archivación](#)
- [Importación de un archivo](#)
- [Llevar a cabo una BMR a partir de un archivo](#)

Comprensión de la restauración Bare Metal Restore para equipos Windows

En esta sección se describe el método para restaurar en equipo protegido con Windows desde hardware igual o diferente con la restauración Bare Metal Restore.

Restauración Bare Metal Restore para equipos con Windows

Los servidores, si funcionan correctamente, realizan las tareas para las que están configurados. Las cosas cambian cuando se produce algún error. Si se produce algún hecho catastrófico, que deje inoperable el servidor, deberán tomarse de inmediato pasos para restaurar todas las funciones de ese equipo.

Rapid Recovery ofrece la capacidad de realizar una restauración Bare Metal Restore (BMR) para equipos con Windows o Linux. BMR es un proceso que restaura toda la configuración de software de un sistema específico. Utiliza el término “Bare Metal” (reconstrucción completa) porque la operación de restauración no solamente recupera los datos del servidor, sino que también reformatea el disco duro y reinstala el sistema operativo y todas las aplicaciones de software. Para realizar una BMR, debe especificar un punto de recuperación desde un equipo protegido y revertir (realizar una restauración) a la máquina física o virtual designada. Si está realizando una restauración en un volumen del sistema, esto se considera una BMR. Si está realizando una restauración y requiere un CD de inicio, esto se considera una BMR. Otras circunstancias en las que puede elegir realizar una restauración completa incluyen una actualización de hardware o la sustitución de un servidor. En ambos casos, la restauración se realiza a partir de un punto de restauración en el hardware actualizado o sustituido.

Rapid Recovery admite sistemas operativos Windows 8, 8.1 y Windows Server 2012, 2012 R2 que se inician desde particiones de EFI FAT32 disponibles para su protección o recuperación, así como volúmenes de Resilient File System (ReFS).

NOTA: La restauración Bare Metal Restore de la configuración de discos de espacios de almacenamiento (una función de Windows 8.1) tampoco se admite en esta versión. En la actualidad, solamente se admiten la restauración completa y la BMR dado que existe una limitación de controlador con ReFS, por lo que la restauración se implementa en modo de usuario, exportación de máquina virtual, etc. Si un Core está protegiendo al menos un volumen agente con el sistema de archivos ReFS, debería instalarse en un equipo bajo Windows 8, Windows 8.1, Windows Server 2012 o Windows Server 2012 R2, ya que estos sistemas operativos proporcionan compatibilidad nativa con ReFS. Si no es así, las funciones estarán limitadas y las operaciones de tipo montaje de una imagen de volumen no funcionarán. La Rapid Recovery Core Console presentará los mensajes de error correspondientes en estos casos.

Solamente los sistemas operativos Linux compatibles están disponibles para su protección o recuperación. Se trata de los sistemas Ubuntu®, Red Hat® Enterprise Linux®, CentOS™ y SUSE® Linux Enterprise Server (SLES®). Para obtener más información, consulte la *Guía de instalación y actualización de Dell Data Protection | Rapid Recovery*.

Es posible realizar una BMR para máquinas físicas o virtuales. Como ventaja añadida, Rapid Recovery le permite realizar una restauración BMR independientemente de si el hardware es igual o distinto. Una restauración BMR en Rapid Recovery separa el sistema operativo de una plataforma específica, lo que ofrece portabilidad.

Ejemplos de la realización de una BMR para hardware similar incluyen la sustitución del disco duro del sistema existente o el intercambio del servidor con errores por un equipo idéntica.

Ejemplos de la realización de una BMR para hardware diferente incluyen la restauración de un sistema con errores con un servidor producido por un fabricante diferente o con una configuración diferente. Este proceso engloba crear una imagen de CD de inicio, grabar la imagen en el disco, iniciar el servidor de destino desde la imagen de inicio, conectar con la instancia de la consola de recuperación, asignar volúmenes, iniciar la recuperación y, a continuación, supervisar el proceso. Cuando la restauración Bare Metal Restore finalice, puede continuar la tarea de carga del sistema operativo y las aplicaciones de software en el servidor restaurado, para luego establecer ajustes exclusivos necesarios para su configuración.

La restauración Bare Metal Restore no solamente se utiliza en casos de recuperación de desastres, sino también para migrar datos al actualizar o sustituir servidores.

Restauración Bare Metal Restore en máquinas Windows

Para realizar una restauración Bare Metal Restore en máquinas Windows, realice las siguientes tareas.

- Creación de una imagen de inicio de Windows. Esta imagen ISO del CD de arranque se utilizará para iniciar la unidad de destino, desde donde se puede acceder a la Universal Recovery Console (consola de recuperación universal) para comunicarse con las copias de seguridad del Core. Consulte el apartado [Descripción de la creación del CD de inicio para equipos Windows](#).
 - Si necesita soporte multimedia físico al iniciar la máquina de destino, transfiera la imagen de ISO del CD de arranque a Medios. Consulte el apartado [Transferencia de la imagen ISO del CD de inicio a soportes](#).
 - En todos los casos, debe cargar la imagen de arranque en el servidor de destino e iniciar el servidor desde la imagen de arranque. Consulte el apartado [Carga del CD de inicio e inicio del equipo de destino](#).

NOTA: Este proceso describe cómo administrar una imagen del CD de arranque desde el cuadro de diálogo Create Boot CD (Crear CD de arranque). También puede realizar estos pasos desde el Restore Machine Wizard (Asistente de restauración de máquinas), comenzando desde la página de CD de arranque del asistente. Accede a esto cuando especifica Recover (Recuperación) en cualquier máquina destino utilizando un CD de arranque desde la página Destination (Destino). Para obtener instrucciones paso a paso para administrar una imagen de arranque de Windows desde el Asistente de recuperación de máquinas como parte de una restauración Bare Metal Restore, consulte [Acerca de la restauración Bare Metal Restore con el Asistente para restaurar un equipo](#).

- Inicie una restauración Bare Metal Restore (BMR) para Windows. Una vez que la máquina de destino se inicia desde el CD de arranque, es posible iniciar la restauración BMR. Consulte el apartado [Uso de la Universal Recovery Console para una BMR](#). Conlleva las siguientes tareas:
 - Iniciar una restauración a partir de un punto de recuperación del Core. Consulte el apartado [Selección de un punto de recuperación e inicio de la BMR](#).
 - Asigne los volúmenes. Ver [Acerca de asignar discos para una restauración Bare Metal Restore](#).
 - Si realiza la restauración en un hardware diferente y el almacenamiento necesario y los controladores de red no están presentes en el CD de arranque, es posible que tenga que cargar los controladores desde un dispositivo multimedia portátil. Para obtener más información, consulte [Carga de controladores mediante la Universal Recovery Console](#).
- Realizar una restauración BMR a partir del Asistente de restauración de máquinas. De manera opcional, los procesos de administración de una imagen de arranque de Windows y para iniciar la restauración BMR, incluidos todos los subsistemas, como tareas, se puede realizar desde el Restore Machine Wizard (Asistente de restauración de máquinas). Para obtener más información sobre cómo iniciar el asistente, consulte los pasos 1 al 5 de [Restauración de volúmenes desde un punto de recuperación](#) y, a continuación, consulte [Acerca de la restauración Bare Metal Restore con el Asistente para restaurar un equipo](#).
- Comprobación de una restauración Bare Metal Restore. Después de iniciar la restauración BMR, puede verificar y supervisar el progreso. Consulte [Comprobación de una restauración Bare Metal Restore](#).
 - Puede supervisar el progreso de la restauración. Consulte el apartado [Visualización del progreso de recuperación](#).
 - Una vez completado, puede iniciar el servidor restaurado y las aplicaciones de software en el servidor. Consulte [Inicio de un servidor de destino restaurado](#).
 - Solucione los problemas del proceso de BMR. Consulte [Solución de problemas de conexiones con la Universal Recovery Console y Reparación de problemas de inicio](#).

Requisitos previos para realizar una restauración Bare Metal Restore para un equipo con Windows

Antes de que pueda empezar el proceso de realizar una restauración Bare Metal Restore para un equipo con Windows, deberá asegurarse de que se cumplen las condiciones y criterios siguientes:

- Una unidad central de procesamiento (CPU) de 64 bits. El CD de inicio de Rapid Recovery contiene el sistema operativo Win PE 5.1. Las restauraciones BMR de Rapid Recovery no son compatibles con CPU basadas en x86. Solo se pueden realizar restauraciones BMR en CPU de 64 bits.

① **NOTA:** Se trata de un nuevo requisito a partir de la versión 6.0 .

- Copias de seguridad del equipo que quiere restaurar. Debe tener un Rapid Recovery Core en funcionamiento que contenga puntos de recuperación del servidor protegido que quiera restaurar.
- Hardware que se va a restaurar (nuevo o antiguo, similar o diferente). El equipo de destino debe cumplir los requisitos de instalación para un Agent. Para obtener información detallada, consulte la Guía de instalación y actualización de Dell Data Protection | Rapid Recovery.
- Soportes y software de imagen. Debe tener un CD o DVD en blanco y software de grabación de discos, o bien software para crear una imagen ISO. Si gestiona máquinas remotamente mediante un software de Virtual Network Computing, como UltraVNC, deberá tener VNC Viewer.
- Controladores de almacenamiento y controladores de adaptador de red compatibles. Si restaura en hardware diferente, debe tener controladores de almacenamiento y controladores de adaptador de red compatibles para el equipo de destino, incluidos controladores RAID, AHCI y de chipset, según sea adecuado.
- Espacio de almacenamiento y particiones, según sea adecuado. Asegúrese de que hay suficiente espacio en el disco duro para crear particiones de destino en el equipo de destino para que contenga los volúmenes de origen. Cualquier partición de destino debería ser como mínimo igual de grande que la partición de origen original.
- Particiones compatibles. Los sistemas operativos Windows 8, Windows 8.1, Windows 10, Windows Server 2012 y Windows Server 2012 R2 que se inicien desde particiones de EFI FAT32 están disponibles para su protección o recuperación, así como volúmenes de Resilient File System (ReFS). Las particiones de UEFI se tratan como volúmenes FAT32 sencillos. Las transferencias incrementales tienen una compatibilidad y una protección completas. Rapid Recovery es compatible con sistemas UEFI para BMR, incluida la partición automática de discos GPT.

Acerca de la restauración Bare Metal Restore con el Asistente para restaurar un equipo

La administración de una imagen de inicio de Windows mediante el asistente conlleva las siguientes acciones:

- Iniciar la creación del CD de inicio.
- Definir la ruta de acceso para la imagen en el equipo Core.
- Seleccionar el entorno de recuperación adecuado para el hardware en el que se desea restaurar.
- Opcionalmente, definir parámetros de conexión del agente restaurado para usar la red o UltraVNC.
- Opcionalmente, insertar controladores para el hardware en el que se desea restaurar.
- Opcionalmente, transferir la imagen de inicio a medios físicos.
- Iniciar el equipo en el que se desean restaurar los datos del CD.
- Conectar con la Consola de recuperación universal.
- Asignar volúmenes.
- Iniciar la restauración Bare Metal Restore desde el punto de recuperación seleccionado en el Core.

① **NOTA:** Este proceso describe cómo administrar una imagen de CD de inicio desde el Asistente para restaurar un equipo, como parte del proceso de realización de una BMR empleando ese asistente. También puede administrar una imagen de inicio desde el cuadro de diálogo Crear CD de inicio. Para obtener información sobre la administración de una imagen de CD de inicio fuera del Asistente para restaurar un equipo, consulte [Descripción de la creación del CD de inicio para equipos Windows](#).

Restauración Bare Metal Restore con el Asistente para restaurar un equipo

Puede utilizar el asistente de restauración para crear un CD de inicio y para realizar una restauración Bare Metal Restore (BMR).

Antes de realizar una BMR, consulte [Requisitos previos para realizar una restauración Bare Metal Restore para un equipo con Windows](#) o [Requisitos previos para realizar una restauración Bare Metal Restore para un equipo Linux](#), según proceda. Si está iniciando su BMR en un equipo con Windows desde la Core Console, consulte [Restauración Bare Metal Restore en máquinas Windows](#).

El equipo protegido debe tener el software agente instalado y puntos de recuperación desde los que realizar la operación de restauración.

- 1 Para restaurar un volumen en un equipo protegido, desplácese hasta la Core Console y haga clic en **Restaurar** en la barra de botones de Rapid Recovery.
Aparecerá el Asistente para restaurar un equipo.
- 2 En la página Equipos, seleccione el equipo protegido que desea restaurar y, a continuación, haga clic en **Siguiente**.
Aparecerá la página Puntos de recuperación.
- 3 Seleccione el punto de recuperación que desea utilizar para restaurar el equipo.
 - Opcionalmente, si desea limitar el número de puntos de recuperación que se muestra, puede filtrar por volúmenes (si está definido) o por fecha de creación del punto de recuperación. También puede buscar un punto de recuperación concreto.
- 4 Haga clic en **Siguiente**.
- 5 En la página Destino, seleccione **Recuperar en cualquier equipo de destino mediante un CD de inicio**.
 - Si todavía no ha cargado un CD de inicio en el equipo que desea restaurar, haga clic en **Siguiente** y, a continuación, continúe con el [paso 6](#).
 - Si ya ha cargado un CD de inicio en el equipo de destino de la BMR, seleccione **Ya tengo un CD de inicio ejecutándose en el equipo de destino**, haga clic en **Siguiente** y, a continuación, vaya al [paso 16](#).
- 6 En la página CD de inicio, en el cuadro Ruta de salida, escriba la ruta de acceso en la que debe almacenarse la imagen ISO del CD de inicio.

NOTA: Si en la unidad compartida en la que desea almacenar la imagen hay poco espacio, puede crear un disco en la ruta de acceso según sea necesario, por ejemplo, F:\filename.iso.

NOTA: La extensión del archivo debe ser .iso. Cuando especifique la ruta de acceso, utilice solamente caracteres alfanuméricos, el guión, la barra diagonal inversa (solamente como delimitador de ruta de acceso) y el punto (solamente para separar nombres de host y dominios). Las letras de la a la z no distinguen entre mayúsculas y minúsculas. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.

- 7 Opcionalmente, para configurar parámetros de red para el equipo de destino o agregar capacidades de UltraVNC, seleccione **Mostrar opciones avanzadas** y realice las siguientes acciones:
 - Para establecer una conexión de red con el destino de la BMR, seleccione **Utilizar la siguiente dirección IP** y, a continuación, especifique la información que se describe en la tabla siguiente.

Tabla 153. Opciones de Conexión de red

Opción	Descripción
Dirección IP	Dirección IP del equipo restaurado.
Máscara de subred	Máscara de subred del equipo restaurado.
Puerta de enlace predeterminada	Especifique la puerta de enlace predeterminada para el equipo restaurado.
Servidor DNS	Especifique el servidor de nombre de dominio para el equipo restaurado.

- Si tiene una cuenta UltraVNC y desea usarla para llevar a cabo la BMR, seleccione **Agregar UltraVNC** y, a continuación, especifique la información que se describe en la tabla siguiente.

Tabla 154. Credenciales de conexión de UltraVNC

Opción	Descripción
Contraseña	Contraseña de su cuenta UltraVNC.
Puerto	Puerto que desea usar para conectarse al destino de la BMR. El puerto predeterminado es 5900.

- 8 Haga clic en **Siguiente**.

- 9
- Para establecer una conexión de red para el equipo restaurado, seleccione **Utilizar la dirección IP siguiente** como se describe en la tabla siguiente.
 - Para definir la información de UltraVNC, seleccione **Agregar UltraVNC** como se describe en la tabla siguiente.
- Utilice esta opción si requiere un acceso remoto en la consola de recuperación. No puede iniciar sesión mediante Microsoft Terminal Services mientras utilice el CD de inicio.

Tabla 155. Conexión UltraVNC

Opción	Descripción
Contraseña	Especifique una contraseña para esta conexión de UltraVNC.
Puerto	Especifique un puerto para esta conexión de UltraVNC. El puerto predeterminado es 5900.

- 10 Cuando esté satisfecho con sus selecciones en la página CD de inicio, haga clic en **Siguiente**.
- 11 Opcionalmente, en la página Inyección de controlador, si tiene pensado restaurar en hardware distinto, inserte los controladores de almacenamiento y demás controladores necesarios para el sistema de destino mediante los siguientes pasos:
- Descargue los controladores desde el sitio web del fabricante del servidor y descompríalos.
 - Comprima cada controlador en un archivo .zip mediante una utilidad de compresión adecuada (por ejemplo, WinZip).
 - En la página Inyección de controlador del Asistente para restaurar un equipo, haga clic en **Agregar un archivo comprimido de controladores**.
 - Desplácese por el sistema de archivos hasta el archivo del controlador comprimido, selecciónelo y, a continuación, haga clic en **Abrir**.
 - Repita los [pasos c y d](#), como corresponda, hasta que haya insertado todos los controladores necesarios.
- Para obtener más información sobre inyección de controladores, consulte [Descripción de la inyección de controladores en un CD de inicio](#).

NOTA: No todas las versiones de Windows admiten la inyección automática de controladores. Si el sistema operativo no la admite, guarde los controladores de forma manual en C:\Program Files\AppRecovery\Core\BootCdKit\Drivers\.

Rapid Recovery crea la imagen ISO del CD de inicio.

- 12 Haga clic en **Siguiente**.
- 13 Inicie el equipo de destino de la BMR y, a continuación, realice una de las acciones siguientes:
- Si puede iniciar el equipo de destino desde la imagen ISO del CD de inicio, hágalo ahora.
 - Si no puede hacerlo, copie la imagen ISO en un soporte físico (un CD o DVD), introduzca el disco en el equipo de destino, configure el equipo para que se inicie desde el CD de inicio y reinicielo desde el CD.

NOTA: Puede que tenga que cambiar la configuración de BIOS del equipo de destino para asegurarse de que el volumen que se carga primero es el CD de inicio.

El equipo de destino, cuando se inicia desde el CD de inicio, muestra la interfaz de la Consola de recuperación universal (URC). Este entorno se utiliza para restaurar la unidad del sistema o volúmenes seleccionados directamente desde el Rapid Recovery Core. Anote la dirección IP y las credenciales de clave de autenticación de la URC, que se actualizan cada vez que inicia desde el CD de inicio.

- 14 En la página Conexión del Asistente para restaurar un equipo, en la Core Console, introduzca la información de autenticación de la instancia de la URC del equipo que quiera restaurar, de la manera siguiente:

Tabla 156. Opciones de autenticación

Opción	Descripción
Dirección IP	Dirección IP que se proporciona en la URC en la máquina de destino.
Clave de autenticación	Clave de autenticación que se proporciona en la URC en la máquina de destino.

- 15 Haga clic en **Siguiente**.

- 16 En la página Asignación de discos, si desea asignar volúmenes manualmente, vaya al [paso 10](#). Si desea asignar volúmenes automáticamente, realice los pasos siguientes:
- a En el menú desplegable Asignación de volúmenes, seleccione **Automático**.
 - b En la lista de volúmenes, asegúrese de que los volúmenes que desea restaurar están seleccionados. Todos los volúmenes están seleccionados de forma predeterminada.
Si no desea restaurar un volumen de la lista, desactive la opción.
- NOTA:** Se debe seleccionar al menos un volumen para realizar la restauración.
- c En el lado derecho, seleccione el disco de destino para la restauración.
 - d Haga clic en **Siguiente**.
 - e En la página Vista previa de asignación de discos, revise los parámetros de las acciones de restauración que seleccionó.
 - f Vaya al [paso 18](#).
- 17 Para asignar volúmenes manualmente, en la página Asignación de discos, realice los pasos siguientes:
- a En el menú desplegable Asignación de volúmenes, seleccione **Manual**.
 - b En la columna Destino, seleccione un volumen de destino que desea restaurar. Opcionalmente, si no desea restaurar un volumen enumerado, cancele la selección de la opción.
- NOTA:** Se debe seleccionar al menos un volumen para realizar la restauración.
- 18 Haga clic en **Finalizar**.
- PRECAUCIÓN:** Todas las particiones y los datos de la unidad de destino se eliminarán de manera permanente, y se reemplazarán por el contenido del punto de recuperación seleccionado, incluidos el sistema operativo y todos los datos.
- 19 Si los volúmenes que quiere restaurar contienen bases de datos de SQL o Microsoft Exchange y si está realizando una restauración en vivo, en la página Desmontar bases de datos, se le pedirá que las desmonte. Opcionalmente, si desea volver a montar estas bases de datos después de que la restauración se haya completado, seleccione **Volver a montar todas las bases de datos automáticamente después de que se haya restaurado el punto de recuperación**.
- 20 Haga clic en **Restore** (Restaurar).
- 21 En el mensaje de estado, haga clic en **Aceptar** para confirmar que el proceso de restauración ha empezado.
Comienza la restauración. Puede ver el progreso en la página Eventos. Para obtener más información, consulte [Visualización de eventos mediante las tareas, las alertas y el diario](#).

Descripción de la creación del CD de inicio para equipos Windows

Una restauración Bare Metal Restore para Windows requiere una imagen de inicio denominada CD de inicio, que se crea definiendo parámetros en la Rapid Recovery Core Console. Esta imagen está adaptada a sus necesidades específicas. Utilizará la imagen para iniciar el equipo con Windows de destino. Basándose en las características específicas de su entorno, puede que necesite transferir esta imagen a un soporte físico, como un CD o DVD. A continuación, deberá cargar virtual o físicamente la imagen de inicio e iniciar el servidor Windows desde la imagen de inicio.

El primer paso al realizar una restauración Bare Metal Restore (BMR) para un equipo Windows es crear el archivo del CD de inicio en la Rapid Recovery Core Console. Se trata de una imagen ISO de inicio que contiene la interfaz de Rapid Recovery Consola de recuperación universal (URC), un entorno que se utiliza para restaurar la unidad del sistema o todo el servidor directamente desde el Rapid Recovery Core.

La imagen ISO del CD de inicio que cree está personalizada para la máquina que se restaura; por lo tanto, debe contener los controladores correctos de red y almacenamiento masivo. Si anticipa que va a restaurar en hardware diferente del del equipo en el que se originó el punto de recuperación, deberá incluir una controladora de almacenamiento y otros controladores en el CD de inicio. Para obtener información sobre cómo insertar esos controladores en el CD de inicio, consulte [Descripción de la inyección de controladores en un CD de inicio](#).

Descripción de la inyección de controladores en un CD de inicio

La imagen del CD de inicio requiere que los controladores de almacenamiento reconozcan las unidades del servidor y los controladores de adaptador de red para comunicarse con el Rapid Recovery Core a través de la red.

Un conjunto genérico de controladores de controlador de almacenamiento y adaptador de red de Windows 8.1 x64 se incluye automáticamente al generar un CD de inicio para Windows. Esto satisface los requisitos de los sistemas Dell más recientes. Los sistemas de otros fabricantes o sistemas Dell más antiguos pueden requerir que inserte controladores de controladora de almacenamiento o adaptador de red al crear el CD de inicio. Si detecta que el CD de inicio que creó no contiene los controladores necesarios para realizar la restauración, también puede cargar controladores en el equipo de destino mediante la URC. Para obtener más información, consulte [Carga de controladores mediante la Universal Recovery Console](#).

Cuando se está creando el CD de inicio, la inyección de controlador se utiliza para facilitar la operabilidad entre la consola de recuperación, el adaptador de red y el almacenamiento en el servidor de destino.

Los datos restaurados desde el punto de recuperación incluyen controladores para el hardware ya existente. Si está realizando una restauración Bare Metal Restore en hardware diferente, también debe insertar controladores de controladora de almacenamiento en el sistema operativo que se está restaurando mediante la URC después de que se hayan restaurado los datos en la unidad. Esto permite que el sistema operativo restaurado se inicie mediante el nuevo conjunto de hardware. Después de que el sistema operativo se inicie tras la restauración, podrá descargar e instalar los controladores adicionales que necesite el sistema operativo para interactuar con su nuevo hardware.

Creación de una imagen ISO de un CD de inicio

CD de inicio es el término que Rapid Recovery utiliza para referirse a la ubicación de almacenamiento portátil de la imagen ISO reservada para realizar una restauración Bare Metal Restore (BMR). La imagen incluye la Consola de recuperación universal (URC) de Rapid Recovery.

Para realizar una restauración BMR en un equipo, debe iniciar el equipo desde el CD de inicio, lo que abre la consola. La consola es lo que permite conectar el destino de la restauración BMR en la ubicación del punto de recuperación que desea utilizar para llevar a cabo la restauración.

- 1 Desde la Rapid Recovery Core Console en la que está protegido el servidor que va a restaurar, en la barra de iconos, haga clic en el menú Más y, a continuación, haga clic en **CD de inicio**.
- 2 En la página de CD de inicio, haga clic en **CD de inicio**.
Se abrirá el cuadro de diálogo Crear CD de inicio.
- 3 En el cuadro de diálogo Crear CD de inicio, en el cuadro de texto **Ruta de salida**, introduzca la ruta de acceso en la que quiera almacenar la imagen ISO del CD de inicio.

NOTA: La extensión del archivo debe ser **.iso**. Cuando especifique la ruta de acceso, utilice solamente caracteres alfanuméricos, el guión, la barra diagonal inversa (solamente como delimitador de ruta de acceso) y el punto (solamente para separar nombres de host y dominios). En las letras de la a a la z no se distingue entre mayúsculas y minúsculas. No utilice espacios. No se permiten otros símbolos o caracteres de puntuación.

- 4 En Opciones de conexión, realice una de las acciones siguientes:
 - Para obtener la dirección IP dinámicamente mediante el protocolo Dynamic Host Configuration Protocol (DHCP), seleccione **Obtener dirección IP automáticamente**.
 - Para especificar una dirección IP estática para la URC, seleccione **Utilizar la siguiente dirección IP** y, a continuación, especifique la siguiente información:
 - Dirección IP
 - Máscara de subred
 - Puerta de enlace predeterminada
 - Servidor DNS

❗ **NOTA:** Debe especificar estos cuatro campos.

- 5 Si necesita acceso remoto a la consola de recuperación y tiene UltraVNC instalado, en Opciones de UltraVNC, realice los pasos siguientes:

❗ **NOTA:** UltraVNC permite administrar la URC de forma remota mientras está en uso. No puede iniciar sesión mediante Microsoft Terminal Services mientras utilice el CD de inicio.

- a Seleccione **Agregar UltraVNC**.
- b Introduzca su **Contraseña de UltraVNC**.
- c Introduzca el **Puerto de UltraVNC**. El puerto predeterminado es 5900.

❗ **NOTA:** Las opciones de UltraVNC solo están disponibles si ya tiene UltraVNC instalado. Para hacer que estas opciones estén disponibles, vaya a <http://www.uvnc.com/downloads/ultravnc/> para descargar UltraVNC versión 1.0.9.1 o posterior para arquitectura x64. Realice la instalación y guarde el archivo winvnc.exe en C:\Program Files\AppRecovery\Core\BootCdKit\UltraVnc_x64\.

- 6 Si tiene pensado restaurar en hardware distinto, insertar los controladores de almacenamiento y demás controladores necesarios para el sistema de destino mediante los siguientes pasos:

❗ **NOTA:** No todas las versiones de Windows admiten la inserción automática de controladores. Si el sistema operativo no la admite, guarde los controladores de forma manual en C:\Program Files\AppRecovery\Core\BootCdKit\Drivers\.

- a Descargue los controladores desde el sitio web del fabricante del servidor y descompríalos.
- b Comprima cada controlador en un archivo .zip mediante una utilidad de compresión adecuada (por ejemplo, WinZip).
- c En el cuadro de diálogo Crear CD de inicio, en el panel Controladores, haga clic en **Agregar un archivo comprimido de controladores**.
- d Desplácese por el sistema de archivos hasta el archivo del controlador comprimido, selecciónelo y, a continuación, haga clic en **Abrir**.
El archivo de controlador aparece en el panel Controladores del cuadro de diálogo Crear CD de arranque.
- e Repita los [pasos c y d](#), como corresponda, hasta que haya agregado todos los controladores necesarios.
- f En el panel Controladores, seleccione los controladores que quiere insertar.

Para obtener más información acerca de la inserción de controladores, consulte [Descripción de la inyección de controladores en un CD de inicio](#)

- 7 Haga clic en **Crear CD de arranque**.

Rapid Recovery crea el CD de inicio y lo guarda con el nombre de archivo que se ha proporcionado.

- 8 Para supervisar el progreso de esta tarea, vaya a la barra de iconos y haga clic en el icono de eventos.

Para obtener más información sobre cómo supervisar eventos de Rapid Recovery, consulte [Visualización de eventos mediante las tareas, las alertas y el diario](#).

Cuando termina la creación de la imagen ISO, aparece un registro de la imagen en la página de CD de inicio, a la que puede tener acceso desde el menú Más de la barra de iconos.

Para acceder a la imagen ISO, vaya a la ruta de salida que ha especificado, o bien haga clic en el enlace de la página de CD de inicio para descargar la imagen en una ubicación desde la que pueda cargarla en el nuevo sistema, por ejemplo, una unidad de red.

Transferencia de la imagen ISO del CD de inicio a soportes

Cuando cree el archivo del CD de inicio, se almacenará como imagen ISO en la ruta de acceso que especificó. Debe poder montar esta imagen como unidad en el servidor en el que esté realizando una restauración Bare Metal Restore.

Puede grabar la imagen ISO del CD de inicio en un disco compacto (CD) o disco de vídeo digital (DVD) accesible desde el arranque del sistema.

Cuando inicie la máquina desde el CD de inicio, la Universal Recovery Console se iniciará automáticamente.

Si realiza una BMR en una máquina virtual, este paso no es obligatorio. Sencillamente cargue la imagen ISO en una unidad y edite la configuración de esa máquina virtual para que se inicie desde esa unidad.

Carga del CD de inicio e inicio del equipo de destino

Cuando haya creado la imagen del CD de inicio, tendrá que iniciar el servidor de destino con el CD de inicio que acaba de crear.

Para conectarse a la Rapid Recovery Core Console o usar Chromium para descargar controladores adicionales, primero debe cargar una controladora Ethernet y un adaptador de red. Para obtener más información, consulte [Carga de controladores mediante la Universal Recovery Console](#).

❗ NOTA: Si ha creado el CD de inicio con DHCP, tendrá que capturar la dirección IP y la contraseña.

- 1 En el nuevo servidor, cargue la imagen del CD de inicio desde la ubicación adecuada y, a continuación, inicie el servidor desde la imagen del CD de inicio para cargar el software Rapid Recovery Agent y Win PE 5.1.
El equipo de destino muestra una pantalla azul de Dell con tres botones de icono en la parte superior de la pantalla.
- 2 Para abrir la interfaz de usuario de Universal Recovery Console de Rapid Recovery, haga clic en el icono de Dell en la parte superior de la pantalla.
La dirección IP y la contraseña del equipo aparecen bajo autenticación.

❗ NOTA: Se generará una nueva contraseña temporal cada vez que la máquina se inicie con el CD de inicio. Anote la dirección IP que aparece en el panel Configuración de adaptadores de red y la contraseña de autenticación que aparece en el panel Autenticación. Necesitará esta información posteriormente, durante el proceso de recuperación de datos para volver a iniciar sesión en la consola.

❗ NOTA: Si no se ha proporcionado ninguna dirección IP, cargue la controladora Ethernet y el adaptador de red.

- 3 Si desea cambiar la dirección IP, selecciónela y haga clic en **Cambiar**.

❗ NOTA: Si especificó una dirección IP en el cuadro de diálogo Crear CD de inicio, la Universal Recovery Console la utiliza y la muestra en la pantalla Configuración de adaptadores de red.

El sistema está preparado para que pueda conectarse al Core, seleccionar un punto de recuperación, y continuar con el proceso de restauración bare metal restore.

Uso de la Universal Recovery Console para una BMR

Antes de iniciar una restauración Bare Metal Restore (BMR) para un equipo con Windows, es preciso que se den las siguientes condiciones:

- Para restaurar un punto de recuperación guardado en el Core, debe contar ya con el hardware adecuado. Para obtener más información, consulte [Requisitos previos para realizar una restauración Bare Metal Restore para un equipo con Windows](#).
- El equipo con Windows de destino para la BMR debe iniciarse mediante la imagen del CD de inicio. Para obtener más información, consulte [Descripción de la creación del CD de inicio para equipos Windows](#).

Una restauración Bare Metal Restore BMR inicia un equipo mediante un punto de recuperación seleccionado. El punto de recuperación incluye controladores del hardware anterior. Si está realizando una restauración en hardware diferente, debe insertar controladores de controlador de almacenamiento en el sistema operativo que se está restaurando mediante la URC después de que se hayan restaurado los datos en la unidad. Esto permite que el sistema operativo restaurado se inicie mediante el nuevo conjunto de hardware. Después de que se inicie el sistema operativo, puede descargar e instalar los controladores adicionales que necesita el sistema operativo para interactuar con el nuevo hardware.

Para iniciar una restauración BMR desde la Rapid Recovery Core Console, realice las tareas siguientes.

- [Selección de un punto de recuperación e inicio de la BMR](#)
- [Acerca de asignar discos para una restauración Bare Metal Restore](#)

- [Carga de controladores mediante la Universal Recovery Console](#)

Este proceso es un paso en [Restauración Bare Metal Restore en máquinas Windows](#).

Acerca de las herramientas de Universal Recovery Console

Universal Recovery Console (URC) incluye el acceso a las herramientas que pueden ayudarle a completar una restauración bare metal restore (BMR).

Puede encontrar las siguientes herramientas haciendo clic en el icono central de la parte superior de la pantalla de presentación de Dell en un destino de BMR que se inicia en la URC.

- **Far Manager.** Esta herramienta es similar al Explorador de Windows. Proporciona una forma de navegar por los archivos del servidor hasta que haya finalizado la BMR e instalado un sistema operativo con su propia función de navegación, como el Explorador de Windows.
- **Chromium.** Este explorador es la base de código abierto base para Google Chrome™ y le permite navegar por Internet en un servidor que tenga una controladora de red cargada a través de la URC.
- **PuTTY.** Esta herramienta es un emulador de terminal de código abierto. En el contexto de una Rapid Recovery BMR, le permite conectarse a un dispositivo de almacenamiento NAS que no incluya una interfaz de usuario. Esta capacidad es posible que sea necesaria si desea realizar una restauración a partir de un archivo y el archivo se encuentra en un NAS.
- **Notepad.** Como en el sistema operativo Windows, esta herramienta le permite escribir notas sin formato y visualizar archivos de registro.
- **Administrador de tareas.** Como en el sistema operativo Windows, esta herramienta le permite administrar los procesos y supervisar el rendimiento del servidor mientras la restauración está en curso.
- **Editor de registros** Como en el sistema operativo Windows, esta herramienta le permite cambiar el registro del sistema del destino de BMR.
- **Símbolo del sistema.** Esta herramienta le permite ejecutar comandos en el destino de BMR fuera de la URC hasta que instale una interfaz de usuario.

Carga de controladores mediante la Universal Recovery Console

Esta función le permite agregar los controladores que no se incluyeron en la imagen ISO pero que son necesarios para una restauración Bare Metal Restore correcta.

Esta tarea es un paso en [Restauración Bare Metal Restore en máquinas Windows](#). Forma parte del proceso para [Uso de la Universal Recovery Console para una BMR](#).

Al crear un CD de inicio, puede agregar los controladores necesarios a la imagen ISO. Después de iniciar el equipo de destino, también puede cargar controladores de almacenamiento o red desde la Universal Recovery Console (URC).

Si está restaurando en hardware diferente, debe insertar controladores de controlador de almacenamiento, RAID, AHCI, de chipset y de otro tipo si no están ya en el CD de inicio. Estos controladores permiten que el sistema operativo haga que todos los dispositivos funcionen correctamente en el servidor de destino una vez que haya reiniciado el sistema tras el proceso de restauración.

Realice los pasos del procedimiento siguiente para cargar controladores mediante la URC.

- [Carga de controladores en la Consola de recuperación universal mediante multimedia portátiles](#)
- [Cómo cargar una controladora en la URC con Chromium](#)

Carga de controladores en la Consola de recuperación universal mediante multimedia portátiles

Este procedimiento tiene los siguientes requisitos previos.

- [Creación de una imagen ISO de un CD de inicio](#)
- [Transferencia de la imagen ISO del CD de inicio a soportes](#)

- [Carga del CD de inicio e inicio del equipo de destino](#)

Lleve a cabo el siguiente procedimiento para utilizar un dispositivo multimedia portátil para cargar controladores en la Consola de recuperación universal (URC).

- 1 En un equipo con conexión a Internet, descargue los controladores del sitio web del fabricante para el servidor y descomprímalos.
- 2 Comprima cada controlador en un archivo .zip mediante una utilidad de compresión adecuada (por ejemplo, WinZip).
- 3 Copie y guarde el archivo .zip de controladores en un dispositivo multimedia portátil, por ejemplo, una unidad USB.
- 4 Quite el soporte del equipo conectado e insértelo en el servidor de destino de inicio.
- 5 En el servidor de destino, cargue el CD de inicio e inicie el equipo.
Aparece la pantalla de presentación de Dell.
- 6 Para iniciar la URC, haga clic en el **icono de Dell**.
La URC se abre en la pestaña del administrador de controladores de CD de inicio.
- 7 Expanda la lista **Otros dispositivos**.
La lista muestra los controladores necesarios para el hardware pero no están en el CD de inicio
- 8 Haga clic con el botón derecho en un controlador de la lista y, a continuación, haga clic en **Cargar controlador**.
- 9 En la ventana Seleccionar modo de carga del controlador, seleccione una de las siguientes opciones:
 - Cargar paquete de único controlador (el controlador se cargará sin verificación para la compatibilidad de dispositivos)
 - Buscar paquetes de controlador en la carpeta (se buscarán controladores para el dispositivo seleccionado en la carpeta seleccionada)
- 10 Expandir la unidad del dispositivo multimedia portátil, seleccione el controlador (con la extensión de archivo .inf) y, a continuación, haga clic en **Aceptar**.
El controlador se carga en el sistema operativo actual.
- 11 En la ventana Información, haga clic en **Aceptar** para confirmar que el controlador se ha cargado correctamente.
- 12 Repita esta acción las veces que sea necesario para cada controlador que desee cargar.

Cómo cargar una controladora en la URC con Chromium

Este procedimiento tiene los siguientes requisitos previos.

- [Creación de una imagen ISO de un CD de inicio](#)
- [Transferencia de la imagen ISO del CD de inicio a soportes](#)
- [Carga del CD de inicio e inicio del equipo de destino](#)

Lleve a cabo el siguiente procedimiento para utilizar el explorador Chromium que viene instalado en el CD de inicio para cargar controladoras mientras está en la URC.

- 1 En el servidor de destino, cargue el CD de inicio e inicie el equipo.
Aparece la pantalla de presentación de Dell.
- 2 Para iniciar la URC, haga clic en el **icono de Dell**.
La URC se abre en la pestaña del administrador de controladores de CD de inicio.
- 3 En el destino de BMR, haga clic en las herramientas (icono central) en la parte superior de la pantalla y, a continuación, haga clic en **Chromium**.
- 4 En el explorador Chromium, vaya a un sitio web donde pueda descargar los controladores necesarios.
- 5 Descargue el controlador o controladores en la ubicación que desee, como una carpeta local o un recurso compartido de archivo de red.
- 6 Expandir la lista **Otros dispositivos**.
La lista muestra los controladores necesarios para el hardware pero no están en el CD de inicio
- 7 Haga clic con el botón derecho en un controlador de la lista y, a continuación, haga clic en **Cargar controlador**.
- 8 En la ventana Seleccionar modo de carga del controlador, seleccione una de las siguientes opciones:
 - Cargar paquete de único controlador (el controlador se carga sin verificación para la compatibilidad de dispositivos)
 - Buscar paquetes de controlador en la carpeta (se buscan controladores para el dispositivo seleccionado en la carpeta seleccionada)

- 9 Navegue a la ubicación en la que guardó el controlador, seleccione el controlador y, a continuación, haga clic en **Aceptar**.
El controlador se carga en el sistema operativo actual.
- 10 En la ventana Información, haga clic en **Aceptar** para confirmar que el controlador se ha cargado correctamente.
- 11 Repita esta acción las veces que sea necesario para cada controlador que desee cargar.

Selección de un punto de recuperación e inicio de la BMR

Una vez que se puede acceder a la Universal Recovery Console en el equipo de destino de bare metal restore (BMR), debe seleccionar el punto de recuperación que desea restaurar.

Desplácese hasta la Core Console para seleccionar qué punto de recuperación quiere cargar y, a continuación, designe la consola de recuperación como el destino para los datos restaurados.

① NOTA: Este paso es obligatorio para realizar una BMR en todos los equipos con Windows y opcional para realizar una BMR en las máquinas con Linux.

Esta tarea es un paso en [Restauración Bare Metal Restore en máquinas Windows](#). Forma parte del proceso para [Uso de la Universal Recovery Console para una BMR](#).

Si está realizando una BMR para un equipo con Linux desde la Core Console, esta tarea también es un paso de [Realización de una restauración Bare Metal Restore para Linux](#). Forma parte del proceso de [Inicio de una restauración Bare Metal Restore para un equipo Linux mediante la línea de comandos](#).

- 1 En la Rapid Recovery Core Console, en la lista de equipos protegidos, haga clic en el nombre del equipo protegido que desee restaurar.
Aparecerá la página Resumen del equipo seleccionado.
- 2 Haga clic en **Puntos de recuperación**.
- 3 Haga clic en el menú desplegable que hay junto al punto de recuperación que desea utilizar para BMR y, a continuación, haga clic en **Restaurar**.
Aparecerá el Asistente para restaurar un equipo.
- 4 Seleccione **Recuperar en cualquier equipo de destino mediante un CD de inicio**.
- 5 Seleccione **Ya tengo un CD de inicio ejecutándose en el equipo de destino**.
Los campos de texto de autenticación aparecen.
- 6 Introduzca la información sobre el equipo que quiera restaurar según se describe en la tabla siguiente.

Tabla 157. Información del equipo de destino

Cuadro de texto	Descripción
Dirección IP	Dirección IP del equipo que desea restaurar. Esta es idéntica a la dirección IP mostrada en la URC.
Clave de autenticación	Contraseña específica con la que conectarse al servidor seleccionado. Esta es idéntica a la clave de autenticación mostrada en la URC.

- 7 Haga clic en **Siguiente**.
Si la información de conexión que introdujo coincide con la URC y si el Core y el servidor de destino pueden identificarse entre sí adecuadamente en la red, se cargarán los volúmenes para el punto de recuperación seleccionado y aparecerá la página Asignación de discos. En este caso, el siguiente paso es asignar volúmenes.
- 8 Continúe con [Acerca de asignar discos para una restauración Bare Metal Restore](#) para obtener más información acerca de las opciones de asignación de disco.

Acerca de asignar discos para una restauración Bare Metal Restore

Una vez conectado a la Universal Recovery Console, debe asignar volúmenes entre los indicados en el punto de recuperación y los volúmenes existentes en el hardware de destino.

Rapid Recovery intenta asignar volúmenes automáticamente. Si acepta la asignación predeterminada, el disco del equipo de destino se borrará y volverá a particionar, y todos los datos ya existentes se eliminarán. La alineación se realizará en el orden en que se enumeran los volúmenes en el punto de recuperación y los volúmenes se asignarán a los discos adecuadamente según su tamaño, etc. Suponiendo que haya suficiente espacio en la unidad de destino, no se necesitará ninguna partición al utilizar la alineación de discos automática. Recuerde que un disco se puede utilizar en varios volúmenes. Si asigna manualmente las unidades, recuerde que no puede utilizar el mismo disco dos veces.

Para la asignación manual, el nuevo equipo debe estar formateado correctamente antes de restaurarlo. El equipo de destino debe tener una partición separada para cada volumen en el punto de recuperación, incluido el volumen reservado para el sistema. Para obtener más información, consulte [Uso de la Universal Recovery Console para una BMR](#).

Realice el procedimiento para una de las siguientes opciones de asignación de disco:

- [Asignar discos virtuales a una restauración BMR automáticamente](#)
- [Asignar discos virtuales a una restauración BMR manualmente](#)

⚠ PRECAUCIÓN: Si bien Rapid Recovery admite particiones FAT32 y ReFS, en la actualidad, solamente se admiten la restauración completa y la BMR, dado que existe una limitación de controlador con ReFS, por lo que la restauración se implementa en modo de usuario, exportación de máquina virtual, etc. Si un Core está protegiendo al menos un volumen agente con el sistema de archivos ReFS, debería instalarse en equipos con Windows 8, Windows 8.1, Windows 10, Windows Server 2012 y Windows Server 2012 R2, ya que proporcionan compatibilidad nativa con ReFS. Si no es así, las funciones están limitadas y las operaciones de tipo montaje de una imagen de volumen no funcionan. La Core Console de Rapid Recovery presenta los mensajes de error pertinentes en estas apariciones.

⚠ PRECAUCIÓN: La restauración Bare Metal Restore de la configuración de discos de espacios de almacenamiento (una función de Windows 8.1) tampoco se admite. Para obtener más detalles, consulte la *Installation and Upgrade Guide* (Guía de instalación y actualización) de *Dell Data Protection | Rapid Recovery*.

Esta tarea es un paso en [Restauración Bare Metal Restore en máquinas Windows](#). Forma parte del proceso para [Uso de la Universal Recovery Console para una BMR](#).

Si está realizando una BMR para un equipo con Linux desde la Core Console, esta tarea también es un paso de [Realización de una restauración Bare Metal Restore para Linux](#). Forma parte del proceso para [Inicio de una restauración Bare Metal Restore para Linux](#).

Asignar discos virtuales a una restauración BMR automáticamente

Este procedimiento permite asignar automáticamente los discos durante una restauración bare metal restore (BMR) mediante el asistente Restore Wizard.

Realice los pasos del siguiente procedimiento para seleccionar automáticamente los volúmenes que desea recuperar y dónde restaurarlos.

- 1 En la página Asignación de discos del Asistente para restaurar un equipo, al lado de Asignación de volúmenes, seleccione **Automático** en el menú desplegable.
- 2 En la tabla de la izquierda, compruebe que los volúmenes adecuados se enumeran y están seleccionados.

i NOTA: Normalmente, en el caso de una BMR, debería restaurar como mínimo el volumen reservado para el sistema y el volumen del sistema (por lo general, pero no siempre, el volumen C:\). Debe seleccionar al menos un volumen para realizar una restauración BMR.

- 3 En la tabla de la derecha, seleccione el disco o discos a los que desea asignar volúmenes en el equipo de destino.
- 4 Haga clic en **Siguiente**.
- 5 En la página Vista previa de asignación, revise la asignación de los volúmenes de punto de recuperación y el volumen de destino de la restauración.

- 6 Para comenzar la restauración, haga clic en **Finalizar**.

PRECAUCIÓN: Si selecciona **Iniciar restauración**, todas las particiones y datos de la unidad de destino se eliminarán de manera permanente, y se reemplazarán por el contenido del punto de recuperación seleccionado, incluido el sistema operativo y los datos.

Asignar discos virtuales a una restauración BMR manualmente

Este procedimiento describe cómo designar qué discos deben almacenarse en qué ubicaciones del equipo restaurado.

Para asignar discos manualmente, primero debe usar DiskPart en la línea de comandos en el equipo de destino de la restauración BMR para crear volúmenes de destino y aplicarles formato. Para obtener más información, consulte la información sobre [opciones de línea de comandos de DiskPart \(Standard 7 SP1\)](#) en Microsoft Developer Network.

Realice los pasos del siguiente procedimiento para seleccionar manualmente los volúmenes que desea recuperar y dónde restaurarlos.

- 1 En la página Asignación de discos del Asistente para restaurar un equipo, al lado de Asignación de volúmenes, seleccione **Manual** en el menú desplegable.

NOTA: Si no hay volúmenes en la unidad del equipo en el que está realizando una restauración Bare Metal Restore (BMR), no verá esta opción ni podrá asignar volúmenes manualmente.

- 2 En el área Asignación de volúmenes, bajo Volumen de origen, verifique que el volumen de origen esté seleccionado y que los volúmenes adecuados se enumeren debajo del mismo y estén seleccionados.
- 3 En Destino, desde el menú desplegable, seleccione el destino adecuado que sea el volumen de destino en el que realizar la restauración BMR del punto de recuperación seleccionado y, a continuación, haga clic en **Restaurar**.
- 4 En el cuadro de diálogo de confirmación, revise la asignación del origen del punto de recuperación y el volumen de destino para la restauración.
- 5 Para iniciar la restauración, haga clic en **Iniciar restauración**.

PRECAUCIÓN: Si selecciona **Comenzar restauración**, todas las particiones y los datos existentes de la unidad de destino se quitarán permanentemente y se sustituirán por el contenido del punto de recuperación seleccionado, incluido el sistema operativo y todos los datos.

Llevar a cabo una BMR a partir de un archivo

Rapid Recovery le permite restaurar un equipo desde cero mediante un punto de recuperación archivado.

Este procedimiento tiene los siguientes requisitos previos.

- [Creación de una imagen ISO de un CD de inicio](#)
- [Carga del CD de inicio e inicio del equipo de destino](#)

Desde la Universal Recovery Console (URC), se puede tener acceso a Rapid Recovery Core y recuperar un punto de recuperación para una restauración. También puede optar por restaurar su equipo sin sistema operativo desde un punto de recuperación almacenado en un archivo. La URC le permite llegar a este archivo si se encuentra en una unidad local, un recurso compartido de red o una cuenta en la nube.

- 1 En la URC, haga clic en la ficha **Restaurar a partir de archivo**.
- 2 En la lista desplegable **Tipo de ubicación**, seleccione la ubicación de su archivo. Puede seleccionar las opciones siguientes:
 - Local
 - Red
 - Nube
- 3 Introduzca las credenciales que se describen en la tabla siguiente según su selección de tipo de ubicación.

Tabla 158. Opciones de credenciales de tipo de ubicación

Tipo de ubicación	Opción	Descripción
Local	Ruta de acceso local	La ubicación actual del archivo.
Red	Ruta de red	La ubicación actual del archivo.
	Usuario	El nombre de usuario para el acceso de recurso compartido de red.
	Contraseña	La contraseña para el acceso de recurso compartido de red.
Nube	Tipo de nube	El proveedor de su ubicación de almacenamiento de la nube. Seleccione una de las opciones siguientes:
		• Microsoft Azure
		• Amazon™ S3
		• Nubes con tecnología OpenStack
		• Archivos de nube de Rackspace®

- 4 Si ha seleccionado un tipo de nube, complete las credenciales que pertenecen a su proveedor de nube.
 - Para Microsoft Azure, realice los pasos siguientes:
 - 1 Introduzca las siguientes credenciales:
 - Nombre de cuenta de almacenamiento
 - Clave de acceso
 - 2 Para el nombre del contenedor, de la lista desplegable, seleccione un contenedor.
 - 3 Para la ruta de acceso de la nube, de la lista desplegable, seleccione la ruta de acceso al archivo.
 - Para Amazon™ S3, lleve a cabo los siguientes pasos:
 - 1 Introduzca las siguientes credenciales:
 - Clave de acceso
 - Clave secreta
 - 2 Para el nombre del contenedor, de la lista desplegable, seleccione un contenedor.
 - 3 Para la ruta de acceso de la nube, de la lista desplegable, seleccione la ruta de acceso al archivo.
 - Para cuentas de archivos con tecnología OpenStack o Rackspace, realice los siguientes pasos:
 - 1 Introduzca la información siguiente:
 - Región
 - Usuario
 - 2 Seleccione una de las opciones siguientes:
 - Contraseña
 - Clave de API
 - 3 En el cuadro de texto, introduzca la información en función de su selección en el paso C.
 - 4 Introduzca la información siguiente:
 - Id. de inquilino
 - URL de autenticación
 - Nombre de contenedor
 - Ruta de la nube
- 5 Haga clic en **Siguiente**.
- 6 En la página **Equipos**, seleccione el equipo protegido que desea restaurar y, a continuación, haga clic en **Siguiente**.
- 7 En la página **Equipos protegidos**, seleccione el punto de recuperación que desee utilizar para restaurar el equipo y, a continuación, haga clic en **Siguiente**.
- 8 En la página **Asignación**, seleccione una de las siguientes opciones y, a continuación, complete los pasos correspondientes:

- En el menú desplegable **Asignación de volúmenes**, seleccione **Automático**.

1 En la tabla de la izquierda, compruebe que los volúmenes adecuados se enumeran y están seleccionados.

NOTA: Normalmente, en el caso de una BMR, debería restaurar como mínimo el volumen reservado para el sistema y el volumen del sistema (por lo general, pero no siempre, el volumen C:\). Debe seleccionar al menos un volumen para realizar una BMR.

2 En la tabla de la derecha, seleccione el disco o discos a los que desea asignar volúmenes en la máquina de destino.

- En el menú desplegable **Asignación de volúmenes**, seleccione **Manual**.

NOTA: Para asignar discos manualmente, primero debe usar DiskPart en la línea de comandos para crear y dar formato a los volúmenes de destino. Para obtener más información, consulte la información sobre [opciones de línea de comandos de DiskPart \(Standard 7 SP1\)](#) en Microsoft Developer Network.

NOTA: Si no hay volúmenes en la unidad del equipo en el que está realizando una restauración Bare Metal Restore (BMR), no verá esta opción ni podrá asignar volúmenes manualmente.

- En **Volúmenes de destino**, en el menú desplegable, seleccione el volumen de destino adecuado para cada volumen en el punto de recuperación.

9 En el cuadro de texto **ruta de acceso para las asignaciones de montaje**, introduzca un destino para el almacenamiento temporal de los archivos de asignación.

La ubicación predeterminada es X:\ProgramData\AppRecovery\IndexEntriesMaps.

NOTA: Para asegurarse de que el destino tiene suficiente espacio libre, divida la capacidad de volumen de montaje total por 1,024. Por ejemplo, mediante la fórmula (Mount volume total capacity) / 1024 = Free space y, a continuación, 1 TB / 1024 = 1 GB.

10 Haga clic en **Restaurar**.

La URC asigna los volúmenes al nuevo disco o discos.

11 Haga clic en **Restaurar**.

La URC restaura los datos en el equipo de destino. Puede ver el progreso en la ficha **Restaurar progreso**.

12 Una vez que se completa la restauración, extraiga el CD de inicio.

13 Para iniciar el equipo de destino BMR en Windows, reinicie el equipo.

Carga de controladores en el sistema operativo

Este procedimiento describe cómo cargar controladores en el sistema operativo en un destino de restauración Bare Metal Restore (BMR).

Para insertar controladores en el sistema operativo, ya ha realizado las tareas siguientes:

- Ha creado un CD de inicio mediante generador de CD de inicio en la Rapid Recovery Core Console. Para obtener más información, consulte [Creación de una imagen ISO de un CD de inicio](#).
- Ha cargado el CD de inicio en destino de BMR. Para obtener más información, consulte [Carga del CD de inicio e inicio del equipo de destino](#).
- Ha cargado los controladores necesarios para almacenamiento y redes. Para obtener más información, consulte [Carga de controladores mediante la Universal Recovery Console](#).
- Ha realizado la restauración con el Asistente para restaurar un equipo de la Rapid Recovery Core Console o en un archivo comprimido desde la Consola de recuperación universal (URC). Para obtener más información, consulte [Restauración Bare Metal Restore con el Asistente para restaurar un equipo](#) y [Llevar a cabo una BMR a partir de un archivo](#).

Después de realizar una restauración, el proceso no está completo hasta que los controladores se insertan en el sistema operativo del destino de restauración Bare Metal Restore (BMR). Esta tarea es adicional a la carga de los controladores en la URC.

1 Después de hacer clic en Restaurar en el procedimiento BMR de su elección (consulte los requisitos previos), haga clic en la pestaña **Administrador de controladores de Windows existente**.

2 En el menú desplegable, seleccione un sistema operativo.

La URC busca los controladores disponibles.

3 Para cargar más controladores, haga clic en **Forzar carga**.

- 4 Desplácese por el sistema de archivos hasta encontrar el archivo de controlador comprimido y, a continuación, selecciónelo.
- 5 Haga clic en **Aceptar**.
La URC carga el controlador en el sistema operativo que seleccionó.
- 6 Repita los [pasos 3 a 5](#) para cada controlador adicional que tenga que cargar.
- 7 Reinicie el equipo de BMR de destino.
La restauración BMR ha finalizado. Si tiene un problema al reiniciar, consulte [Reparación de problemas de inicio](#).

Realización de una restauración Bare Metal Restore para Linux

En Rapid Recovery, puede realizar una restauración bare metal restore (BMR) para un equipo con Linux, incluida una restauración del volumen del sistema. Cuando realice una restauración en un equipo con Linux, revertirá al punto de recuperación del volumen de inicio. Las funciones de BMR son compatibles al utilizar la utilidad `local_mount` de la línea de comandos y desde dentro de la IU de la Core Console.

⚠ PRECAUCIÓN: Antes de iniciar el proceso de BMR, asegúrese de que todos los equipos Linux que desea restaurar no incluyen una partición de inicio ext2. Cualquier BMR se realiza en un equipo con una partición ext2, el proceso normalmente dará como resultado un equipo que no puede iniciarse. Para realizar una BMR en este caso, tendrá que convertir cualquier partición ext2 a ext3, ext4 o XFS antes de iniciar la protección y la copia de seguridad del equipo.

⚠ PRECAUCIÓN: Cuando inicia un equipo Linux restaurado por primera vez tras una BMR, Rapid Recovery toma una imagen base del equipo restaurado. Dependiendo de la cantidad de datos del equipo, este proceso tarda más tiempo que al tomar una instantánea incremental. Para obtener más información sobre las imágenes base y las instantáneas incrementales, consulte [Comprensión del calendario de programación de protección..](#)

Para realizar una restauración Bare Metal Restore para máquinas con Linux, realice las tareas siguientes.

- Gestione una imagen de inicio de Linux. Esta imagen ISO de inicio del Live DVD de Linux se utilizará para arrancar la unidad de destino, desde la que puede acceder a la Universal Recovery Console para comunicarse con copias de seguridad del Core. Consulte [Administración de una imagen de inicio de Linux](#).
 - Para obtener la imagen de inicio para BMR, primero debe determinar qué imagen necesita y, a continuación, descargarla desde el Portal de licencias. Consulte [Acerca de la imagen ISO de inicio para Linux](#) seguido de [Descarga de una imagen ISO de inicio para Linux](#).
 - Si necesita soportes físicos para arrancar el equipo con Linux de destino, deberá transferir la imagen ISO a un soporte. Consulte [Almacenamiento de la imagen ISO del Live DVD en soportes](#).
 - En cualquier caso, deberá cargar la imagen de inicio en el servidor de destino e iniciar el servidor desde la imagen de inicio. Consulte [Carga del Live DVD e inicio del equipo de destino](#).
 - Después de cargar el soporte, debe conectar el equipo Linux a Rapid Recovery Core. Consulte [Conexión al destino de la restauración BMR desde el Rapid Recovery Core](#).
- Gestione particiones. Puede que deba crear o montar particiones antes de realizar una BMR en un equipo con Linux. Consulte [Administración de particiones de Linux](#).
 - El sistema Linux en el que esté realizando una BMR debe tener las mismas particiones que los volúmenes de origen del punto de recuperación. Puede que necesite crear particiones adicionales en el sistema de destino, si es necesario. Consulte [Creación de particiones en la unidad de destino](#).
 - Si está realizando una BMR manual, primero deberá montar particiones. Consulte [Montaje de particiones desde la línea de comandos](#). Los pasos para montar particiones se incluyen en el proceso para realizar una BMR desde la línea de comandos. Consulte [Inicio de una restauración Bare Metal Restore para un equipo Linux mediante la línea de comandos](#).
Si va a utilizar el particionamiento automático para la BMR en la Core Console, no necesita montar particiones. Rapid Recovery restaurará las mismas particiones que las incluidas en los puntos de recuperación que se están restaurando.
- Inicie una restauración Bare Metal Restore para Linux. Una vez se haya iniciado el equipo de destino desde la imagen de inicio del Live DVD, podrá iniciar la BMR. Las tareas obligatorias dependen de si va a realizar esto desde la interfaz de usuario de Rapid Recovery o desde la línea de comandos mediante la utilidad `local_mount`. Consulte [Inicio de una restauración Bare Metal Restore para Linux](#).
 - Si va a utilizar la Core Console, deberá iniciar una restauración desde un punto de recuperación del Core. Consulte [Selección de un punto de recuperación e inicio de la BMR](#).
 - Si va a utilizar la Core Console, deberá asignar los volúmenes desde la IU. Consulte [Acerca de asignar discos para una restauración Bare Metal Restore](#).

- Opcionalmente, si realiza una restauración desde la línea de comandos, podrá usar la utilidad Pantalla para mejorar su capacidad de desplazarse y ver los comandos en la consola terminal. Esta utilidad se abre de manera predeterminada. Si la cierra, puede iniciarla de nuevo. Para obtener más información, consulte [Inicio de la utilidad Pantalla](#).
- Si va a utilizar local_mount, todas las tareas se realizarán en la línea de comandos. Para obtener más información, consulte [Inicio de una restauración Bare Metal Restore para un equipo Linux mediante la línea de comandos](#).
- Verifique una restauración Bare Metal Restore. Tras iniciar la restauración Bare Metal Restore, podrá verificar y supervisar su progreso. Consulte [Verificación de la restauración Bare Metal Restore desde la línea de comandos](#).
 - Puede supervisar el progreso de su restauración. Consulte [Visualización del progreso de recuperación](#).
 - Una vez completada, podrá iniciar el servidor restaurado. Consulte [Inicio de un servidor de destino restaurado](#).
 - Solucione los problemas del proceso de BMR. Consulte [Solución de problemas de conexiones con la Universal Recovery Console y Reparación de problemas de inicio](#).

Requisitos previos para realizar una restauración Bare Metal Restore para un equipo Linux

Antes de que pueda empezar el proceso de realizar una restauración Bare Metal Restore para un equipo con Linux, deberá asegurarse de que se cumplen las condiciones y criterios siguientes:

- Copias de seguridad del equipo que quiere restaurar. Debe tener un Rapid Recovery Core en funcionamiento que contenga puntos de recuperación del servidor protegido que quiera restaurar.
- Hardware que se va a restaurar (nuevo o antiguo, similar o diferente). El equipo de destino debe cumplir los requisitos de instalación para un Agent. Para obtener información detallada, consulte la Guía de instalación y actualización de Rapid Recovery.
- Imagen de inicio del Live DVD. Obtenga la imagen ISO del Live DVD de Linux, que incluye una versión de inicio de Linux. Descarga de LMU desde el Dell Data Protection | Portal de licencias de Rapid Recovery en <https://licenseportal.com>. Si tiene algún problema al descargar el Live DVD, póngase en contacto con el Soporte de Rapid Recovery de Dell.
- Soportes y software de imagen. Si está utilizando soportes físicos, debe tener un CD o DVD en blanco y software de grabación de discos, o bien software para crear una imagen ISO.
- Controladores de almacenamiento y controladores de adaptador de red compatibles. Si restaura hardware diferente, debe tener controladores de almacenamiento y controladores de adaptador de red compatibles para el equipo de destino, incluidos controladores RAID, AHCI y de chipset para el sistema operativo de destino, según sea adecuado.
- Espacio de almacenamiento y particiones, según sea adecuado. Asegúrese de que hay suficiente espacio en el disco duro para crear particiones de destino en el equipo de destino para que contenga los volúmenes de origen. Cualquier partición de destino debería ser como mínimo igual de grande que la partición de origen original.
- Restaure la ruta de acceso. Identifique la ruta de acceso para la restauración, que es la ruta de acceso del descriptor del archivo del dispositivo. Para identificar la ruta de acceso del descriptor del archivo del dispositivo, utilice el comando `fdisk` desde una ventana del terminal.

Administración de una imagen de inicio de Linux

Una restauración Bare Metal Restore para Linux requiere una imagen de inicio del Live DVD, que puede descargar desde el Dell Data Protection | Portal de licencias de Rapid Recovery. Utilizará esta imagen para iniciar el equipo con Linux de destino. Basándose en las características específicas de su entorno, puede que necesite transferir esta imagen a un soporte físico, como un CD o DVD. A continuación, deberá cargar virtual o físicamente la imagen de inicio e iniciar el servidor Linux desde la imagen de inicio.

❗ | NOTA: El Live DVD se denominaba anteriormente Live CD.

La gestión de una imagen de inicio de Linux es un paso en [Realización de una restauración Bare Metal Restore para Linux](#).

Puede realizar las siguientes tareas:

Acerca de la imagen ISO de inicio para Linux

El primer paso al realizar una restauración Bare Metal Restore (BMR) para un equipo con Linux es descargar la imagen ISO del Live DVD de Linux desde el Dell Data Protection | Portal de licencias de Rapid Recovery. El Live DVD funciona con todos los sistemas de archivos de

Linux admitidos por Rapid Recovery e incluye una versión de inicio de Linux, la utilidad de pantalla y la interfaz de la Consola de recuperación universal (URC) de Rapid Recovery. La Consola de recuperación universal de Rapid Recovery es un entorno que se utiliza para restaurar la unidad del sistema o todo el servidor directamente desde el Rapid Recovery Core.

① NOTA: International Organization for Standardization (ISO) (Organización internacional de normalización) es un organismo internacional de representantes de diversas organizaciones nacionales que establecen los estándares del sistema de archivos. ISO 9660 es un sistema de archivos estándar que se utiliza para soportes de disco óptico para el intercambio de datos y que admite diversos sistemas operativos. Una imagen ISO es un archivo de archivado o imagen de disco que contiene datos por cada sector del disco, así como el sistema de archivos del disco.

Descarga de una imagen ISO de inicio para Linux

Debe descargar la imagen ISO del Live DVD que coincida con su versión de Rapid Recovery. La versión actual de Live DVD está disponible desde el Dell Data Protection | Portal de licencias de Rapid Recovery en <https://licenseportal.com>. Si necesita una versión diferente, póngase en contacto con el Soporte de Rapid Recovery de Dell.

① NOTA: Para obtener más información sobre el Dell Data Protection | Portal de licencias de Rapid Recovery, consulte la Guía de usuario de Dell Data Protection | Portal de licencias de Rapid Recovery.

Esta tarea es un paso en [Realización de una restauración Bare Metal Restore para Linux](#). Forma parte del proceso para [Administración de una imagen de inicio de Linux](#).

Realice los pasos de este procedimiento para descargar la imagen ISO del Live DVD.

- 1 Inicie sesión en el Dell Data Protection | Portal de licencias de Rapid Recovery en <https://licenseportal.com>.
- 2 Acceda al área Descargas.
- 3 Desplácese hasta Aplicaciones basadas en Linux y, desde la sección Live DVD de Linux, haga clic en **Descargar**.
- 4 Guarde la imagen ISO del Live DVD. Si está restaurando una máquina virtual, puede guardarla en una nueva ubicación de red y establecer que la máquina virtual arranque desde una unidad de CD o DVD asociada a la imagen ISO.
- 5 Si está realizando una restauración desde un equipo físico, grabe la imagen ISO del CD de inicio en un disco compacto (CD) o disco de vídeo digital (DVD) desde el que pueda iniciarse el equipo de destino. Para obtener más información, consulte [Almacenamiento de la imagen ISO del Live DVD en soportes](#).

Almacenamiento de la imagen ISO del Live DVD en soportes

Cuando descarga el archivo del Live DVD de Linux, se almacena como una imagen ISO en la ruta que especificó. Debe poder iniciar el equipo con Linux de destino desde la imagen del Live DVD.

Esta tarea es un paso en [Realización de una restauración Bare Metal Restore para Linux](#). Forma parte del proceso para [Administración de una imagen de inicio de Linux](#).

Grabe la imagen ISO del CD de inicio en un disco compacto (CD) o disco de vídeo digital (DVD).

Si realiza una BMR en una máquina virtual, este paso no es obligatorio. Solo cargue la imagen ISO en una unidad y edite la configuración del equipo de esa máquina virtual para que se inicie desde esa unidad. También puede utilizar la exportación virtual para restaurar una máquina virtual Linux. Para obtener más información, consulte [Exportación de VM](#).

Carga del Live DVD e inicio del equipo de destino

Después de obtener la imagen ISO del Live DVD, deberá iniciar el equipo con Linux desde el Live DVD recién creado.

Esta tarea es un paso de [Realización de una restauración Bare Metal Restore para Linux](#). Forma parte del proceso para [Administración de una imagen de inicio de Linux](#).

- 1 Desplácese hasta el nuevo servidor y cargue la imagen del Live DVD desde la ubicación adecuada. Especifique que el servidor se iniciará desde la imagen del Live DVD.
- 2 Inicie el equipo.

Aparecerá una pantalla emergente de Rapid Recovery y se abrirá una ventana de terminal, que muestra la dirección IP y una contraseña de autenticación para el equipo.

NOTA: Se generará una nueva contraseña temporal cada vez que el equipo se inicie con la imagen del Live DVD.

- 3 Anote la dirección IP y la contraseña de autenticación que aparecen en la pantalla de introducción. Necesitará esta información posteriormente, durante el proceso de recuperación de datos para volver a iniciar sesión en la consola.

Conexión al destino de la restauración BMR desde el Rapid Recovery Core

Una vez iniciado el equipo con Linux de destino con el Live DVD, este equipo está listo para que se conecte a él desde el Core e inicie el proceso de restauración Bare Metal Restore. Puede realizar este proceso utilizando cualquiera de estos dos métodos:

- Iniciando una restauración desde la Rapid Recovery Core Console. Para obtener más información, consulte [Inicio de una restauración Bare Metal Restore para Linux](#).
- Iniciando una restauración desde la línea de comandos mediante la utilidad aamount. Para obtener más información, consulte [Inicio de una restauración Bare Metal Restore para un equipo Linux mediante la línea de comandos](#).

Administración de particiones de Linux

Al realizar una BMR, la unidad de destino en la que vaya a restaurar datos debe tener las mismas particiones que en el punto de recuperación que esté restaurando. Puede que necesite crear particiones para cumplir este requisito.

Puede iniciar la restauración desde la línea de comandos mediante la utilidad aamount, o bien puede iniciar la restauración desde la Rapid Recovery Core Console. Si restaura mediante la interfaz de usuario, primero deberá montar las particiones.

La gestión de particiones de Linux es un paso en [Realización de una restauración Bare Metal Restore para Linux](#).

Puede realizar las siguientes tareas:

Vínculos relacionados

[Creación de particiones en la unidad de destino](#)

[Formateo de particiones en la unidad de destino](#)

[Montaje de particiones desde la línea de comandos](#)

Creación de particiones en la unidad de destino

A menudo, al realizar una BMR, la unidad de destino es un nuevo volumen que puede estar compuesto por una única partición. La unidad del equipo de destino debe tener la misma tabla de partición que en el punto de recuperación, incluido el tamaño de los volúmenes. Si la unidad de destino no contiene las mismas particiones, deberá crearlas antes de realizar la restauración Bare Metal Restore. Utilice la utilidad fdisk para crear particiones en la unidad de destino iguales a las particiones de la unidad de origen.

PRECAUCIÓN: El siguiente procedimiento es sólo un ejemplo. Los entornos del cliente son distintos. Debe cambiar los comandos que utiliza para que coincidan con las especificaciones de su entorno.

Esta tarea es un paso en [Realización de una restauración Bare Metal Restore para Linux](#). Forma parte del proceso para [Administración de particiones de Linux](#).

- 1 Opcionalmente, puede usar la utilidad Pantalla. Esta utilidad se inicia de manera predeterminada y permanece activa hasta que reinicia el equipo.

NOTA: Si la cierra de forma explícita y desea volver a abrirla, consulte [Inicio de la utilidad Pantalla](#).

- 2 Desde la línea de comandos, introduzca el siguiente comando y, a continuación, pulse **Intro** para cambiar los privilegios para ejecutar como administrador y, a continuación, enumere las particiones de disco existentes:

```
sudo fdisk -l
```

Aparecerá una lista de todos los volúmenes.

En este ejemplo se da por hecho que el volumen que quiere particionar es /dev/sda. Si su volumen es diferente (por ejemplo, en el caso de unidades anteriores, puede que vea /dev/hda), cambie los comandos de la manera correspondiente.

- 3 Para crear una nueva partición de inicio, introduzca el siguiente comando y, a continuación, pulse **Intro**:

```
sudo fdisk /dev/sda
```

- 4 Para crear una nueva partición de inicio, introduzca el siguiente comando y, a continuación, pulse **Intro**:

```
n
```

- 5 Para crear una nueva partición principal, introduzca el siguiente comando y, a continuación, pulse **Intro**:

```
p
```

- 6 Para especificar el número de partición, introduzca el número de partición y, a continuación, pulse **Intro**. Por ejemplo, para especificar la partición 1, escriba 1 y, a continuación, pulse **Intro**.

- 7 Para utilizar el primer sector, 2048, pulse **Intro**.

- 8 Asigne una cantidad adecuada a la partición de inicio introduciendo el símbolo más y la cantidad de asignación y, a continuación, pulse **Intro**.

Por ejemplo, para asignar 500 M para la partición de inicio, escriba lo siguiente y, a continuación, pulse **Intro**:

```
+512000K
```

- 9 Para cambiar de un indicador de inicio a la partición de inicio (para que la partición sea de inicio), escriba el siguiente comando y, a continuación, pulse **Intro**:

```
a
```

- 10 Para asignar un indicador de inicio a la partición adecuada, escriba el número de la partición y, a continuación, pulse **Intro**. Por ejemplo, para asignar un indicador de inicio a la partición 1, escriba 1 y, a continuación, pulse **Intro**.

- 11 Continúe realizando particiones en el disco duro según sea necesario.

- 12 Para guardar todos los cambios en la utilidad fdisk, escriba el siguiente comando y, a continuación, pulse **Intro**:

```
w
```

Formateo de particiones en la unidad de destino

Después de crear particiones en un nuevo volumen en la unidad de destino para llevar a cabo la restauración bare metal restore, si no va a utilizar la partición automática, debe formatear las particiones antes de que se puedan montar. Si se da esta situación, siga este procedimiento para dar formato a particiones con formatos ext3, ext4 o XFS.

Para el resto de casos, no es necesario que formatee las particiones, tal y como se describe en este tema.

Esta tarea es un paso en [Realización de una restauración Bare Metal Restore para Linux](#). Forma parte del proceso para [Administración de particiones de Linux](#).

- 1 Opcionalmente, puede usar la utilidad Pantalla. Esta utilidad se inicia de manera predeterminada y permanece activa hasta que reinicia la máquina.

NOTA: Si la cierra de forma explícita y desea volver a abrirla, consulte [Inicio de la utilidad Pantalla](#).

- 2 Desde la línea de comandos, introduzca el siguiente comando y, a continuación, pulse **Intro** para cambiar los privilegios para ejecutar como administrador y, a continuación, enumere las particiones de disco existentes:

```
sudo fdisk -l
```

Aparecerá una lista de todos los volúmenes.

En este ejemplo se da por hecho que la partición que quiere formatear es /dev/sda1. Si su volumen es diferente (por ejemplo, en el caso de unidades anteriores, puede que vea /dev/hda), cambie los comandos de la manera correspondiente.

- 3 Seleccione uno de los siguientes comandos en base al formato que desee usar para la partición de destino:

- Para formatear una partición con formato ext3, introduzca el siguiente comando y, a continuación, pulse **Intro**:

```
sudo mkfs.ext3 /dev/sda1
```

- Para formatear una partición con formato ext4, introduzca el siguiente comando y, a continuación, pulse **Intro**:

```
sudo mkfs.ext4 /dev/sda1
```

- Para formatear una partición con formato XFS, introduzca el siguiente comando y, a continuación, pulse **Intro**:

```
sudo mkfs.xfs /dev/sda1
```

Se formateará la partición seleccionada con el formato elegido.

- 4 Si tiene que dar formato a otras particiones, repita este procedimiento.

Montaje de particiones desde la línea de comandos

Si está realizando una BMR mediante la Rapid Recovery Core Console, primero deberá montar las particiones adecuadas en el equipo de destino. Realice esta acción desde la línea de comandos de la Universal Recovery Console.

Esta tarea es un paso en [Realización de una restauración Bare Metal Restore para Linux](#). Forma parte del proceso para [Administración de particiones de Linux](#).

Realice los pasos de este procedimiento para montar particiones en el equipo con Linux antes de realizar una restauración.

- 1 Desde la línea de comandos, introduzca el siguiente comando y, a continuación, pulse **Intro** para cambiar los privilegios para ejecutar como administrador y, a continuación, enumere las particiones de disco existentes:

```
sudo fdisk -l
```

Aparecerá una lista de todos los volúmenes.

- 2 Dé formato a todas las particiones que necesite para realizar la BMR en el directorio de montaje. Estas deben coincidir con los volúmenes que hay en el punto de recuperación. Por ejemplo, si el volumen que quiere montar se denomina sda1 y el directorio de montaje, mnt, escriba el siguiente comando y, a continuación, pulse **Intro**:
- 3 Monte todas las particiones que necesite para realizar la BMR en el directorio de montaje. Estas deben coincidir con los volúmenes que hay en el punto de recuperación. Por ejemplo, si el volumen que quiere montar se denomina sda1 y el directorio de montaje, mnt, escriba el siguiente comando y, a continuación, pulse **Intro**:

```
mount /dev/sda1 /mnt
```

- 4 Repita el [Paso 3](#) según sea necesario hasta que haya montado todos los volúmenes requeridos.

Una vez se hayan montado los volúmenes, podrá realizar una restauración en el equipo con Linux de destino desde la Rapid Recovery Core Console. Consulte [Inicio de una restauración Bare Metal Restore para Linux](#).

Inicio de una restauración Bare Metal Restore para Linux

Antes de iniciar una restauración Bare Metal Restore (BMR) para un equipo con Linux, es preciso que se den las siguientes condiciones:

- Para restaurar un punto de recuperación guardado en el Core, debe contar ya con el hardware adecuado. Para obtener más información, consulte [Requisitos previos para realizar una restauración Bare Metal Restore para un equipo Linux](#).
- El equipo con Linux de destino para la BMR debe iniciarse mediante la imagen de inicio del Live DVD. Para obtener más información, consulte [Administración de una imagen de inicio de Linux](#).
- El número de volúmenes del equipo con Linux que va a restaurarse debe coincidir con el número de volúmenes del punto de recuperación. También debe decidir si va a restaurar desde la Rapid Recovery Core Console o desde la línea de comandos mediante local_mount. Para obtener más información, consulte [Administración de particiones de Linux](#).
- Si va a restaurar desde la IU de la Core Console, el primer paso para iniciar una BMR es seleccionar el punto de recuperación adecuado y, a continuación, iniciar la restauración en el hardware especificando la dirección IP y la contraseña temporal que obtuvo de la Universal Recovery Console. A continuación, deberá asignar las unidades e iniciar la restauración.

Este proceso es un paso en [Realización de una restauración Bare Metal Restore para Linux](#).

Para iniciar una BMR desde la Rapid Recovery Core Console, realice las tareas siguientes.

- [Selección de un punto de recuperación e inicio de la BMR](#)
- [Acerca de asignar discos para una restauración Bare Metal Restore](#)

Si está restaurando desde la línea de comandos mediante la utilidad local_mount, primero debe establecer los privilegios adecuados, montar volúmenes, ejecutar local_mount, obtener información sobre el Core de la lista de equipos, conectarse al Core, obtener una lista de puntos de recuperación, seleccionar el punto de recuperación que quiere revertir mediante una restauración Bare Metal Restore e iniciar la restauración.

Opcionalmente, puede que quiera iniciar la utilidad Pantalla.

Para iniciar una BMR desde la línea de comandos, realice las tareas siguientes.

- [Inicio de la utilidad Pantalla](#)
- [Inicio de una restauración Bare Metal Restore para un equipo Linux mediante la línea de comandos](#)

Inicio de la utilidad Pantalla

En el Live DVD se incluye Pantalla, una utilidad que está disponible cuando inicia desde el Live DVD en la Universal Recovery Console. Pantalla permite que los usuarios gestionen varios shells simultáneamente a través de una única sesión de shell seguro (SSH) o ventana de consola. Esto le permite realizar una tarea en una ventana de terminal (como verificar volúmenes montados) y, mientras se está ejecutando, abrir o cambiar a otra instancia de shell para realizar otra tarea (como ejecutar la utilidad `local_mount`).

La utilidad Pantalla también tiene su propio búfer de desplazamiento hacia atrás, que le permite desplazar la pantalla para ver mayores cantidades de datos, como una lista de puntos de recuperación.

NOTA: Esta utilidad se proporciona por comodidad; el uso de la utilidad Pantalla es opcional.

La utilidad Pantalla se inicia en el equipo iniciado con el Live DVD de forma predeterminada. Sin embargo, si ha cerrado esta aplicación, deberá iniciar la utilidad Pantalla desde el Live DVD mediante el procedimiento siguiente.

Si se inició el equipo desde el Live DVD, en la ventana de terminal introduzca `screen` y pulse **Intro**.
Se abrirá la utilidad Pantalla.

Inicio de una restauración Bare Metal Restore para un equipo Linux mediante la línea de comandos

Una vez que la imagen ISO del Live DVD sea accesible en el equipo en el que quiera realizar una BMR y el número y tamaño de los volúmenes coincidan entre el equipo de destino y el punto de recuperación en el que quiera realizar una restauración Bare Metal Restore, podrá iniciar una restauración desde la línea de comandos mediante la utilidad `local_mount`.

NOTA: Este componente anteriormente se denominaba `amount`.

Si desea realizar una BMR mediante la IU de la Rapid Recovery Core Console, consulte [Selección de un punto de recuperación e inicio de la BMR](#).

NOTA: Al realizar este procedimiento, no intente montar puntos de recuperación en la carpeta `/tmp`, que contiene los archivos de `rapidrecovery-vdisk` (anteriormente, `aavdisk`).

Esta tarea es un paso en [Realización de una restauración Bare Metal Restore para Linux](#). Forma parte del proceso para [Inicio de una restauración Bare Metal Restore para un equipo Linux mediante la línea de comandos](#).

Realice los pasos de este procedimiento para seleccionar un punto de recuperación en el Core para revertir al equipo de destino de BMR física o virtual.

- 1 Para ejecutar la utilidad `local_mount` de Rapid Recovery como raíz, escriba el siguiente comando y, a continuación, pulse **Intro**:

```
sudo local_mount
```
- 2 Para enumerar los equipos protegidos, escriba el siguiente comando y, a continuación, pulse **Intro**:

```
lm
```
- 3 Cuando se le pida, introduzca la información de conexión para el Rapid Recovery Core como se describe en la tabla siguiente, pulsando **Intro** después de cada comando obligatorio:

Tabla 159. Información de conexión del Rapid Recovery Core

Cuadro de texto	Descripción	Obligatorio
Dirección IP o nombre de host del Rapid Recovery Core	Dirección IP o nombre de host del Rapid Recovery Core.	Sí
Dominio	El dominio del Rapid Recovery Core. Esto es opcional.	No
Usuario	Nombre de usuario de un administrador en el Core.	Sí
Contraseña	Contraseña utilizada para conectar al usuario administrativo con el Core.	Sí

Aparecerá una lista que muestra los equipos protegidos por este Rapid Recovery Core. Enumera los equipos encontrados por número de elemento de línea, el nombre mostrado del host o dirección IP y un número de ID del equipo.

- Para enumerar los puntos de recuperación del equipo que quiere restaurar, escriba el comando de enumeración de puntos de recuperación mediante la sintaxis siguiente y, a continuación, pulse **Intro**:

```
lr <machine_line_item_number>
```

NOTA: También puede introducir el número de ID del equipo en este comando en lugar del número de elemento de línea.

Aparecerá una lista con los puntos de recuperación base e incrementales de ese equipo. Esta lista incluye:

- Un número de elemento de línea
- Un sello de fecha y hora
- Una lista con letras de los volúmenes dentro del punto de recuperación
- La ubicación del volumen
- El tamaño del punto de recuperación
- Un número de ID del volumen que incluye un número de secuencia al final, que identifica el punto de recuperación

- Para seleccionar el punto de recuperación para una restauración, introduzca el siguiente comando y, a continuación, pulse **Intro**:

```
r <recovery_point_ID_number> <path>
```

PRECAUCIÓN: Debe asegurarse de que el volumen del sistema no está montado.

NOTA: Si inició el equipo desde el Live DVD, el volumen del sistema no está montado.

Este comando revierte la imagen del volumen especificada por el ID del Core en la ruta de acceso especificada. La ruta de acceso para la restauración es la ruta de acceso del descriptor del archivo del dispositivo y no es el directorio en el que está montado.

NOTA: También puede especificar un número de línea en el comando en lugar del número de ID del punto de recuperación para identificar al punto de recuperación. En ese caso, utilice el número de línea del Agent o el equipo (desde la salida `lm`), seguido por el número de línea del punto de recuperación y la letra del volumen (de la lista con letras de los volúmenes dentro del punto de recuperación), seguido por la ruta de acceso. Por ejemplo:

```
r <machine_line_item_number> <base_image_recovery_point_line_number> <volume_letter> <path>
```

Por ejemplo, escriba:

```
r 1 24 a /dev/sda1
```

En este comando, `<path>` es el descriptor de archivo del volumen real.

- Cuando se le pregunte si quiere continuar, introduzca s de Sí y, a continuación, pulse **Intro**.

Después de que comience la restauración, aparecerá una serie de mensajes que le notificarán el estado de finalización de la restauración.

① **NOTA:** Si recibe un mensaje de excepción, la información detallada relativa a dicha excepción podrá encontrarse en el archivo `local_mount.log`. El archivo `local_mount.log` se encuentra en `/var/log/appassure`.

- 7 Tras una restauración correcta, salga de `local_mount` escribiendo `exit` y, a continuación, pulse **Intro**.
- 8 Su siguiente paso será verificar la restauración. Para obtener más información, consulte [Verificación de la restauración Bare Metal Restore desde la línea de comandos](#).

Restauración de volúmenes para un equipo Linux mediante la línea de comandos

En Rapid Recovery, puede restaurar volúmenes en sus equipos Linux protegidos mediante la utilidad `local_mount` de la línea de comandos.

① **NOTA:** Este proceso se denominaba anteriormente una *reversión*. Al realizar este procedimiento, no intente montar puntos de recuperación en la carpeta `/tmp`, que contiene los archivos de `rapidrecovery-vdisk` (anteriormente, `aavdisk`). La restauración de volúmenes también es compatible para los equipos protegidos dentro de la Rapid Recovery Core Console. Consulte [Restauración de volúmenes desde un punto de recuperación](#) para obtener más información.

⚠ **PRECAUCIÓN:** Para restaurar el sistema o la partición raíz (`/`) o el sistema operativo completo, consulte [Realización de una restauración Bare Metal Restore para Linux](#).

- 1 Ejecute la utilidad Rapid Recovery `local_mount` como raíz, por ejemplo:

```
sudo local_mount
```

- 2 En la solicitud de montaje de Rapid Recovery, introduzca el siguiente comando para enumerar las máquinas protegidas.

```
lm
```

- 3 Cuando se le solicite, introduzca la dirección IP o nombre del host del servidor Rapid Recovery Core.

- 4 Introduzca las credenciales de inicio de sesión, es decir, el nombre de usuario y la contraseña, para este servidor.

Aparecerá una lista que muestra los equipos protegidos por este servidor de Rapid Recovery. En la lista aparecerán los equipos protegidos encontrados por número de elemento de línea, dirección de host/IP y un número de identificación del equipo, por ejemplo, `7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba:2`.

- 5 Introduzca el siguiente comando para enumerar los puntos de recuperación montados actualmente para el equipo especificado:

```
lr <machine_line_item_number>
```

① **NOTA:** Tenga en cuenta que también puede introducir el número de ID del equipo en este comando en lugar del número de elemento de línea.

Aparecerá una lista que muestra los puntos de recuperación base e incrementales de ese equipo. Esta lista incluye un número de elemento de línea, fecha/marca de tiempo, ubicación del volumen, tamaño del punto de recuperación y número de ID del volumen que incluye un número secuencial al final (por ejemplo, `"293cc667-44b4-48ab-91d8-44bc74252a4f:2"`), que identifica al punto de recuperación.

- 6 Introduzca el siguiente comando para seleccionar un punto de recuperación para realizar la restauración:

```
r <volume_recovery_point_ID_number> <device_path>
```

Este comando restaura la imagen del volumen especificada por la identificación del Core a la ruta de acceso especificada. La ruta de acceso para la restauración es la ruta de acceso del descriptor del archivo del dispositivo y no es el directorio en el que está montado.

- También puede especificar un número de línea en el comando en lugar del número de ID del punto de recuperación para identificar al punto de recuperación. En ese caso, utilizaría el número de línea del equipo protegido (desde la salida `lm`), seguido por el número de línea del punto de recuperación y la letra del volumen, seguido por la ruta de acceso, de este modo: `r <número_de_elemento_de_línea_de_la_máquina> <número_de_línea_del_punto_de_recuperación> <letra_del_volumen> <ruta_de_acceso>`. En este comando, `<ruta_de_acceso>` es el descriptor del archivo para el propio volumen.

Por ejemplo, si la salida `lm` enumera tres equipos protegidos y especifica el comando `lr` para el equipo protegido número 2, y desea restaurar el punto de recuperación 23 volumen b en el volumen que estaba montado en el directorio `/dev/sda5`, el comando sería:

```
r2 23 b /dev/sda5
```

NOTA: Se puede restaurar en / si es necesario. Si realiza una restauración Bare Metal Restore mediante un Live DVD, se supone que desea restaurar en otro equipo. Para obtener más información, consulte [Inicio de una restauración Bare Metal Restore para Linux](#).

- 7 Cuando se le pregunte si quiere continuar, introduzca y para Sí.
Cuando continúe la restauración, aparecerá una serie de mensajes que le notificarán el estado.
- 8 Tras una restauración correcta, la utilidad `local_mount` montará y volverá a adjuntar automáticamente el módulo de kernel en el volumen restaurado si el destino se protegió y montó anteriormente. Si no es así, deberá montar el volumen restaurado en el disco local y, a continuación, debería verificar que los archivos se han restaurado (por ejemplo, puede utilizar el comando `sudo mount` y luego el comando `ls`).

Comprobación de una restauración Bare Metal Restore

Una vez que haya realizado una restauración Bare Metal Restore (BMR), puede comprobar el progreso de la restauración. Cuando la acción se haya realizado correctamente, podrá iniciar el servidor restaurado. Se incluyen algunos pasos de solución de problemas si encuentra dificultades al conectarse a la Universal Recovery Console para realizar la restauración y para reparar problemas de inicio con el equipo restaurado.

Puede realizar las siguientes tareas:

Vínculos relacionados

- [Visualización del progreso de recuperación](#)
- [Inicio de un servidor de destino restaurado](#)
- [Solución de problemas de conexiones con la Universal Recovery Console](#)
- [Reparación de problemas de inicio](#)

Visualización del progreso de recuperación

Realice los pasos de este procedimiento para ver el progreso de la restauración de los datos desde un punto de recuperación (incluida la restauración Bare Metal Restore) iniciado desde la Rapid Recovery Core Console.

- 1 Después de iniciar el proceso de restauración de datos desde un punto de recuperación, mientras la tarea está en curso, puede ver su progreso desde el menú desplegable Tareas en ejecución en la Core Console.
- 2 Opcionalmente, puede ver información detallada en la página Eventos. Para obtener más información acerca de la supervisión de eventos de Rapid Recovery, consulte [Visualización de tareas, alertas y eventos](#).

Inicio de un servidor de destino restaurado

Realice los pasos de este procedimiento para iniciar el servidor de destino restaurado.

NOTA: Antes de iniciar el servidor de destino restaurado, debería verificar que la recuperación se haya realizado correctamente. Para obtener más información, consulte [Visualización del progreso de recuperación](#).

Esta tarea es un paso en [Restauración Bare Metal Restore en máquinas Windows](#). Forma parte del proceso para [Comprobación de una restauración Bare Metal Restore](#).

- 1 En el servidor de destino, compruebe que la Rapid Recovery Universal Recovery Console está activa.
- 2 Expulse el CD de inicio (o desconecte el soporte físico con la imagen del CD de inicio) del servidor restaurado.
- 3 En la Universal Recovery Console, haga clic en el icono del menú de alimentación de la parte superior de la pantalla y, a continuación, haga clic en **Reiniciar**.
- 4 Especifique que el sistema operativo se inicie con normalidad.
- 5 Inicie la sesión en el equipo. El sistema debe restaurarse al estado capturado en el punto de recuperación.

Solución de problemas de conexiones con la Universal Recovery Console

A continuación se indican pasos de solución de problemas para conectarse a la imagen del CD de inicio como parte del proceso de [Selección de un punto de recuperación e inicio de la BMR](#).

Si aparece un error que indique que el Core no se ha podido conectar al servidor remoto, es probable que la causa sea una de las distintas causas posibles.

- Verifique que la dirección IP y la contraseña actual que aparecen en la URC son idénticas a la información que introdujo en el cuadro de diálogo Instancia de la consola de recuperación.
- Para llegar al servidor en el que se restaurarán datos, el Core debe poder identificar al servidor en la red. Para determinar si la identificación del servidor es posible, puede abrir un símbolo del sistema en el Core y hacer ping en la dirección IP del servidor de BMR de destino. También puede abrir un símbolo del sistema en el servidor de destino y hacer ping en la dirección IP del Core de Rapid Recovery.
- Verifique que la configuración del adaptador de red es compatible entre el Core y el servidor de BMR de destino.

Reparación de problemas de inicio

Este procedimiento tiene los siguientes requisitos previos.

- [Creación de una imagen ISO de un CD de inicio](#)
- [Carga del CD de inicio e inicio del equipo de destino](#)
- [Carga de controladores mediante la Universal Recovery Console](#)

Realice los pasos de este procedimiento para reparar problemas de arranque. Recuerde que si está restaurando en hardware diferente, debe insertar controladores de controladora de almacenamiento, RAID, AHCI, de chipset y de otro tipo si no están ya en el CD de inicio. Estos controladores permiten que el sistema operativo haga que todos los dispositivos funcionen correctamente en su servidor de destino. Para obtener más información, consulte [Carga de controladores mediante la Universal Recovery Console](#). Realice el procedimiento siguiente para reparar problemas de arranque en su servidor de destino.

- 1 Desde la Universal Recovery Console, haga clic en la ficha **Administrador de controladores de Windows existente**.
- 2 Haga clic en **Reparar problemas de inicio**.
Los parámetros de arranque del registro de inicio del servidor de destino se repararán automáticamente.

Verificación de la restauración Bare Metal Restore desde la línea de comandos

Dell recomienda realizar los siguientes pasos para verificar que una restauración Bare Metal Restore se ha realizado desde la línea de comandos.

Esta tarea es un paso en [Realización de una restauración Bare Metal Restore para Linux](#).

Vínculos relacionados

- [Realización de una comprobación del sistema de archivos en el volumen restaurado](#)
- [Uso de la línea de comandos para hacer que un equipo Linux pueda iniciarse](#)

Realización de una comprobación del sistema de archivos en el volumen restaurado

Una vez que haya ejecutado una restauración Bare Metal Restore desde la línea de comandos, debería realizar una comprobación del sistema de archivos en el volumen restaurado para asegurarse de que los datos restaurados del punto de recuperación no están dañados.

Esta tarea es un paso en [Realización de una restauración Bare Metal Restore para Linux](#). Forma parte del proceso para [Verificación de la restauración Bare Metal Restore desde la línea de comandos](#).

Realice la tarea siguiente para realizar una comprobación del sistema de archivos en el volumen restaurado.

- 1 Desde la línea de comandos en la Universal Recovery Console del equipo con Linux que ha restaurado, para verificar si se han montado las particiones adecuadas, escriba el siguiente comando y, a continuación, pulse **Intro**:

```
df
```

- 2 Si el volumen restaurado no está montado, vaya al [Paso 3](#). Si el volumen restaurado está montado, desmóntelo escribiendo el siguiente comando y, a continuación, pulsando Intro:

```
umount <mount point>
```

- 3 Ejecute una comprobación del sistema de archivos en los volúmenes restaurados escribiendo el siguiente comando y, a continuación, pulse Intro:

```
fsck -f <volume>
```

Si fsck devuelve un valor correcto, el sistema de archivos estará verificado.

- 4 Vuelva a montar los volúmenes adecuados escribiendo el siguiente comando con el formato `mount <volume> <folder>` y, a continuación, pulse **Intro**.

Por ejemplo, si la ruta de acceso de los volúmenes es `prod/sda1` y la carpeta en la que quiere montarlos es `mnt`, escriba lo siguiente y, a continuación, pulse **Intro**:

```
mount /dev/sda1 /mnt
```

Uso de la línea de comandos para hacer que un equipo Linux pueda iniciarse

Una vez haya realizado una comprobación del sistema de archivos correcta en el volumen restaurado, deberá crear particiones de inicio.

GNU Grand Unified Bootloader (GRUB) es un cargador de inicio que permite que los administradores configuren qué sistema operativo o configuración de kernel específica se utiliza para iniciar el sistema. Después de una BMR, el archivo de configuración para GRUB debe modificarse para que el equipo utilice el identificador universalmente único (UUID) adecuado para el volumen raíz. Antes de este paso, debe montar los volúmenes raíz y de inicio, así como comprobar los UUID de cada uno. Esto garantizará que pueda iniciar desde la partición.

❗ NOTA: Este procedimiento se aplica a equipos Linux que utilizan GRUB1 o GRUB2. Cuando utilice este procedimiento, asegúrese de que la partición de inicio está en buen estado y protegida.

GRUB o GRUB2 normalmente se instala con los sistemas operativos Linux. Puede realizar este procedimiento utilizando la versión que viene con su distribución de Linux. Si una versión de GRUB no está instalada, tendrá que volver a instalar la versión predeterminada adecuada para su distribución de Linux.

⚠ PRECAUCIÓN: Cuando inicia un equipo Linux restaurado por primera vez tras una BMR, Rapid Recovery toma una imagen base del equipo restaurado. Dependiendo de la cantidad de datos del equipo, este proceso tarda más tiempo que al tomar una instantánea incremental. Para obtener más información sobre las imágenes base y las instantáneas incrementales, consulte [Comprensión del calendario de programación de protección..](#)

Esta tarea es un paso en [Realización de una restauración Bare Metal Restore para Linux](#). Forma parte del proceso para [Verificación de la restauración Bare Metal Restore desde la línea de comandos](#).

Realice la tarea siguiente para crear particiones de inicio mediante la línea de comandos.

- 1 Primero deberá montar el volumen raíz y luego el volumen de inicio. Monte cada volumen restaurado utilizando el siguiente comando:

- a Para montar el volumen raíz, escriba el siguiente comando y, a continuación, pulse **Intro**:

```
mount /<restored volume[root]> /mnt
```

Por ejemplo, si `/dev/sda2` es el volumen raíz, escriba `mount /dev/sda2 /mnt` y, a continuación, pulse **Intro**.

- b Para montar el volumen de inicio, escriba el siguiente comando y, a continuación, pulse **Intro**:

```
mount /<restored volume[boot]> /mnt/boot
```

Por ejemplo, si `/dev/sda1` es el volumen de inicio, escriba `mount /dev/sda1 /mnt/boot` y, a continuación, pulse **Intro**.

❗ | NOTA: Algunas configuraciones del sistema pueden incluir el directorio de inicio como parte del volumen raíz.

- 2 Si el tamaño del volumen aumenta (es decir, si el volumen de destino en el nuevo equipo Linux es mayor que el volumen que tenía el punto de recuperación), deberá eliminar todos los archivos de datos de mapa de bits existentes.
- 3 Obtenga el identificador universalmente único (UUID) de los nuevos volúmenes utilizando el comando `blkid`. Escriba lo siguiente y, a continuación, pulse **Intro**:

```
blkid [volume]
```

❗ | NOTA: También se puede usar el comando `ls -l /dev/disk/by-uuid`.

- 4 Si realiza una BMR en un disco totalmente nuevo en el equipo de destino, comente la partición intercambiada en `fstab` en su volumen raíz.
- 5 La modificación de las rutas de acceso de `fstab` y `mtab` debería realizarse en el volumen restaurado, no en el Live DVD. No es necesario modificar rutas de acceso en el Live DVD. Prepárese para la instalación de Grand Unified Bootloader (GRUB) escribiendo los siguientes comandos. Después de cada comando, pulse **Intro**:

```
mount --bind /dev /mnt/dev
```

```
mount --bind /proc /mnt/proc
```

```
mount --bind /sys /mnt/sys
```

- 6 Cambie el directorio raíz escribiendo el siguiente comando y, a continuación, pulsando **Intro**:

```
chroot /mnt /bin/bash
```

- 7 Obtenga el UUID anterior de la partición o particiones de los puntos de recuperación del archivo `/etc/fstab` y compárelo con los UUID de las particiones raíz (para Ubuntu y CentOS), de inicio (para CentOS y RHEL) o de datos escribiendo el siguiente comando y, a continuación, pulsando **Intro**:

```
less /mnt/etc/fstab
```

- 8 Obtenga el UUID anterior de la partición o particiones de los puntos de recuperación del archivo `/etc/mtab` y compárelo con los UUID de las particiones raíz (para Ubuntu y CentOS), de inicio (para CentOS y RHEL) y de datos escribiendo el siguiente comando y, a continuación, pulsando **Intro**:

```
less /mnt/etc/mtab
```

- 9 Si usa SLES 11, instale GRUB introduciendo los siguientes comandos, pulsando **Intro** en cada uno:

```
grub-install --recheck /dev/sda
```

```
grub-install /dev/sda
```

- 10 Si utiliza Ubuntu, CentOS 6.x, RHEL 6.x u Oracle Linux 6.x, instale GRUB; para ello, escriba el comando siguiente y, a continuación, pulse **Intro**:

```
grub-install /dev/sda
```

- 11 Si utiliza SLES 12, CentOS 7, RHEL 7 u Oracle 7, instale GRUB2; para ello, escriba el comando siguiente y, a continuación, pulse **Intro**:

```
grub2-install /dev/sda
```

- 12 Tras completar la instalación, ejecute una de las siguientes actualizaciones:

- Para SLES:

```
grub-install.unsupported --recheck /dev/sda
```

```
grub-install.unsupported /dev/sda
```

```
update-grub
```

❗ | NOTA: Si no existe el comando `update-grub` en su distribución de Linux, omita esta opción.

- Para otras distribuciones:

```
grub-install /dev/sda
```

```
update-grub
```

❗ | NOTA: Si no existe el comando `update-grub` en su distribución de Linux, omita esta opción.

- 13 Quite el disco Live DVD de la unidad de CD-ROM o DVD y reinicie el equipo con Linux.

Creación y visualización de informes

En esta sección se proporciona una descripción general de informes disponibles en el Core Rapid Recovery y en la Consola de administración central Rapid Recovery.

Temas:

- [Acerca de los informes de Rapid Recovery](#)
- [Central Management Console](#)

Acerca de los informes de Rapid Recovery

Puede generar informes a partir de la Core Console de Rapid Recovery. Algunos de estos informes también están disponibles desde la Consola de administración central.

Los informes disponibles se describen en las tablas siguientes.

Tabla 160. Informes de Rapid Recovery

El tipo de informe	Descripción
Informe de trabajos	Ofrece un informe sobre el estado de los trabajos correctos, los trabajos con fallos y los trabajos con errores. Los trabajos con fallos se pueden ver en un informe de error. Este tipo de trabajo se puede ejecutar desde la Core Console y la Consola de administración central. • Cuando se ejecuta desde el Core, este informe puede especificar los detalles de uno o más Cores. De manera predeterminada, este conjunto de información incluye los trabajos para todos los equipos (cada equipo protegido, replicado o de punto de recuperación únicamente en los Cores especificados). En los parámetros del informe, puede personalizar el informe. Use los filtros para seleccionar o excluir algunos equipos. También puede seleccionar o excluir los trabajos que son independientes de equipo, en cuyo caso el informe muestra solo el estado para los trabajos de Core. • Cuando se ejecuta desde la perspectiva de un equipo protegido desde la Core Console, el informe resultante muestra el estado de los trabajos solo para ese equipo protegido. • Cuando se ejecuta desde la Consola de administración central, este informe puede especificar los detalles de cualquier combinación de Cores o grupos de Cores configurados en la Consola. Los únicos parámetros configurables son el tipo de informe y el rango de fechas. Para obtener más información sobre este tipo de informe, consulte Descripción del informe de trabajo.
Informe de error	Proporciona información sobre los trabajos de Core con fallos para los criterios especificados. Este tipo de trabajo se puede ejecutar desde la Core Console y la Consola de administración central. • Cuando se ejecuta desde el Core, este informe puede incluir detalles del equipo protegido o excluirlos. Como el informe de trabajos, este informe solo se puede ejecutar desde un equipo protegido seleccionado en el Core. El informe resultante muestra detalles sobre los trabajos con fallos solo para el equipo protegido seleccionado. • Cuando se ejecuta desde la Consola de administración central, este informe puede especificar los eventos con fallos de cualquier combinación de Cores o grupos de Cores configurados en la Consola. Los únicos parámetros configurables son el tipo de informe y el rango de fechas.

El tipo de informe	Descripción
	Para obtener más información sobre este tipo de informe, consulte Comprensión del informe de error .
Informe de resumen	Proporciona información de resumen. De manera predeterminada, este conjunto de información incluye los trabajos para todos los equipos (cada equipo protegido, replicado o de punto de recuperación únicamente en los Cores especificados). En los parámetros del informe, puede personalizar el informe. Use los filtros para seleccionar o excluir algunos equipos. También puede seleccionar o excluir los trabajos que son independientes de equipo, en cuyo caso el informe muestra solo el estado para los trabajos de Core. Este informe no está disponible desde la perspectiva de cualquier equipo protegido único. Este tipo de trabajo se puede ejecutar desde la Core Console y la Consola de administración central. • Cuando se ejecuta desde la Core Console, las categorías de la información de este informe incluyen el Core, la licencia y el repositorio. La información se muestra en forma de lista, gráfico y tabla. • Cuando se ejecuta desde la Consola de administración central, este informe puede especificar información de resumen de Cores o grupos de Cores configurados en la Consola. Los únicos parámetros configurables son el tipo de informe y el rango de fechas. Las categorías de la información de este informe incluyen el Core, la licencia y el repositorio. El informe de resumen también incluye un informe sobre equipos protegidos y el de los trabajos correctos para todos los trabajos. La información se muestra en forma de lista, gráfico y tabla. Para obtener más información sobre este tipo de informe, consulte Comprensión del informe de resumen.
Informe de repositorio	Este tipo de informe le proporciona un informe de todos los repositorios en el Core o los Cores seleccionados. También puede seleccionar un único repositorio disponible en el Core. Este informe está disponible solo desde la Core Console y desde la perspectiva del Core. Para obtener más información sobre este tipo de informe, consulte Descripción del informe del repositorio.
Informe programado	También puede programar cualquiera de estos informes desde la Core Console. La programación de un informe hace que el informe que especifique se genere de forma repetida en el programa que defina. De forma opcional, puede establecer las notificaciones por correo electrónico cada vez que se genera un informe. Para obtener más información sobre la programación, modificación, pausa o eliminación de informes, consulte Administración de informes programados desde la Core Console.

En función del tipo de informe y los parámetros que haya seleccionado, puede generar un informe en uno o más Cores de Rapid Recovery o para uno o más equipos protegidos.

Desde la Consola de administración central, puede generar un informe para cualquier combinación de Core o grupos de Cores configurados en esa Consola.

Generación de un informe desde la Core Console

Puede generar informes a petición desde la Core Console. Deben aplicarse las siguientes reglas:

- Todos los informes se pueden generar desde la perspectiva del Core.
- Además, se pueden generar dos tipos de trabajos (el informe de trabajos y el informe de error) desde la perspectiva de un equipo protegido. En estos informes, los datos se generan solo para que pertenezcan al equipo seleccionado.
- Los informes de error contienen datos solo si han fallado los trabajos seleccionado en los Cores seleccionados (o equipos protegidos).

El método para generar informes a petición es similar, si el informe se genera a partir del objetivo del Core o si se genera desde la perspectiva de un equipo protegido. Sin embargo, la navegación es algo diferente.

También puede programar informes para generarlos de forma repetida. Para obtener más información sobre la programación, modificación, pausa o eliminación de informes, consulte [Administración de informes programados desde la Core Console](#).

Generación de un informe del Core a petición

Como se describe en el tema [Acerca de los informes de Rapid Recovery](#), se pueden generar todos los informes disponibles desde la Core Console.

Realice los pasos del siguiente procedimiento para generar un informe desde la perspectiva del Rapid Recovery Core.

- 1 Desplácese hasta la Core Console de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Más) y, a continuación, seleccione **Informes**.
Aparece la página **Informe de trabajos**. A la derecha del nombre del informe en el título de la página hay una flecha hacia abajo, con la que puede seleccionar otro tipo de informe.

Si desea generar un informe de trabajos, continúe con el [paso 6](#) para empezar a especificar los criterios del informe.
- 3 Para elegir otro tipo de informe, haga clic en la flecha situada a la derecha del nombre del informe para ver un menú con los informes disponibles.
- 4 Para definir informes programados, consulte [Programación de un informe](#).
- 5 Para generar solo un informe de repositorio, vaya al [paso 11](#).
- 6 Para generar un informe de resumen, de fallos o de resumen de trabajos, en el menú desplegable **Intervalo de fechas**, seleccione un intervalo de fechas.

Si no se elige un rango de fechas, se usa la opción predeterminada, últimos 31 días. Puede elegir entre las opciones de la siguiente tabla.

Opción	Descripción
Últimas 24 horas	Informe sobre la actividad del último día, en relación con la hora en que se genera el informe.
Últimos 7 días	Informe sobre la actividad de la última semana, en relación con la hora en que se genera el informe.
Últimos 31 días	Informe sobre la actividad de los 31 últimos días, en relación con la hora en que se genera el informe.
Últimos 90 días	Informe sobre la actividad de los 90 últimos días, en relación con la hora en que se genera el informe.
Últimos 365 días	Informe sobre la actividad del último año, en relación con la hora en que se genera el informe.
Todo el tiempo	Este periodo de tiempo abarca la vida útil del Core.
Personalizado	Este período de tiempo requiere que se especifiquen las fechas de inicio y finalización.
Mes hasta la fecha	Informe sobre la actividad desde el primer día del mes natural en curso hasta la fecha en que se genera el informe.
Año hasta la fecha	Informe sobre la actividad desde el primer día del año natural en curso hasta la fecha en que se genera el informe.

NOTA: En todos los casos, no hay datos para el informe anteriores a la implementación del Core, ni anteriores a la protección de los equipos en el Core.

- 7 En el caso de un informe de trabajos o de errores, en el menú desplegable **Cores de destino**, seleccione los Cores para los que desee generar el informe.
La selección predeterminada incluye todos los Cores disponibles.
- 8 En el menú desplegable **Equipos protegidos**, seleccione los equipos para los que desea generar el informe.
De manera predeterminada, en esta información se incluyen los trabajos para todos los equipos protegidos: todos los equipos protegidos, equipos replicados y equipos de punto de recuperación únicamente de los Cores especificados. Puede usar los parámetros de informe para personalizar el informe. Use los filtros para seleccionar o excluir equipos. También puede seleccionar o excluir los trabajos que son independientes del equipo, en cuyo caso el informe solo muestra el estado de los trabajos del Core.

Puede elegir entre:

Opción	Descripción
Seleccionar todo	Esta opción le permite seleccionar todos los equipos protegidos de este Core.

NOTA: Puede seleccionar todos los equipos y, a continuación, borrar algunos de ellos para especificar solo un subconjunto de la totalidad.

Opción	Descripción
Independiente de equipo	Seleccione esta opción para generar un informe que incluya los trabajos de un Core pero no de equipos concretos. Trabajos como la creación o eliminación de un repositorio, o la creación de un CD de inicio, no están asociados a un equipo concreto. Si va a implementar el software agente en un equipo que aún no está protegido, este tipo de trabajo también se considera independiente del equipo. Estos trabajos no tienen un equipo protegido en la columna de equipo protegido del informe resultante. Por el contrario, si implementa el software agente en un equipo ya protegido en el Core, el nombre del equipo protegido se incluye en el informe. No se considera independiente del equipo.
Equipos protegidos	Esta opción enumera todos los equipos protegidos de este Core. Puede seleccionarlos todos o solo algunos de los equipos protegidos.
Solo puntos de recuperación	Esta opción muestra los equipos que estuvieron protegidos, pero todavía tienen puntos de recuperación guardados en el repositorio.
[Cores de origen]	Si el Core es un Core de destino y replica puntos de recuperación de cualquier equipo protegido de un Core de origen, aparece el nombre de ese Core de origen (en mayúsculas). Esta opción enumera todos los equipos protegidos de ese Core de origen. Puede seleccionar todos los equipos replicados en este Core de destino o seleccionar solo algunos de ellos.
[Grupos personalizados]	Si tiene grupos personalizados creados en este Core, el nombre de cada grupo personalizado aparece como opción. Aparece cada objeto del grupo personalizado. Puede seleccionar todos los objetos en el grupo o solo algunos de ellos.

9 Si va a generar un informe de resumen, vaya al [paso 12](#).

10 En el caso de informes de trabajos, errores o de resumen de trabajos, en el menú desplegable **Tipos de trabajo**, seleccione los tipos de trabajo que desee.

De manera predeterminada, en esta información se incluyen todos los trabajos de los equipos protegidos seleccionados. Puede usar los parámetros de informe para personalizar el informe. Use los filtros para seleccionar o excluir los trabajos de la categoría de trabajos principales y todos los trabajos de la categoría de otros trabajos. También puede expandir cada una de estas categorías al definir parámetros de trabajo y seleccionar solo los tipos de trabajo de cada categoría que desea incluir en el informe. Active la casilla de cualquier tipo de trabajo para seleccionarlo o borrarlo. Puede seleccionar todos los trabajos de una u otra categoría, o solo algunos de ellos.

Puede elegir entre los siguientes tipos de **otros** trabajos:

11 En el caso de un informe de repositorio, en el menú Repositorios, seleccione los repositorios que desea incluir en el informe.

La selección predeterminada incluye todos los repositorios disponibles.

12 Haga clic en **Vista previa** para generar el informe con los criterios especificados.

Si no se encuentran los criterios de informe que ha seleccionado, el informe se genera, pero contiene una fila vacía. Por ejemplo, si no hay errores, el contenido de la columna Error es nulo en el informe.

13 Realice una de las siguientes acciones:

- Vea el informe generado en línea.
- Actualice el informe dinámicamente cambiando los criterios; a continuación, vuelva a hacer clic en **Vista previa**.
- Use el menú **Informes** para seleccionar un formato de exportación (incluido el formato predeterminado, PDF) y, a continuación, haga clic en  para exportar el informe. Para obtener más información sobre el menú Informes, consulte [Uso del menú de informes](#).
- Use la **barra de herramientas Informes** para ver, modificar o imprimir el informe. Para obtener más información sobre la barra de herramientas Informes, consulte [Uso de la barra de herramientas de informes](#).

Generación de un informe de equipo protegido a petición

Puede generar un informe de trabajos o un informe de error para cualquier equipo protegido.

Realice los pasos del procedimiento siguiente para generar un informe para un equipo protegido.

- 1 Desplácese hasta la Core Console de Rapid Recovery.
- 2 Desde el menú Equipos protegidos, haga clic en el equipo protegido para el que quiere ver un informe.

Aparece la página de resumen de los equipos protegidos seleccionados.

- 3 En la parte superior de la página, desde las opciones del menú que se encuentran al lado del nombre del equipo protegido, haga clic en la flecha hacia abajo junto a **Informes** y, a continuación, seleccione un tipo de informe.
 - Si desea generar un informe de todos los trabajos que pertenecen a este equipo protegido, incluidos los trabajos con fallos, haga clic en **Informe de trabajos** y empiece especificando los criterios de su informe.
 - Si desea generar una lista de los trabajos con fallos que pertenece solo a este equipo protegido, haga clic en **Informe de error** y empiece especificando los criterios de su informe.
- 4 Para un informe de error o de trabajos, desde el menú desplegable **Rango de fechas**, seleccione un rango de fechas.
Si no se elige un rango de fechas, se utiliza la opción predeterminada (Últimos 31 días). Puede elegir entre las opciones de la siguiente tabla.

Opción	Descripción
Últimas 24 horas	Actividad de los informes del último día, relativa a la hora en que generó el informe.
Últimos 7 días	Actividad de los informes de la última semana, relativa a la hora en que generó el informe.
Últimos 31 días	Actividad de los informes de los últimos 31 días, relativa a la hora en que generó el informe.
Últimos 90 días	Actividad de los informes de los últimos 90 días, relativa a la hora en que generó el informe.
Últimos 365 días	Actividad de los informes del último año, relativa a la hora en que generó el informe.
Todo el tiempo	Este periodo de tiempo abarca la vida útil del Core.
Personalizado	Este periodo de tiempo requiere que especifique las fechas de inicio y finalización.
Mes hasta la fecha	Actividad de los informes a partir del primer día del mes hasta la fecha del calendario actual en que generó el informe.
Año hasta la fecha	Actividad de los informes a partir del primer día del año hasta la fecha del calendario actual en que generó el informe.

NOTA: En todos los casos, no hay disponibles datos para el informe anteriores a la implementación del Core, ni anteriores a la protección de los equipos en el Core.

- 5 Desde el menú desplegable **Tipos de trabajos**, seleccione los tipos de trabajos adecuados.
De manera predeterminada, este conjunto de información incluye todos los trabajos para los equipos protegidos seleccionados. En los parámetros del informe, puede personalizar el informe. Use los filtros para seleccionar o excluir todos los trabajos de las categorías Trabajos principales y Otros trabajos. O puede expandir cada una de estas categorías al definir parámetros de trabajo y seleccionar solo los tipos de trabajo de cualquiera de las dos categorías que quiere que aparezcan en el informe. Haga clic en la casilla de verificación de cualquier tipo de trabajo para borrar o seleccionar ese tipo. Puede seleccionar algunos o todos los trabajos de una u otra categoría.
- 6 Haga clic en **Vista previa** para generar el informe con los criterios especificados.
Si no se encuentran los criterios del informe que ha seleccionado, aun así, se genera el informe, pero contiene una fila en blanco. Por ejemplo, si no hay errores, el contenido de la columna Error es nulo en el informe.
- 7 Realice una de las siguientes acciones:
 - Ver el informe generado en línea.
 - Actualice el informe de forma dinámica cambiando cualquiera de los criterios y, a continuación, haciendo clic de nuevo en **Vista previa**.
 - Utilice el **menú Informes** para seleccionar un formato de exportación y exportar el informe. Para obtener más información sobre el menú Informes, consulte [Uso del menú de informes](#).
 - Utilice la **barra de herramientas Informes** para ver, manipular o imprimir el informe. Para obtener más información sobre la barra de herramientas Informes, consulte [Uso de la barra de herramientas de informes](#).

Administración de informes programados desde la Core Console

Puede programar cualquiera de los informes disponibles desde la Core Console. La programación de un informe hace que éste se genere repetidamente en el futuro. El programa define si el informe se va a generar de forma diaria, semanal o mensual.

De manera opcional, Rapid Recovery permite enviar una notificación por correo electrónico a uno o más destinatarios cuando se genera cada informe. El correo electrónico especifica el tipo, el formato y el rango de fechas del informe e incluye el informe como un adjunto.

NOTA: Antes de que pueda enviar los informes por correo electrónico, debe configurar un servidor SMTP para el Core. Para obtener más información, consulte [Configuración de un servidor de correo electrónico](#).

Si elige o no enviar notificaciones por correo electrónico, puede guardar los informes generados de forma local o en una ubicación de red accesible al servidor del Core.

Debe especificar la notificación y la entrega por correo electrónico o una ubicación para guardar los informes. También puede elegir ambas opciones.

Esta sección incluye los siguientes temas:

Vínculos relacionados

- [Programación de un informe](#)
- [Modificación de una programación de informe](#)
- [Cómo pausar, reanudar o eliminar un informe programado](#)

Programación de un informe

Puede programar un informe disponible desde la Core Console. El informe genera el programa que definió hasta que pause o elimine el informe.

Debe especificar la notificación y la entrega por correo electrónico o una ubicación para guardar los informes. También puede elegir ambas opciones.

Complete los pasos de este procedimiento para programar un informe.

- Desplácese hasta la Core Console de Rapid Recovery.
- En la barra de iconos, haga clic en  (Más) y, a continuación, seleccione **Informes**. Aparece la página **Informe de trabajos**. Aparece una flecha hacia abajo a la derecha del nombre del informe actual.
- Haga clic en la flecha situada a la derecha del nombre del informe y, en el menú desplegable, seleccione **Informes programados**. Aparece la página **Informes programados**.
- Para programar la generación de un informe de forma repetida, haga clic en **Agregar**. Aparece el **Definir Asistente de programación de informes**.
- En la página **Configuración** del asistente, introduzca los detalles para el informe que quiere programar y, a continuación, haga clic en **Siguiente**. Estas opciones de configuración se describen en la tabla siguiente.

Tabla 161. Opciones de configuración del informe programado

Equipo	Informes disponibles
Nombre	Escriba el nombre de visualización que quiere asignar a este programa particular. El nombre predeterminado es Schedule report 1. Límite su nombre a 64 caracteres o menos. No utilice caracteres prohibidos ni frases prohibidas .
Formato de informe	Seleccione un formato de salida de informe. Si no selecciona un valor, se utiliza el formato predeterminado (pdf).
El tipo de informe	Seleccione el tipo de informe que desea generar de forma repetida.
Etiquetas	Seleccione las etiquetas que desea que aparezcan en el informe programado. Se requiere al menos una etiqueta.

Equipo	Informes disponibles
	La función Grupos personalizados permite agrupar objetos de Core en un contenedor lógico, para el que define una etiqueta. Mediante el parámetro Etiquetas del asistente Definir Asistente de programación de informes, puede seleccionar un grupo personalizado para el que se ejecutan los informes programados. Si no hay etiquetas personalizadas, las opciones disponibles en el menú desplegable Etiquetas incluyen Seleccionar todo y Equipos protegidos. Si aparecen grupos personalizados, cada grupo aparece como una opción. Puede seleccionar o borrar cualquiera de las opciones para incluir o excluir esos objetos en el informe programado.
Equipo protegido	Seleccione uno o más equipos protegidos que se incluirán en el informe. Esta opción no está disponible para el informe de repositorio.
Tipos de trabajo	Seleccione los tipos de trabajo que desea que aparezcan en el informe. De manera predeterminada, este conjunto de información incluye los trabajos para todos los equipos (cada equipo protegido, replicado o de punto de recuperación únicamente en los Cores especificados). En los parámetros del informe, puede personalizar el informe. Use los filtros para seleccionar o excluir algunos equipos. También puede seleccionar o excluir los trabajos que son independientes del equipo, en cuyo caso el informe solo muestra el estado de los trabajos del Core. Los parámetros de Tipos de trabajos no están disponibles para los tipos de informes Resumen del Core y Repositorio programado.

- 6 En la página **Destino** del asistente, seleccione un destino para los informes que quiere programar. Debe seleccionar uno de los siguientes y es posible que seleccione ambos. Cuando esté satisfecho con el resultado, haga clic en **Siguiente**.
- En el campo **Enviar a las direcciones de correo electrónico**, introduzca una o más direcciones de correo electrónico válidas para notificar a los usuarios por mensaje de correo electrónico cuando se genera un informe programado.
- NOTA:** Si no especifica las notificaciones por correo electrónico y la entrega, debe especificar una ubicación de almacenamiento.
- Seleccione **Guardar como archivo** para guardar los archivos del informe generado en una ubicación que especifique y, en el menú desplegable **Tipo de ubicación**, seleccione una opción de almacenamiento local, de red o de nube. A continuación, en el campo **Ubicación**, especifique información adicional de la ubicación como se describe en la tabla siguiente.

Tabla 162. Opciones de ubicación para los informes programados

Tipo de ubicación	Descripción del tipo de ubicación	Ubicación
Local	Seleccione el tipo de ubicación Local para guardar los informes generados en una ruta de acceso local accesible para el Core.	Especifique la ruta de acceso en el campo Ubicación. Escriba una ubicación accesible de forma local para el Core. Por ejemplo, para guardar los informes en la carpeta Informes en la unidad D, introduzca D:\Reports\.
Red	Seleccione el tipo de ubicación Red para guardar los informes generados en una ruta de acceso accesible para el Core en la red. Especifique la ruta de acceso en el campo Ubicación.	Especifique la ruta de acceso en el campo Ubicación. Escriba una ubicación accesible para el Core desde la red. Utilice el formato \\nombreServidor\nombreRecursoCompartido. Por ejemplo, para guardar los informes en el servidor Datos en la carpeta compartida denominada Informes, introduzca \\Data\Reports\. Especificar credenciales de red en los campos Nombre de usuario y Contraseña.

Tipo de ubicación	Descripción del tipo de ubicación	Ubicación
Nube	Seleccione el tipo de ubicación Nube para guardar los informes generados en una cuenta de almacenamiento de nube configurada en el Core. La cuenta de almacenamiento debe estar ya definida antes de realizar este paso. Para obtener información sobre cómo configurar una cuenta de almacenamiento de nube para trabajar con el Core, consulte Administración de cuentas de nube.	Desde el campo Cuenta, seleccione la cuenta de almacenamiento de nube adecuada que se va a utilizar para guardar los informes generados. Desde el campo Contenedor, especifique un contenedor adecuado en la cuenta de almacenamiento. Desde el campo Nombre de la carpeta, especifique una carpeta en la que se van a guardar los informes generados en el futuro.

- 7 Cuando esté satisfecho con sus opciones de destino, haga clic en **Siguiente**.
- 8 En la página del asistente de **calendario de programación**, desde el menú **Enviar datos**, seleccione una opción para determinar la frecuencia en la que se debe generar el informe que especificó. Puede generar informes diaria, semanal o mensualmente. Cada opción tiene sus propios parámetros, tal como se describe en la tabla siguiente.

Tabla 163. Opciones de frecuencia para generar informes programados

Frecuencia	Detalles de frecuencia	Parámetros de frecuencia
Diariamente	Genera y guarda o envía el informe especificado una vez al día a la hora especificada. La hora predeterminada para esta acción es las 12:00 AM (en función de la hora del servidor del Core).	Para cambiar la hora predeterminada en la que se genera el informe, en el campo de texto Hora, escriba un valor nuevo o utilice los controles para cambiar la hora, los minutos y AM o PM.
Semanalmente	Genera y guarda o envía una vez por semana el informe especificado a una hora especificada del día especificado. La hora predeterminada para esta acción es las 12:00 del domingo (en función de la hora del servidor del Core).	Para cambiar el día predeterminado en que se genera el informe, desde el menú Día de la semana, seleccione un día de la semana. Para cambiar la hora predeterminada en la que se genera el informe, en el campo de texto Hora, escriba un valor nuevo o utilice los controles para cambiar la hora, los minutos y AM o PM.
Mensualmente	Genera y guarda o envía una vez al mes el informe especificado en una fecha y hora específica del día. La fecha predeterminada para esta acción es el primer día de cada mes a las 12:00 AM (en función de la hora del servidor del Core).	Para cambiar la fecha predeterminada en que se genera el informe, desde el menú Día del mes, seleccione una fecha. Para cambiar la hora predeterminada en la que se genera el informe, en el campo de texto Hora, escriba un valor nuevo o utilice los controles para cambiar la hora, los minutos y AM o PM.

- 9 De manera opcional, en la página del asistente **Programa**, si desea evitar que el informe programado se genere hasta que reanude los informes en pausa, seleccione **Realizar pausa en la creación de informes inicialmente**.
Si quiere que este informe se genere según lo programado, desmarque esta opción.
- 10 Cuando esté satisfecho con el programa, haga clic en **Finalizar** para salir del asistente y guardar su trabajo.
La nueva programación de un informe aparece en la tabla de resumen Informes de resumen.

Modificación de una programación de informe

Una vez que se ha programado un informe, puede modificar cualquiera de sus parámetros o en detalles. Puede editar la información de configuración del informe (nombre del informe, formato de salida, tipo de informe) incluidos los repositorios. También puede cambiar opciones de notificación por correo electrónico y el destino para guardar el informe generado. Por último, también puede cambiar la programación del informe.

Realice los pasos de este procedimiento para modificar los parámetros de un informe programado.

- 1 Desplácese hasta la Core Console de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Más) y, a continuación, seleccione **Informes**.
Aparece la página **Informe de trabajos**. Una flecha hacia abajo aparece a la derecha del nombre del informe actual.
- 3 Haga clic en la flecha que hay a derecha del nombre del informe y, en el menú desplegable, seleccione **Informes programados**.
Aparece la página **Informes programados**.
- 4 En la tabla de resumen de informes programados, en la fila del informe que desea modificar, haga clic en el icono de configuración  y, a continuación, seleccione **Editar**.
Aparece el **Asistente para definir la programación de informes**.
- 5 Desplácese por las páginas del asistente y cambie los parámetros necesarios. Para obtener más información sobre los parámetros de este asistente, consulte el tema [Programación de un informe](#).
- 6 En la página **Programa** página del asistente, haga clic en **Finalizar** para cerrar el asistente y guardar los cambios.
El asistente se cierra y se modifica la programación del informe.

Cómo pausar, reanudar o eliminar un informe programado

Una vez se haya programado un informe, lo genera en el programa definido. Si quiere detener de forma temporal la generación de un informe programado, puede pausar el programa.

Si un informe programado se pone en pausa y desea reanudar la generación del informe, puede reanudar el informe tal como se describe en este procedimiento.

Si actualmente está generando un informe programado y ya no necesita generar ese informe, puede eliminarlo.

Para determinar si cualquier informe programado está en pausa, compruebe la columna de estado de la tabla de resumen de informes programados. Una esfera verde indica un informe programado activo; una esfera amarilla indica un programa pausado y una esfera roja indica un error.

Realice los pasos de este procedimiento para poner en pausa, reanudar o eliminar un programa para un informe.

- 1 Vaya a la Core Console de Rapid Recovery.
- 2 En la barra de iconos, haga clic en  (Más) y, a continuación, seleccione **Informes**.
Aparece la página **Informe de trabajos**. Aparece una flecha hacia abajo a la derecha del nombre del informe actual.
- 3 Haga clic en la flecha situada a la derecha del nombre del informe y, en el menú desplegable, seleccione **Informes programados**.
Aparece la página **Informes programados**.
- 4 En la tabla de resumen Informes programados, vea el estado de todos los informes programados, mediante los indicadores de colores.
- 5 Para cada informe que desea pausar o reanudar, seleccione la casilla de verificación de la primera columna.
- 6 Desde las opciones Informes programados que se encuentran encima de la tabla de resumen, haga lo siguiente:
 - Para pausar la generación de los informes seleccionados, haga clic en **Pausar**.
 - Para reanudar la generación de informes programados que se ha pausado, haga clic en **Reanudar**.
 - Para eliminar los programas seleccionados de los informes programados existentes, haga clic en **Eliminar**.
La eliminación de un informe programado solo impide la generación de informes futuros. Si se han guardado los informes programados anteriores, no se eliminan.

Uso del menú de informes

El menú Informes aparece en la parte superior de la página cuando se visualiza Informes. Este menú incluye un título del informe, que es también un menú desplegable que permite ver los tipos de informes disponibles. Debajo de este menú hay uno o varios filtros que le ayudarán a definir su criterios de informe.

Los filtros concretos disponibles dependen del tipo de informe. Para obtener información sobre los parámetros correspondientes a cada tipo de informe, consulte el tema en el que se describen los tipos de informe.

En la parte derecha del menú Informes hay ciertos controles. Estos controles, que se describen en la siguiente tabla, ayudan a generar y exportar el informe.

Tabla 164. Controles del menú Informes

Elemento de la IU	Descripción
Botón Vista previa	Haga clic en el botón Vista previa para generar un informe basado en el tipo de informe seleccionado y los parámetros de informe especificados en los filtros.
Menú desplegable de formato de exportación	El menú desplegable de exportación permite seleccionar un formato de salida del informe. Si no selecciona un valor, se usa el formato predeterminado (pdf).
Botón/icono Descargar	El botón Descargar permite exportar el informe generado en el tipo de formato seleccionado en el menú de exportación.

Los informes incluyen unidades de medida que permiten determinar más fácilmente si una columna se representa en GB, TB o segundos.

Si no le gusta el aspecto de un informe generado o exportado, puede cambiar la fuente utilizada en los informes. Para obtener más información, consulte [Administración de la configuración de informes](#).

Una vez que se genera un informe, puede usar la barra de herramientas de informes.

Vínculos relacionados

- [Descripción del informe de trabajo](#)
- [Comprensión del informe de error](#)
- [Comprensión del informe de resumen](#)
- [Información de los informes de la administración central de Cores de la consola](#)

Uso de la barra de herramientas de informes

Una vez lo haya creado en el menú Informes, el informe aparece debajo de una barra de herramientas Informes. La barra de herramientas puede ayudarle a manipular salida del informe, incluido el guardado y la impresión de los informes.

En la parte izquierda de la barra de herramientas, hay una opción de la barra lateral Alternar. Esta herramienta expande o contrae la barra lateral, lo que da acceso a algunas opciones de visualización más. A la derecha de la barra de herramientas, la opción Herramientas expande un menú desplegable que proporciona controles de navegación de informe. Los elementos de la barra de herramientas Informes se describen en la tabla siguiente.

Tabla 165. Icono de la barra de herramientas de informes

Icono	Descripción
	Barra lateral Alternar. Todas las páginas del informe se muestran como imágenes en miniatura. Otras opciones de la barra lateral no son compatibles.
	Barra lateral: Mostrar las imágenes en miniatura. Esta es la vista predeterminada para todas las páginas de un informe generado.
	Barra lateral: Mostrar resumen del documento. Esta función no es compatible.
	Barra lateral: Mostrar archivos adjuntos. No hay archivos adjuntos para los informes. Esta función no es compatible.
	Buscar. Permite buscar texto dentro del informe generado. Incluye las opciones para resaltar todo el texto que coincide con los criterios que ha introducido y también para hacer coincidir mayúsculas y minúsculas.
	Página anterior. Mover la vista del informe a la página anterior.
	Página siguiente. Pasar a la página siguiente en la vista del informe.
	Introducir número de página. Haga clic en el campo de texto del número de página, introduzca un número de página válido y pulse Entrar para pasar a esa página en la vista del informe.
	Alejar. Permite alejar la vista del informe generado. Cada vez que hace clic aleja más, hasta un mínimo del 25%.
	Acercar. Permite acercar la vista del informe generado. Cada vez que hace clic acerca más, hasta un máximo del 1000%.
	Zoom automático. Permite controlar la vista del zoom del informe generado, incluida la vista por tamaño real, ajuste de página, ancho completo o porcentaje, incluido el 50%, 75%, 100%, 125%, 150%, 200%, 300% o 400%.
	Abrir archivo. Permite navegar por el sistema de archivos para buscar y abrir un informe guardado.
	Imprimir. Permite imprimir el informe generado.
	Herramientas. El menú desplegable Herramientas se expande o contrae al hacer clic en este icono. Las opciones Herramientas se describen a continuación.
	Herramientas: Ir a la primera página. Permite navegar a la primera página del informe generado.
	Herramientas: Ir a la última página. Permite navegar a la última página del informe generado.
	Herramientas: Girar en el sentido de las agujas del reloj. Esta opción rota el lienzo del informe generado en el sentido de las agujas del reloj.

Icono	Descripción
	Herramientas: Girar en sentido contrario a las agujas. Esta opción rota el lienzo del informe generado en el sentido contrario a las agujas del reloj.
	Herramientas: Herramienta de mano. Cuando se selecciona esta herramienta, permite mover el informe haciendo clic y arrastrándolo a lo largo de la pantalla.
	Herramientas: Propiedades de documento. Proporciona información sobre las propiedades del documento del informe generado. Haga clic en Cerrar para cerrar la ventana.

Para obtener información sobre cómo generar un informe, consulte [Generación de un informe desde la Core Console](#). Para obtener información sobre cómo generar un informe para varios Cores en la Consola de administración central, consulte [Creación de un informe desde la Consola de administración central](#).

Descripción del informe de trabajo

El informe de trabajos está disponible para el Core de Rapid Recovery y los equipos protegidos en el Core. Este informe ofrece un método de ver el estado de los trabajos realizados por un Core o un equipo protegido seleccionado. Las filas o columnas que aparecen en el informe sin datos indican que el parámetro probado era nulo. Por ejemplo, si una columna (por ejemplo, Errores) aparece sin información, no se han producido errores para el registro seleccionado. Si el informe genera una fila en blanco, el trabajo del registro seleccionado refleja una actividad independiente de equipo.

Para obtener información sobre cómo generar un informe de trabajos del Core, consulte [Generación de un informe del Core a petición](#). Para obtener información sobre cómo generar un informe de trabajos para un equipo protegido, consulte [Generación de un informe de equipo protegido a petición](#).

Cuando genera un informe de trabajos, los detalles del informe incluyen lo siguiente:

- Criterios de selección del informe
- Una tabla de resumen que muestra una fila para cada trabajo en el rango de fechas que haya especificado. Además de incluir el Core, el equipo protegido y el tipo de trabajo adecuados, cada fila incluye:
 - Un resumen del trabajo
 - El estado del trabajo
 - Los errores relacionados con el trabajo
 - Las fechas de inicio y finalización del trabajo
 - La duración del trabajo en segundos
 - El trabajo total en MB

Si la información no es relevante para una categoría específica, la celda aparece sin información en el informe. Por ejemplo, si el Core para un equipo protegido especificado no tiene errores, la columna Error está en blanco en aquella fila del informe.

Comprensión del informe de resumen de trabajos

El informe de resumen de trabajos está disponible al realizar informes solo desde la perspectiva del Core; este informe no está disponible desde los informes de un equipo protegido. Este informe tiene un único resumen, que muestra información de resumen sobre todos los trabajos realizados en el Core, incluido un recuento de trabajos con errores, pasados y cancelados. Muestra más información que el informe de trabajos, porque especifica cada trabajo en una línea independiente del informe.

Para obtener información sobre cómo generar un informe de resumen de trabajos, consulte [Generación de un informe desde la Core Console](#).

Los parámetros de este tipo de informe incluyen:

- Intervalo de fechas
- Equipos protegidos
- Tipos de trabajo

Al generar un informe de resumen de trabajos, los detalles del informe incluyen los criterios de selección del informe, así como información sobre equipos protegidos, volúmenes y tipos de trabajos.

Información del Core

La parte del Core del informe de resumen incluye datos con respecto al Core de Rapid Recovery que se está reportando. Esta información incluye:

- El número de equipos protegidos del Rapid Recovery Core
- El número de equipos con trabajos con fallos

Resumen de equipos protegidos

La parte de Equipos protegidos del informe de resumen incluye datos de todos los equipos protegidos por el Rapid Recovery Core seleccionado y los volúmenes de esos equipos.

El gráfico muestra una línea para cada tipo de trabajo de cada equipo e incluye la proporción de trabajos realizados correctamente (de cualquier tipo), el número de trabajos pasados, el número de trabajos con errores y de trabajos cancelados. (Los trabajos cancelados no se tienen en cuenta para estas estadísticas).

Comprensión del informe de error

El informe de errores es un subconjunto del informe de trabajos y está disponible para el Core de Rapid Recovery y los equipos protegidos en el Core. Un informe de error solo incluye los trabajos cancelados y con fallos indicados en el informe de trabajos y los compila en un único informe que se puede imprimir y exportar. Si el informe se genera con una fila en blanco, no hay errores en el rango de fechas especificado de los criterios de su informe.

❗ NOTA: Los resultados de los parámetros de los equipos protegidos y de los Core de destino aparecen solo para el informe a nivel del Core.

Para obtener información sobre cómo generar un informe de trabajos del Core, consulte [Generación de un informe del Core a petición](#). Para obtener información sobre cómo generar un informe de trabajos para un equipo protegido, consulte [Generación de un informe de equipo protegido a petición](#).

Cuando se genera un informe de error, aparece una tabla de resumen que muestra una fila para cada trabajo en el rango de fechas especificado. Además de incluir el Core, el equipo protegido y el tipo de trabajo adecuados, cada fila incluye:

- Un resumen del trabajo
- El estado del trabajo
- Los errores relacionados con el trabajo
- Las fechas de inicio y finalización del trabajo
- La duración del trabajo en segundos
- El trabajo total en MB

Comprensión del informe de resumen

El informe de resumen está disponible para uno o más núcleos. Este informe no está disponible en los informes de un equipo protegido. El informe de resumen incluye información sobre los repositorios del Core de Rapid Recovery seleccionado y sobre los equipos protegidos por ese Core. La información aparece como dos resúmenes dentro de un informe.

Para obtener información sobre cómo generar un informe de resumen, consulte [Generación de un informe desde la Core Console](#).

Los parámetros de este tipo de informe incluyen:

- Intervalo de fechas
- Equipos protegidos

Al generar un informe de resumen, los detalles del informe incluyen los criterios de selección del informe, así como información sobre repositorios y equipos protegidos.

Información del Core

La parte del Core del informe de resumen incluye datos con respecto al Core de Rapid Recovery que se está reportando. Esta información incluye:

- La clave de licencia (identificador)
- La versión actual del software de Core de Rapid Recovery

Resumen de repositorios

La parte de repositorios del informe de resumen incluye datos de los repositorios ubicados en el Core de Rapid Recovery seleccionado. Esta información incluye:

- El número de repositorios en el Core de Rapid Recovery
- Un resumen de repositorios en el Core.

Resumen de equipos protegidos

La parte de Equipos protegidos del informe de resumen incluye datos de todos los equipos protegidos por los Cores de Rapid Recovery seleccionado. Incluye un gráfico y una tabla de resumen.

El gráfico muestra los equipos protegidos por el índice de trabajos correctos (de cualquier tipo), comparado con los trabajos con fallos. (Los trabajos cancelados no se tienen en cuenta para estas estadísticas).

La X o eje horizontal muestra el número de equipos protegidos. La Y o eje vertical muestra los niveles de trabajos correctos. Específicamente, el eje Y muestra, por equipo protegido, cuántos de ellos habían:

- Trabajos no realizados
- Tasa de menos del 50% correctos
- Tasa del 50% o más correctos
- Tasa del 100% correctos

Debajo del gráfico aparece información sobre los equipos protegidos. Esta información incluye:

- La cantidad de equipos protegidos

- El número de equipos protegidos con trabajos con fallos
- Una tabla de resumen, por equipo protegido, que muestra lo siguiente:
 - Nombre del equipo protegido
 - Volúmenes protegidos por el equipo
 - Espacio protegido, en GB (total y actual)
 - Velocidad de cambio por día (promedio y mediana)
 - Estadísticas del trabajo (satisfactorio, completado, con fallos, cancelado)
 - Si se ha aplicado el cifrado
- La versión del Core

Descripción del informe del repositorio

El informe de repositorio incluye información sobre los repositorios del Core de Rapid Recovery seleccionado y sobre los equipos protegidos por ese Core. La información aparece como dos resúmenes dentro de un informe.

Para obtener información sobre cómo generar un informe de repositorio del Core, consulte [Generación de un informe del Core a petición](#).

Los parámetros de este tipo de informe solo incluyen repositorios.

Al generar un informe de repositorio, los detalles del informe de cada repositorio incluyen una lista de resumen de repositorios en el Core.

Central Management Console

La Consola de administración central de Rapid Recovery es un componente opcional destinado para entornos con uno o más Core de Rapid Recovery. Este componente es un portal web que proporciona una interfaz central donde podrá agrupar, administrar y generar informes para varios Cores.

Los requisitos del sistema operativo para la Consola de administración central son idénticos a los del Core de Rapid Recovery. Estos componentes se pueden instalar en el mismo equipo o en distintos equipos, según sus necesidades.

Después de la instalación, debe configurar la Consola de administración central agregando Cores que desee administrar, ya sea de forma individual o como parte de grupos de Cores.

ⓘ | NOTA: Debe ejecutar el instalador con privilegios de administrador local.

Los sistemas operativos Windows 8, 8.1, y 10 y Windows Server 2012 y 2012 R2 deben tener la función ASP.NET 4.5 instalada en el servidor para que la interfaz gráfica de usuario se cargue correctamente. Esta configuración se incluye como parte del instalador Rapid Recovery.

Para obtener más información sobre cómo instalar este componente, consulte el tema "Instalación de la Consola de administración central Rapid Recovery en la *Guía de instalación y actualización de Dell Data Protection | Rapid Recovery*.

Para obtener más información sobre la configuración de este componente, consulte el tema [Configuración de la Consola de administración central Rapid Recovery](#) en la *Guía de usuario de Dell Data Protection | Rapid Recovery*.

Para obtener más información sobre cómo comprender la interfaz de usuario de este componente, consulte el tema [Descripción de la Consola de administración central de Rapid Recovery](#) en la *Guía de usuario Dell Data Protection | Rapid Recovery*.

Descripción de la Consola de administración central de Rapid Recovery

Al abrir la consola de administración central, se muestra la información en la vista Consola. La página de **bienvenida** aparece, y se pueden ver los siguientes elementos:

Tabla 166. Elementos de la interfaz de usuario en la Consola de administración central Rapid Recovery

Elemento de la IU	Descripción
Área de marca	Para entornos típicos, la parte superior izquierda de la Consola de administración central recibe el nombre del producto principal Dell Data Protection Rapid Recovery. Al hacer clic en cualquier parte del área del nombre, se redirecciona al usuario del navegador web a la documentación del producto del sitio web de asistencia técnica de Dell.
Área de navegación izquierda	El área de navegación izquierda aparece bajo el área de marca, en el lado izquierdo de la interfaz de usuario. Las funciones del área de navegación se diferencian según el modo seleccionado en la parte superior derecha de la Consola de administración central Modo de consola. En el área de navegación, en el modo de consola, al hacer clic en cualquier Core o grupo de Cores se abre el que está seleccionado en la Rapid Recovery Core Console. Modo de informes. En el área de navegación, en el modo de informes, seleccionar Cores o grupos de Cores determina el conjunto de información que aparecerá cuando genere los informes. Modo de administración. En el área de navegación, en el modo de administración, puede navegar a través de opciones disponibles para los Cores y grupos de Cores. También puede agregar y eliminar Cores y grupos de Cores en el modo de administración. Al hacer clic en las flechas se expande y contrae el menú. Se incluyen los siguientes niveles de jerarquía: organización, grupos de Cores, y Cores. Si hace clic en la flecha izquierda, el área de navegación se contraerá. Para expandir el área de navegación, haga clic en la flecha derecha.
Menú Vínculos	Póngase en contacto con Dell Support. Abre el sitio web de asistencia de Dell en una nueva ventana de navegación, que proporciona acceso a Chat en vivo, tutoriales de vídeo, artículos de la base de conocimientos de Rapid Recovery, preguntas más frecuentes y más.
Menú Vínculos	Documentación. Abre el sitio web de asistencia de Dell en una nueva ventana de navegación, que proporciona acceso a Chat en vivo, tutoriales de vídeo, artículos de la base de conocimientos de Rapid Recovery, preguntas más frecuentes y más.
Menú Vínculos	Versión. Muestra la versión actual de la Consola de administración central. Al hacer clic en este enlace, se abre el cuadro de diálogo Acerca de.
Menú Vínculos	Selector de modo. En la parte superior derecha del menú Vínculos, el nombre del usuario de Windows actual que ha iniciado sesión aparece en un menú desplegable. Desde este menú, puede cambiar la vista de la Consola de administración central. Puede seleccionar las vistas siguientes: Consola. Este es el modo predeterminado, que le permite ver los Cores y los grupos de Cores en su entorno desde una sola ubicación. Informes. Desde este modo, puede generar, ver y exportar informes a partir de los Cores configurados en esta consola. Administrar. Desde el modo de administración, puede quitar o añadir cores adicionales para la Consola de administración central, individuales o en grupos. Idioma. En las versiones que se admite la localización, la opción de idiomas está en la lista. Al seleccionar esta opción se abre el cuadro de diálogo Cambiar el idioma, desde el que podrá seleccionar un idioma de visualización de la Consola de administración central. .

Elemento de la IU	Descripción
	Borrar caché de cuenta. Seleccione esta opción para borrar la información existente de la cuenta del usuario que ha iniciado sesión.

Puede cambiar la vista de la Consola de administración central seleccionando una opción del selector de modo (menú desplegable de la parte superior derecha de la página). Por ejemplo:

- Para administrar Cores o grupos de Cores que ya se han configurado, utilice la vista Consola.
- Para configurar la Consola de administración central, cambie a la vista Administrar.
- Para generar informes, cambie a la vista Informes.

Los núcleos que puede ver y administrar aparecen en el menú de navegación que se encuentra a la izquierda. Puede configurar los núcleos individuales u organizarlos por grupo. Puede restringir el acceso a los Cores en grupos específicos con los grupos o nombres de usuario de Windows.

Configuración de la Consola de administración central Rapid Recovery

La configuración de la Consola de administración central Rapid Recovery implica agregar Cores y grupos de Cores, establecer su configuración y especificar la configuración de acceso para los grupos, si es necesario.

Una vez completada la configuración, puede administrar la configuración y todos los Cores desde una ubicación central.

Para configurar la Consola de administración central, puede realizar todas las tareas que se enumeran los vínculos relacionados siguientes.

Vínculos relacionados

- [Adición de un Core a la Consola de administración central](#)
- [Configuración de los ajustes del Core en la Consola de administración central](#)
- [Adición de un grupo de Cores a la Consola de administración central](#)
- [Configuración de los ajustes del grupo de Cores](#)
- [Configuración del acceso del grupo de Cores](#)

Adición de un Core a la Consola de administración central

Si desea agregar un Core a un grupo de Cores, primero se debe crear un grupo. Para obtener más información, consulte [Adición de un grupo de Cores a la Consola de administración central](#). También es posible editar los datos de Core posteriormente para especificar un grupo.

Agregue uno o varios Cores a la Consola de administración central para administrarlos o generar informes desde una única interfaz.

Complete los pasos del siguiente procedimiento para agregar un grupo de Cores a la Consola de administración central.

- 1 En la Consola de administración central Rapid Recovery haga clic en el menú desplegable del selector de modo y seleccione **Gestionar**.
La página se actualiza y muestra los iconos Agregar Core, Agregar grupo y Eliminar.
- 2 En la parte superior del menú de navegación que se encuentra a la izquierda, haga clic en **Agregar Core**.
Aparecerá la página **Agregar Core**.
- 3 Introduzca la información requerida para conectarse al Core, tal y como se describe en la siguiente tabla.

Tabla 167. Agregar datos de Core

Cuadro de texto	Descripción
Grupo principal	De forma opcional, si desea que el Core se una a un grupo Core existente, seleccione el grupo principal de la organización apropiada.
Nombre mostrado	Introduzca un nombre mostrado para el Core. El nombre de visualización debe limitarse a 150 caracteres o menos. La práctica recomendada es mantener este nombre por debajo de los 33 caracteres. No utilice caracteres no permitidos o frases no permitidas. Para obtener más información sobre el uso de caracteres o frases prohibidas, consulte la <i>Guía de usuario de Dell Data Protection Rapid Recovery</i>.
Nombre de host	Introduzca la dirección IP para acceder al Core. Si el Core que está agregando es el servidor actual, puede utilizar el host local.
Puerto	Introduzca un número de puerto para la conexión. El valor predeterminado es 8006.
Nombre de usuario	Introduzca un nombre de usuario para acceder al servicio de Core para el Core recién agregado.
Contraseña	Introduzca una contraseña para acceder al servicio de Core para el Core recién agregado.

- Haga clic en **Probar conexión** para probar la configuración.
Si la prueba es satisfactoria, se muestra un mensaje de confirmación. Haga clic en **Aceptar** para cerrar el mensaje de confirmación.
- Haga clic en **Guardar**.
Se guardan los cambios, y el Core se agrega ahora al grupo principal.

Vínculos relacionados

[Adición de un grupo de Cores a la Consola de administración central](#)

Configuración de los ajustes del Core en la Consola de administración central

Complete los pasos del siguiente procedimiento para configurar los ajustes de Core en la Consola de administración central.

- En la Consola de administración central Rapid Recovery haga clic en el menú desplegable del selector de modo y seleccione **Gestionar**.
La página se actualiza y muestra los iconos Agregar Core, Agregar grupo y Eliminar.
- En el menú de navegación que se encuentra a la izquierda, haga clic en el nombre de los correspondientes Core.
Aparecerá la página **Configuración** del Core seleccionado.
- En la ficha Configuración, modifique la información para el Core tal y como se describe en la siguiente tabla.

Tabla 168. Configuración del Core

Cuadro de texto	Descripción
Grupo principal	Seleccione el grupo principal de los Cores para la configuración del nuevo Core que desee agregar.
Nombre mostrado	Introduzca un nombre mostrado para el Core.
Nombre de usuario	Introduzca el nombre de usuario para el Core.

Cuadro de texto	Descripción
Contraseña	Introduzca la contraseña para el Core.
¿Cómo debe conectarse el portal de administración a [nombre del Core]?	Seleccione la opción que especifica la conexión. Puede elegir: - Usar la última dirección IP conocida del [nombre del Core] (xxx.xxx.xxx.xxx), o - Usar el nombre de host o la dirección IP [nombre de host o IP]. Si elige especificar la conexión a través del uso de un nombre de host o de la dirección IP, necesitará introducir la información apropiada en el campo nombre de host o de dirección.
¿En qué puerto se escucha [nombre del Core]?	Seleccione cualquiera de las opciones de puerto. Puede elegir: - Puerto predeterminado (8006), o - Puerto personalizado [port] Si elige especificar el puerto, introduzca el número de puerto en el campo Personalizar.

- Haga clic en **Probar conexión**.
Si la prueba es satisfactoria, aparecerá un mensaje indicándole que la conexión es correcta.
- Haga clic en **Guardar**.

Adición de un grupo de Cores a la Consola de administración central

Complete los pasos del siguiente procedimiento para agregar un grupo de Cores a la Consola de administración central de Rapid Recovery.

- En la Consola de administración central Rapid Recovery haga clic en el menú desplegable del selector de modo y seleccione **Gestionar**.
La página se actualiza y muestra los iconos Agregar Core, Agregar grupo de Cores y Eliminar.
- De la parte superior del menú de navegación que se encuentra a la izquierda, haga clic en **Agregar grupo**.
Aparece la página **Agregar grupo**.
- Seleccione el grupo principal y el nombre mostrado tal y como se describe en la siguiente tabla.

Tabla 169. Incorporación de un grupo de Cores

Cuadro de texto	Descripción
Grupo principal	Seleccione el grupo principal de los Cores para el nuevo grupo de Cores que quiere agregar.
Nombre mostrado	Introduzca un nombre para el grupo de Cores. El nombre de visualización debe limitarse a 150 caracteres o menos. La práctica recomendada es mantener este nombre por debajo de los 33 caracteres. No utilice caracteres no permitidos o frases no permitidas. Para obtener más información sobre el uso de caracteres o frases prohibidas, consulte la <i>Guía de usuario de Dell Data Protection Rapid Recovery</i>.

- Haga clic en **Guardar**.

Vínculos relacionados

[Adición de un grupo de Cores a la Consola de administración central](#)

Configuración de los ajustes del grupo de Cores

Antes de que pueda configurar los ajustes del grupo de Core, o acceder a ellos, debe crear el grupo. Para obtener más información, consulte [Adición de un grupo de Cores a la Consola de administración central](#).

Complete los pasos del siguiente procedimiento para configurar la configuración del grupo de Cores.

- 1 En la Consola de administración central Rapid Recovery haga clic en el menú desplegable del selector de modo y seleccione **Gestionar**.
La página se actualiza y muestra los iconos Agregar Core, Agregar grupo de Cores y Eliminar.
- 2 En el menú de navegación que se encuentra a la izquierda, haga clic en el nombre del grupo de Cores que desea configurar.
Aparece la página Configuración del grupo de Cores seleccionado.
- 3 Modifique la información para el grupo de Cores, según se describe en la siguiente tabla.

Tabla 170. Configuración del grupo de Cores

Cuadro de texto	Descripción
Grupo principal	Seleccione el grupo principal de los Cores para la configuración del nuevo grupo de Cores que quiere agregar.
Nombre mostrado	Introduzca un nombre para el grupo de Cores. El nombre de visualización debe limitarse a 150 caracteres o menos. La práctica recomendada es mantener este nombre por debajo de los 33 caracteres. No utilice caracteres no permitidos o frases no permitidas. Para obtener más información sobre el uso de caracteres o frases prohibidas, consulte la Guía de usuario de Dell Data Protection Rapid Recovery.

- 4 Haga clic en **Guardar**.

Configuración del acceso del grupo de Cores

Antes de que pueda configurar los ajustes del grupo de Core, o acceder a ellos, debe crear el grupo. Para obtener más información, consulte [Adición de un grupo de Cores a la Consola de administración central](#).

Para agregar o ver Cores en la Consola de administración central, la cuenta de usuario actual debe ser miembro del grupo de administradores del dominio de Active Directory. De manera alternativa, puede proporcionar acceso a grupos o usuarios individuales mediante este procedimiento.

Complete los pasos del siguiente procedimiento para configurar el acceso del grupo de Cores.

- 1 En la Consola de administración central Rapid Recovery haga clic en el menú desplegable del selector de modo y seleccione **Gestionar**.
La página se actualiza y muestra los iconos Agregar Core, Agregar grupo y Eliminar.
- 2 En el menú de navegación que se encuentra a la izquierda, haga clic en el nombre del grupo de Cores que desea configurar.
Aparece la página **Configuración** del grupo de Cores seleccionado.
- 3 Haga clic en la ficha **Acceso**.
La configuración de acceso del grupo de Cores aparece.
- 4 Haga clic en **Agregar**.
Se muestra el cuadro de diálogo **Permitir acceso**. Puede proporcionar acceso a una persona, o a un grupo.
- 5 Realice una de las siguientes acciones:
 - Si desea proporcionar acceso a una persona, a continuación, en el campo de texto, introduzca **Nombre**, introduzca el nombre de la persona, y, a continuación, haga clic en **Usuario**. Esta es la opción predeterminada.
Por ejemplo, escriba Administrador (o, si el equipo está en un dominio, [nombre de dominio] \Administrator).
 - Si desea proporcionar acceso a un grupo, entonces introduzca el nombre del grupo en el campo de texto **Nombre** y, a continuación, haga clic en **Grupo**.
Por ejemplo, escriba AdminGroup (o, si el equipo está en un dominio, [nombre de dominio] \AdminGroup).
- 6 Haga clic en **Comprobar nombre** para validar el nombre de usuario o grupo al que haya especificado que se puede acceder.
Si el nombre introducido es válido, aparece un mensaje de verificación de cuenta.
- 7 Una vez que ha introducido y validado un nombre, haga clic en **Guardar**.

Se cierra el cuadro de diálogo **Permitir acceso** y se guardan los cambios. El nombre de acceso aparece en la ficha Acceso del grupo de Cores.

Información de los informes de la administración central de Cores de la consola

Rapid Recovery le permite generar y ver informes de tareas, informes de fallo e información de resumen de varios Cores de Rapid Recovery. Los detalles sobre los Cores se presentan en tablas de resumen con las mismas categorías descritas en las secciones [Descripción del informe de trabajo](#), [Comprensión del informe de error](#) y [Comprensión del informe de resumen](#).

Para obtener más información sobre cómo generar un informe para varios Cores, consulte [Creación de un informe desde la Consola de administración central](#).

Creación de un informe desde la Consola de administración central

Realice el procedimiento siguiente para generar un informe para varios Cores de Rapid Recovery desde la Consola de administración central.

- 1 Desde la Consola de administración central de Rapid Recovery, haga clic en el menú desplegable Selector de modo en la esquina superior derecha y seleccione **Informes**.
Aparece la página de selección de informes. Se selecciona CoreJobReport de forma predeterminada. A la derecha del nombre del informe, aparece una flecha hacia abajo, desde la que puede seleccionar otro tipo de informe.
- 2 Desde el menú de navegación izquierdo, seleccione cualquier combinación de los Cores individuales o de los grupos de Cores de Rapid Recovery que quiere incluir en el informe.
- 3 Desde el menú desplegable Tipo de informe, seleccione el tipo de informe que desea generar. Puede elegir entre las opciones siguientes:
 - Informe de trabajos
 - Informe de errores
 - Informe de resumen
 - Informe de resumen de trabajos

Para obtener más información acerca de estos tipos de informe, consulte [Acerca de los informes de Rapid Recovery](#).

- 4 Desde el menú desplegable Rango de fechas, seleccione un rango de fechas.
Puede elegir entre las opciones de la siguiente tabla.

Opción	Descripción
Día	Actividad de los informes del último día, relativa a la hora en que generó el informe.
Semana	Actividad de los informes de la última semana, relativa a la hora en que generó el informe.
Mes	Actividad de los informes de los últimos 31 días, relativa a la hora en que generó el informe.
Año	Actividad de los informes del último año, relativa a la hora en que generó el informe.
Todo el tiempo	Este periodo de tiempo abarca la vida útil del Core.
Personalizado	Este periodo de tiempo requiere que especifique las fechas de inicio y finalización.

NOTA: En todos los casos, no hay datos de informe disponibles de antes de implementar el software del Core o de antes de que se protegieran los equipos en el Core.

- 5 Realice una de las siguientes acciones:
 - Haga clic en **Vista previa** para generar y ver el informe que se genere en línea.
 - Actualice el informe de forma dinámica cambiando los criterios del informe y, a continuación, haciendo clic de nuevo en **Vista previa**.
 - Elija un formato de exportación (incluido el formato predeterminado, XLSX) y haga clic en **Descargar**.

- Utilice la **barra de herramientas Informes** para ver, manipular o imprimir el informe. Para obtener más información sobre la barra de herramientas Informes, consulte [Uso de la barra de herramientas de informes](#).

Comprensión de la utilidad Administración de línea de comandos de Rapid Recovery

Dell Data Protection | Rapid Recovery se compone de varios componentes de software. Los componentes clave relevantes para este tema incluyen lo siguiente:

- El Core de Rapid Recovery gestiona la autenticación para equipos protegidos, los calendarios de programación para la transferencia de datos de la copia de seguridad y replicación, la exportación a máquinas virtuales, informes y bare metal restore (BMR) para hardware similar o diferente.
- Rapid Recovery Agent se encarga de las instantáneas del volumen y de la transferencia rápida de datos al repositorio administrado por el Core.
- La utilidad Administración de línea de comandos de Rapid Recovery, cmdutil.exe, proporciona acceso a terceros para administrar la funcionalidad del sistema. Esta herramienta permite la secuenciación de las funciones de administración de Rapid Recovery.

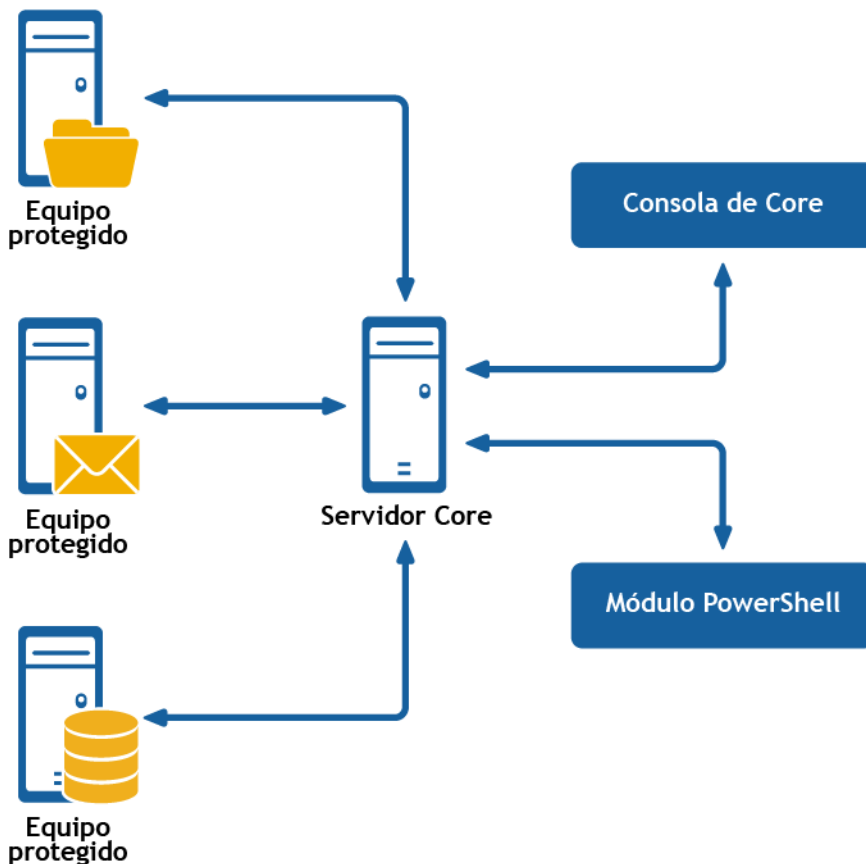


Ilustración 13. La Administración de línea de comandos de Rapid Recovery proporciona funciones de la línea de comandos

La Administración de línea de comandos de Rapid Recovery es una utilidad de línea de comandos para Windows que permite a los usuarios interactuar con el servidor de Core de Rapid Recovery. Ofrece algunas de las mismas funciones que la interfaz gráfica de usuario de Rapid Recovery. Por ejemplo, la utilidad Administración de línea de comandos de Rapid Recovery puede montar puntos de recuperación o forzar una instantánea.

La utilidad Administración de línea de comandos de Rapid Recovery se incrusta en todas las instalaciones del Core de Rapid Recovery. Para abrir la utilidad Administración de línea de comandos para una instalación predeterminada, navegue hacia la ruta de acceso **C:\Program Files\AppRecovery\Core\CoreService** y haga doble clic en el archivo `cmdutil.exe`.

En el modo de línea de comandos, se pueden transferir los indicadores de acción a la utilidad Administración de línea de comandos de Rapid Recovery mediante una selección de opciones y calificadores de comandos para realizar funciones de gestión limitadas.

Temas:

- [Comandos](#)
- [Traducción](#)

Comandos

En esta sección se describen los comandos y opciones disponibles para la utilidad Administración de línea de comandos de Rapid Recovery. Los siguientes comandos están disponibles para usarse:

- [Archivado](#)
- [CancelActiveJobs](#) (Cancelar trabajos activos)
- [CheckRepository](#)
- [CreateArchiveRepository](#)
- [CreateBootCD](#)
- [CreateRepository](#) (Crear repositorio)
- [DeleteRepository](#)
- [Dismount](#) (Desmontar)
- [DismountArchiveRepository](#)
- [EditEsxServer](#)
- [Forzar](#)
- [ForceAttach](#) (Forzar conexión)
- [ForceChecksum](#) (Forzar suma de comprobación)
- [ForceLogTruncation](#) (Forzar truncamiento del registro)
- [ForceMount](#) (Forzar montaje)
- [ForceReplication](#) (Forzar replicación)
- [ForceRollup](#) (Forzar consolidación)
- [ForceVirtualStandby](#)
- [Ayuda](#)
- [List](#) (Enumerar)
- [Montar](#)
- [MountArchiveRepository](#)
- [NewCloudAccount](#)
- [OpenDvmRepository](#)
- [Pausar](#)
- [Proteger](#)
- [Proteger clúster](#)
- [ProtectEsxServer](#)
- [RemoveAgent](#)
- [RemoveArchiveRepository](#)
- [RemovePoints](#) (Eliminar puntos)

- [RemoveScheduledArchive](#)
- [RemoveVirtualStandby](#)
- [Replicación](#)
- [Replicación](#)
- [RestoreAgent](#)
- [RestoreArchive](#) (Restaurar archivo)
- [RestoreUrc](#)
- [Reanudar](#)
- [SeedDrive](#)
- [StartExport](#) (Iniciar exportación)
- [UpdateRepository](#) (Actualizar repositorio)
- [Versión](#)
- [VirtualStandby](#)

Archivado

Las empresas suelen utilizar almacenamiento a largo plazo para archivar tanto los datos de conformidad como los de no conformidad. La función de archivo de Rapid Recovery es compatible con la retención ampliada de datos de conformidad y de no conformidad. El administrador puede guardar un archivo en la ubicación de red o de almacenamiento local especificando las credenciales y el parámetro `-path`.

Uso

El uso del comando es el siguiente:

```
/archive -core [host name] -user [user name] -password [password] -all | -protectedserver [name | IP address] -path [location] -startdate [time string] -enddate [time string] -archiveusername [name] -archivepassword [password] -comment [text]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `archive`:

Tabla 171. Opciones de comando Archive

Opción	Descripción
<code>-?</code>	Muestra el mensaje de ayuda.
<code>-core</code>	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
<code>-user</code>	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
<code>-password</code>	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
<code>-all</code>	Archivar todos los puntos de recuperación para todos los el equipos protegidos del Core.

Opción	Descripción
-protectedserver	Equipo protegido con puntos de recuperación que se deben archivar. Puede especificar varios nombres de equipo entre comillas dobles y separados por espacios.
-path	Ruta de acceso donde deben colocarse los datos archivados; por ejemplo: d:\work\archive o ruta de acceso de red \\servername\sharename.
-startdate	Fecha de inicio para seleccionar puntos de recuperación por fecha de creación. El texto del comentario se debe poner entre comillas dobles, por ejemplo, "04/30/2012 02:55 PM".
-enddate	Opcional. Fecha de finalización para seleccionar puntos de recuperación por fecha de creación. El valor se debe poner entre comillas dobles; por ejemplo, "05/31/2012 11:00 AM". Se utiliza el sistema de tiempo actual de forma predeterminada.
-archiveusername	Opcional. Nombre de usuario para el equipo remoto. Solo es requerido para la ruta de red.
-archivepassword	Opcional. Contraseña para el equipo remoto. Solo es requerido para la ruta de red.
-comment	Opcional. El texto del comentario se debe poner entre comillas dobles, por ejemplo, -comment "comment goes here...".

Ejemplos:

Todos los puntos de recuperación con fechas de creación que empiezan desde 04/30/2012 02:55 PM para todos los equipos del Core:

```
>cmdutil /archive -core 10.10.10.10 -user administrator -password 23WE0#$$sdd -path d:\work\archive -startdate "04/30/2012 02:55 PM" -all
```

Puntos de recuperación de archivo que entran en un rango de fechas para dos equipos protegidos:

```
>cmdutil /archive -core 10.10.10.10 -user administrator -password 23WE0#$$sdd -protectedserver "10.20.30.40" "20.20.10.1" -path d:\work\archive -startdate "04/30/2012 02:55 PM" -enddate "05/31/2012 11:00 AM"
```

CancelActiveJobs (Cancelar trabajos activos)

Utilice el comando `cancelactivejobs` para cancelar la ejecución de todos los trabajos en curso de un tipo específico, como una transferencia o replicación.

Uso

El uso del comando es el siguiente:

```
/cancelactivejobs -core [host name] -user [user name] -password [password] -jobtype [job type filter]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `cancelactivejobs`:

Tabla 172. Opciones de comando CancelActiveJobs

Opción	Descripción
-?	Mostrar ayuda sobre el comando.
-core	Opcional. Dirección IP del equipo host Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también debe proporcionar un nombre de usuario. Si no proporciona ninguna, se utilizan las credenciales del usuario que ha iniciado sesión.
-protectedserver	Determina el equipo protegido en el que deben cancelarse los trabajos.
-all	Seleccione y cancele eventos del tipo especificado para todos los servidores protegidos.
-jobtype	Opcional. Especifica el filtro del tipo de trabajo. Los valores disponibles son: • 'transfer' (transferencia de datos) • 'repository' (mantenimiento de repositorio) • 'replication' (replicaciones locales y remotas) • 'backup' (copia de seguridad y restauración) • 'bootcdbuilder' (crear CD de inicio) • 'diagnostics' (cargar registros) • 'exchange' (comprobación de archivos de Exchange Server) • 'export' (exportación del punto de recuperación) • 'pushinstall' (agentes de implementación) • 'restore' (restauración del punto de recuperación) • 'rollup' (consolidaciones del punto de recuperación) • 'sqlattach' (comprobaciones de la conectividad del Agent) • 'mount' (montaje de repositorio) De forma predeterminada, todos los trabajos del tipo especificado se cancelan.

Ejemplo:

Cancelar todos los trabajos de transferencia en Core 10.10.10.10:

```
>cmdutil /cancelactivejobs -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -jobtype transfer
```

CheckRepository

Puede usar el comando CheckRepository para verificar la integridad de un repositorio DVM existente creado en el AppAssure Core o Rapid Recovery Core.

Uso

El uso del comando es el siguiente:

```
/checkrepository -repository [repository name] | -all [check all repositories] -core [host name] -user [user name] -password [password] name] -force
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `CheckRepository`:

Tabla 173. Opciones del comando `CheckRepository`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-all	Opcional. Esta opción comprueba todos los repositorios DVM asociados al Core.
-repository	Nombre del repositorio DVM.
-force	Opcional. Esta opción realiza la comprobación sin confirmación.

Ejemplo:

Iniciar la comprobación del repositorio DVM:

```
>cmdutil /checkrepository -repository "Repository1" -core 10.10.10.10 -user administrator -password 23WE@#sdd
```

CreateArchiveRepository

Al crear un repositorio de archivación, se crea un destino para el contenido de un archivo comprimido programado. Esta función permite montar un punto de recuperación de archivos comprimidos y restaurar un equipo sin importar dichos archivos.

Uso

El uso del comando es el siguiente:

```
/createarchiverepository -core [host name] -user [user name] -password [password] name] -name [archive repository name] -path [path to the archive] -archiveusername [network user name] -
```

archivepassword [network password] -cloudaccountname [name of the cloud account] -cloudcontainer [name of the cloud container]

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `CreateArchiveRepository`:

Tabla 174. Opciones del comando `CreateArchiveRepository`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-name	Obligatorio. Nombre del repositorio de archivación.
-path	Ruta de acceso al archivo comprimido existente. Puede ser una ubicación local, de red o de nube. Por ejemplo, d:\trabajo\archivComprimido o \\nombreServidor\nombreRecursoCompartido.
-archiveusername	Opcional. Esta opción es el inicio de sesión en el equipo remoto. Solo es requerida para la ruta de red.
-archivepassword	Opcional. Esta opción es la contraseña para el equipo remoto. Solo es requerida para la ruta de red.
-cloudaccountname	Opcional. Esta opción es el nombre de visualización de una cuenta de nube existente. Solo es requerida para la ruta de nube.
-cloudcontainer	Opcional. Contenedor de nube donde está la archivación. Solo es requerida para la ruta de nube.

Ejemplos:

Cree un repositorio de archivación con el nombre "NuevoArchivoComprimido:"

```
>cmdutil /createarchiverepository -name NewArchive -core 10.10.10.10 -user administrator -password 23WE@#sdd -path d:\work\archive
```

Además, si un archivo comprimido contiene más de una ubicación, el comando debe incluir las rutas de acceso a todos los segmentos ordenados de 1 a N, donde N es igual al número de segmentos.

Cree un repositorio de archivación con el nombre "NuevoArchivoComprimidoSegmentos:"

```
>cmdutil /createarchiverepository -name NewSegmentArchive -path1 \\RemmoteServer1\Share\Archive\Segment1 -archiveusername1 Administrator -archivepassword1 23WE@#sdd -path2 Archives\NewSegment -cloudcontainer2 ArchiveContainer -cloudaccountname AmazonS3Local - path3 d:\work\archive\Third
```

CreateBootCD

Este comando le permite crear un CD de inicio de restauración Bare Metal Restore (BMR) sin tener que utilizar la Rapid Recovery Core Console.

Uso

El uso del comando es el siguiente:

```
/createbootcd -ip [IP address] -mask -defaultgateway -dnsserver -vncpassword -vncport -isofilepath [destination for the boot image]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `CreateBootCD`:

Tabla 175. Opciones del comando CreateBootCD

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-ip	Opcional. Esta opción especifica la dirección IP del equipo de destino para la BMR. De manera predeterminada, se genera automáticamente.
-mask	Opcional. Esta opción especifica la máscara de subred del equipo de destino para la BMR. De manera predeterminada, se genera automáticamente.
-defaultgateway	Opcional. Esta opción especifica la puerta de enlace predeterminada del equipo de destino para la BMR. De manera predeterminada, se genera automáticamente.
-dnsserver	Opcional. Esta opción especifica el servidor DNS del equipo de destino para la BMR. De manera predeterminada, se genera automáticamente.
-vncpassword	Opcional. Esta opción especifica la contraseña de usuario para una cuenta UltraVNC existente. De manera predeterminada, esta opción está vacía.
-vncport	Opcional. Esta opción especifica el puerto que se va a usar para UltraVNC. Se puede cambiar solo si ha utilizado la opción <code>-vncpassword</code> . De manera predeterminada, el puerto es 5900.
-isofilepath	Opcional. Esta opción especifica la ruta de acceso al archivo del CD de inicio. La ruta de acceso predeterminada es <code>C:\ProgramData\AppRecovery\Boot CDs</code> .

Ejemplo:

Crear un CD de inicio:

```
>cmdutil /createbootcd -ip 192.168.20.188 -mask 255.255.255.0 -defaultgateway 192.168.20.2 -dnsserver 192.168.20.2 -isofilepath D:\bcd\newbcd3.iso
```

CreateRepository (Crear repositorio)

Use el comando `createrepository` para crear un nuevo repositorio DVM en un equipo local o en una ubicación de uso compartido de CIFS.

Uso

El uso del comando cuando se crea un repositorio en una ubicación local es el siguiente:

```
/createrepository -name [repository name] -size [size allocated for repository] -datapath [data path of repository] -metadatapath [metadata path of repository] -core [host name] -user [user name] -password [password]
```

El uso del comando cuando se crea un repositorio DVM en una ubicación compartida es el siguiente:

```
/createrepository -name [repository name] -size [size allocated for repository] -uncpath [path for data and metadata] -shareusername [user name for share location] -sharepassword [password for share user name] -concurrentoperations [number of operations to occur at one time] -core [host name] -user [user name] -password [password]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `createrepository`:

Tabla 176. Opciones de comando CreateRepository

Opción	Descripción
-?	Mostrar ayuda sobre el comando.
-core	Opcional. Dirección IP del equipo host Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-name	Nombre de repositorio.
-size	Tamaño de la ubicación de almacenamiento del repositorio. Las unidades disponibles son b, Kb, Mb, Gb, Tb y Pb.
-datapath	Solo para la ubicación local. Determina la ruta de acceso a datos de la ubicación de almacenamiento del repositorio.
-metadatapath	Solo para la ubicación local. Determina la ruta de acceso a metadatos de la ubicación de almacenamiento del repositorio.
-uncpath	Solo para la ubicación compartida. Determina las rutas de acceso a metadatos y datos de la ubicación de almacenamiento del repositorio.
-shareusername	Solo para la ubicación compartida. Determina el nombre de usuario en la ubicación compartida.

Opción	Descripción
-sharepassword	Solo para la ubicación compartida. Determina la contraseña para la ubicación compartida.
-comment	Opcional. Descripción del repositorio.
-concurrentoperations	Opcional. Número máximo de operaciones que pueden estar pendientes simultáneamente. Valor predeterminado: 64

Ejemplos:

Crear un repositorio DVM en una ubicación local:

```
>cmdutil /createrepository -name "Repository 1" -size 200 Gb -datapath d:\repository -
metadatapath d:\repository -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd
```

Crear un repositorio DVM en una ubicación compartida:

```
>cmdutil /createrepository -name "Repository 1" -size 200 Gb -uncpath \\share\repository -
shareusername login -sharepassword pass123 -comment "First repository." -concurrentoperations 8
-core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd
```

DeleteRepository

Puede usar el comando DeleteRepository para quitar un repositorio DVM completo creado en el AppAssure Core o Rapid Recovery Core.

Uso

El uso del comando es el siguiente:

```
/deleterepository -core [host name] -user [user name] -password [password] name] -name
[repository name] | -a [all repositories]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comandoDeleteRepository:

Tabla 177. Opciones del comando DeleteRepository

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.

Opción	Descripción
-a	Opcional. Esta opción elimina todos los repositorios DVM asociados al Core.
-name	Nombre del repositorio DVM que desea eliminar.

Ejemplo:

Eliminar todos los repositorios DVM:

```
>cmdutil /deleterepository -a
```

Eliminar el repositorio con el nombre "nombreRepositorio":

```
>cmdutil /deleterepository -name RepositoryName
```

Dismount (Desmontar)

Use el comando `dismount` para desmontar un punto de recuperación montado especificado por la opción `-path`, desmontar puntos del Agent seleccionado por el parámetro `-protectedserver` o desmontar todos los puntos de recuperación montados (`-all`).

Uso

El uso del comando es el siguiente:

```
/dis[mount] -core [host name] -user [user name] -password [password] [-all | -protectedserver [name | IP address] | -path [location]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `dismount`:

Tabla 178. Opciones de comando Dismount

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-all	Desmonta todos los puntos de recuperación montados.
-protectedserver	Desmonta todos los puntos de recuperación montados para el agente actual.

Opción	Descripción
-path	Desmonta el punto de montaje seleccionado.

Ejemplo:

Desmontar un punto de recuperación montado en la carpeta c:\mountedrecoverypoint:

```
>cmdutil /dismount -core 10.10.10.10 -user administrator -password 23WE@#sdd -path c:\mountedRecoveryPoint
```

DismountArchiveRepository

Después de recuperar la información que desea desde un archivo comprimido montado, debe desmontar el archivo comprimido para evitar posibles problemas.

Uso

El uso del comando es el siguiente:

```
/dismountarchiverepository -core [host name] -user [user name] -password [password] name] -name [archive repository name]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `DismountArchiveRepository`:

Tabla 179. Opciones del comando DismountArchiveRepository

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-name	Obligatorio. Nombre del repositorio de archivación.

Ejemplos:

Desmontar el repositorio denominado "NuevoArchivoComprimido:"

```
>cmdutil /dismountarchiverepository -name NewArchive -core 10.10.10.10 -user administrator -password 23WE@#sdd -path d:\work\archive
```

EditEsxServer

Puede utilizar el comando `editEsxServer` siempre que desee realizar cambios en el número de máquinas virtuales VMware ESX(i) que desea proteger sin agentes.

Uso

El uso del comando es el siguiente:

```
/editEsxServer -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -add | -remove -virtualMachines [virtual machines collection | all] -autoProtect [object ID or name collection]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `editEsxServer`:

Tabla 180. Opciones del comando EditEsxServer

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-repository	Obligatorio. Nombre del repositorio asociado con el Core que desea utilizar para proteger la máquina virtual. ⓘ NOTA: El nombre debe escribirse entre comillas dobles.
-protectedserver	Utilice esta opción para editar objetos de vCenter y ESX(i) para un equipo protegido específico.
-add	Utilice esta opción para agregar un objeto de vCenter o ESXi especificado.
-remove	Utilice esta opción para quitar un objeto de vCenter o ESXi especificado.
-virtualmachines	Opcional. Esta opción permite generar una lista de las máquinas virtuales que desea proteger.
-autoprotect	Opcional. Esta opción permite generar una lista de nuevas máquinas virtuales que desea proteger automáticamente.

Ejemplos:

Proteger automáticamente objetos de vCenter o ESXi específicos de un servidor vCenter o ESXi con el Core:

```
>cmdutil /editEsxServer -protectedserver 10.10.8.150 -add -autoprotect "Folder1" "Folder2"
```

Forzar

El comando `force` fuerza una instantánea de un servidor protegido especificado. Forzar una instantánea permite forzar una transferencia de datos para el equipo protegido actual. Cuando se fuerza una instantánea, la transferencia empezará de inmediato o se añadirá a la cola. Solo se transferirán los datos que hayan cambiado con respecto a un punto de recuperación previo. Si no hay punto de recuperación previo, se transferirán todos los datos de los volúmenes protegidos.

Uso

El uso del comando es el siguiente:

```
/force [snapshot] default | [base] [-all | -protectedserver [name | IP address]] -core [host name] -user [user name] -password [password]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `force`:

Tabla 181. Opciones de comando Force

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-force	Opcional. Tipo de instantánea que se debe crear. Valores disponibles: 'snapshot' (instantánea incremental) y 'base' (instantánea de imagen base). De forma predeterminada, se realiza una instantánea incremental.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-all	Fuerza las instantáneas en todos los equipos del Core.
-protectedserver	Forzar una instantánea para un equipo protegido especificado.

Ejemplo:

Forzar una instantánea para todos los equipos del Core:

```
>cmdutil /force snapshot -core 10.10.10.10 -user administrator -password 23WE@#sdd -all
```

ForceAttach (Forzar conexión)

El comando `forceattach` le permite forzar una comprobación de capacidad de conexión de archivos de base de datos SQL. Cuando fuerza una comprobación de capacidad de conexión, la comprobación comienza inmediatamente.

Uso

El uso del comando es el siguiente:

```
/forceattach -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -rpn [number | numbers] | -time [time string]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `forceattach`:

Tabla 182. Opciones de comando ForceAttach

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-protectedserver	Equipo protegido en el que realizar la comprobación de conectividad.
-rpn	Número secuencial de un punto de recuperación en el que realizar comprobaciones (ejecutar comando/enumerar rps para obtener los números). Para realizar comprobaciones sobre varios puntos de recuperación puede especificar varios números separados por espacios.
-time	Seleccionar un punto de recuperación por su tiempo de creación. Debe especificar el momento exacto con el formato "mm/dd/aaaa hh:mm tt" (por ejemplo, "2/24/2012 09:00 AM"). Tenga esto en cuenta para especificar los valores de fecha y hora de la zona horaria establecida en su PC.

Ejemplo:

Realizar comprobaciones de conectividad para los puntos de recuperación con los números 5 y 7:

```
>cmdutil /forceattach -core 10.10.10.10 -user administrator -password 23WE@#$sdd -  
protectedserver 10.10.5.22 -rpn 5 7
```

ForceChecksum (Forzar suma de comprobación)

El comando `forcechecksum` le permite forzar una comprobación de integridad para cualquier Base de datos de mensajes de Exchange (MDB) que esté presente en el punto o puntos de recuperación especificados. Cuando fuerza una comprobación de suma de comprobación, el comando comienza inmediatamente.

Uso

El uso del comando es el siguiente:

```
/forcechecksum -core [host name] -user [user name] -password [password] -protectedserver [name  
| IP address] -rpn [number | numbers] -time [time string]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `forcechecksum`:

Tabla 183. Opciones de comando ForceChecksum

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-protectedserver	Equipo protegido en el que realizar la comprobación de suma de comprobación.
-rpn	Número secuencial de un punto de recuperación en el que realizar comprobaciones (ejecutar comando/enumerar rps para obtener los números). Para realizar comprobaciones sobre varios puntos de recuperación puede especificar varios números separados por espacios.
-time	Seleccionar un punto de recuperación por su tiempo de creación. Debe especificar el momento exacto con el formato "mm/dd/aaaa hh:mm tt" (por ejemplo, "2/24/2012 09:00 AM"). Tenga esto en cuenta para especificar los valores de fecha y hora de la zona horaria establecida en su PC.

Ejemplo:

Realizar una comprobación de suma de comprobación para los puntos de recuperación con los números 5 y 7:

```
>cmdutil /forcechecksum -core 10.10.10.10 -user administrator -password 23WE@#sdd -  
protectedserver 10.10.5.22 -rpn 5 7
```

ForceLogTruncation (Forzar truncamiento del registro)

Forzar el truncamiento del registro le permite realizar este trabajo una vez, bajo demanda. Trunca inmediatamente los registros del equipo Agent de SQL Server especificado.

Uso

El uso del comando es el siguiente:

```
/[forcelogtruncation | flt] -core [host name] -user [user name] -password [password] -  
protectedserver [name | IP address]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `forcelogtruncation`:

Tabla 184. Opciones de comando ForceLogTruncation

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
- protectedserver	Equipo protegido en el que realizar el truncamiento del archivo de registro.

Ejemplo:

Forzar truncamiento del registro para un servidor protegido:

```
>cmdutil /forcelogtruncation -core 10.10.10.10 -user administrator -password 23WE@#sdd -  
protectedserver 10.10.20.20
```


ForceMount (Forzar montaje)

Use el comando `forcemount` para realizar una comprobación de la capacidad de montaje del punto de recuperación puntual. Esto determina si se pueden montar o no el punto o puntos de recuperación especificados o si se pueden utilizar para restaurar los datos con copia de seguridad. Debe enumerar uno o más puntos de recuperación específicos en los que realizar la comprobación o un rango de tiempo durante el que crear los puntos de recuperación.

Uso

El uso del comando es el siguiente:

```
/forcemount -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -rpn [number | numbers] | -time [time string]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `forcemount`:

Tabla 185. Opciones de comando ForceMount

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-protectedserver	Equipo protegido en el que realizar la comprobación de la capacidad de montaje.
-rpn	Número secuencial de un punto de recuperación en el que realizar comprobaciones (ejecutar comando/enumerar rps para obtener los números). Para realizar comprobaciones sobre varios puntos de recuperación puede especificar varios números separados por espacios.
-time	Seleccionar un punto de recuperación por su tiempo de creación. Debe especificar el momento exacto con el formato "mm/dd/aaaa hh:mm tt" (por ejemplo, "2/24/2012 09:00 AM"). Tenga esto en cuenta para especificar los valores de fecha y hora de la zona horaria establecida en su PC.

Ejemplo:

Realizar comprobaciones de la capacidad de montaje para los puntos de recuperación con los números 5 y 7:

```
>cmdutil /forcemount -core 10.10.10.10 -user administrator -password 23WE@#sdd -protectedserver 10.10.20.20 -rpn 5 7
```

ForceReplication (Forzar replicación)

Use el comando `forcereplication` para forzar una transferencia puntual de datos replicados desde el Core de origen al Core de destino. Puede replicar un servidor protegido específico o replicar todos los servidores protegidos. Los servidores protegidos deben estar ya configurados para la replicación.

Uso

El uso del comando es el siguiente:

```
/[forcereplication |frep] -core [host name] -user [user name] -password [password] -targetcore [host name] -all | -protectedserver [name | IP address]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `forcereplication`:

Tabla 186. Opciones de comando ForceReplication

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no se proporciona ninguno, entonces se utilizan las credenciales para el usuario que haya iniciado sesión.
-targetcore	Nombre de host del Core de destino en el que se debe forzar la replicación.
-protectedserver	Equipo protegido que desea replicar.
-all	Fuerce la replicación en todos los equipos que se están replicando en el Core de destino.

Ejemplo:

Forzar la replicación en un servidor protegido en un Core de destino específico:

```
>cmdutil /forcereplication -target core 10.10.10.10 -protectedserver 10.20.30.40
```

ForceRollup (Forzar consolidación)

Utilice el comando `forcerollup` para forzar la consolidación de los puntos de recuperación en un equipo protegido.

Uso

El uso del comando es el siguiente:

```
/[forcerollup | fro] -core [host name] -user [user name] -password [password] -protectedserver [name | IP address]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `forcerollup`:

Tabla 187. Opciones de comando ForceRollup

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no se proporciona ninguno, entonces se utilizan las credenciales para el usuario que haya iniciado sesión.
-protectedserver	Opcional. Equipo protegido en el que realizar la consolidación.

Ejemplo:

Forzar consolidación para el Agent 10.10.10.1 en el Core:

```
>cmdutil /forcerollup -core 10.10.10.10 - user administrator -password 23WE@#sdd -  
protectedserver 10.10.10.1
```

ForceVirtualStandby

La exportación de datos desde una máquina protegida a un equipo virtual crea una máquina en modo de espera virtual. Si tiene una configuración de exportación virtual continua, puede utilizar este comando para forzar Rapid Recovery a fin de exportar datos a petición, independientemente de la hora programada.

Uso

El uso del comando es el siguiente:

```
/forcevirtualstandby -core [host name] -user [user name] -password [password login] -  
protectedserver [name] | -all
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `ForceVirtualStandby`:

Tabla 188. Opciones del comando ForceVirtualStandby

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-protectedserver	El nombre o nombres separados por espacios de máquinas virtualizadas.
-all	Este comando especifica si se fuerzan todas las exportaciones virtuales programadas.

Ejemplos:

Fuerce todas las exportaciones virtuales en espera:

```
>cmdutil /forcevirtualstandby -all
```

Fuerce las exportaciones virtuales en espera de dos equipos:

```
>cmdutil /forcevirtualstandby -protectedserver 10.10.35.48 10.10.35.69
```

Ayuda

El comando `help` muestra una lista de los comandos disponibles y sus definiciones. También proporciona información sobre los derechos de autor y detalles de la versión.

Uso

El uso del comando es el siguiente:

```
/help
```

Ejemplo:

Solicitar ayuda de línea de comandos:

```
>cmdutil /help
```

List (Enumerar)

El comando `list` devuelve información sobre todos los puntos de recuperación, trabajos activos, trabajos completados, trabajos con errores, puntos de recuperación no válidos (con error), puntos de recuperación válidos (aprobados), montajes, servidores protegidos, volúmenes, servidores virtualizados, volúmenes no protegidos, clústeres, grupos de protección, bases de datos de SQL, bases de datos de Exchange, servidores replicados y repositorios para el Agent especificado o lista de servidores protegidos actualmente por el Core. De forma predeterminada, el resultado son los registros más recientes. Puede enumerar todos los registros o especificar cuántos registros se muestran usando un parámetro de número. Este parámetro debe contener la letra "l" para los puntos de recuperación más recientes y "f" para el primer punto de recuperación. Cada punto de recuperación tiene su propio número, que el administrador puede usar para el montaje.

Uso

El uso del comando es el siguiente:

```
/list [rps | passed | failed | mounts | volumes | protectedservers | activejobs | completed jobs | failedjobs | virtualizedservers | unprotectedvolumes | clusters | protectiongroups | sqldatabases | exchangemailstores | replicatedservers | repositories] -protectedserver [name | IP address] -core [host name] -user [user name] -password [password] -number [all | l<number> | f<number> | <number>] -jobtype
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `list`:

Tabla 189. Opciones de comando List

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-list	Seleccione una de las opciones siguientes: • todos los puntos de recuperación ('rps') • puntos de recuperación válidos ('passed') • puntos de recuperación no válidos ('failed') • montajes ('mounts') • volúmenes protegidos ('volumes') • volúmenes no protegidos ('unprotectedvolumes') • equipos protegidos ('protectedservers') • trabajos activos ('activejobs') • trabajos con error ('failedjobs') • trabajos completados ('completedjobs') • servidores virtualizados ('virtualizedservers') • clústeres ('clusters') • grupos de protección ('protectiongroups') • bases de datos de SQL Server ('sqldatabases') • bases de datos de MS Exchange ('exchangemailstores') • servidores replicados ('replicatedservers') • repositorios ('repositories')

Opción	Descripción
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-all	Solo para trabajos de visualización. Muestre todos los eventos de un tipo específico (activo/con error/completado) en el servidor Core.
-protectedserver	Equipo protegido con puntos de recuperación para mostrar.
-number	Opcional. Número de elementos de datos para mostrar. Utilice solo con los siguientes especificadores: "rps", "activejobs", "completedjobs", "failedjobs". Los valores disponibles son: - all (recuperar todos los elementos de datos) - l[número] o [número] (devuelve los mejores ## datos) - f[número] (recuperar los primeros ## datos) Solo entra en vigor cuando se muestran puntos de recuperación y trabajos.
-jobtype	Opcional. Salida de filtro por tipo de trabajo. Los valores disponibles son: 'transfer' (transferencia de datos) 'repository' (mantenimiento de repositorio) 'replication' (replicaciones locales y remotas) 'backup' (copia de seguridad y restauración) 'bootcdbuilder' (crear CD de inicio) 'diagnostics' (cargar registros) 'exchange' (comprobación de archivos de Exchange Server) 'export' (exportar punto de recuperación) 'pushinstall' (Agents de implementación) 'restore' (restauraciones de punto de recuperación) 'rollup' (consolidaciones de los equipos protegidos) 'sqlattach' (comprobaciones de la conectividad del Agent)) 'mount' (montaje de repositorio)

Ejemplos:

Enumerar los 30 puntos de recuperación más recientes:

```
>cmdutil /list rps -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22 -number 130
```

Ver todos los trabajos de transferencia de datos con errores realizados por un equipo protegido:

```
>cmdutil /list failed jobs -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22 -number all -jobtype transfer
```

Montar

El comando `mount` monta una instantánea de una o varias unidades. Puede especificar si el montaje debe ser de lectura, escritura o solo lectura con escrituras anteriores. La selección predeterminada es solo lectura.

Uso

El uso del comando es el siguiente:

```
/mount -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -mounttype [read | write | readOnlyWithPreviousWrites] -drives [drive names] -volumes [volume names] -path [location] -rpn [number | numbers] | -time [time string]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `mount`:

Tabla 190. Opciones de comando Mount

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-protectedserver	Equipo protegido con un punto o puntos de recuperación para montaje.
-mounttype	Opcional. Especifica un modo de montaje. Los valores disponibles son: 'read' (read-only), 'readOnlyWithPreviousWrites' (solo lectura con escrituras previas), 'write' (modificable). El modo predeterminado es read-only.
-volumes	Opcional. Lista de nombres de volumen que deben montarse. Si no se especifican, se montarán todos los volúmenes. Los valores deben estar entre comillas dobles y separados por espacios; por ejemplo: "c:" "d:". No utilice barras finales en nombres de volúmenes.
-path	Ruta de acceso a una carpeta del servidor de Core en el que se debe montar el punto de recuperación. Si no existe, se crea automáticamente una carpeta.
-rpn	Opcional. El número secuencial de un punto de recuperación que se va a montar (use el comando <code>list rps</code> para obtener los números). Especifique varios números separados por espacios para montar varios puntos de recuperación con un único comando. En este caso, los datos de cada punto de recuperación se almacenarán en una carpeta secundaria distinta. Nota: si no se especifica ninguna opción (-time o -rpn), se monta el punto de recuperación que haya aprobado la comprobación de integridad más recientemente.

Opción	Descripción
-time	Opcional. Determina el punto o puntos de recuperación que se deben seleccionar para montaje. Los valores disponibles incluyen: 'latest', 'passed', fecha y hora exactas en el formato "mm/dd/aaaa hh:mm tt" (por ejemplo, "2/24/2012 09:00 AM"). Tenga esto en cuenta para especificar los valores de fecha y hora de la zona horaria establecida en su PC. Si no se especifica ninguna opción (-time o -rpn), entonces se monta el punto de recuperación que haya aprobado la comprobación de integridad más recientemente.
-localdrive	Opcional. Realice el montaje en el disco de usuario en un PC local.

Ejemplos:

Montar los puntos de recuperación más recientes que contengan los volúmenes "c:\\" y "d:\\" en modo de solo lectura:

```
>cmdutil /mount -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22 -path c:\mountedrecoverypoint -mounttype read -volumes "c:" "d:"
```

Montar los puntos de recuperación con números 2 y 7:

```
>cmdutil /mount -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22 -path c:\mountedrecoverypoint -rpn 2 7
```

MountArchiveRepository

Para restaurar datos desde un archivo comprimido en Rapid Recovery, primero debe montarlo.

Uso

El uso del comando es el siguiente:

```
/mountarchiverepository -core [host name] -user [user name] -password [password] -name [archive repository name]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `mountarchiverepository`:

Tabla 191. Opciones del comando MountArchiveRepository

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.

Opción	Descripción
-name	Obligatorio. Nombre del repositorio de archivación.

Ejemplos:

Monte el repositorio denominado "NuevoArchivoComprimido:"

```
>cmdutil /mountarchiverepository -name NewArchive
```

NewCloudAccount

Utilice el comando NewCloudAccount para agregar una cuenta para un proveedor de nube al Core de Rapid Recovery. A continuación, puede utilizar la cuenta para almacenar archivos de retención o replicación.

Uso

El uso del comando es el siguiente:

```
/newcloudaccount -core [host name] -user [user name] -password [password] -displayname [name for the account] -type [cloud account provider] -username [user name for the account] -key [secret key] -region [region for account] tenanatid [tenant ID] -authurl [authorization URL]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comandoNewCloudAccount:

Tabla 192. Opciones del comando NewCloudAccount

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-displayname	El nombre que desea utilizar para la cuenta de nube.
-type	El tipo de cuenta de nube. Los valores compatibles son: - amazon - openstack - rackspace - windowsazure "windows azure"

Opción	Descripción
	• azure
-username	El nombre de usuario de la cuenta de nube que desea agregar. Esta es la credencial que usa en el proceso de autenticación. La propiedad tiene las siguientes variaciones en función del tipo de nube: • Amazon - Clave de acceso • OpenStack - Nombre de usuario • Rackspace -Nombre de usuario • Windows Azure - Nombre de la cuenta de almacenamiento
-key	La clave de autenticación para la cuenta de nube que desea agregar. Esta es la credencial que usa en el proceso de autenticación. La propiedad tiene las siguientes variaciones en función del tipo de nube: • Amazon - Clave secreta • OpenStack - Clave API • Rackspace - Clave API • Windows Azure - Clave de acceso
-region	La región de la cuenta de nube que desee agregar. Esta opción se requiere únicamente para la creación de cuentas de OpenStack y Rackspace.
-tenantid	El ID se utiliza para autenticar una cuenta de nube de OpenStack. Esta opción se requiere únicamente para la creación de cuentas de OpenStack.
-authurl	La URL que utiliza para autenticar una cuenta de nube de OpenStack. Esta opción se requiere únicamente para la creación de cuentas de OpenStack.

Ejemplos:

Agregue una nueva cuenta de nube con el nombre "Cuenta de Amazon S3" con la clave de acceso "akey" y la clave secreta "skey".

```
>cmdutil /newcloudaccount -displayname "Amazon S3 Account" -type amazon -username akey -key skey
```

OpenDvmRepository

Utilice este comando para quitar un repositorio DVM completo creado en el AppAssure Core o Rapid Recovery Core.

Uso

El uso del comando es el siguiente:

```
/opendvmrepository -localpath [local path] -sharepath [network share path] -shareusername [user name for network share] -sharepassword [network share password]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `OpenDvmRepository`:

Tabla 193. Opciones del comando OpenDvmRepository

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-localpath	La ruta de acceso a la carpeta con un repositorio DVM en el Core local.
-sharepath	La ruta de acceso a la carpeta con el repositorio DVM en un recurso compartido de CIFS.
-shareusername	El nombre de usuario que utiliza para iniciar sesión en la carpeta compartida.
-sharepassword	La contraseña que utiliza para iniciar sesión en la carpeta compartida.

Ejemplo:

Abra un repositorio DVM existente en el equipo local:

```
>cmdutil /opendvmrepository -localpath E:\Repository
```

Pausar

Un administrador puede pausar las instantáneas, exportar a una máquina virtual o replicar un Core. El comando `pause` acepta tres parámetros: `snapshot` y `vmexportreplication`. Sólo se puede especificar un parámetro. Una instantánea se puede pausar hasta un momento determinado si se especifica un parámetro de tiempo.

Los usuarios pueden pausar las replicaciones de tres modos:

- En un Core de origen para todas las máquinas protegidas. (`-[outgoing]`).
El administrador debe especificar el nombre del equipo remoto emparejado con la replicación saliente para pausar la replicación saliente en el Core de origen:

```
>cmdutil /pause replication /o 10.10.12.10
```

- En un Core de origen para una única máquina protegida. (`-protectedserver`):

```
>cmdutil /pause replication /protectedserver 10.10.12.97
```

- En un Core de destino (`-incoming`).

Si el Core local es un Core de destino, el administrador puede pausar la replicación especificando el Core de origen mediante el parámetro `incoming` (entrante):

```
>cmdutil /pause replication /i 10.10.12.25
```

Uso

El uso del comando es el siguiente:

```
/pause [snapshot | vmexport | replication] -core [host name] -user [user name] -password [password] -all | -protectedserver [name | IP address] -incoming [host name] | outgoing [host name] -time [time string]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `pause`:

Tabla 194. Opciones de comando `Pause`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-pause	[snapshots], [replication] o [vmexport].
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-all	Opcional. Pausa todos los agents en el Core seleccionado.
-protectedserver	Opcional. Pausa el servidor protegido actual.
-incoming	Opcional. Nombre de host del Core remoto que se replica en el equipo Core.
-outgoing	Opcional. Nombre de host del Core de destino remoto en el que se replican los datos.
-time	Opcional. La hora, en formato 'Día-Horas-Minutos', a la que se reanudarán las instantáneas (solo para pausa de instantáneas).

Ejemplos:

Pausar la creación de instantáneas para un servidor protegido específico:

```
>cmdutil /pause snapshot -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.10.4
```

Pausar la creación de instantáneas para un equipo protegido y reanudarla después de tres días, 20 horas y 50 minutos:

```
>cmdutil /pause snapshot -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.10.4 -time 3-20-50
```

Pausar la exportación a una máquina virtual para todos los equipos protegidos en el Core:

```
>cmdutil /pause vmexport -core 10.10.10.10 /user administrator -password 23WE@#$sdd -all
```

Pausar la replicación saliente en el Core para un equipo protegido específico:

```
>cmdutil /pause replication -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.1.76
```

Pausar la replicación saliente para todos los equipos protegidos del Core de destino:

```
>cmdutil /pause replication -core 10.10.10.10 -user administrator -password -23WE@#sdd -  
outgoing 10.10.1.63
```

Pausar la replicación entrante para todos los equipos protegidos del Core de destino:

```
>cmdutil /pause replication -core 10.10.10.10 -user administrator -password 23WE@#sdd -  
incoming 10.10.1.82
```

Proteger

El comando `protect` agrega un servidor con protección de un Core.

Uso

El uso del comando es el siguiente:

```
/protect -core [host name] -user [user name] -password [password] -repository [name] -agentname  
[name | IP address] -agentusername [user name] -agentpassword [password] -agentport [port] -  
volumes [volume names]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `protect`:

Tabla 195. Opciones de comando Protect

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-repository	Nombre de un repositorio del Core donde se deben almacenar los datos de equipos protegidos. El nombre se debe poner entre comillas dobles.
-agentname	Nombre o dirección IP del servidor que desea proteger.
-agentusername	Nombre de usuario para el servidor que se debe proteger.
-agentpassword	Contraseña para el servidor que se debe proteger.
-agentport	Número de puerto de servidor protegido.
-volumes	Lista de volúmenes para proteger. Los valores deben estar entre comillas dobles y separados por un espacio. No utilice barras finales en nombres de volúmenes; por ejemplo: "c:" "d:".

Ejemplo:

Proteger volúmenes específicos de un servidor con el Core:

```
>cmdutil /protect -core 10.10.10.10 -username administrator -password 23WE@#sdd -repository "Repository 1" -agentname 10.10.9.120 -agentport 5002 -agentusername administrator agentpassword 12345 -volumes "c:" "d:"
```

Proteger clúster

El comando `protectcluster` agrega un clúster con protección de un Core.

Uso

El uso del comando es el siguiente:

```
/protectcluster -core [host name] -user [user name] -password [password] -repository [name] -clustername [name | IP address] -clusterusername [user name] -clusterpassword [password] -clusterport [port] -clustervolumes [volume names] -clusternodes [cluster nodes collection]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `protectcluster`:

Tabla 196. Opciones de comando ProtectCluster

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-repository	Nombre de un repositorio del Core donde se deben almacenar los datos de equipos protegidos. El nombre se debe poner entre comillas dobles.
-clustername	Nombre o dirección IP del clúster que desea proteger.
-clusterusername	Nombre de usuario para el clúster que se debe proteger.
-clusterpassword	Contraseña para el clúster que se debe proteger.
-clusterport	Número de puerto de servidor de clúster protegido.

Opción	Descripción
-clustervolumes	Lista de volúmenes para proteger. Los valores deben estar entre comillas dobles y separados por un espacio. No utilice barras finales en nombres de volúmenes; por ejemplo: "c:" "d:".
-clusternodes	Lista de nodos de clúster y volúmenes que desea proteger en cada nodo.

Ejemplo:

Proteger volúmenes específicos de un servidor de clúster con el Core:

```
>cmdutil /protectcluster -core 10.10.10.10 -username administrator -password 23WE0#$sdd -
repository "Repository 1" -clustername 10.10.8.150 -clusterport 8006 -clusterusername
clusterAdmin clusterpassword password -volumes "C:\ClusterStorage\Volum1" -clusternodes
nodeName 10.10.8.150 volumes "c:" nodeName 10.10.8.151 volumes "c:"
```

ProtectEsxServer

Puede usar el comando `protectesxserver` siempre que desee agregar una máquina virtual VMware ESX(i) a la protección.

Uso

El uso del comando es el siguiente:

```
/protectesxserver -core [host name] -user [user name] -password [password] -repository
[repository name] -server [name | IP address] -serverusername [user name] -serverpassword
[password for server login] -serverport [port] -virtualMachines [virtual machines collection |
all] -autoProtect [object ID or name collection]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `protectesxserver`:

Tabla 197. Opciones del comando ProtectEsxServer

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-repository	Obligatorio Nombre del repositorio asociado con el Core que desea utilizar para proteger la máquina virtual.
 NOTA: El nombre debe escribirse entre comillas dobles.	

Opción	Descripción
-server	Nombre o dirección IP del servidor vCenter o ESXi que desea proteger.
-serverusername	Nombre de usuario para iniciar sesión en el servidor vCenter o ESXi que desea proteger.
-serverpassword	Contraseña para iniciar sesión en el servidor vCenter o ESXi que desea proteger.
-serverport	Opcional. Número de puerto del servidor vCenter o ESXi que desea proteger.
-virtualmachines	Opcional. Esta opción permite generar una lista de las máquinas virtuales que desea proteger.
-autoprotect	Opcional. Esta opción permite generar una lista de nuevas máquinas virtuales que desea proteger automáticamente.

Ejemplos:

Proteger máquinas virtuales concretas desde un servidor vCenter o ESXi con el Core:

```
>cmdutil /protectesxserver -core 10.10.10.10 -user admin -password password -repository "Repository 1" -server 10.10.8.150 -serverport 443 -serverusername root -serverpassword password -virtualmachines "VM1" "VM2" -autoprotect "Folder1"
```

RemoveAgent

El comando `RemoveAgent` le permite retirar un equipo de la protección de un Core y eliminar opcionalmente los puntos de recuperación del equipo retirado. Si no elimina los puntos de recuperación, Rapid Recovery los retiene y los etiqueta como un equipo con puntos de recuperación únicamente.

Uso

El uso del comando es el siguiente:

```
/removeagent -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -deleterecoverypoints
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `RemoveAgent` :

Tabla 198. Opciones de comando `RemoveAgent`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.

Opción	Descripción
<code>-password</code>	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
<code>-protectedserver</code>	El nombre o la dirección IP del servidor que desea retirar de la protección.
<code>-deleterecoverypoints</code>	Opcional. Elimina todos los puntos de recuperación del equipo que desea retirar.

Ejemplo:

Retirar un equipo de la protección y eliminar los puntos de recuperación asociados:

```
>cmdutil /removeagent -protectedserver 10.10.1.1 -deleterecoverypoints
```

RemoveArchiveRepository

Puede usar el comando `removearchiverepository` para eliminar un repositorio del Rapid Recovery Core.

Uso

El uso del comando es el siguiente:

```
/removearchiverepository -core [host name] -user [user name] -password [password] name] -name [archive repository name]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `removearchiverepository`:

Tabla 199. Opciones del comando RemoveArchiveRepository

Opción	Descripción
<code>-?</code>	Muestra el mensaje de ayuda.
<code>-core</code>	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
<code>-user</code>	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
<code>-password</code>	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
<code>-name</code>	Obligatorio. Nombre del repositorio de archivación.

Ejemplos:

Extraer el repositorio denominado "NuevoArchivoCompromido" del Core local:

```
>cmdutil /removearchiverepository -name NewArchive
```

RemovePoints (Eliminar puntos)

El comando `removepoints` le permite eliminar puntos de recuperación específicos de un equipo protegido.

Uso

El uso del comando es el siguiente:

```
/removepoints -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -rpn [number | numbers] | -time [time string]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `removepoints`:

Tabla 200. Opciones de comando RemovePoints

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-protectedserver	El nombre o la dirección IP del servidor en el que desea eliminar puntos de recuperación.
-rpn	Opcional. Número secuencial de un punto de recuperación que se va a eliminar (use el comando <code>/list rps</code> para obtener los números). Especifique varios números separados por espacios para eliminar múltiples puntos de recuperación con un único comando.
-time	Opcional. Determina el punto o puntos de recuperación que se deben eliminar por hora de creación. Especifique el momento exacto con el formato "mm/dd/yyyy hh:mm tt" (por ejemplo, "2/24/2012 09:00 AM"). Tenga en cuenta que debe especificar los valores de hora y fecha de la zona horaria definidos en su PC.

Ejemplo:

Eliminar los puntos de recuperación con los números 5 y 7:

```
>cmdutil /removepoints -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22 -rpn 5 7
```

RemoveScheduledArchive

Utilice este comando para interrumpir un archivo continuo programado de Rapid Recovery.

Uso

El uso del comando es el siguiente:

```
/removescheduledarchive -core [host name] -user [user name] -password [password] name] -all -ids [id | id1 id2]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `removescheduledarchive`:

Tabla 201. Opciones del comando RemoveScheduledArchive

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-all	Esta opción especifica si quitar todos los archivos programados asociados con este Core.
-ids	Utilice esta opción para generar una lista con los ID de cada archivo programado que desee eliminar. Separar múltiples ID con espacios.

Ejemplos:

Eliminar todos los archivos programados.

```
>cmdutil /removescheduledarchive -all
```

Eliminar un archivo programado:

```
>cmdutil /removescheduledarchive -ids 6c123c39-5058-4586-bd0c-7c375e72017b
```

RemoveVirtualStandby

Utilice este comando para interrumpir la exportación continua de datos a una máquina virtual en la utilidad de comandos Rapid Recovery.

Uso

El uso del comando es el siguiente:

```
/removevirtualstandby -core [host name] -user [user name] -password [password login] -protectedserver [name] | -all
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `removevirtualstandby`:

Tabla 202. Opciones del comando RemoveVirtualStandby

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-protectedserver	El nombre o los nombres separados por espacios de los equipos virtualizados.
-all	Este comando especifica si desea eliminar todas las exportaciones virtuales programadas.

Ejemplos:

Extraiga todas las exportaciones virtuales en espera:

```
>cmdutil /removevirtualstandby -all
```

Extraiga todas las exportaciones virtuales en espera para dos equipos:

```
>cmdutil /removevirtualstandby -protectedserver 10.10.35.48 10.10.35.69
```

Replicación

Use el comando `Replicate` para configurar la replicación entre dos Rapid Recovery Core.

Uso

El uso del comando es el siguiente:

```
/replicate -request [email | email customer ID] -targetserver [host name | hostname port |  
hostname user name password | hostname port user name password] -replicationname [name] -  
seeddrive [localpath | network path username password] [comment] -protectedserver [name | name  
repository]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `Replicate`:

Tabla 203. Opciones del comando Replicate

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no se proporciona ninguno, entonces se utilizan las credenciales para el usuario que haya iniciado sesión
-request	Opcional. Especifique esta opción si desea utilizar una suscripción a un proveedor externo que proporcione servicios de copia de seguridad y recuperación de desastres externos.
-targetserver	Nombre del servidor en el que desea establecer la replicación. Incluye los siguientes parámetros: • puerto • nombre de usuario • password El parámetro de puerto es opcional, con un valor predeterminado de 8006. Si ha utilizado la opción <code>request</code>, también debe utilizar el nombre de usuario y la contraseña del servidor de destino.
-replicationname	Opcional. Utilice el nombre de la tarea de replicación si no utiliza la opción <code>request</code> .
-seeddrive	Opcional. Utilice esta opción para especificar una unidad de inicialización para la transferencia de datos inicial. El parámetro de comentario es opcional.
-protectedserver	Lista de equipos protegidos que desea replicar. Si utiliza la opción <code>request</code> , enumere solo los nombres o las direcciones IP de los sistemas protegidos. De lo contrario, enumere los equipos protegidos y el nombre de repositorio remoto correspondiente.

Ejemplo:

Replicar dos equipos protegidos en el Core remoto usando una unidad de inicialización desde un recurso compartido de red:

```
>cmdutil /replicate -targetserver 10.10.1.100 Administrator 123Q -replicationname  
ReplicationName -seeddrive Network \\10.10.1.100\seeddrive Administrator 123Q -protectedserver  
10.10.1.1 Repository1 10.10.1.2 Repository2
```

Replicación

Use el comando `replication` para controlar la replicación existente entre dos Rapid Recovery Cores y administrar las solicitudes de replicación pendientes.

NOTA: Este comando sigue al comando `Replicate`, que establece la conexión, denominada emparejamiento, entre los Cores y usa una unidad de inicialización para la transferencia de datos inicial. Para obtener más información acerca de este comando, consulte [Replicación](#).

Uso

El uso del comando es el siguiente:

```
/replication [-list [incoming | outgoing | pending] -accept | -deny | -ignore | -delete | -  
edit] -id [replication ID] -protectedserver [name | name repository] -responsecomment [comment] -  
deleterecoverypoints -scheduletype [type] -dailystarttime [time] -dailyendtime [time] -  
weekdaystarttime [time] -weekdayendtime [time] -weekendstarttime [time] -weekendendtime [time]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `replication`:

Tabla 204. Opciones del comando Replication

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no se proporciona ninguno, entonces se utilizan las credenciales para el usuario que haya iniciado sesión
-list	Lista de trabajos de replicación entrantes o salientes o solicitudes de replicación pendientes.
-accept	Acepta la solicitud de replicación.
-deny	Deniega la solicitud de replicación

Opción	Descripción
-ignore	Omite la solicitud de replicación
-delete	Use esta opción para eliminar un trabajo de replicación existente o un equipo del trabajo de replicación. Especifique solo el parámetro -id para eliminar toda una relación de replicación, o especifique los parámetros -id y -protectedserver para eliminar de la replicación solo equipos concretos.
-edit	Modifica la programación de trabajos de replicación existentes.
-id	Identificador del trabajo de replicación o la solicitud de replicación pendiente. Puede ser el identificador de un Core remoto, el nombre del host, la identificación del cliente, la dirección de correo electrónico o la identificación de la solicitud de replicación pendiente.
-protectedserver	Al responder a una solicitud de replicación, use esta opción para aplicar su respuesta a la lista de servidores protegidos con un nombre o identificación de repositorio. Use el parámetro "all" para aplicar la respuesta a todos los equipos solicitados.
-responsecomment	Comentario que se proporciona con la respuesta a una solicitud de replicación pendiente.
-deleterecoverypoints	Use esta opción si también deben eliminarse puntos de recuperación específicos de un equipo replicado eliminado.
-scheduletype	Si usa la opción -edit, esta opción especifica el tipo de programa de replicación. Incluya uno de los cuatro valores siguientes: • atalltimes: replicar automáticamente en cualquier momento. • daily: replicar todos los días. Especifique los parámetros -dailystarttime y -dailyendtime. • custom: cuando se usa la replicación diaria, use este valor para programar la replicación en días laborables o fines de semana. Especifique los parámetros -weekdaystarttime, -weekdayendtime, -weekendstarttime y -weekendendtime.
-dailystarttime	Se usa únicamente para el valor de todos los días de la opción -scheduletype. Se utiliza para establecer un intervalo de tiempo en el que debe tener lugar la replicación. Use esta opción para especificar la primera hora del día en la que desea que se inicie la replicación.
-dailyendtime	Se usa únicamente para el valor de todos los días de la opción -scheduletype. Se utiliza para establecer un intervalo de tiempo en el que debe tener lugar la replicación. Use esta opción para especificar la última hora del día en la que desea que se inicie la replicación.
-weekdaystarttime	Se usa únicamente para el valor de personalización de la opción -scheduletype. Se utiliza para establecer un intervalo de tiempo en el que debe tener lugar la replicación. Use esta opción para especificar la primera hora de un día laborable en la que desea que se inicie la replicación.
-weekdayendtime	Se usa únicamente para el valor de personalización de la opción -scheduletype. Se utiliza para establecer un intervalo de tiempo en el que debe tener lugar la replicación. Use esta opción para especificar la última hora de un día laborable en la que desea que se inicie la replicación.
-weekendstarttime	Se usa únicamente para el valor de personalización de la opción -scheduletype. Se utiliza para establecer un intervalo de tiempo en el que debe tener lugar la replicación. Use esta opción para especificar la primera hora del fin de semana en la que desea que se inicie la replicación.
-weekendendtime	Se usa únicamente para el valor de personalización de la opción -scheduletype. Se utiliza para establecer un intervalo de tiempo en el que debe tener lugar la replicación. Use esta opción para especificar la última hora del fin de semana en la que desea que se inicie la replicación.

Ejemplo:

Enumerar todas las replicaciones entrantes:

```
>cmdutil /replication -list incoming
```

Aceptar las solicitudes de replicación pendientes para dos equipos protegidos:

```
>cmdutil /replication -accept -id customer@email.address -protectedserver 10.10.1.1 Repository1  
10.10.1.2 Repository2 -responsecomment A response comment
```

Denegar una solicitud de replicación pendiente:

```
>cmdutil /replication -deny -id customer@email.address
```

Eliminar una replicación existente con los puntos de recuperación replicados:

```
>cmdutil /replication -delete -id RemoteServerHostname -deleterecoverypoints
```

Quitar dos equipos de una replicación existente:

```
>cmdutil /replication -delete -id "156d7a46-8e44-43f4-9ed8-60d998e582bf" -protectedserver  
10.10.1.1 10.10.1.2
```

Modificar un programa de replicación con horas específicas para días laborables y fines de semana:

```
>cmdutil /replication -edit -id RemoteServerHostName -scheduletype custom -weekdaystarttime  
"9:00 AM" -weekdayendtime "6:00 PM" -weekendstarttime "9:00 AM" -weekendendtime "6:00 PM"
```

RestoreAgent

El comando `restoreagent` permite restaurar un equipo o volumen protegidos de un determinado punto de recuperación de Rapid Recovery.

Uso

El uso del comando es el siguiente:

```
/restoreagent -protectedserver [name | IP address] -rpn [recovery point number] -volumes [IDs |  
names | all] -targetmachine [name] -targetvolume [volume name] -forcedismount -autorestart
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `restoreagent`:

Tabla 205. Opciones del comando RestoreAgent

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.

Opción	Descripción
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-protectedserver	Nombre o dirección IP del servidor que desea restaurar.
-rpn	Número de identificación del punto de recuperación que desea utilizar para restaurar el equipo. Para encontrar el número correcto, utilice el comando <code>list rps</code> .
-volumes	Identificaciones o nombres de los volúmenes que desea restaurar. Para restaurar todos los volúmenes protegidos, utilice <code>-volumes all</code> .
-targetmachine	Nombre del equipo en el que desea restaurar el equipo protegido.
-targetvolume	Nombre o ID del volumen en el que desea restaurar el equipo.
-forcedismount	Opcional. Use esta opción para forzar el desmontaje de la base de datos a petición.
-autorestart	Opcional. Use este comando si es necesario reiniciar un equipo de Exchange Server.

Ejemplo:

Restaura un equipo en un equipo protegido con la dirección IP 192.168.20.130, incluyendo la opción de forzar desmontaje de la base de datos.

```
>cmdutil /restoreagent -protectedserver 192.168.20.130 -rpn 259 -volumes "F:" "E:" "C:" -targetmachine 192.168.20.174 -targetvolume "E:" "G:" "F:" -forcedismount
```

RestoreArchive (Restaurar archivo)

Este comando restaura un archivo desde un archivo local o comparte y coloca los datos restaurados en un repositorio especificado.

Uso

El uso del comando es el siguiente:

```
/restorearchive -core [host name] -user [user name] -password [password] -all | -protectedserver [name | IP address] -repository [name] -archiveusername [name] -archivepassword [password] -path [location]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `restorearchive`:

Tabla 206. Opciones de comando RestoreArchive

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-all	Restaure los datos para todos los equipos protegidos desde los archivos de registro.
-protectedserver	Equipo protegido con puntos de recuperación para restaurar. Puede especificar varios nombres de equipo entre comillas dobles y separados por espacios.
-repository	Nombre de un repositorio del Core donde se deben colocar los puntos de recuperación restaurados. El nombre se debe poner entre comillas dobles.
-archiveusername	Opcional. Nombre de usuario para el equipo remoto. Solo es requerido para la ruta de red.
-archivepassword	Opcional. Contraseña para el equipo remoto. Solo es requerido para la ruta de red.
-path	Ubicación de los datos archivados que se deben restaurar; por ejemplo: d:\work\archive o ruta de acceso de red \servername\sharename.

Ejemplos:

Restaurar datos archivados para todos los servidores protegidos:

```
>cmdutil /restorearchive -core 10.10.10.10 -username administrator -password 23WE@#sdd -all -repository repository1 -path d:\work\archive
```

Restaurar datos archivados de servidores protegidos específicos:

```
>cmdutil /restorearchive -core 10.10.10.10 -username administrator -password 23WE@#sdd -protectedserver "10.10.20.30" "20.10.10.5" -repository repository1 -path d:\work\archive
```

RestoreUrc

El comando `restoreurc` permite restaurar un equipo protegido o volumen desde un punto de recuperación de Rapid Recovery determinado en un equipo sin sistema operativo mediante la consola de recuperación universal (URC).

Uso

El uso del comando es el siguiente:

```
/restoreurc -protectedserver [name | IP address] -rpn [recovery point number] -volumes [IDs | names | all] -targetmachine [IP address] -urcpassword [password from the URC] -targetdisk [disk number | all]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `restoreurc`:

Tabla 207. Opciones del comando RestoreUrc

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-protectedserver	Nombre o dirección IP del servidor en el que desea restaurar la URC.
-rpn	Número de identificación del punto de recuperación que desea utilizar para restaurar el equipo. Para encontrar el número correcto, utilice el comando <code>list rps</code> .
-volumes	Identificaciones o nombres de los volúmenes que desea restaurar. Para restaurar todos los volúmenes protegidos, utilice <code>-volumes all</code> .
-targetmachine	Nombre del equipo en el que desea restaurar el equipo protegido.
-urcpassword	Clave de autenticación de la URC.
-targetdisk	Números de los discos en los que desea restaurar el equipo. Para seleccionar todos los discos del equipo mediante la URC, utilice <code>-targetdisk all</code> .

Ejemplo:

Restaurar un equipo en los discos 0 y 1 del equipo mediante la URC, cuando la dirección IP del equipo de la URC es 192.168.20.175:

```
>cmdutil /restoreurc -protectedserver 192.168.20.130 -rpn 259 -volumes "C:" "E:" -targetmachine 192.168.20.175 -urcpassword ***** -targetdisk 0 1
```

Reanudar

El administrador puede utilizar este comando para reanudar las instantáneas, exportar a una máquina virtual o replicar un Core. Debe especificar la necesidad de reanudarlas mediante un parámetro. Son válidos los siguientes parámetros: `snapshot`, `vmexport`, y `replication`. Consulte [Pausar](#) para obtener más información.

Uso

El uso del comando es el siguiente:

```
/resume [snapshot | vmexport | replication] -core [host name] -user [user name] -password [password] -all | -protectedserver [name | IP address] -incoming [host name] | outgoing [host name] -time [time string]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `resume`:

Tabla 208. Opciones de comando Resume

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-restore	[snapshots], [replication] o [vmexport].
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-all	Reanudar todos los Agents en el Core seleccionado.
-protectedserver	Reanudar el servidor protegido actual.
-incoming	Nombre de host del Core remoto que se replica en el equipo Core.
-outgoing	Nombre de host del Core de destino remoto en el que se replican los datos.

Ejemplos:

Reanudar instantáneas para un servidor protegido específico:

```
>cmdutil /resume snapshot -core 10.10.10.10 -user administrator -password 23WE@#$$sdd -protectedserver 10.10.10.4
```

Reanudar la exportación a una máquina virtual para todos los equipos protegidos del Core:

```
>cmdutil /resume vmexport -core 10.10.10.10 -user administrator -password 23WE@#$sdd -all
```

Reanudar la replicación saliente en el Core para un equipo protegido específica:

```
>cmdutil /resume replication -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.1.76
```

Reanudar la replicación saliente para todos los equipos protegidos del Core de destino:

```
>cmdutil /resume replication -core 10.10.10.10 -user administrator -password 23WE@#$sdd -outgoing 10.10.1.63
```

Reanudar la replicación entrante para todos los equipos protegidos del Core de destino:

```
>cmdutil /resume replication -core 10.10.10.10 -user administrator -password 23WE@#$sdd -incoming 10.10.1.82
```

SeedDrive

Puede utilizar una unidad de inicialización para la transferencia de datos inicial al establecer la replicación de Rapid Recovery.

Uso

El uso del comando es el siguiente:

```
/seeddrive [-list | -startcopy | -startconsume | -abandon] -path [local | network path] -seeddriveusername [user name] -seeddrivepassword [password] -remotecore [name] [-targetcore [name or IP] | -protectedserver [name] | -all] -usecompatibleformat
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `seeddrive`:

Tabla 209. Opciones del comando SeedDrive

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-list	Lista de unidades de inicialización pendientes con información ampliada.
-startcopy	Inicia la copia en la unidad de inicialización.
-startconsume	Inicia el consumo de la unidad de inicialización.

Opción	Descripción
-abandon	Abandona la solicitud de unidad de inicialización pendiente.
-path	Ruta de acceso local o de red a la unidad de inicialización.
-seeddriveusername	Opcional. Nombre de usuario para la ubicación de red de la unidad de inicialización.
-seeddrivepassword	Opcional. Contraseña para la ubicación de red de la unidad de inicialización.
-targetcore	Opcional. Utilizar solo con la opción-copy. Es el nombre o la dirección IP del Core remoto. Todas las máquinas protegidas que se replican en este Core reciben puntos de recuperación de unidad de inicialización.
-remotecore	Utilizar solo con la opción-consume. Es el nombre del Core remoto desde el que se crean o consumen los puntos de recuperación de la unidad de inicialización.
-protectedserver	Nombre o dirección IP del equipo protegido que se utiliza para crear o consumir los puntos de recuperación de la unidad de inicialización. Por ejemplo: -protectedserver "10.10.60.48" "10.10.12.101".
-all	Esta opción especifica si consumir o copiar todos los equipos protegidos disponibles.
-usecompatibleformat	El nuevo formato de archivación ofrece un mejor rendimiento, aunque no es compatible con los Core anteriores. Utilice esta opción cuando trabaje con un AppAssure Core heredado.

Ejemplos:

Enumerar las unidades de inicialización pendientes:

```
>cmdutil /seeddrive -list
```

Copiar dos equipos protegidos en la unidad de inicialización del recurso compartido de red:

```
>cmdutil /seeddrive -startcopy -remotecore TargetCoreName -path \\10.10.1.1\Share\Seed\ -seeddriveusername Administrator -seeddrivepassword 12345 -usecompatibleformat
```

Iniciar el consumo de la unidad de inicialización:

```
>cmdutil /seeddrive -startconsume -path \\10.10.1.1\Share\Seed\ -seeddriveusername Adminsitrator -seeddrivepassword 12345 -remotecore RemoteCoreName
```

Abandonar un solicitud de unidad de inicialización pendiente:

```
>cmdutil /seeddrive -abandon RemoteCoreHostName
```

StartExport (Iniciar exportación)

El comando `startexport` fuerza una exportación puntual de datos desde un equipo protegido a un servidor virtual. Puede exportar a un ESXi, VMware Workstation, Hyper-V o máquina virtual VirtualBox. Si se exporta a ESXi, debe especificar el aprovisionamiento en disco compacto o grueso.

Uso

El uso del comando es el siguiente:

```
/startexport -exporttype [esxi | vm | hyperv | vb] -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -volumes [volume names] -rpn [recovery point number | numbers] | -time [time string] -vmname [virtual machine name] -hostname [virtual host name] -hostport [virtual hostport number] -hostusername [virtual host user name] -hostpassword [virtual host password] [-ram [total megabytes] | -usesourceram] -diskprovisioning [thin | thick] -diskmapping [automatic | manual | withvm] -targetpath [location] -pathusername [user name] -pathpassword [password] [-uselocalmachine]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `startexport`:

Tabla 210. Opciones de comando StartExport

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-exporttype	Realice la exportación de datos desde un servidor protegido a un servidor ESXi ('esxi'), servidor de VMware Workstation ('vm'), servidor Hyper-V ('hyperv') o servidor VirtualBox ('vb').
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-protectedserver	Equipo protegido con puntos de recuperación que se deben exportar.
-volumes	Opcional. Lista de nombres de volumen que deben exportarse. Si no se especifican, se exportarán todos los volúmenes. Los valores deben estar entre comillas dobles y separados por espacios; por ejemplo: "c:" "d:". No utilice barras finales en nombres de volúmenes.
-rpn	Opcional. Número secuencial de un punto de recuperación para exportación (utilice el comando <code>Get-RecoveryPoints</code> para obtener los números). Si no se especifica ninguna opción ('time' o 'rpn'), entonces se exporta el punto de recuperación más reciente.
-time	Opcional. Determina el punto o puntos de recuperación que se deben seleccionar para la exportación. Debe especificar el momento exacto con el formato "mm/dd/yyyy hh:mm tt" (por ejemplo, "2/24/2012 09:00 AM"). Asegúrese de especificar los valores de fecha y hora de la zona horaria establecida en su PC. Nota: Si no se especifica ninguna opción ('time' o 'rpn'), entonces se exporta el punto de recuperación más reciente.
-vmname	Nombre de Windows de la máquina virtual.
-hostname	Solo para exportaciones virtuales de ESXi e Hyper-V. Nombre de host del servidor virtual.
-linuxhostname	Solo para exportaciones de VirtualBox. Nombre de host del servidor virtual.

Opción	Descripción
-hostport	Solo para exportaciones virtuales de ESXi e Hyper-V. Número de puerto del servidor virtual.
-hostusername	Solo para exportaciones virtuales de ESXi e Hyper-V. Nombre de usuario del host del servidor virtual.
-hostpassword	Solo para exportaciones virtuales de ESXi e Hyper-V. Contraseña del host del servidor virtual.
-ram	Use esta opción para asignar una cantidad específica de RAM en el servidor virtual.
-usesourceram	Opcional. Use esta opción para asignar la misma cantidad de RAM en el servidor virtual que la que tiene el equipo de origen.
-diskprovisioning	Use esta opción solo para exportaciones de ESXi. Opcional. Cantidad de espacio en disco que desea asignar en la máquina virtual. Use una de las dos especificaciones siguientes: - Grueso: esta especificación hace que el disco virtual tenga el mismo tamaño que la unidad original en el equipo protegido. - Compacto: esta especificación asigna la cantidad de espacio en disco real ocupado en la unidad original y unos megabytes más. La especificación predeterminada es "compacto".
-diskmapping	Use esta opción solo para exportaciones de ESXi. Opcional. Esta opción determina cómo asignar los discos del equipo protegido a la máquina virtual. Use uno de los valores siguientes: - Automático: este valor asigna los discos automáticamente. - Manual: este valor permite asignar los discos manualmente. - withvm: este valor almacena los discos virtuales en un almacén de datos que seleccione el usuario. El valor predeterminado es "automático".
-targetpath	Solo para exportaciones de VMware Workstation o VirtualBox. Esta opción especifica la ruta de acceso de red local (o de Linux, solo para VirtualBox) a la carpeta en la que desee almacenar los archivos de la máquina virtual.
-pathusername	Solo para exportaciones de VMware Workstation. Es el nombre de usuario del equipo de red. Solo se requiere cuando especifica una ruta de red en la opción -targetpath.
-pathpassword	Solo para exportaciones de VMware Workstation. Es la contraseña del equipo de red. Solo se requiere cuando especifica una ruta de red en la opción -targetpath.
-uselocalmachine	Solo para exportaciones de Hyper-V. Opcional. Use este comando para conectarse al servidor local de Hyper-V. Esta opción omite las opciones -hostname, -hostport, -hostusername y -hostpassword.

Ejemplos:

Exportar datos a una máquina virtual de ESXi con un nombre específico y la misma cantidad de RAM y tamaño en disco que el servidor protegido de origen:

```
>cmdutil /startexport -exporttype esxi -core 10.10.10.10 -user administrator -password 23WE0#$sdd -protectedserver 10.10.5.22 -vmname Win2008-Smith -hostname 10.10.10.23 -hostport 443 -hostusername root -hostpassword 12QWsdxc@# -usesourceram -diskprovisioning thick
```

Crear un archivo de equipo de VMware Workstation en la unidad local con datos protegidos desde el punto de recuperación #4:

```
>cmdutil /startexport -exporttype vmstation -core 10.10.10.10 -user administrator -password 23WE0#$sdd -protectedserver 10.10.5.22 -rpn 4 -vmname Win2008-Smith -targetpath c:\virtualmachines -ram 4096
```


Crear archivos de equipo de Hyper-V que se deben almacenar en un equipo remoto:

```
>cmdutil /startexport -exporttype hyperv -core 10.10.10.10 -user administrator -password 23WE@#  
$sdd -protectedserver 10.10.5.22 -vmlocation \\WIN7-Bobby\virtualmachines -hostname 10.10.10.23  
-hostport 443 -hostusername root -hostpassword 12QWsdxc@# -ram 4096
```

UpdateRepository (Actualizar repositorio)

El comando `updaterepository` añade una nueva ubicación de almacenamiento a un repositorio existente.

Uso

El uso del comando es el siguiente:

```
/updaterepository -name [repository name] -size [size of the repository] [-datapath [data path]  
-metadatapath [metadata path] | [-uncpath [UNC path] -shareusername [share user name] -  
sharepassword [share password] -core [host name] -user [user name] -password [password]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `updaterepository` :

Tabla 211. Opciones de comando UpdateRepository

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-name	Nombre de repositorio.
-size	Tamaño de la ubicación de almacenamiento del repositorio. Las unidades disponibles son b, Kb, Mb, Gb, Tb y Pb.
-datapath	Solo para la ubicación local. Determina la ruta de acceso a datos de la ubicación de almacenamiento del repositorio.
-metadatapath	Solo para la ubicación local. Determina la ruta de acceso a metadatos de la ubicación de almacenamiento del repositorio.
-uncpath	Solo para la ubicación compartida. Determina las rutas de acceso a metadatos y datos de la ubicación de almacenamiento del repositorio.
-shareusername	Solo para la ubicación compartida. Determina el nombre de usuario en la ubicación compartida.
-sharepassword	Solo para la ubicación compartida. Determina la contraseña para la ubicación compartida.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.

Ejemplos:

Crear una nueva ubicación de almacenamiento en un repositorio DVM local:

```
>cmdutil /updaterepository -name "Repository 1" -size 200Gb -datapath d:\repository -  
metadatapath d:\repository -core 10.10.10.10:8006 -username administrator -password 23WE@#$sdd
```

Crear una ubicación de almacenamiento para un repositorio DVM en una ubicación compartida:

```
>cmdutil /updaterepository -name "Repository 1" -size 200Gb -uncpath \\share\repository -  
shareusername login -sharepassword 23WE@#$sdd -core 10.10.10.10:8006 -username administrator -  
password 23WE@#$sdd
```

Versión

El comando `version` muestra información sobre la versión del software Rapid Recovery instalado en el servidor especificado. Si no especifica un Core o un servidor protegido, la información devuelta se aplica al Core en el que está trabajando en ese momento.

Uso

El uso del comando es el siguiente:

```
/[version | ver] -protectedserver [name | IP address]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `version`:

Tabla 212. Opciones de comando Version

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-protectedserver	Opcional. El equipo protegido del que desea ver la información de versión. Si no especifica un equipo protegido, la devolución es la información sobre el equipo del Core en el que está trabajando.

Ejemplo:

Mostrar la información sobre la versión de Rapid Recovery instalada en el Rapid Recovery Core actual:

```
>cmdutil /version
```

VirtualStandby

Puede usar el comando `virtualstandby` para exportar datos de un equipo protegido de Rapid Recovery a una máquina virtual compatible.

Uso

El uso del comando es el siguiente:

```
/virtualstandby -edit -exporttype [esxi | vm | hyperv | vb] -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -volumes [volume names] -vmname [virtual machine name] -gen2 -hostname [virtual host name] -hostport [virtual host port number] -hostusername [virtual host user name] -hostpassword [virtual host password] [-ram [total megabytes] | -usesourceram] -diskprovisioning [thin | thick] -diskmapping [automatic | manual | withvm] -targetpath [location] -pathusername [user name] -pathpassword [password] [-uselocal machine] -initialexport
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `virtualstandby`:

Tabla 213. Opciones del comando VirtualStandby

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-exporttype	Esta opción exporta los datos de un equipo protegido a uno de los siguientes servidores virtuales especificado: • esxi (ESXi) • vm (VMware Workstation) • hyperv (Hyper-V) • vb (VirtualBox)
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza en el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también debe proporcionar una contraseña. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no proporciona ninguno, entonces se utilizan las credenciales del usuario registrado.
-protectedserver	Use esta opción para especificar el equipo protegido cuyos puntos de recuperación desea exportar.
-volumes	Opcional. Use esta opción para generar una lista con los nombres de los volúmenes que desea exportar. Si no especifica volúmenes, se exportarán todos los volúmenes del punto de recuperación. Especifique los valores entre comillas dobles y separados con un espacio, por ejemplo, "c:" "d:". No use barras finales en los nombres de volúmenes.
-ram	Use esta opción para asignar una cantidad específica de RAM en el servidor virtual.

Opción	Descripción
-usesourceram	Opcional. Use esta opción para asignar la misma cantidad de RAM en el servidor virtual que la que tiene el equipo de origen.
-vmname	Nombre de Windows de la máquina virtual.
-gen2	Opcional. Esta opción especifica la generación 2 del servidor de VM. Si no especifica la generación, el comando utiliza la generación 1. Los siguientes sistemas operativos admiten la generación 2: - Windows - Windows Server 2012 R2 - Windows 8,1 - Ubuntu Linux - CentOs - RHEL - Oracle Linux 7
-hostname	Solo para exportaciones virtuales de ESXi e Hyper-V. Nombre de host del servidor virtual.
-linuxhostname	Solo para exportaciones de VirtualBox. Nombre de host del servidor virtual.
-hostport	Solo para exportaciones virtuales de ESXi e Hyper-V. Número de puerto del servidor virtual.
-hostusername	Solo para exportaciones virtuales de ESXi e Hyper-V. Nombre de usuario del host del servidor virtual.
-hostpassword	Solo para exportaciones virtuales de ESXi e Hyper-V. Contraseña del host del servidor virtual.
-diskprovisioning	Solo para exportaciones de ESXi. Opcional. Cantidad de espacio en disco que desea asignar en la máquina virtual. Use una de las dos especificaciones siguientes: - Grueso: esta especificación hace que el disco virtual tenga el mismo tamaño que la unidad original en el equipo protegido. - Compacto: esta especificación asigna la cantidad de espacio en disco real ocupado en la unidad original y unos megabytes más. La especificación predeterminada es "compacto".
-diskmapping	Solo para exportaciones de ESXi. Opcional. Esta opción determina cómo asignar los discos del equipo protegido a la máquina virtual. Use uno de los valores siguientes: - Automático: este valor asigna los discos automáticamente. - Manual: este valor permite asignar los discos manualmente. - withvm: este valor almacena los discos virtuales en un almacén de datos que seleccione el usuario. El valor predeterminado es "automático".
-targetpath	Solo para exportaciones de VMware Workstation o VirtualBox. Esta opción especifica la ruta de acceso de red local (o de Linux, solo para VirtualBox) a la carpeta en la que desee almacenar los archivos de la máquina virtual.
-pathusername	Solo para exportaciones de VMware Workstation. Es el nombre de usuario del equipo de red. Solo se requiere cuando especifica una ruta de red en la opción -targetpath.
-pathpassword	Solo para exportaciones de VMware Workstation. Escriba una contraseña para la ruta de acceso de red. Solo se requiere cuando especifica una ruta de red en la opción -targetpath.
-uselocalmachine	Solo para exportaciones de Hyper-V. Opcional. Use este comando para conectarse al servidor local de Hyper-V. Esta opción omite las opciones -hostname, -hostport, -hostusername y -hostpassword.

Opción	Descripción
-edit	Opcional. Esta opción permite editar máquinas virtuales existentes. Pasa por alto las opciones -exporttype y -initialexport.
-initialexport	Opcional. Esta opción especifica si se debe iniciar una exportación de máquina virtual a petición inicial después de configurar un servidor virtual en espera virtual continuo.

Ejemplos:

Configurar una exportación en espera virtual a una máquina virtual ESXi con el nombre, la cantidad de RAM y el tamaño del disco del servidor protegido de origen:

```
>cmdutil /virtualstandby -exporttype esxi -core 10.10.10.10 -user administrator -password 23WE@#
$sd -protectedserver 10.10.5.22 -vmname Win2008-Smith -hostname 10.10.10.23 -hostport 443 -
hostusername root -hostpassword 12QWsdxc@# -usesourceram -diskprovisioning thick
```

Configurar una exportación en espera virtual a un archivo de máquina de VMware Workstation en la unidad local:

```
>cmdutil /virtualstandby -exporttype vm -core 10.10.10.10 -user administrator -password 23WE@#
$sd -protectedserver 10.10.5.22 -vmname Win2008-Smith -targetpath c:\virtualmachines -ram 4096
```

Configurar una exportación en espera virtual a archivos de máquina virtual Hyper-V y almacenarlos en un equipo remoto:

```
>cmdutil /virtualstandby -exporttype hyperv -core 10.10.10.10 -user administrator -password
23WE@#$sd -protectedserver 10.10.5.22 -vmname Win2008-Smith -vmlocation \\WIN7-Bobby
\virtualmachines -hostname 10.10.10.23 -hostport 443 -hostusername root -hostpassword
12QWsdxc@# -ram 4096
```

Traducción

Cuando se ejecuta en el mismo equipo en el que el Core de Rapid Recovery está instalado, la utilidad Administración de línea de comandos de Rapid Recovery basa su idioma de visualización en el conjunto de idioma para el Core de Rapid Recovery. En esta versión, los idiomas admitidos incluyen inglés, español, chino (simplificado), francés, coreano, alemán, japonés y portugués (Brasil).

Si la utilidad Administración de línea de comandos de Rapid Recovery está instalada en un equipo separado, el inglés es el único idioma admitido.

Referencias de la Core Console

Este apéndice incluye tablas de referencia que describen muchas de las funciones e iconos disponibles en la Rapid Recovery Core Console. Sirve como complemento para el capítulo [Descripción de la Core Console de Rapid Recovery](#) de *Dell Data Protection | Rapid Recovery User Guide* (Guía de usuario de Dell Data Protection | Rapid Recovery).

Temas:

- [Visualización de la interfaz para el usuario de la Core Console](#)
- [Visualización del panel de máquinas protegidas](#)

Visualización de la interfaz para el usuario de la Core Console

La Core Console es la IU principal con la que los usuarios interactúan con Rapid Recovery. Cuando inicia sesión en la Core Console de Rapid Recovery, verá los siguientes elementos.

Tabla 214. Elementos de la IU incluidos en la Core Console

Elemento de la IU	Descripción
Área de marca	Para los entornos típicos, la parte superior izquierda de la Core Console es la marca con el nombre completo del producto, incluido el logotipo de Dell. Al hacer clic en cualquier parte de los resultados de área de la marca en la apertura de una nueva pestaña en el navegador web, se muestra documentación del producto en el sitio web de asistencia.
Barra de botones	La barra de botones, que aparece a la derecha del área de marca, contiene botones a los que se puede acceder desde cualquier parte de la Consola de Core. Estos botones inician asistentes para llevar a cabo tareas comunes, como la protección de un equipo; la realización de una restauración a partir de un punto de recuperación; la creación, conexión o importación de un archivo; o la replicación desde este Core de origen a un Core de destino. Cada botón de la barra de botones se describe en mayor detalle en la tabla Tabla 215. Botones y menús de la barra de botones .
Ejecución del recuento de tareas	Muestra el número de trabajos que se están ejecutando actualmente. Este valor es una dinámica basada en el estado del sistema. Cuando hace clic en el menú desplegable, verá un resumen del estado de todos los trabajos que se están ejecutando actualmente. Puede elegir la cancelación del trabajo haciendo clic en la X de cualquier trabajo.
Acciones (menú desplegable)	El menú Ayuda incluye las siguientes opciones: • Ayuda. Abre la ayuda del producto, que se abre en una ventana independiente del navegador. • Documentación. Abre la documentación técnica Rapid Recovery en el sitio web de soporte de Dell. • Soporte. Abre el sitio web de asistencia de Dell, que proporciona acceso a Chat en vivo, tutoriales de vídeo, artículos de la base de conocimientos de Rapid Recovery, preguntas más frecuentes y más. • Guía de inicio rápido. La Guía de inicio rápido es una guía de tareas sugeridas para configurar y usar Rapid Recovery. La guía se abre automáticamente cada vez que inicia sesión en la Core Console, a no ser que desactive esta función. También puede abrir la Guía de inicio rápido desde el menú Ayuda. Para obtener más información sobre la Guía de inicio rápido, consulte Comprensión de la Guía de inicio rápido.

Elemento de la IU	Descripción
	• Acerca de. Abre el cuadro de diálogo Acerca del Core de Dell Data Protection Rapid Recovery, que incluye la información de la versión y una descripción del software.
Fecha y hora del servidor	La hora actual del equipo que ejecuta el servicio del Core de Rapid Recovery aparece en la parte superior derecha de la Consola de Core. Al pasar el ratón sobre la hora, también aparece la fecha del servidor. Se trata de la fecha y hora registrada por el sistema para eventos como la creación de registros, programaciones e informes. Por ejemplo, cuando se aplican planificaciones de protección, se utiliza la hora mostrada en la Core Console. Esto sucede incluso aunque la zona horaria sea distinta en el servidor de la base de datos o en el equipo cliente donde se esté ejecutando el navegador.
Barra de iconos	La barra de iconos incluye una representación gráfica para las funciones principales accesibles en la Consola de Core. Se muestra en el lateral izquierdo de la interfaz de usuario (UI), directamente por debajo del área de marca. Al hacer clic en el elemento apropiado de la barra de iconos le lleva a la sección correspondiente de la UI donde puede gestionar esa función. Cada icono de la barra de iconos se describe en mayor detalle en la tabla Tabla 216. Barra de iconos.
Área de navegación izquierda	El área de navegación izquierda se muestra en el lateral izquierdo de la interfaz de usuario, por debajo de la barra de iconos. • El área de navegación de la izquierda contiene el texto filtrar y el menú Equipos protegidos. • Si ha agregado replicación a este Core, este área contiene un menú Equipos replicados. • Si tiene algún equipo que se retirara de la protección pero que tenga guardados puntos de recuperación, entonces este área contiene un menú Solo puntos de recuperación. • Si agregó cualquier grupo personalizado, entonces este área contiene un menú Grupo personalizado. • Si ha conectado un archivo, a continuación, esta área contiene un menú de archivos conectados. Puede alternar la visualización del área de navegación izquierda. Esto resulta útil cuando tiene que ver más contexto en el área de navegación principal de la IU. Para ocultar esta sección, haga clic en el borde de color gris entre las áreas de navegación izquierda y principal. Para mostrar este elemento de la IU de nuevo, haga clic en el borde de color gris de nuevo. Cada elemento del área de navegación izquierda se describe en mayor detalle en la tabla Tabla 218. Área de navegación izquierda y menús.
Ayuda sensible al contexto	 Desde la Core Console de Rapid Recovery, cada vez que haga clic en el icono Ayuda (un signo de interrogación azul), se abre una ventana de navegador cuyo tamaño se puede modificar con dos marcos. El marco izquierdo contiene un árbol de navegación que muestra temas de la guía del usuario de Dell Rapid Recovery. El marco derecho muestra el contenido del tema de la ayuda seleccionado. Siempre es posible ampliar el árbol de navegación de la ayuda para mostrar la ubicación del tema seleccionado en su jerarquía. Puede explorar todos los temas de la Guía del usuario utilizando esta función de ayuda sensible al contexto. Cierre el navegador cuando haya terminado de explorar temas. También puede abrir la ayuda desde la opción Ayuda del menú Ayuda.

Barra de botones

Los detalles sobre la barra de botones aparecen en la tabla siguiente.

Tabla 215. Botones y menús de la barra de botones

Elemento de la IU	Descripción
Barra de botones: botón y menú proteger	 El botón Proteger inicia el Asistente para proteger un equipo, desde el que puede proteger un único equipo en el Core de Rapid Recovery. Para otras opciones de protección adicionales, podrá acceder al menú desplegable que hay junto a este botón, que incluye las opciones siguientes. - La opción Proteger equipo es otro método para iniciar el Asistente para proteger un equipo para proteger un único equipo. - La opción Proteger clúster le permite conectar con un clúster de servidores. - La opción Proteger varios equipos abre el Asistente para proteger varios equipos, que le permite proteger dos o más equipos de forma simultánea. - La opción Implementar el software de Agent permite instalar el software de Agent Rapid Recovery en uno o varios equipos al mismo tiempo. Esta función utiliza el asistente para implementar el software de Agent.
Barra de botones: botón y menú restaurar	 El botón Restaurar abre el Asistente para restaurar un equipo que le permite restaurar datos procedentes de puntos de recuperación guardados desde un equipo protegido. Para otras opciones de exportación y restauración adicionales, podrá acceder al menú desplegable que hay junto a este botón, que incluye las opciones siguientes. - La opción Restaurar equipo es otro método para iniciar el Asistente para restaurar un equipo para restaurar datos. - La opción Montar punto de recuperación inicia el Asistente de montaje, que permite montar puntos de recuperación desde un equipo protegido. - La opción Exportación de la VM abre el Asistente de exportación. Desde este asistente puede crear una máquina virtual a partir de puntos de recuperación guardados en el Core de Rapid Recovery. Tiene la opción de crear una exportación única, o puede definir parámetros para una máquina virtual que se actualice continuamente después de cada instantánea de un equipo protegido.
Barra de botones: botón y menú Archivo comprimido	 El botón Archivo comprimido abre el Asistente de archivación. Desde el asistente, puede crear una archivación única desde los puntos de recuperación seleccionados o crear un archivo comprimido y guardarlo continuamente para que lo archive en función del programa que defina. Para otras opciones de archivo comprimido adicionales, podrá acceder al menú desplegable que hay junto a este botón, que incluye las opciones siguientes. - La opción Crear archivo comprimido es otro método para iniciar el asistente de creación de archivo comprimido para crear una archivación única o una archivación continua. - La opción Importar archivo comprimido inicia el Asistente de importación de archivo comprimido, que permite importar un archivo comprimido. - La opción Adjuntar archivo comprimido monta un archivo comprimido para poder leer el contenido como un sistema de archivos.
Barra de botones: botón Replicación	 El botón Replicación abre el Asistente para replicación. Desde el asistente, puede especificar un Core de destino, seleccionar equipos protegidos en el Core de origen y replicar puntos de recuperación desde los equipos seleccionados en el Core de destino en el repositorio que especifique. Puede pausar la replicación al definirla o puede comenzar la replicación inmediatamente. Además, puede especificar si una unidad de inicialización se utilizará para copiar los datos de puntos de recuperación en el Core de destino.

Barra de iconos

Los detalles sobre la barra de iconos aparecen en la tabla siguiente.

Tabla 216. Barra de iconos

Elemento de la IU	Descripción	
Barra de iconos	La barra de iconos incluye una representación gráfica para las funciones principales accesibles en la Consola de Core. Al hacer clic en el elemento apropiado le lleva a la sección correspondiente de la interfaz de usuario donde puede gestionar esa función. Los iconos de la barra de iconos incluyen:	
Barra de iconos: icono de inicio		Inicio. Haga clic en el botón Inicio para navegar hasta la página Inicio del Core.
Barra de iconos: icono de replicación		Replicación. Haga clic en el icono Replicación para ver o gestionar replicas entrantes o salientes.
Barra de iconos: icono de espera virtual		Espera virtual. Haga clic en el icono Espera virtual para exportar información desde un punto de recuperación a una máquina virtual arrancable.
Barra de iconos: icono de eventos		Eventos. Haga clic en el icono Eventos para ver un registro de todos los eventos del sistema relacionados con el Core de Rapid Recovery.
Barra de iconos: icono Configuración		Configuración. Haga clic en el icono Configuración para ver o administrar la configuración del Core de Rapid Recovery. Puede realizar una copia de seguridad o restaurar los valores de la configuración del Core. Puede establecer una configuración general para los puertos de control o mostrar los aspectos. Además, puede configurar los ajustes en las categorías siguientes: actualizaciones automáticas; trabajos nocturnos; configuración de la cola de transferencias; configuración del tiempo de espera del cliente; configuración de la caché de deduplicación de DVM; configuración de Replay Engine; e implementar la configuración. Puede ver o cambiar las conexiones de la base de datos; la configuración de un servidor SMTP; las cuentas de almacenamiento en la nube y cambiar la configuración del tipo de letra de los informes. Puede establecer la configuración de conectabilidad de SQL; la configuración de trabajo del Core; los ajustes de licencia; la configuración de SNMP; y la configuración de vSphere.
Barra de iconos: icono Más		Más. Haga clic en el icono Más para acceder a otras características importantes. Cada una tiene un icono propio que se enumera a continuación.
Barra de iconos: icono Más	Información del sistema	 Información del sistema. Haga clic en Información del sistema para mostrar los datos acerca del servidor del Core de Rapid Recovery. Puede ver el nombre de host, el SO, la arquitectura y la memoria del Core. Puede ver el nombre que se muestra en la Core Console. También puede ver el nombre de dominio completamente cualificado del Core de su red, así como la ruta de acceso para sus metadatos de caché y las cachés de deduplicación. Para obtener más información sobre cómo cambiar el nombre de visualización, consulte Funcionamiento de la información del sistema para el Core. Para obtener más información sobre la caché de deduplicación, consulte Funcionamiento de la caché de deduplicación y las ubicaciones de almacenamiento. Para obtener más información sobre el ajuste de la configuración, consulte Configuración de los valores de caché de la deduplicación de DVM.
Barra de iconos: icono Más	Archivos comprimidos	 Archivos comprimidos. Rapid Recovery permite administrar los archivos comprimidos de la información del Core. Puede ver información acerca de

Elemento de la IU	Descripción		
			archivos programados o conectados, y puede agregar, comprobar o importar los archivos.
Barra de iconos: icono Más	Montajes		Montajes. Permite ver y desmontar montajes locales, así como ver y desconectar montajes remotos.
Barra de iconos: icono Más	CD de arranque		CD de arranque. Permite administrar los CD de arranque, que se utilizan normalmente para una restauración completa (BMR). Puede crear una imagen ISO del CD de arranque, eliminar una imagen existente o hacer clic en la ruta de acceso para abrir o guardar la imagen.
Barra de iconos: icono Más	Repositorios		Repositorios. Permite ver y administrar los repositorios asociados con el Core.
Barra de iconos: icono Más	Claves de cifrado		Claves de cifrado. Permite ver, administrar, importar o agregar las claves de cifrado que puede aplicar a los equipos protegidos. Si no se utiliza, puede eliminar las claves de cifrado.
Barra de iconos: icono Más	Cuentas en la nube		Cuentas en la nube. Permite ver y administrar las conexiones entre el Core y las cuentas de almacenamiento en la Nube.
Barra de iconos: icono Más	Política de retención		Política de retención. Permite ver y modificar la política de retención del Core, incluidos el tiempo para conservar puntos de recuperación antes de consolidarlos y finalmente eliminarlos.
Barra de iconos: icono Más	Notificaciones		Notificaciones. Permite configurar las notificaciones sobre los eventos del Core, definir la configuración de servidor SMTP para las notificaciones por correo electrónico y establecer la reducción de repeticiones para suprimir las notificaciones del mismo evento.
Barra de iconos: icono Más	Descargas		Descargas. Puede descargar el instalador web del software de Agent, Local Mount Utility o los archivos MIB que contienen información de eventos para utilizarla en un navegador SNMP.
Barra de iconos: icono Más	Informes		Informes. Permite acceder a los informes de Core o programar informes para generarlos en una base constante.
Barra de iconos: icono Más	Core Log		Core Log. Permite descargar el archivo de Core log con fines de diagnóstico.

Menú de navegación izquierdo

El conjunto completo de menús que puede aparecer en el área de navegación izquierda se describe en la siguiente tabla:

Tabla 217. Opciones del menú de navegación izquierdo

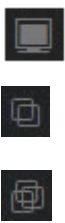
Elemento de la IU	Descripción
Menú Equipos protegidos	El menú Equipos protegidos aparece como el primer menú del área de navegación izquierda si hay uno o más equipos protegidos en el Core.

Elemento de la IU	Descripción
	Si hace clic en un nombre de equipo específico que se muestre en el panel, aparece una página de resumen, que muestra la información de resumen del equipo seleccionado. Para obtener más información sobre lo que puede realizar en la página Resumen, consulte Visualización de información de resumen de un equipo protegido .
Menú Equipos replicados	Si aparece el nombre de otro Core de Rapid Recovery como un menú de navegación de nivel superior, el Core en el que visualiza Core Console es un Core de destino. El menú recibe el nombre después del Core de origen, y cada equipo que aparece debajo representa un equipo de ese Core de origen que se ha replicado en el destino. Si el Core de destino replica los puntos de recuperación de más de un Core de origen, cada Core de origen aparece como su propio menú de navegación en el área de navegación izquierda. Si hace clic en un nombre de equipo específico que se muestre en el menú de un equipo replicado, aparece una página de resumen, que muestra la información de resumen del equipo replicado seleccionado. Para obtener más información acerca de la replicación, consulte Replicación.
Menú Solo puntos de recuperación	Si aparece un menú SOLO PUNTOS DE RECUPERACIÓN, el Core conserva los puntos de recuperación de un equipo una vez se haya protegido o replicado. Mientras que el equipo no continúe con la captura de nuevas instantáneas, los puntos de recuperación previamente capturados permanecen en el Core. Estos puntos de recuperación pueden utilizarse para la recuperación a nivel de archivos, pero no pueden utilizarse para una recuperación completa sin sistema operativo, para restaurar volúmenes completos, o para agregar datos de instantáneas.
Menú Grupos personalizados	Si ha creado un grupo personalizado, el menú Grupos personalizados aparece en el menú de navegación. Los grupos personalizados son contenedores lógicos que se utilizan para agrupar los equipos (por ejemplo, por función, organización o ubicación geográfica). Los grupos personalizados pueden contener objetos heterogéneos (equipos protegidos, equipos replicados, entre otros). Puede definir la etiqueta de un grupo personalizado; como ocurre en otros menús, el nombre aparece en letras mayúsculas. Puede realizar acciones para elementos similares en un grupo personalizado al hacer clic en la flecha derecha del título del grupo personalizado. Por ejemplo, puede forzar una instantánea de cada equipo protegido de un grupo personalizado. Para obtener más información sobre la creación y administración de grupos personalizados, consulte Comprensión de los grupos personalizados.
Menú archivos comprimidos adjuntos	Si conecta los archivos al Core, cada archivo aparece en el menú de navegación izquierdo. La etiqueta es el nombre del archivo. Cada equipo que aparece en la lista se incluye en el archivo.

Los detalles acerca de los elementos en el área de navegación izquierda aparecen en la tabla siguiente.

Tabla 218. Área de navegación izquierda y menús

Elemento de la IU	Descripción
Filtro de texto de los menús de los equipos	 El filtro de texto es un campo de texto que le permite filtrar los elementos que se muestran en los menús de los equipos protegidos, equipos replicados y equipos con puntos de recuperación únicamente. Si escribe los criterios en este tipo de filtro solo los equipos que cumplen los criterios se mostrarán en los menús correspondientes.
Expandir y contraer detalles	 Haga clic en la flecha situada a la derecha del filtro de texto para expandir y contraer los detalles de los menús de los equipos protegidos, equipos replicados y equipos con puntos de recuperación únicamente.

Elemento de la IU	Descripción
Menú Equipos protegidos	 El menú Equipos protegidos aparece en el área de navegación izquierda de la IU. En este menú puede ver todos los equipos protegidos, los clústeres protegidos o los equipos replicados configurados en su Core. Si tiene grupos protegidos o equipos con puntos de recuperación únicamente, también aparecerán como una parte de este menú. Puede contraer o expandir la vista de cualquiera de estos equipos protegidos en su Core haciendo clic en la fecha del lado izquierdo de esta etiqueta del menú. El icono que se visualiza representa el tipo de equipo: • Un icono de equipo simple representa un equipo físico o una VM protegida con el software de Agent Rapid Recovery instalado. • Un icono de varios equipos representa un clúster protegido. • Un icono de equipo doble hueco representa un VMware de una MV con protección sin agentes. • Un icono de equipo triple hueco representa un host VMware vCenter. Si hace clic en el menú Equipos protegidos, se abrirá la página Equipos protegidos, que muestra todos los equipos protegidos de este Core en el panel Equipos protegidos. Para obtener más información, consulte Visualización del menú Equipos protegidos.
Menú Equipos replicados	Si está replicando equipos desde otro Core de Rapid Recovery, el nombre de ese Core aparecerá como un menú separado en el menú Equipos protegidos. Cada una de los equipos replicados en este Core de destino desde el Core de origen enumerado aparecen en este menú. Para cada equipo replicado, el icono indica el tipo de equipo que se está replicando. Por ejemplo, si se replica un solo equipo, el icono muestra un equipo. Si se replica un clúster de servidor, el icono representa un clúster. Puede contraer o ampliar la vista de cualquiera de estos equipos replicados haciendo clic en la fecha del lado izquierdo de esta etiqueta del menú. Puede realizar acciones en todos los equipos replicados desde el menú Equipos replicados. Si hace clic en el menú Equipos replicados, aparece la página Equipos. Esta página muestra los equipos protegidos en otro Core (de origen) que se replican en este Core de destino. Para obtener más información, consulte Visualización de equipos replicados en el menú de navegación.
Menú Solo puntos de recuperación	Si se retiraron de la protección equipos protegidos anteriormente por el Core, pero no se eliminaron los puntos de recuperación, entonces aparece el menú Solo puntos de recuperación. Cada uno de los equipos protegidos anteriormente con puntos de recuperación conservados se muestra en esta lista. Puede contraer o ampliar la vista de los equipos con puntos de recuperación únicamente haciendo clic en la fecha del lado izquierdo de esta etiqueta del menú. Puede eliminar los puntos de recuperación de todos los equipos con solo puntos de recuperación en este Core desde el menú Solo puntos de recuperación. Si hace clic en el menú Solo puntos de recuperación, se abrirá la página Equipos, que muestra todos los equipos en los que se guardaron puntos de recuperación. Para obtener más información, consulte Visualización en el menú Solo puntos de recuperación.
Menú Grupos personalizados	Si su Core incluye grupos personalizados, el área de navegación izquierda incluye un menú Grupos personalizados. Cada objeto de ese grupo personalizado se visualiza en esta lista. Puede contraer o expandir la vista de cualquiera de los grupos personalizados en su Core haciendo clic en la flecha del lado izquierdo de esta etiqueta del menú. Puede realizar acciones para elementos parecidos en el grupo desde el menú Grupos personalizados. Si hace clic en el menú Grupos personalizados, se abrirá la página Equipos, que muestra un panel para cada uno de los objetos de Rapid Recovery que aparecen en su grupo: equipos protegidos, equipos replicados y equipos

Elemento de la IU	Descripción

	con puntos de recuperación únicamente. Para obtener más información, consulte Visualización en el menú Grupos personalizados .
Menú archivos comprimidos adjuntos	 Si adjunta los archivos comprimidos a su Core, el área de navegación izquierda incluye un menú para cada archivo comprimido adjunto. Se visualiza en esta lista cada una de los equipos protegidos incluidos en el archivo comprimido. La etiqueta del menú utiliza el nombre especificado al guardar el archivo. Puede contraer o expandir la vista de cualquiera de los archivos comprimidos adjuntos a su Core haciendo clic en la fecha del lado izquierdo de esta etiqueta del menú. Puede realizar acciones para elementos parecidos en el grupo desde el menú archivos comprimidos adjuntos. Si hace clic en el menú archivos comprimidos adjuntos, se abrirá la página Equipos, que muestra un panel para cada uno de los objetos de Rapid Recovery que aparecen en su grupo: equipos protegidos, equipos replicados y equipos con puntos de recuperación únicamente. Para obtener más información, consulte Visualización en el menú Grupos personalizados.

Visualización del panel de máquinas protegidas

El panel de máquinas protegidas contiene información sobre todas las máquinas protegidas en este Core de Rapid Recovery. Para cada máquina protegida (si las hay), verá enmuerada la información descrita en la tabla siguiente.

Tabla 219. Información acerca de cada máquina protegida

Elemento UI	Descripción
Select Item (Seleccionar elemento)	En cada fila de la tabla de resumen, puede seleccionar la casilla de verificación para llevar a cabo acciones en la lista de opciones de menú sobre la tabla.
Type (Tipo)	Muestra el tipo de máquina.
Status indicator (Indicador de estado)	Los círculos de color en la columna Status (Estado) indican si una máquina está en línea o si es inaccesible. Si coloca el cursor sobre el círculo de color, aparecerá la condición de estado. Las condiciones de estado pueden ser verde (en línea y protegido), amarillo (protección pausada), rojo (error de autenticación) y el gris (fuera de línea o inaccesible).
Encryption status (Estado de cifrado)	El ícono de bloqueo indica el estado de cifrado de la máquina protegida seleccionada. Si se muestra un candado abierto, significa que no hay cifrado. Si se muestra un candado cerrado, significa que se han establecido las claves de cifrado. Para obtener más información sobre el cifrado, consulte Descripción de las claves de cifrado .
Display name (Nombre)	El nombre de host de la máquina protegida.
Last snapshot (Última instantánea)	Muestra la fecha y la hora de la última transferencia de copia de seguridad de esta máquina.
Repository Name (Nombre del repositorio)	Indica el repositorio en el que se almacenan los datos de esta máquina.
Recovery Points (Puntos de recuperación)	Muestra el número de puntos de recuperación y cuánto espacio ocupan en el repositorio.
Version (Versión)	La versión del software del Agent de Rapid Recovery cargada en la máquina.

Elemento UI	Descripción
Actions (Acciones)	Al hacer clic en el menú desplegable de Configuración en esta columna, verá una lista de acciones para llevar a cabo específicamente en la máquina protegida seleccionada.

Si alguna de las máquinas que se protege este Core están configuradas en espera virtual, verá información adicional como se describe en la tabla siguiente.

Tabla 220. Información de las máquinas protegidas configuradas en espera virtual

Elemento UI	Descripción
Last Export (Última exportación)	Fecha y hora de la última exportación virtual.
Destination (Destino)	El destino donde guardar la máquina protegida como máquina virtual. Por ejemplo, ESXi, VMWare Workstation, Hyper-V o VirtualBox.
Status (Estado)	Estado de máquina configurada en espera virtual. Las condiciones de estado pueden ser "In Sync" (En sincronización), "Paused" (Pausada) y "Not enabled" (No habilitada).

En el menú desplegable de Acciones del panel de las máquinas protegidas, puede realizar las acciones que se describen en la siguiente tabla. Algunas de las opciones solo aparecen en servidores Exchange o SQL Server, como se indica

Tabla 221. Acciones disponibles en el panel de máquinas protegidas

Elemento UI	Descripción
Force Snapshot (Forzar instantánea)	Le permite forzar una instantánea acumulada o una imagen base de todos los volúmenes protegidos en la máquinas protegidas seleccionadas. Para obtener más información, consulte Cómo forzar una instantánea .
One-time export (Exportación única)	Inicia el Virtual Machine Export Wizard (Asistente de exportación de máquina virtual). Este asistente le permite realizar una exportación única de datos de un punto de recuperación de una máquina protegida a una máquina virtual en cualquier formato de máquina virtual compatible. Para obtener más información, consulte Exportación de VM .
Virtual Standby (En espera virtual)	Inicia el Virtual Machine Export Wizard (Asistente de exportación de máquina virtual). Este asistente le permite realizar un estado de espera virtual para exportar datos de un punto de recuperación de una máquina protegida a una máquina virtual en cualquier formato de máquina virtual compatible. Para obtener más información, consulte Exportación de VM .
Mount (Montaje)	Inicia el Mount Wizard (Asistente de montaje). Este asistente le permite montar puntos de recuperación desde la máquina protegida seleccionada.
Recovery Points (Puntos de recuperación)	Abre la página de resumen de los puntos de recuperación.
Restore (Restaurar)	Se inicia el Restore Machine Wizard (Asistente de restauración de la máquina). Este proceso le permite restaurar datos a partir de puntos de recuperación en el Core a una máquina protegida. Para obtener más información, consulte Restauración de volúmenes desde un punto de recuperación .
Remove Machine (Eliminar máquina)	Elimina la máquina seleccionada de la protección del Core de Rapid Recovery, que le permite eliminar o conservar los puntos de recuperación que ya se encuentran en el Core de Rapid Recovery. Para obtener más información, consulte Retirada de un equipo .

Puede realizar acciones en dos o más de las máquinas que se enumeran en la cuadrícula de máquinas protegidas. Para llevar a cabo acciones en varias máquinas, seleccione la casilla de marcación de cada máquina protegida. A continuación, desde el menú sobre la tabla de resumen, puede realizar cualquiera de las acciones que se describen en la siguiente tabla.

Tabla 222. Hay acciones adicionales disponibles en el panel de máquinas protegidas cuando se seleccionan las máquinas.

Elemento UI	Descripción
Force Snapshot (Forzar instantánea)	Le permite forzar una instantánea acumulada de todos los volúmenes protegidos en la máquinas protegidas seleccionadas. Para obtener más información, consulte Cómo forzar una instantánea .
Force Base Image (Forzar imagen base)	Le permite forzar una imagen base de todos los volúmenes protegidos en la máquinas protegidas seleccionadas. Para obtener más información, consulte Cómo forzar una instantánea .
Protection > Pause or Resume (Protección > Pausar o reanudar)	Le permite pausar la protección de las máquinas seleccionadas (si la protección está activada), o le permite reanudar la protección para el las máquinas seleccionadas (si la protección está pausada). Para obtener más información, consulte Puesta en pausa y reanudación de la protección .
Replication (Replicación)	Le permite activar, forzar, copiar, pausar o reanudar la replicación. También puede copiar puntos de recuperación existentes a una unidad de inicialización. Para obtener más información, consulte Administración de configuraciones de replicación .
Cancel (Cancelar)	Le permite cancelar todas las operaciones activas en el momento de las máquinas seleccionadas, o le permite cancelar las instantáneas que solo se están realizando en el momento en las máquinas seleccionadas. Esto no afecta a las operaciones programadas para el futuro.
Remove Machines (Eliminar máquinas)	Elimina la máquina seleccionada de la protección del Core de Rapid Recovery, que le permite eliminar o conservar los puntos de recuperación que ya se encuentran en el Core de Rapid Recovery. Para obtener más información, consulte Retirada de un equipo .

En el menú desplegable Configuration (Configuración) de cada máquina protegida, puede realizar las acciones enumeradas en la tabla siguiente. Algunas de las opciones solo aparecen en servidores Exchange o SQL Server, como se indica.

Tabla 223. Acciones disponibles en el panel de máquinas protegidas

Elemento UI	Descripción
Force Snapshot (Forzar instantánea)	Le permite forzar una instantánea acumulada o una imagen base de uno o varios volúmenes en la máquina seleccionada. Para obtener más información, consulte Cómo forzar una instantánea .
Force Log Truncation for Exchange (Forzar el truncamiento del registro de Exchange)	En máquinas protegidas con Exchange Server, fuerza truncaciones de registros de Exchange, con lo que libera espacio en el servidor de Exchange. Para obtener más información, consulte Forzado del truncamiento de registros para un equipo SQL .
Force Log Truncation for SQL (Forzar el truncamiento del registro de SQL)	En máquinas protegidas con SQL Server, fuerza truncaciones de registros de SQL Server, con lo que libera espacio en el servidor de SQL. Para obtener más información, consulte Forzado del truncamiento de registros para un equipo SQL .
Export (Exportar)	Inicia el Export Wizard (Asistente de exportación). Este asistente le permite exportar datos de puntos de recuperación de una máquina protegida a una máquina virtual en cualquier formato de máquina virtual compatible. Puede realizar una exportación única o configure esperavirtual para realizar exportaciones continuas. Para obtener más información, consulte Exportación de VM .
Mount (Montaje)	Se abre el cuadro de diálogo Mount Recovery Point (Montar punto de recuperación), que le permite examinar los datos de la instantánea a través guardados el Core Rapid Recovery para montar un punto de recuperación

Elemento UI	Descripción
	específico. Para obtener más información, consulte Montaje de un punto de recuperación o Montaje de un volumen de punto de recuperación en un equipo Linux , respectivamente.
Recovery Points (Puntos de recuperación)	Se abre la pestaña Recovery Points (Puntos de la máquina del Agent seleccionada. Para obtener más información, consulte Administración de instantáneas y puntos de recuperación .
Restore (Restaurar)	Se inicia el Restore Machine Wizard (Asistente de restauración de la máquina). Este proceso le permite restaurar datos a partir de puntos de recuperación en el Core a una máquina protegida. Para obtener más información, consulte Restauración de volúmenes desde un punto de recuperación .
Remove Machine (Eliminar máquina)	Elimina la máquina seleccionada de la protección del Core de Rapid Recovery, que le permite eliminar o conservar los puntos de recuperación que ya se encuentran en el Core de Rapid Recovery. Para obtener más información, consulte Retirada de un equipo .

Visualización de eventos de un equipo protegido

En la página **Eventos**, puede ver los trabajos que se han realizado o que están en curso en el equipo protegido que seleccionó. Los botones de la parte superior de la página le permiten navegar a listas de trabajos en cada una de las tres categorías de actividades:

- **Tareas.** Un trabajo que Rapid Recovery debe realizar para operar correctamente.
- **Alertas.** Una notificación relacionada con una tarea o evento que incluye errores y advertencias.
- **Diario.** Un compuesto de todas las tareas y alertas del equipo protegido.

La siguiente tabla incluye las descripciones de cada elemento de la página **Eventos**.

Tabla 224. Elementos de la página Eventos

Elemento de la IU	Descripción
Palabra clave de la búsqueda	Le permite buscar un elemento específico dentro de cada categoría. Solo disponible para tareas.
De	Para restringir los resultados, puede introducir una fecha en la que empezar la búsqueda. Solo disponible para tareas.
Hasta	Para restringir los resultados, puede introducir una fecha en la que detener la búsqueda. Solo disponible para tareas.
Iconos de estado	Cada icono representa un estado de trabajo diferente. En el caso de alertas y tareas, al hacer clic en uno de los iconos podrá filtrar la lista por ese estado, generando básicamente un informe. Al hacer clic en el icono una segunda vez elimina el filtro para ese estado. Puede filtrar por más de un estado. Los estados incluyen: • Activo. Un trabajo que está en curso. • En cola. Un trabajo que está esperando que otro trabajo finalice antes de poder iniciarse. • Esperando. Un trabajo que está esperando su aprobación o finalización, como una unidad de inicialización. (Para obtener más información acerca de las unidades de inicialización, consulte Replicación.) • Finalizado. Un trabajo que se ha realizado correctamente. • Con fallo. Un trabajo que ha fallado y no se completó.
Icono de servicio	Este botón agrega trabajos de servicios a la lista de trabajos. Cuando hace clic en este icono, aparece un icono de servicio más pequeño en cada icono de estado, que le permite filtrar por trabajos de servicio que tienen esos estados (si los hubiera). Los ejemplos de trabajos de servicios incluyen la eliminación de archivos de índice o retirar un equipo de la protección.

Elemento de la IU	Descripción
Lista desplegable Tipo de exportación	La lista desplegable incluye los formatos con los que puede exportar el informe del evento. Solo disponible para tareas. Incluye los siguientes formatos: • PDF • HTML • CSV • XLS • XLSX
 (icono Exportar)	Convierte el informe del evento al formato que seleccionó. Solo disponible para tareas.
Selección de página	Los informes de eventos pueden incluir varios trabajos en múltiples páginas. Los números y las flechas de la parte inferior de la página Eventos permiten navegar a las páginas adicionales del informe.

La página **Eventos** muestra todos los eventos de una tabla. La siguiente tabla enumera la información que se muestra para cada elemento.

Tabla 225. Información detallada para la tabla de resumen de los eventos

Elemento de la IU	Descripción
Estado	Muestra el estado de la tarea, alerta o el elemento diario. Está disponible para las alertas o los elementos diario; haga clic en el encabezado para filtrar los resultados por estado.
Nombre	Nombre está disponible solo para las tareas. Este campo de texto enumera el tipo de tarea que se ha completado para este equipo protegido. Algunos ejemplos incluyen la transferencia de volúmenes, el mantenimiento del repositorio, la consolidación, la realización de comprobaciones de la capacidad de montaje, la realización de comprobaciones de suma de comprobación, y así sucesivamente.
Hora de inicio	Disponible para las tareas, alertas y los elementos diario. Muestra la fecha y la hora en las que se inició el trabajo o la tarea.
Hora de finalización	Solo disponible para tareas. Muestra la fecha y la hora en las que se completó la tarea.
 Detalles del trabajo	Solo disponible para tareas. Se abre el cuadro de diálogo Supervisar tarea activa por lo que puede ver los detalles de un trabajo específico o una tarea. Estos detalles incluyen una ID para el trabajo, la velocidad a la que el Core transfirió los datos (si corresponde), el tiempo transcurrido para que el trabajo se complete, el trabajo total en cantidad de gigabytes y cualquier tarea secundaria relacionada con el trabajo.
Mensaje	Disponible para las alertas y los elementos diario. Este campo de texto proporciona un mensaje descriptivo de la alerta o el elemento diario.

Visualización del menú Más para máquinas protegidas

El menú **More (Más)** ofrece opciones adicionales para ayudar a administrar una máquina protegida. Para acceder a estas herramientas, haga clic en el menú desplegable y seleccione más de una de las opciones descritas en la tabla siguiente.

Tabla 226. Herramientas a las que se puede acceder desde la opción Más para máquinas protegidas.

Elemento UI	Descripción
	Muestra información sobre la máquina protegida, información del sistema, los volúmenes, los procesadores, los adaptadores de red, y las direcciones IP de esta máquina.

Elemento UI	Descripción
Información del sistema	Para obtener más información, consulte Visualización de la información del sistema de un equipo protegido :
 Montajes	Desde el panel de montajes locales, puede ver o desmontar volúmenes montados localmente. Desde el panel de montajes remotos, puede ver o desmontar volúmenes montados con la utilidad Local Mount Utility. Para obtener información sobre cómo desmontar volúmenes, consulte Desmontaje de puntos de recuperación. Para obtener información sobre cómo montar un punto de recuperación localmente, consulte Montaje de un punto de recuperación o Montaje de un volumen de punto de recuperación en un equipo Linux, respectivamente.
 Retention Policy (Política de retención)	Le permite especificar una política de retención de la máquina seleccionada. Puede optar por usar la política predeterminada del Core, o bien puede diferenciar la política de retención para esta máquina solamente. Para obtener más información, consulte Personalización de la configuración de la política de retención de una máquina protegida .
 Notificaciones	Le permite especificar un grupo de notificación personalizada para eventos relacionados con la máquina seleccionada. Esta configuración no modifica las notificaciones que ya se han configurado en el Core. Para obtener más información, consulte Configuración de grupos de notificación .
 Registro de agentes	Le permite descargar y visualizar el archivo de registro para una máquina protegida mediante el software del Agent de Rapid Recovery. Para obtener más información, consulte Descarga y visualización del archivo de registro de un equipo protegido .

Descripción del módulo PowerShell de Rapid Recovery

Dell Data Protection | Rapid Recovery se compone de varios componentes de software. Entre los componentes clave relevantes para este tema se incluyen los siguientes:

- El Core de Rapid Recovery gestiona la autenticación para equipos protegidos, los calendarios de programación para la transferencia de datos de la copia de seguridad y replicación, la exportación a máquinas virtuales, informes y bare metal restore (BMR) para hardware similar o diferente.
- El Rapid Recovery Agent se encarga de las instantáneas del volumen y de la transferencia rápida de datos al repositorio administrado por el Core.
- El módulo PowerShell de Rapid Recovery es una utilidad de Windows que permite a los usuarios interactuar con el servidor del Core mediante comandos de Windows PowerShell®. Este módulo ofrece algunas de las mismas funciones que ofrece la interfaz gráfica de usuario (GUI) de la Core Console de Rapid Recovery. Por ejemplo, el módulo PowerShell de Rapid Recovery puede montar puntos de recuperación de Rapid Recovery o forzar una instantánea de un equipo protegido.

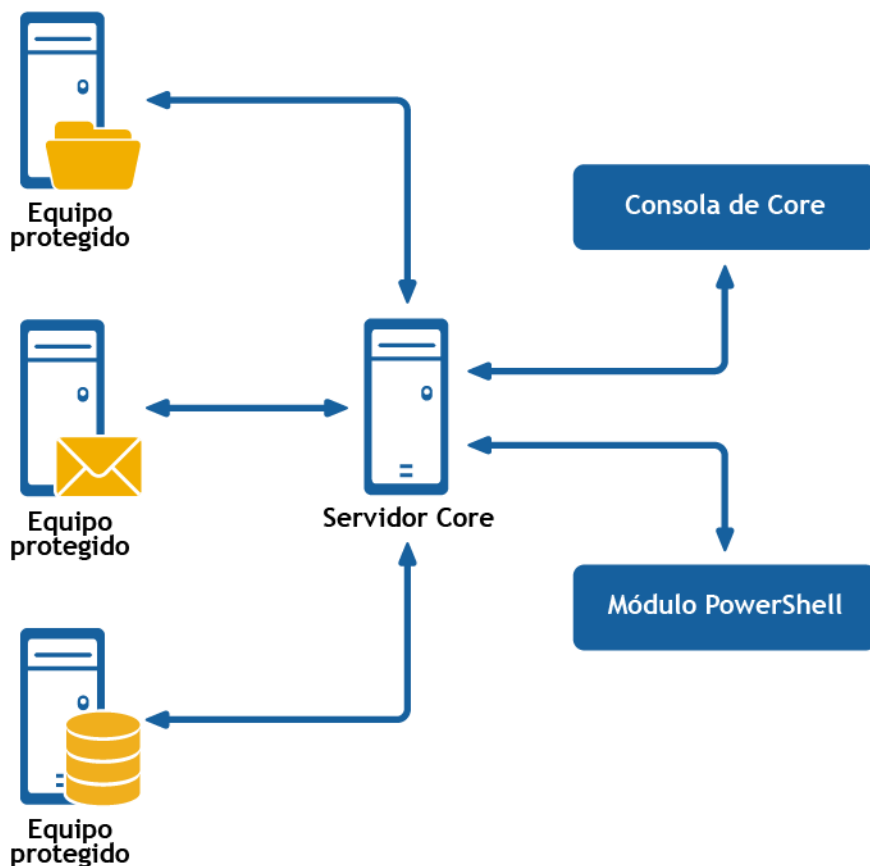


Ilustración 14. El módulo PowerShell interactúa con el Core de Rapid Recovery

PowerShell es un entorno conectado con el framework .NET de Microsoft diseñado para automatización administrativa. En esta sección se describe el módulo PowerShell de Rapid Recovery y los cmdlets que los administradores pueden utilizar para crear ciertas funciones sin interacción con la interfaz gráfica de usuario (GUI) del Core de Rapid Recovery.

NOTA: Puede ejecutar también secuencias de comandos de PowerShell como pre y post secuencias de comandos. Para obtener más información y secuencias de comandos de muestra, consulte [Extensión de trabajos de Rapid Recovery mediante secuencias de comandos](#).

Temas:

- [Requisitos previos para utilizar PowerShell](#)
- [Trabajo con comandos y cmdlets](#)
- [Cmdlets del módulo Rapid Recovery PowerShell](#)
- [Localización](#)
- [Calificadores](#)

Requisitos previos para utilizar PowerShell

Para poder usar el módulo PowerShell de Rapid Recovery, debe tener instalado Windows PowerShell 2.0 o posterior. Debido a las nuevas funciones introducidas en PowerShell 3.0, que incluyen un acceso más sencillo a las propiedades de objetos, acceso Web de PowerShell, así como compatibilidad con llamadas REST, Dell recomienda el uso de PowerShell 3.0 o posterior.

NOTA: asegúrese de colocar el archivo `powershell.exe.config` en el directorio de inicio de PowerShell. Por ejemplo, C:\WindowsPowerShell\powershell.exe.config.

powershell.exe.config

```
<?xml version="1.0"?>
<configuration>
  <startup useLegacyV2RuntimeActivationPolicy="true">
    <supportedRuntime version="v4.0.30319"/>
    <supportedRuntime version="v2.0.50727"/>
  </startup>
</configuration>
```

Inicio de PowerShell e importación del módulo

Al revés de lo que sucede en los módulos del sistema, el módulo PowerShell de Rapid Recovery no se carga de forma predeterminada. Puede abrir Windows PowerShell para cada sesión con privilegios administrativos y, a continuación, importar el módulo. Complete los pasos de este procedimiento para iniciar PowerShell e importar el módulo PowerShell de Rapid Recovery.

- 1 Abra una sesión de símbolo del sistema con privilegios elevados para Windows PowerShell. Por ejemplo, introduzca Windows PowerShell en el menú Inicio y para la aplicación Windows PowerShell resultante, haga clic con el botón derecho del ratón y seleccione **Ejecutar como administrador**.
Se abrirá Windows PowerShell en una nueva ventana del símbolo del sistema.
- 2 Introduzca el siguiente comando y, a continuación, pulse Intro:
`Import-Module "RapidRecoveryPowerShellModule"`
Se importará el módulo PowerShell de Rapid Recovery para su sesión actual. Puede empezar a ejecutar cmdlets en la ventana del símbolo del sistema existente.

Trabajo con comandos y cmdlets

Cmdlets son comandos especializados en una secuencia de comandos de Windows PowerShell que realizan una única función. Un cmdlet se expresa normalmente como un par de verbo-sustantivo. El resultado devuelto por un cmdlet es un objeto.

Puede canalizar comandos de PowerShell, lo que permite que el resultado de un cmdlet se canalice como entrada para otro cmdlet. Como ejemplo sencillo, puede solicitar la lista de comandos del módulo PowerShell de Rapid Recovery y clasificar esa lista por nombres. La secuencia de comandos de ejemplo para esto es:

```
Get-Command -module rapidrecoverypowershellmodule | sort-object name
```

Cómo obtener ayuda y ejemplos de cmdlets

Tras abrir PowerShell e importar el módulo PowerShell de Rapid Recovery, puede solicitar información adicional en cualquier momento utilizando el cmdlet `Get-Help <nombre_comando>`. Por ejemplo, para obtener información sobre el cmdlet de exportación de máquina virtual, introduzca el siguiente cmdlet y pulse Intro:

```
Get-Help Start-VMExport
```

El objeto devuelto incluye el nombre de comando, la sinopsis, la sintaxis y cualquier opción que pueda utilizar con el comando.

Otro método para obtener ayuda para un cmdlet específico es introducir el nombre de comando seguido de `-?`. Por ejemplo:

```
Start-VMExport -?
```

También puede solicitar ejemplos de un cmdlet ejecutando el siguiente comando:

```
>Get-Help Start-VMExport -examples
```

Cmdlets del módulo Rapid Recovery PowerShell

Esta sección describe los cmdlets y opciones disponibles del módulo Rapid Recovery PowerShell. Todos los cmdlets del módulo Rapid Recovery PowerShell admiten los siguientes parámetros comunes:

- Verbose
- Depuración
- ErrorAction
- ErrorVariable
- WarningAction
- WarningVariable
- OutBuffer
- OutVariable

Para obtener más información, utilice `Get-Help about_commonparameters`.

Los cmdlets disponibles se enumeran en la tabla siguiente.

Tabla 227. Cmdlets del módulo PowerShell de Rapid Recovery

Nombre de cmdlet	Descripción
Edit-EsxiVirtualStandby	Edita una configuración existente en espera virtual de ESXi.
Edit-HyperVVirtualStandby	Edita una configuración existente en espera virtual de Hyper-V.
Edit-VBVirtualStandby	Edita una configuración existente en espera virtual de VirtualBox.
Edit-VMVirtualStandby	Edita una configuración existente en espera virtual de VMware Workstation.
Edit-ScheduledArchive	Edita una configuración de archivo comprimido programado existente.

Nombre de cmdlet	Descripción
Get-ActiveJobs	Recupera una recopilación de los trabajos activos.
Get-CloudAccounts	Obtiene información acerca de las cuentas de nube guardadas en el Core.
Get-Clusters	Recupera una recopilación de los clústeres protegidos.
Get-CompletedJobs	Recupera una recopilación de los trabajos completados.
Get-ExchangeMailStores	Recupera una recopilación de los almacenes de correo de Exchange.
Get-Failed	Obtiene información acerca de los puntos de recuperación con fallos.
Get-FailedJobs	Recupera una recopilación de los trabajos con fallos.
Get-Mounts	Muestra todos los puntos de recuperación montados.
Get-Passed	Obtiene información acerca de los puntos de recuperación aprobados.
Get-ProtectedServers	Obtiene información acerca de los servidores protegidos.
Get-ProtectionGroups	Recupera una recopilación de los grupos de protección.
Get-QueuedJobs	Recupera una colección de trabajos a la espera en cola.
Get-RecoveryPoints	Obtiene información acerca de los puntos de recuperación.
Get-ReplicatedServers	Obtiene información acerca de los servidores replicados.
Get-Repositories	Obtiene información acerca de repositorios.
Get-ScheduledArchive	Obtiene información acerca de trabajos de archivación periódicos.
Get-SqlDatabases	Recupera una recopilación de bases de datos SQL.
Get-UnprotectedVolumes	Recupera una recopilación de los volúmenes sin protección.
Get-VirtualizedServers	Obtiene información acerca de los servidores virtualizados.
Get-Volumes	Obtiene información acerca de volúmenes.
New-Base	Fuerza una instantánea de imagen base.
New-CloudAccount	Añade una nueva cuenta de nube al Core.
New-EncryptionKey	Crea una nueva clave de cifrado.
New-EsxiVirtualStandby	Crea un nuevo equipo virtual en espera virtual ESXi.
New-HyperVVirtualStandby	Crea un nuevo equipo virtual en espera virtual Hyper-V.
New-Mount	Puntos de recuperación de montaje.
New-Replication	Configura y fuerza una replicación.
New-Repository	Crea un nuevo repositorio DVM.
New-ScheduledArchive	Programa un nuevo archivo periódico.
New-Snapshot	Fuerza una instantánea.
New-VBVirtualStandby	Crea un nuevo equipo virtual en espera virtual VirtualBox.
New-VMVirtualStandby	Crea un nuevo equipo virtual en espera virtual VMware Workstation.
Push-Replication	Forzar replicación.

Nombre de cmdlet	Descripción
Push-Rollup	Fuerza la consolidación.
Remove-Agent	Quita la protección de un equipo.
Remove-Mount	Desmonta un punto de recuperación.
Remove-Mounts	Desmonta todos los puntos de recuperación montados.
Remove-RecoveryPoints	Eliminar puntos de recuperación de un equipo protegido.
Remove-Repository	Elimina un repositorio DVM existente.
Remove-ScheduledArchive	Interrumpe un archivo comprimido programado.
Remove-VirtualStandby	Elimina un equipo virtual en espera virtual del Core.
Resume-Replication	Reanuda la replicación.
Resume-RepositoryActivity	Reanuda la actividad del repositorio.
Resume-ScheduledArchive	Reanuda un archivo comprimido programado.
Resume-Snapshot	Reanuda la instantánea.
Resume-VirtualStandby	Reanuda la exportación de datos a un equipo virtual en espera virtual.
Start-Archive	Archiva los puntos de recuperación.
Start-AttachabilityCheck	Fuerza una comprobación de conectabilidad para las bases de datos de MS SQL protegidas.
Start-ChecksumCheck	Fuerza una comprobación de suma de comprobación para los almacenes de correo de Exchange protegidos.
Start-EsxiExport	Fuerza la exportación a un servidor ESXi.
Start-HypervExport	Fuerza la exportación a un servidor Hyper-V.
Start-LogTruncation	Forzar el truncamiento del registro.
Start-MountabilityCheck	Fuerza una comprobación de capacidad de montaje para los almacenes de correo de Exchange protegidos.
Start-Protect	Pone un servidor bajo protección.
Start-ProtectCluster	Pone un clúster bajo protección.
Start-RepositoryCheck	Fuerza una comprobación de repositorio DVM.
Start-RestoreArchive	Restaura la archivación con puntos de recuperación.
Start-ScheduledArchive	Fuerza una transferencia de datos de un archivo comprimido programado.
Start-VBExport	Fuerza la exportación a un servidor VirtualBox.
Start-VirtualStandby	Fuerza una transferencia de datos a un equipo virtual en espera virtual existente.
Start-VMExport	Fuerza la exportación a un servidor VMWare Workstation.
Stop-ActiveJobs	Cancela los trabajos activos.
Suspend-Replication	Realiza una pausa en la replicación.
Suspend-RepositoryActivity	Realiza una pausa en la actividad de un repositorio.

Nombre de cmdlet	Descripción
Suspend-ScheduledArchive	Realiza una pausa en la transferencia de datos de un archivo comprimido programado.
Suspend-Snapshot	Realiza una pausa en la instantánea.
Suspend-VirtualStandby	Realiza una pausa en la transferencia de datos a un equipo virtual en espera virtual.
Update-Repository	Agrega extensión al repositorio DVM.

Edit-EsxiVirtualStandby

El comando `Edit-EsxiVirtualStandby` le permite utilizar PowerShell para realizar cambios en una exportación virtual existente a una máquina virtual ESXi (VM).

Uso

El uso del comando es el siguiente:

```

Edit-EsxiVirtualStandby [-HostName <String>] [-HostPort <String>] [-HostUserName <String>] [-HostPassword <String>] [-DiskProvisioning <String>] [-DiskMapping <String>] [-ProtectedServer <String>] [-Volumes <String[]>] [-VMName <String>] [-UseSourceRam] [-Ram <String>] [-User <String>] [-Core <String>] [-Password <String>] [-Verbose] [-Debug] [-ErrorAction <ActionPreference>] [-WarningAction <ActionPreference>] [-ErrorVariable <String>] [-WarningVariable <String>] [-OutVariable <String>] [-OutBuffer <Int32>]

```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `Edit-EsxiVirtualStandby`:

Tabla 228. Opciones del comando Edit-EsxiVirtualStandby

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Muestra los trabajos de un equipo protegido específico, indicado por dirección IP.
-all	Muestra todos los trabajos, incluyendo los realizados por el Core y todos los servidores protegidos.
-number	Opcional. Determine cuántas entradas se visualizarán. Los valores disponibles son:

Opción	Descripción
	all (mostrar todos los trabajos); l[número] o [número] (recupera los ## trabajos más recientes ordenados por ejecución y hora); f[número] (muestra los ## primeros trabajos de recuperación ordenados por ejecución y hora). Se muestran los 20 trabajos más recientes de forma predeterminada.
-jobtype	Opcional. Especifica el filtro de tipo de trabajo. Los valores disponibles son: 'transfer' (transferencia de datos), 'repository' (mantenimiento de repositorio), 'replication' (replicaciones locales y remotas), 'backup' (restauración y copia de seguridad), 'bootcdbuilder' (crear CD de inicio), 'diagnostics' (cargar registros), 'exchange' (comprobación de archivos de Exchange Server), 'export' (exportación de punto de recuperación), 'pushinstall' (agentes de implementación), 'rollback' (restauración desde un punto de recuperación), 'rollup' (despliegues de puntos de recuperación), 'sqlattach' (comprobaciones de la conectabilidad de Agent) y 'mount' (montaje de repositorio). De forma predeterminada, todos los trabajos del tipo especificado se devuelven.
-time	Opcional. Filtra los resultados por fecha y hora en la que se inició el trabajo. Los tipos de entrada disponibles incluyen: #d o DD (donde # es un número para el periodo de tiempo de días antes de ahora hasta ahora) #h o #H (donde # es un número para el periodo de horas antes de ahora hasta ahora) “hora fecha1”, “hora fecha 2” (para mostrar un intervalo personalizado de tiempo desde una fecha específica que aparece antes de la coma hasta una fecha específica que sigue a la coma).

Ejemplo:

Enumerar todos los trabajos activos en el Core local:

```
>Get-activejobs -all
```

Edit-Hyper VVirtualStandby

El comando `Edit-HyperVVirtualStandby` le permite usar PowerShell para realizar cambios en una exportación virtual existente a una máquina virtual Hyper-V (VM).

Uso

El uso del comando es el siguiente:

```
Edit-HyperVVirtualStandby [-HostName <String>] [-HostPort <String>] [-HostUserName <String>] [-HostPassword <String>] [-VMLocation <String>] [-UseLocalMachine] [-gen2] [-UseVhdx] [-ProtectedServer <String>] [-Volumes <String[]>] [-VMName <String>] [-UseSourceRam] [-Ram <String>] [-User <String>] [-Core <String>] [-Password <String>] [-Verbose] [-Debug] [-ErrorAction <ActionPreference>] [-WarningAction <ActionPreference>] [-ErrorVariable <String>] [-WarningVariable <String>] [-OutVariable <String>] [-OutBuffer <Int32>]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `Edit-HyperVVirtualStandby`:

Tabla 229. Opciones del comando Edit-HyperVVirtualStandby

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Muestra los trabajos de un equipo protegido específico, indicado por dirección IP.
-all	Muestra todos los trabajos, incluyendo los realizados por el Core y todos los servidores protegidos.
-number	Opcional. Determine cuántas entradas se visualizarán. Los valores disponibles son: all (mostrar todos los trabajos); l[número] o [número] (recupera los ## trabajos más recientes ordenados por ejecución y hora); f[número] (muestra los ## primeros trabajos de recuperación ordenados por ejecución y hora). Se muestran los 20 trabajos más recientes de forma predeterminada.
-jobtype	Opcional. Especifica el filtro de tipo de trabajo. Los valores disponibles son: 'transfer' (transferencia de datos), 'repository' (mantenimiento de repositorio), 'replication' (replicaciones locales y remotas), 'backup' (restauración y copia de seguridad), 'bootcdbuilder' (crear CD de inicio), 'diagnostics' (cargar registros), 'exchange' (comprobación de archivos de Exchange Server), 'export' (exportación de punto de recuperación), 'pushinstall' (agentes de implementación), 'rollback' (restauración desde un punto de recuperación), 'rollup' (despliegues de puntos de recuperación), 'sqlattach' (comprobaciones de la conectabilidad de Agent) y 'mount' (montaje de repositorio). De forma predeterminada, todos los trabajos del tipo especificado se devuelven.
-time	Opcional. Filtra los resultados por fecha y hora en la que se inició el trabajo. Los tipos de entrada disponibles incluyen: #d o DD (donde # es un número para el periodo de tiempo de días antes de ahora hasta ahora) #h o #H (donde # es un número para el periodo de horas antes de ahora hasta ahora) "hora fecha1", "hora fecha 2" (para mostrar un intervalo personalizado de tiempo desde una fecha específica que aparece antes de la coma hasta una fecha específica que sigue a la coma).

Ejemplo:

Enumerar todos los trabajos activos en el Core local:

```
>Get-activejobs -all
```

Edit-ScheduledArchive

El comando `Edit-ScheduledArchive` permite utilizar PowerShell para realizar cambios en un archivo comprimido programado existente.

Uso

El uso del comando es el siguiente:

```
Edit-ScheduledArchive -core [host name] -user [login] -password [password] -all | -protectedserver [name | IP address | "[name1 | IP address1]" "[name2 | IP address2]"] -path [location] -cloudaccountname [name] -cloudcontainer [name] -recycleaction [type] -scheduletype [type] -dayofweek [name] -dayofmonth [number] -time [time] -initialpause -id [id]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `Edit-ScheduledArchive`:

Tabla 230. Opciones del comando `Edit-ScheduledArchive`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	El equipo protegido con los puntos de recuperación que desea archivar. Puede especificar varios nombres de equipo entre comillas dobles y separados por comas.
-all	Archivar puntos de recuperación para todos los equipos protegidos.
-path	La ruta de acceso en la que quiere guardar los datos archivados. Por ejemplo: - Equipo local: "d:\work\archive" - Ruta de red: "\\servername\sharename" - Carpeta de una cuenta de nube: "Folder Name"  NOTA: El número de símbolos no debe ser mayor de 100 para las ubicaciones locales y de red, ni mayor de 150 para una ubicación de la nube.
-cloudaccountname	Opcional. Solo se utiliza para la archivación de la nube. El nombre de la cuenta de nube donde quiere guardar el archivo.

Opción	Descripción
-cloudcontainer	Opcional. Solo se utiliza para la archivación de la nube. El nombre del contenedor de la nube de la cuenta de nube elegida, donde se guardará el archivo. Cuando se utiliza esta opción, debe especificar también el parámetro "-cloudaccountname".
-recycleaction	El tipo de acción de reciclaje. Se especifica mediante uno de los cuatro valores siguientes: "replacethiscore" - Sobrescribe los datos archivados que ya existan y que pertenecen a este Core, pero deja intactos los datos del resto de Cores. "erasescompletely" - Borra todos los datos archivados del directorio antes de escribir el nuevo archivo. "incremental"- Le permite añadir puntos de recuperación a un archivo existente. Compara los puntos de recuperación para evitar duplicar datos que ya hay en el archivo.
-scheduletype	Tipo de intervalo de programación. Especifica la opción con uno de los cuatro valores siguientes: "daily" - Para la archivación creada diariamente de forma automática. "weekly" - Para la archivación creada semanalmente de forma automática. Debe especificar el parámetro " - dayofweek". "monthly" - Para la archivación creada mensualmente de forma automática. Debe especificar el parámetro " - dayofmonth". Si un mes no tiene el día especificado, por ejemplo, "31", no habrá archivo comprimido ese mes. "lastdayofmonth" - Para la creación automática de un archivo comprimido el último día de cada mes.
-dayofweek	Se usa solo para la opción "weekly" del parámetro "-scheduletype". El día de la semana en el que desee crear automáticamente el archivo comprimido (por ejemplo, "lunes").
-dayofmonth	Se usa solo para la opción "monthly" del parámetro "-scheduletype". El día (número) del mes en el que desea crear el archivo comprimido automáticamente (por ejemplo, "15").
-time	La hora del día a la que desea crear una archivación.
-initialpause	Opcional. Especifique esta opción si desea una archivación con pausa inicial después de configurar el calendario de programación de archivación.
-id	El identificador del archivo comprimido programado que desee editar.

Ejemplo:

Editar un archivo programado en el Core local:

```
>Edit-ScheduledArchive -protectedserver protectedserver1 -path d:\work\archive -
cloudaccountname cloud1 -cloudcontainer cloudarchives -recycleaction incremental -scheduletype
daily -time 12:00 AM -initialpause -i
d archiveid
```

Edit-VBVirtualStandby

El comando `Edit-VBVirtualStandby` le permite usar PowerShell para realizar cambios en una exportación virtual existente a una máquina virtual VirtualBox (VM).

Uso

El uso del comando es el siguiente:

```
Edit-VBVirtualStandby [-TargetPath <String>] [-PathUserName <String>] [-PathPassword <String>]
[-LinuxHostName <String>] [-HostPort <UInt32>] [-AccountUserName <String>] [-AccountPassword
```

```
<String>] [-ProtectedServer <String>] [-Volumes <String[]>] [-VMName <String>] [-UseSourceRam]
[-Ram <String>] [-User <String>] [-Core <String>] [-Password <String>] [-Verbose] [-Debug] [-
ErrorAction <ActionPreference>] [-WarningAction <ActionPreference>] [-ErrorVariable <String>] [-
WarningVariable <String>] [-OutVariable <String>] [-OutBuffer <Int32>]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `Edit-VBVirtualStandby`:

Tabla 231. Opciones del comando `Edit-VBVirtualStandby`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Muestra los trabajos de un equipo protegido específico, indicado por dirección IP.
-all	Muestra todos los trabajos, incluyendo los realizados por el Core y todos los servidores protegidos.
-number	Opcional. Determine cuántas entradas se visualizarán. Los valores disponibles son: all (mostrar todos los trabajos); l[número] o [número] (recupera los ## trabajos más recientes ordenados por ejecución y hora); f[número] (muestra los ## primeros trabajos de recuperación ordenados por ejecución y hora). Se muestran los 20 trabajos más recientes de forma predeterminada.
-jobtype	Opcional. Especifica el filtro de tipo de trabajo. Los valores disponibles son: 'transfer' (transferencia de datos), 'repository' (mantenimiento de repositorio), 'replication' (replicaciones locales y remotas), 'backup' (restauración y copia de seguridad), 'bootcdbuilder' (crear CD de inicio), 'diagnostics' (cargar registros), 'exchange' (comprobación de archivos de Exchange Server), 'export' (exportación de punto de recuperación), 'pushinstall' (agentes de implementación), 'rollback' (restauración desde un punto de recuperación), 'rollup' (despliegues de puntos de recuperación), 'sqlattach' (comprobaciones de la conectabilidad de Agent) y 'mount' (montaje de repositorio). De forma predeterminada, todos los trabajos del tipo especificado se devuelven.
-time	Opcional. Filtra los resultados por fecha y hora en la que se inició el trabajo. Los tipos de entrada disponibles incluyen: #d o DD (donde # es un número para el periodo de tiempo de días antes de ahora hasta ahora) #h o #H (donde # es un número para el periodo de horas antes de ahora hasta ahora) "hora fecha1", "hora fecha 2" (para mostrar un intervalo personalizado de tiempo desde una fecha específica que aparece antes de la coma hasta una fecha específica que sigue a la coma).

Ejemplo:

Enumerar todos los trabajos activos en el Core local:

```
>Get-activejobs -all
```

Edit-VMVirtualStandby

El comando `Edit-VMVirtualStandby` permite usar PowerShell para realizar cambios en una exportación virtual existente a una máquina virtual (VM) de VMware Workstation.

Uso

El uso del comando es el siguiente:

```
Edit-VMVirtualStandby [-TargetPath <String>] [-PathUserName <String>] [-PathPassword <String>]
[-ProtectedServer <String>] [-Volumes <String[]>] [-VMName <String>] [-UseSourceRam] [-Ram <String>] [-User
<String>] [-Core <String>]
[-Password <String>] [-Verbose] [-Debug] [-ErrorAction <ActionPreference>] [-WarningAction
<ActionPreference>] [-ErrorVariable <String>] [-WarningVariable <String>] [-OutVariable <String>] [-OutBuffer
<Int32>]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `Edit-VMVirtualStandby`:

Tabla 232. Opciones del comando Edit-VMVirtualStandby

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Muestra los trabajos de un equipo protegido específico, indicado por dirección IP.
-all	Muestra todos los trabajos, incluyendo los realizados por el Core y todos los servidores protegidos.
-number	Opcional. Determine cuántas entradas se visualizarán. Los valores disponibles son:

Opción	Descripción
	all (mostrar todos los trabajos); l[número] o [número] (recupera los ## trabajos más recientes ordenados por ejecución y hora); f[número] (muestra los ## primeros trabajos de recuperación ordenados por ejecución y hora). Se muestran los 20 trabajos más recientes de forma predeterminada.
-jobtype	Opcional. Especifica el filtro de tipo de trabajo. Los valores disponibles son: 'transfer' (transferencia de datos), 'repository' (mantenimiento de repositorio), 'replication' (replicaciones locales y remotas), 'backup' (restauración y copia de seguridad), 'bootcdbuilder' (crear CD de inicio), 'diagnostics' (cargar registros), 'exchange' (comprobación de archivos de Exchange Server), 'export' (exportación de punto de recuperación), 'pushinstall' (agentes de implementación), 'rollback' (restauración desde un punto de recuperación), 'rollup' (despliegues de puntos de recuperación), 'sqlattach' (comprobaciones de la conectabilidad de Agent) y 'mount' (montaje de repositorio). De forma predeterminada, todos los trabajos del tipo especificado se devuelven.
-time	Opcional. Filtra los resultados por fecha y hora en la que se inició el trabajo. Los tipos de entrada disponibles incluyen: #d o DD (donde # es un número para el periodo de tiempo de días antes de ahora hasta ahora) #h o #H (donde # es un número para el periodo de horas antes de ahora hasta ahora) "hora fecha1", "hora fecha 2" (para mostrar un intervalo personalizado de tiempo desde una fecha específica que aparece antes de la coma hasta una fecha específica que sigue a la coma).

Ejemplo:

Enumerar todos los trabajos activos en el Core local:

```
>Get-activejobs -all
```

Get-ActiveJobs

El comando `Get-ActiveJobs` devuelve todos los trabajos activos desde el Core. El parámetro `-jobtype` se puede utilizar para observar trabajos específicos.

Uso

El uso del comando es el siguiente:

```
Get-ActiveJobs -core [host name] -user [user name] -password [password] -all |
-protectedserver [server name or IP address] -number [all | f[number] | l[number] | number] -
jobtype [type] -time [time]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Get-ActiveJobs`:

Tabla 233. Opciones del comando Get-ActiveJobs

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Muestra los trabajos de un equipo protegido específico, indicado por dirección IP.
-all	Muestra todos los trabajos, incluyendo los realizados por el Core y todos los servidores protegidos.
-number	Opcional. Determine cuántas entradas se visualizarán. Los valores disponibles son: all (mostrar todos los trabajos); l[número] o [número] (recupera los ## trabajos más recientes ordenados por ejecución y hora); f[número] (muestra los ## primeros trabajos de recuperación ordenados por ejecución y hora). Se muestran los 20 trabajos más recientes de forma predeterminada.
-jobtype	Opcional. Especifica el filtro de tipo de trabajo. Los valores disponibles son: 'transfer' (transferencia de datos), 'repository' (mantenimiento de repositorio), 'replication' (replicaciones locales y remotas), 'backup' (restauración y copia de seguridad), 'bootcdbuilder' (crear CD de inicio), 'diagnostics' (cargar registros), 'exchange' (comprobación de archivos de Exchange Server), 'export' (exportación de punto de recuperación), 'pushinstall' (agentes de implementación), 'rollback' (restauración desde un punto de recuperación), 'rollup' (despliegues de puntos de recuperación), 'sqlattach' (comprobaciones de la conectabilidad de Agent) y 'mount' (montaje de repositorio). De forma predeterminada, todos los trabajos del tipo especificado se devuelven.
-time	Opcional. Filtra los resultados por fecha y hora en la que se inició el trabajo. Los tipos de entrada disponibles incluyen: #d o DD (donde # es un número para el periodo de tiempo de días antes de ahora hasta ahora) #h o #H (donde # es un número para el periodo de horas antes de ahora hasta ahora) "hora fecha1", "hora fecha 2" (para mostrar un intervalo personalizado de tiempo desde una fecha específica que aparece antes de la coma hasta una fecha específica que sigue a la coma).

Ejemplo:

Enumerar todos los trabajos activos en el Core local:

```
>Get-activejobs -all
```


Get-Clusters

El comando `Get-Clusters` devuelve información sobre los clústeres de servidores protegidos en el Core.

Uso

El uso del comando es el siguiente:

```
Get-Clusters -core [host name] -user [user name] -password [password]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Get-Clusters`:

Tabla 234. Opciones del comando `Get-Clusters`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.

Ejemplo:

Enumerar los clústeres de servidores protegidos en el Core local:

```
>Get-Clusters
```

Get-CompletedJobs

El comando `Get-CompletedJobs` devuelve una lista de los trabajos completados en el Core. El parámetro `-jobtype` se puede utilizar para observar trabajos específicos.

Uso

El uso del comando es el siguiente:

```
Get-CompletedJobs -core [host name] -user [user name] -password [password] -all |  
-protectedserver [server name or IP address] -number [all | f[number] | l[number] | number] -  
jobtype [type] -time [time]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Get-CompletedJobs`:

Tabla 235. Opciones del comando `Get-CompletedJobs`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Muestra los trabajos de un equipo protegido específico, indicado por dirección IP.
-all	Muestra todos los trabajos, incluyendo los realizados por el Core y todos los servidores protegidos.
-number	Opcional. Determine cuántas entradas se visualizarán. Los valores disponibles son: all (mostrar todos los trabajos); l[número] o [número] (recupera los ## trabajos más recientes ordenados por ejecución y hora); f[número] (muestra los ## primeros trabajos de recuperación ordenados por ejecución y hora). Se muestran los 20 trabajos más recientes de forma predeterminada.
-jobtype	Opcional. Especifica el filtro de tipo de trabajo. Los valores disponibles son: 'transfer' (transferencia de datos), 'repository' (mantenimiento de repositorio), 'replication' (replicaciones locales y remotas), 'backup' (restauración y copia de seguridad), 'bootcdbuilder' (crear CD de inicio), 'diagnostics' (cargar registros), 'exchange' (comprobación de archivos de Exchange Server), 'export' (exportación de punto de recuperación), 'pushinstall' (agentes de implementación), 'rollback' (restauración desde un punto de recuperación), 'rollup' (despliegues de puntos de recuperación), 'sqlattach' (comprobaciones de la conectabilidad de Agent) y 'mount' (montaje de repositorio). De forma predeterminada, todos los trabajos del tipo especificado se devuelven.
-time	Opcional. Filtra los resultados por fecha y hora en la que se inició el trabajo. Los tipos de entrada disponibles incluyen: #d o DD (donde # es un número para el periodo de tiempo de días antes de ahora hasta ahora) #h o #H (donde # es un número para el periodo de horas antes de ahora hasta ahora) "hora fecha1", "hora fecha2" (para mostrar un intervalo personalizado de tiempo desde una fecha específica que aparece antes de la coma hasta una fecha específica que sigue a la coma).

Ejemplo:

Enumerar todos los trabajos activos en el Core local:

```
>Get-CompletedJobs -all
```

Enumera todos los trabajos de repositorio de creación completados en el Core local:

```
>Get-CompletedJobs -jobtype repository
```

Get-ExchangeMailStores

El comando `Get-ExchangeMailStores` devuelve información sobre los almacenes de correo en servidores Exchange Server protegidos por el Core.

Uso

El uso del comando es el siguiente:

```
Get-ExchangeMailStores -core [host name] -user [user name] -password [password]  
-protectedserver [server name or IP address]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Get-ExchangeMailStores`:

Tabla 236. Opciones del comando Get-ExchangeMailStores

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Muestra los trabajos de un equipo protegido específico, indicado por dirección IP.

Ejemplo:

Enumerar los almacenes de correo de Exchange para el servidor Exchange para el Core local:

```
>Get-ExchangeMailStores -protectedserver 10.10.10.10
```

Get-Failed

El comando `Get-Failed` devuelve información sobre los puntos de recuperación con fallos en el Core local.

Uso

El uso del comando es el siguiente:

```
Get-Failed -core [host name] -user [user name] -password [password] -all |  
-protectedserver [server name or IP address] -number [all | f[number] | l[number] | number]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Get-Failed` :

Tabla 237. Opciones de comando `Get-Failed`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Muestra los trabajos de un equipo protegido específico, indicado por dirección IP.
-number	Opcional. Determine cuántas entradas se visualizarán. Los valores disponibles son: all (mostrar todos los trabajos); l[número] o [número] (recupera los ## trabajos más recientes ordenados por ejecución y hora); f[número] (muestra los ## primeros trabajos de recuperación ordenados por ejecución y hora). Se muestran los 20 trabajos más recientes de forma predeterminada.

Ejemplo:

Enumerar todos los puntos de recuperación con fallos:

```
>Get-failed -protectedserver 10.10.10.10
```

Get-FailedJobs

El comando `Get-FailedJobs` devuelve todos los trabajos con fallos desde el Core local.

Uso

El uso del comando es el siguiente:

```
Get-FailedJobs -core [host name] -user [user name] -password [password] -all |  
-protectedserver [server name or IP address] -number [all | f[number] | l[number] | number] -  
jobtype [type] -time [time]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Get-FailedJobs`:

Tabla 238. Opciones del comando `Get-FailedJobs`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Muestra los trabajos de un equipo protegido específico, indicado por dirección IP.
-all	Muestra todos los trabajos, incluyendo los realizados por el Core y todos los servidores protegidos.
-number	Opcional. Determine cuántas entradas se visualizarán. Los valores disponibles son: all (mostrar todos los trabajos); l[número] o [número] (recupera los ## trabajos más recientes ordenados por ejecución y hora); f[número] (muestra los ## primeros trabajos de recuperación ordenados por ejecución y hora). Se muestran los 20 trabajos más recientes de forma predeterminada.
-jobtype	Opcional. Especifica el filtro de tipo de trabajo. Los valores disponibles son: 'transfer' (transferencia de datos), 'repository' (mantenimiento de repositorio), 'replication' (replicaciones locales y remotas), 'backup' (restauración y copia de seguridad), 'bootcdbuilder' (crear CD de inicio), 'diagnostics' (cargar registros), 'exchange' (comprobación de archivos de Exchange Server), 'export' (exportación de punto de recuperación), 'pushinstall' (agentes de implementación), 'rollback' (restauración desde un punto de recuperación), 'rollup' (despliegues de puntos de recuperación), 'sqlattach' (comprobaciones de la conectabilidad de Agent) y 'mount' (montaje de repositorio). De forma predeterminada, todos los trabajos del tipo especificado se devuelven.
-time	Opcional. Filtra los resultados por fecha y hora en la que se inició el trabajo. Los tipos de entrada disponibles incluyen: #d o DD (donde # es un número para el periodo de tiempo de días antes de ahora hasta ahora) #h o #H (donde # es un número para el periodo de horas antes de ahora hasta ahora)

Opción	Descripción
	"hora fecha1", "hora fecha 2" (para mostrar un intervalo personalizado de tiempo desde una fecha específica que aparece antes de la coma hasta una fecha específica que sigue a la coma).

Ejemplo:

Enumerar todos los trabajos con fallos en el Core local:

```
>Get-FailedJobs -all
```

Enumera todos los trabajos de copia de seguridad de creación fallidos en el Core local:

```
>Get-FailedJobs -type backup
```

Get-Mounts

El comando `Get-Mounts` devuelve todos los puntos de recuperación montados en el Core local.

Uso

El uso del comando es el siguiente:

```
Get-Mounts -core [host name] -user [user name] -password [password] -protectedserver [server name or IP address]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Get-Mounts`:

Tabla 239. Opciones del comando Get-Mounts

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Muestra los trabajos de un equipo protegido específico, indicado por dirección IP.

Ejemplo:

Mostrar todos los puntos de recuperación montados:

```
>Get-Mounts -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22
```

Get-Passed

El comando `Get-Passed` devuelve información sobre puntos de recuperación que han superado las comprobaciones de verificación en el Core.

Uso

El uso del comando es el siguiente:

```
Get-Passed -core [host name] -user [user name] -password [password] -protectedserver [server name or IP address] -number [all | f[number] | l[number] | number]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Get-Passed`:

Tabla 240. Opciones del comando `Get-Passed`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.

Ejemplo:

Enumerar todos los puntos de recuperación del Core local que superaron las comprobaciones de verificación:

```
>Get-Passed -protectedserver 10.10.10.10
```

Get-ProtectedServers

El comando `Get-ProtectedServers` devuelve información sobre los equipos protegidos en el Core local.

Uso

El uso del comando es el siguiente:

```
Get-ProtectedServers -core [host name] -user [user name] -password [password]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Get-ProtectedServers` :

Tabla 241. Opciones del comando Get-ProtectedServers

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.

Ejemplo:

Enumerar todos los equipos protegidos actualmente en el Core local:

```
>Get-ProtectedServers
```

Get-ProtectionGroups

El comando `Get-ProtectionGroups` devuelve información sobre los grupos de protección del Core local.

Uso

El uso del comando es el siguiente:

```
Get-ProtectionGroups -core [host name] -user [user name] -password [password] -all |  
-protectedserver [server name or IP address]
```


Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Get-ProtectionGroups`:

Tabla 242. Opciones del comando `Get-ProtectionGroups`

Opción	Descripción
<code>-?</code>	Muestra el mensaje de ayuda.
<code>-core</code>	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
<code>-user</code>	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
<code>-password</code>	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
<code>-protectedserver</code>	Muestra los trabajos de un equipo protegido específico, indicado por dirección IP.

Ejemplo:

Enumerar todos los grupos de protección en el Core local:

```
>Get-ProtectionGroups -protectedserver 10.10.10.10
```

Get-QueuedJobs

El comando `Get-QueuedJobs` devuelve todos los trabajos a la espera de ser iniciados desde el Core.

Uso

El uso del comando es el siguiente:

```
Get-QueuedJobs -core [host name] -user [login] -password [password] -all | -protectedserver  
[name | IP address] -number [all | f[number] | l[number] | number] -jobtype [type] -time [time]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `Get-ActiveJobs`:

Tabla 243. Opciones del comando Get-ActiveJobs

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Muestra los trabajos de un equipo protegido específico, indicado por dirección IP.
-all	Muestra todos los trabajos, incluyendo los realizados por el Core y todos los servidores protegidos.
-number	Opcional. Determine cuántas entradas se visualizarán. Los valores disponibles son: all (mostrar todos los trabajos); l[número] o [número] (recupera los ## trabajos más recientes ordenados por ejecución y hora); f[número] (muestra los ## primeros trabajos de recuperación ordenados por ejecución y hora). Se muestran los 20 trabajos más recientes de forma predeterminada.
-jobtype	Opcional. Especifica el filtro de tipo de trabajo. Los valores disponibles son: 'transfer' (transferencia de datos), 'repository' (mantenimiento de repositorio), 'replication' (replicaciones locales y remotas), 'backup' (restauración y copia de seguridad), 'bootcdbuilder' (crear CD de inicio), 'diagnostics' (cargar registros), 'exchange' (comprobación de archivos de Exchange Server), 'export' (exportación de punto de recuperación), 'pushinstall' (agentes de implementación), 'rollback' (restauración desde un punto de recuperación), 'rollup' (despliegues de puntos de recuperación), 'sqlattach' (comprobaciones de la conectabilidad de Agent) y 'mount' (montaje de repositorio). De forma predeterminada, todos los trabajos del tipo especificado se devuelven.
-time	Opcional. Filtra los resultados por fecha y hora en la que se inició el trabajo. Los tipos de entrada disponibles incluyen: #d o DD (donde # es un número para el periodo de tiempo de días antes de ahora hasta ahora) #h o #H (donde # es un número para el periodo de horas antes de ahora hasta ahora) "hora fecha1", "hora fecha 2" (para mostrar un intervalo personalizado de tiempo desde una fecha específica que aparece antes de la coma hasta una fecha específica que sigue a la coma).

Ejemplo:

Enumerar todos los trabajos en cola en el Core local:

```
>Get-QueuedJobs -all
```

Get-RecoveryPoints

El comando `Get-RecoveryPoints` devuelve información sobre los puntos de recuperación de equipos protegidos en el Core local.

Uso

El uso del comando es el siguiente:

```
Get-RecoveryPoints -core [host name] -user [user name] -password [password]
-protectedserver [server name or IP address] -number [all | f[number] | l[number] | number]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Get-RecoveryPoints`:

Tabla 244. Opciones del comando `Get-RecoveryPoints`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Muestra los trabajos de un equipo protegido específico, indicado por dirección IP.
-number	Opcional. Determine cuántas entradas se visualizarán. Los valores disponibles son: all (mostrar todos los trabajos); l[número] o [número] (recupera los ## trabajos más recientes ordenados por ejecución y hora); f[número] (muestra los ## primeros trabajos de recuperación ordenados por ejecución y hora). Se muestran los 20 trabajos más recientes de forma predeterminada.

Ejemplo:

Enumerar los puntos de recuperación de los equipos protegidos en el Core local:

```
>Get-RecoveryPoints -protectedserver 10.10.10.10
```

Get-ReplicatedServers

El comando `Get-ReplicatedServers` devuelve información sobre los equipos replicados en el Core.

Uso

El uso del comando es el siguiente:

```
Get-ReplicatedServers -core [host name] -user [user name] -password [password]
```

Dell le recomienda que tenga en cuenta la seguridad cuando utilice comandos para devolver valores. Por ejemplo, este comando devuelve la contraseña de administrador de cada servidor replicado. Si se ha utilizado en un entorno MSP del Core de destino, puede exponer la contraseña de inicio de sesión del usuario administrador. Para los entornos con datos de repositorio cifrados, esto no supone un problema de seguridad importante.

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Get-ReplicatedServers`:

Tabla 245. Opciones del comando `Get-ReplicatedServers`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.

Ejemplo:

Enumerar todos los servidores replicados en el Core local:

```
>Get-ReplicatedServers
```

Get-Repositories

El comando `Get-Repositories` devuelve información sobre los repositorios del Core.

Uso

El uso del comando es el siguiente:

```
Get-Repositories -core [host name] -user [user name] -password [password]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Get-Repositories`:

Tabla 246. Opciones del comando `Get-Repositories`

Opción	Descripción
<code>-?</code>	Muestra el mensaje de ayuda.
<code>-core</code>	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
<code>-user</code>	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
<code>-password</code>	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.

Ejemplo:

Enumerar los repositorios en el Core local:

```
>Get-Repositories
```

Get-ScheduledArchives

El comando `Get-ScheduledArchives` permite usar PowerShell para ver la información acerca de las archivaciones programadas de Rapid Recovery relacionados con este Core.

Uso

El uso del comando es el siguiente:

```
Get-ScheduledArchives -core [host name] -user [login] -password [password]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `Get-ScheduledArchives`:

Tabla 247. Opciones del comando Get-ScheduledArchives

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.

Ejemplo:

Obtener información acerca de las archivaciones programadas en este Core:

```
>Get-ScheduledArchives -core 10.10.10.10 -user administrator -password password
```

Get-SqlDatabases

El comando `Get-SqlDatabases` devuelve una lista de las bases de datos SQL desde el equipo protegido especificado.

Uso

El uso del comando es el siguiente:

```
Get-SqlDatabases -core [host name] -user [user name] -password [password]  
-protectedserver [server name or IP address]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Get-SqlDatabases`:

Tabla 248. Opciones del comando Get-SqlDatabases

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.

Opción	Descripción
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Muestra los trabajos de un equipo protegido específico, indicado por dirección IP.

Ejemplo:

Enumerar todos los trabajos de bases de datos SQL en el Core local:

```
>Get-SqlDatabases -protectedserver 10.10.10.10
```

Get-UnprotectedVolumes

El comando `Get-UnprotectedVolumes` devuelve información sobre volúmenes que están disponibles para la protección pero que no están protegidos en estos momentos en el Core.

Uso

El uso del comando es el siguiente:

```
Get-UnprotectedVolumes
-core [host name] -user [user name] -password [password] -protectedserver [server name or IP address]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Get-UnprotectedVolumes`:

Tabla 249. Opciones del comando `Get-UnprotectedVolumes`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Muestra los trabajos de un equipo protegido específico, indicado por dirección IP.

Ejemplo:

Enumerar todos los volúmenes disponibles para la protección (pero que no están protegidos) en el equipo del Agent especificado:

```
>Get-UnprotectedVolumes -protectedserver 10.10.10.10
```

Get-VirtualizedServers

El comando `Get-VirtualizedServers` devuelve información sobre servidores virtualizados.

Uso

El uso del comando es el siguiente:

```
Get-VirtualizedServers -core [host name] -user [user name] -password [password]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Get-VirtualizedServers` :

Tabla 250. Opciones del comando `Get-VirtualizedServers`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.

Ejemplo:

Enumerar todos los servidores virtualizados en el Core local:

```
>Get-VirtualizedServers
```

Get-Volumes

El comando `Get-Volumes` devuelve información sobre los volúmenes en un equipo especificado que está protegido por el Core.

Uso

El uso del comando es el siguiente:

```
Get-Volumes -core [host name] -user [user name] -password [password]  
-protectedserver [server name or IP address]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Get-Volumes`:

Tabla 251. Opciones del comando `Get-Volumes`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Muestra los trabajos de un equipo protegido específico, indicado por dirección IP.

Ejemplo:

Enumerar todos los volúmenes del equipo especificado:

```
>Get-Volumes -protectedserver 10.10.10.10
```

New-Base

El comando `New-Base` fuerza una imagen base dando como resultado una transferencia de datos para el equipo protegido actualmente. Cuando se fuerza una imagen base, la transferencia empezará de inmediato o se añadirá a la cola. Solo se transferirán los datos que hayan cambiado con respecto a un punto de recuperación previo. Si no hay punto de recuperación previo, se transferirán todos los datos de los volúmenes protegidos.

Uso

El uso del comando es el siguiente:

```
New-Base [[-all] | -protectedserver [machine name]] -core [host name] -user [user name] -  
password [password]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `New-Base`:

Tabla 252. Opciones del comando `New-Base`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-all	Imagen base para todos los Agents.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Forzado para el nombre de del equipo protegido actual.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.

Ejemplo:

Forzar una imagen de base para todos los equipos protegidos:

```
>New-Base -all
```

New-CloudAccount

El comando `New-CloudAccount` permite agregar una nueva cuenta de nube al Core de Rapid Recovery.

Uso

El uso del comando es el siguiente:

```
New-CloudAccount -core [host name] -user [login] -password [password] -displayname [display  
name] -type [cloud acco  
unt type] -username [user name] - key [secret key] -region [region] - tenantid [tenant Id] -  
authurl [authorization  
url]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `New-CloudAccount`:

Tabla 253. Opciones del comando New-CloudAccount

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-displayname	El nombre de la cuenta de nube que se visualiza.
-type	El tipo de cuenta de nube que desea agregar. Los valores compatibles son: - amazon - openstack - rackspace - windowsazure "windows azure" - azure
-username	El nombre de usuario para la cuenta de nube que desee agregar. Se utiliza en el proceso de autenticación. Esta propiedad se resuelve como "Clave de acceso" para Amazon™ Cloud, "Nombre de usuario" para Rackspace y OpenStack, y "Nombre de cuenta de almacenamiento" para la cuentas de nube de Windows Azure.
-key	La clave para la cuenta de nube que desee agregar. Se utiliza en el proceso de autenticación. Esta propiedad se resuelve como "Clave secreta" para Amazon™ Cloud, "Clave de Api" para Rackspace y OpenStack, y "Clave de acceso" para la cuentas de nube de Windows Azure.
-region	La región de la cuenta de nube que desee agregar. Esta propiedad se requiere únicamente para la creación de cuentas de nube de RackSpace y OpenStack.
-tenantid	El identificador que se utiliza en el proceso de autenticación de una cuenta de nube OpenStack. Esta opción se requiere únicamente para la creación de cuentas de nube de OpenStack.
-authurl	La URL que se utiliza en el proceso de autenticación de una cuenta de nube OpenStack. Esta opción se requiere únicamente para la creación de cuentas de nube de OpenStack.

Ejemplo:

Cree una nueva cuenta de nube Amazon™ S3 denominada "Cuenta de Amazon S3" con la clave de acceso "akey" y la clave secreta "skey".

```
>New-CloudAccount -displayname "Amazon S3 Account" -type Amazon -username akey -key skey
```

New-EncryptionKey

El comando `New-EncryptionKey` le permite crear una nueva clave de cifrado para proteger sus datos de la copia de seguridad de Rapid Recovery.

Uso

El uso del comando es el siguiente:

```
New-EncryptionKey -core [host name] -user [login] -password [password] -name [encryption key name] -passphrase [passphrase] -comment [comment]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `New-EncryptionKey`:

Tabla 254. Opciones del comando New-EncryptionKey

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-name	El nombre de la clave de cifrado que desea crear.
-passphrase	La frase de contraseña para la clave de cifrado que desea crear.
-comment	Opcional. La descripción de la clave de cifrado.

Ejemplo:

Crear una clave de cifrado en la controladora seleccionada:

```
>New-EncryptionKey -name EncryptionKey1 -passphrase 123456
```

New-EsxiVirtualStandby

El comando de PowerShell `New-EsxiVirtualStandby` permite crear un nuevo equipo en espera virtual ESXi con Rapid Recovery.

Uso

El uso del comando es el siguiente:

```
New-EsxiVirtualStandby -core [host name] -user [login] -password [password] -protectedserver  
[name | IP address] -volumes [volumes names] -vmname [virtual machine name] -hostname [virtual  
host name] -hostport [virtual host port number] -hostusername [virtual host login] -  
hostpassword [virtual host password] [-ram [total megabytes] | -usesourceram] -diskprovisioning  
[thin | thick] -diskmapping [automatic | manual | withvm] -initialexport
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `New-EsxiVirtualStandby`:

Tabla 255. Opciones del comando `New-EsxiVirtualStandby`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Muestra los trabajos de un equipo protegido específico, indicado por dirección IP.
-volumes	Opcional. Enumere los nombres de los volúmenes que desee exportar. Si no se especifica, se exportarán todos los volúmenes de los puntos de recuperación. Los valores deben estar entre comillas dobles y separados por espacios; por ejemplo, "c:", "d:".  NOTA: No utilice barras finales en nombres de volúmenes.
-vmname	Nombre de Microsoft Windows de la máquina virtual.
-hostname	Nombre del host del servidor virtual.
-hostport	El número de puerto que se debe utilizar para la comunicación con el servidor virtual.
-hostusername	Nombre de usuario para iniciar sesión en el host del servidor virtual.
-hostpassword	Contraseña para iniciar sesión en el host del servidor virtual.
-ram	Asignar una cantidad específica de RAM en el servidor virtual.
-usesourceram	Opcional. Asigna la misma cantidad de RAM en el servidor virtual que la que tiene el equipo protegido de origen.

Opción	Descripción
-diskprovisioning	Opcional. Cantidad de espacio en disco que se debe asignar en la máquina virtual. Los valores disponibles son: - Grueso: especifique 'grueso' para hacer el disco virtual tan grande como la unidad original en el servidor protegido. - Compacto: especifique 'compacto' para asignar la cantidad de espacio en disco real ocupada en la unidad original más algunos megabytes adicionales. El aprovisionamiento de discos predeterminado es 'compacto'.
-diskmappingjg	Opcional. Determina cómo asignar los discos del punto de recuperación a la máquina virtual. Los valores disponibles son: 'Automático' 'manual' 'withvm' La configuración predeterminada es 'Automático'.
-initialexport	Opcional. Especifique esta opción si tiene que iniciar la exportación de una máquina virtual a petición inicial después de configurar la espera virtual.

Ejemplo:

Cree un nuevo servidor en espera virtual ESXi:

```
>New-EsxiVirtualStandby -protectedserver 10.10.10.4 -vmname ExportedMachine -hostname 10.10.10.127 -hostport 443 -hostusername root -hostpassword pass123 -usesourceram -diskprovisioning thin -diskmapping auto
```

New-HyperVVirtualStandby

El comando de PowerShell New-HyperVVirtualStandby permite crear una nueva máquina virtual Hyper-V (VM) con Rapid Recovery.

Uso

El uso del comando es el siguiente:

```
New-HyperVVirtualStandby -core [host name] -user [login] -password [password] -protectedserver [name | IP address]
    -volumes [volumes names] -vmname [virtual machine name] [-gen2] -useVhdx [-uselocalmachine]
| -hostname [virtual host name] -hostport [virtual host port number] -hostusername [virtual host login] -
hostpassword [virtual host password] -vmlocation [location] [-ram [total megabytes] | -usesourceram] -initialexport
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comandoNew-HyperVVirtualStandby:

Tabla 256. Opciones del comando New-HyperVVirtualStandby

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Muestra los trabajos de un equipo protegido específico, indicado por dirección IP.
-volumes	Opcional. Enumere los nombres de los volúmenes que desee exportar. Si no se especifica, se exportarán todos los volúmenes de los puntos de recuperación. Los valores deben estar entre comillas dobles y separados por espacios; por ejemplo, "c:", "d:". <i>i</i> NOTA: No utilice barras finales en nombres de volúmenes.
-vmname	Nombre de Microsoft Windows de la máquina virtual.
-gen2	Opcional. Especifique utilizar la segunda generación de VM. Si no se especifica, se utiliza la generación 1. Rapid Recovery admite la generación 2 de Windows Server 2012 R2 a través de Windows 8.1.
-usevhdx	Opcional. Si se especifica esta opción, Rapid Recovery utiliza el formato de disco VHDX para crear la máquina virtual. Si no lo hace, utiliza el formato del disco VHD. La generación 2 solo utiliza el formato VHDX.
-uselocalmachine	Opcional. Conectar al servidor Hyper-V local. Cuando se especifica este valor, Rapid Recovery ignora las siguientes opciones: • nombre de host • hostport • hostusername • hostpassword
-hostname	Nombre del host del servidor virtual.
-hostport	El número de puerto que se debe utilizar para la comunicación con el servidor virtual.
-hostusername	Nombre de usuario para iniciar sesión en el host del servidor virtual.
-hostpassword	Contraseña para iniciar sesión en el host del servidor virtual.
-vmlocation	Ruta de acceso local o de red a la carpeta donde quiere guardar los archivos de la máquina virtual.
-ram	Asignar una cantidad específica de RAM en el servidor virtual.
-usesourceram	Opcional. Asigna la misma cantidad de RAM en el servidor virtual que la que tiene el equipo protegido de origen.
-initialexport	Opcional. Especifique esta opción si tiene que iniciar la exportación de una máquina virtual a petición inicial después de configurar la espera virtual.

Ejemplo:

Cree un nuevo equipo en espera virtual Hyper-V:

```
>New-HyperVVirtualStandby -core [host name] -user [login] -password [password] -protectedserver [name | IP address]
    -volumes [volumes names] -vmname [virtual machine name] [-gen2] -useVhdx [-uselocalmachine]
| -hostname [virtual host name] -hostport [virtual host port number] -hostusername [virtual host login] -
hostpassword [virtual host password] -vmlocation [location] [-ram [total megabytes] | -usesourceram] -initialexport
```

New-Mount

El comando `New-Mount` monta una instantánea de una o varias unidades.

Uso

El uso del comando es el siguiente:

```
New-Mount -core [host name] -user [user name] -password [password] -protectedserver [machine name] -mounttype [read | write | readonlywithpreviouswrites] -drives [drive names] -path [location] -time [MM/DD/YYYY hh:mm:ss tt | passed | latest] -rpn [number]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `New-Mount`:

Tabla 257. Opciones del comando New-Mount

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-protectedserver	Dirección IP del servidor protegido o nombre del equipo (depende de cómo se ha protegido el equipo concreto).
-time	Opcional. Marca de tiempo del punto de recuperación que se debe montar. Deberá indicarse con el formato especificado en el SO en el PC actual. El administrador puede obtener el punto de recuperación más reciente especificando latest o el punto de recuperación comprobado por última vez mediante el valor del parámetro pasado. De manera predeterminada, la opción latest es la elegida.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.

Opción	Descripción
-path	Ruta de acceso del equipo Core en la que se montarán los puntos de recuperación.
-mounttype	Opcional. Especifica un modo de montaje. Las opciones disponibles son 'read', 'readOnlyWithPreviousWrites' (solo lectura con escrituras previas), 'write' (modificable). El modo predeterminado es read-only.
-volumes	Opcional. Lista de nombres de volúmenes que se deben montar separados por espacios. Si el nombre del volumen contiene espacios o caracteres especiales, deben especificarse usando comillas dobles. Si no se especifican, se montarán todos los volúmenes.
-drivers	Opcional. Lista de nombres de volúmenes que se deben montar separados por comas. Si no se especifican, se montarán todos los volúmenes. ❗ NOTA: Esta opción está obsoleta, utilice ' -volumes ' en su lugar.
-rpn	Opcional. Número de punto de recuperación para el montaje. Puede obtenerlo usando el comando get-mounts. Especifique varios números para el parámetro rpn para montar diferentes puntos con un único comando. ❗ NOTA: Si establece una matriz de puntos para montaje, cada punto se ubicará en un directorio secundario independiente. El nombre describe la hora en la que se creó el punto de recuperación. Cuando solicite desmontarlos, todos los directorios secundarios se quitarán. Debe quitar el directorio principal manualmente.

Ejemplo:

```
>New-Mount -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22 -path C:\MountedRecoveryPoint -mounttype read -volumes c "d, ko"
```

Montar una matriz de puntos de recuperación:

```
>New-Mount -rpn 10 52 41 -protectedserver localhost -path "D:/Folder for mount"
```

Montar un punto de recuperación con una determinada hora:

```
>New-Mount -protectedserver 10.10.5.56 -path "D:/Folder for mount" -time "8/24/2012 11:46 AM"
```

Resume-Replication

El comando `New-Replication` permite configurar y forzar la replicación de uno o más servidores protegidos.

Uso

El uso del comando es el siguiente:

```
New-Replication -core [host name] -user [login] -password [password] -targetserver [host name] -protectedserver [name | IP address]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `New-Replication`:

Tabla 258. Opciones del comando New-Replication

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-replicationname	Nombre de la configuración de replicación en el Core de destino.
-targetserver	El nombre de host, el nombre de usuario y la contraseña del Core de destino.
-protectedserver	El nombre del equipo protegido y el repositorio en el Core de destino para configurar la replicación.

Ejemplo:

Crear nueva replicación para el equipo protegido con IP 10.10.10.4:

```
>New-Replication -targetserver 10.10.10.128 -protectedserver 10.10.10.4
```

New-Repository

El comando `New-Repository` crea un nuevo repositorio DVM en el Core de Rapid Recovery. El tamaño especificado debe estar comprendido entre 250 MB y 16 TB.

Uso

El uso del comando es el siguiente:

```
New-Repository | -name [name] -size [size] -datapath [location] -metadatapath [location]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `New-Repository` :

Tabla 259. Opciones del comando New-Repository

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-name	Nombre de repositorio.
-size	Tamaño de extensión del repositorio. Las unidades disponibles son b, Kb, MB, GB, TB y PB.
-datapath	Solo para la ubicación local. Determina la ruta de acceso a los datos de la extensión del repositorio.
-metadatapath	Solo para la ubicación local. Determina la ruta de acceso a los metadatos de la extensión del repositorio.
-uncpath	Solo para la ubicación compartida. Determina las rutas de acceso a los datos y metadatos de la extensión del repositorio.
-shareusername	Solo para la ubicación compartida. Determina el inicio de sesión para la ubicación compartida.
-sharepassword	Solo para la ubicación compartida. Determina la contraseña para la ubicación compartida.
-comment	Opcional. Descripción del repositorio.
-concurrent Operations	Opcional. Número máximo de operaciones que pueden estar pendientes simultáneamente. Valor predeterminado: 64.

Ejemplo:

Crear un nuevo repositorio DVM del tamaño mínimo en la unidad local E:

```
>New-Repository -name Repository2 -size 250Mb -datapath e:\Repository\Data -metadatapath e:\Repository\Metadata
```

New-ScheduledArchive

El comando `New-ScheduledArchive` permite utilizar PowerShell para realizar cambios en un archivo comprimido programado existente.

Uso

El uso del comando es el siguiente:

```
New-ScheduledArchive -core [host name] -user [login] -password [password] -all | -protectedserver [name | IP address] -path [location] -archiveusername [name] -archivepassword [password] -cloudaccountname [name] -cloudcontainer [name] -recycleaction [type] -schdeuletype [type] -dayofweek [name] -dayofmonth [number] -time [time]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `New-ScheduledArchive`:

Tabla 260. Opciones del comando `New-ScheduledArchive`

Opción	Descripción
<code>-?</code>	Muestra el mensaje de ayuda.
<code>-core</code>	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
<code>-user</code>	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
<code>-password</code>	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
<code>-protectedserver</code>	El equipo protegido con los puntos de recuperación que desea archivar. Puede especificar varios nombres de equipo entre comillas dobles y separados por comas.
<code>-all</code>	Archivar puntos de recuperación para todos los equipos protegidos.
<code>-path</code>	La ruta de acceso en la que quiere guardar los datos archivados. Por ejemplo: • Equipo local: "d:\work\archive" • Ruta de red: "\\servername\sharename" • Carpeta de una cuenta de nube: "Folder Name" NOTA: El número de símbolos no debe ser mayor de 100 para las ubicaciones locales y de red, ni mayor de 150 para una ubicación de la nube.
<code>-archiveusername</code>	Opcional. El nombre de usuario para iniciar sesión en el equipo remoto. Solo es obligatoria para la ruta de red.
<code>-archivepassword</code>	Opcional. La contraseña para iniciar sesión en el equipo remoto. Solo es obligatoria para la ruta de red.
<code>-cloudaccountname</code>	Opcional. Solo se utiliza para la archivación de la nube. El nombre de la cuenta de nube donde quiere guardar el archivo.
<code>-cloudcontainer</code>	Opcional. Solo se utiliza para la archivación de la nube. El nombre del contenedor de la nube de la cuenta de nube elegida, donde se guardará el archivo. Cuando se utiliza esta opción, debe especificar también el parámetro " <code>-cloudaccountname</code> ".
<code>-recycleaction</code>	El tipo de acción de reciclaje. Se especifica mediante uno de los cuatro valores siguientes: • "replacethiscore" - Sobrescribe los datos archivados que ya existan y que pertenecen a este Core, pero deja intactos los datos del resto de Cores. • "erasescompletely" - Borra todos los datos archivados del directorio antes de escribir el nuevo archivo. • "incremental"- Le permite añadir puntos de recuperación a un archivo existente. Compara los puntos de recuperación para evitar duplicar datos que ya hay en el archivo.

Opción	Descripción
-scheduletype	Tipo de intervalo de programación. Especifica la opción con uno de los cuatro valores siguientes: "daily" - Para la archivación creada diariamente de forma automática. "weekly" - Para la archivación creada semanalmente de forma automática. Debe especificar el parámetro "-dayofweek". "monthly" - Para la archivación creada mensualmente de forma automática. Debe especificar el parámetro "-dayofmonth". Si un mes no tiene el día especificado, por ejemplo, "31", no habrá archivo comprimido ese mes. "lastdayofmonth" - Para la creación automática de un archivo comprimido el último día de cada mes.
-dayofweek	Se usa solo para la opción "weekly" del parámetro "-scheduletype". El día de la semana en el que desee crear automáticamente el archivo comprimido (por ejemplo, "lunes").
-dayofmonth	Se usa solo para la opción "monthly" del parámetro "-scheduletype". El día (número) del mes en el que desea crear el archivo comprimido automáticamente (por ejemplo, "15").
-time	La hora del día a la que desea crear una archivación.
-initialpause	Opcional. Especifique esta opción si desea una archivación con pausa inicial después de configurar el calendario de programación de archivación.

Ejemplos:

Archive todos los puntos de recuperación con las fechas de creación a partir del 30/04/2012 14:55 para todas las máquinas en el Core, y vuelva a colocar datos archivados preexistentes que pertenecen a este Core:

```
>New-ScheduledArchive -core 10.10.10.10 -user administrator -password 23WE@#$sdd -path "d:\work\archive" -s
tartdate "04/30/2012 02:55 PM" -all -recycleaction replacethiscore
```

Archive los puntos de recuperación que se enmarcan dentro de un intervalo de fechas para dos equipos protegidos y borre todos los datos archivados del directorio antes de escribir el archivo nuevo:

```
>New-ScheduledArchive -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver "10.20.30.40" "20.20.10.1" -path "d:\work\archive" -startdate "04/30/2012 02:55
PM" -enddate "05/31/2012 11:00 AM" -recycleaction erasecompletely
```

Cree un archivo incremental para todos los puntos de recuperación con las fechas de creación a partir del 30/04/2012 14:55 para todos los equipos en el Core a la cuenta de nube con el nombre "Amazon S3" y un contenedor denominado "Contenedor":

```
>New-ScheduledArchive -core 10.10.10.10 -user administrator -password 23WE@#$sdd -path
"ArchiveOnCloud" -cloudaccountname "Amazon S3" -cloudcontainer "Container" -startdate
"04/30/2012 02:55 PM" -all -recycleaction incremental
```

New-Snapshot

El comando New-Snapshot fuerza una instantánea que produce una transferencia de datos del equipo protegido actualmente. Cuando se fuerza una instantánea, la transferencia empezará de inmediato o se añadirá a la cola. Solo se transferirán los datos que hayan cambiado con respecto a un punto de recuperación previo. Si no hay punto de recuperación previo, se transferirán todos los datos de los volúmenes protegidos.

Uso

El uso del comando es el siguiente:

```
New-Snapshot [-all] | -protectedserver [machine name]] -core [host name] -user [user name] -password [password]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `New-Snapshot`:

Tabla 261. Opciones del comando New-Snapshot

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-all	Fuerza todos los equipos protegidos.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Forzado para el nombre de del equipo protegido actual.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.

Ejemplo:

Forzar una instantánea para todos los equipos protegidos:

```
>New-Snapshot -all
```

New-VBVirtualStandby

El comando `New-VBVirtualStandby` le permite usar PowerShell para crear una nueva exportación virtual a una máquina virtual VirtualBox (VM).

Uso

El uso del comando es el siguiente:

```
New-VBVirtualStandby -core [host name] -user [login] -password [password] -protectedserver [name | IP address] -volumes [volumes names] -vmname [virtual machine name] [-ram [total megabytes] | -usesourceram] -linuxhostname [linux hostname] -hostport [linux port] -targetpath [location] -pathusername [login] -pathpassword [password] -initialexport
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `New-VBVirtualStandby`:

Tabla 262. Opciones del comando `New-VBVirtualStandby`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Muestra los trabajos de un equipo protegido específico, indicado por dirección IP.
-volumes	Opcional. Enumere los nombres de los volúmenes que desee exportar. Si no se especifica, se exportarán todos los volúmenes de los puntos de recuperación. Los valores deben estar entre comillas dobles y separados por espacios; por ejemplo, "c:", "d:". ❗ NOTA: No utilice barras finales en nombres de volúmenes.
-vmname	Nombre de Microsoft Windows de la máquina virtual.
-ram	Asignar una cantidad específica de RAM en el servidor virtual.
-usesourceram	Opcional. Asigna la misma cantidad de RAM en el servidor virtual que la que tiene el equipo protegido de origen.
-linuxhostname	El nombre de host del servidor Linux VirtualBox.
-hostport	El puerto del servidor Linux VirtualBox .
-targetpath	La ruta de acceso local, de red o de Linux a la carpeta en la que desee almacenar los archivos de la máquina virtual.
-pathusername	El nombre de usuario para iniciar sesión en el equipo de red. Solo se necesita cuando se especifica una ubicación de red de la ruta de acceso de destino.
-pathpassword	La contraseña para iniciar sesión en el equipo de red. Solo se necesita cuando se especifica una ubicación de red de la ruta de acceso de destino.
-accountusername	Opcional. Puede especificar una cuenta de usuario con la que registrar la máquina virtual exportada. Es el nombre de usuario para iniciar sesión en la cuenta de usuario. Utilice esta opción solo para un equipo local o de red.
-accountpassword	Opcional. Puede especificar una cuenta de usuario con la que registrar la máquina virtual exportada. Es la contraseña para iniciar sesión en la cuenta de usuario. Utilice esta opción solo para un equipo local o de red.
-initialexport	Opcional. Especifique esta opción si tiene que iniciar la exportación de una máquina virtual a petición inicial después de configurar la espera virtual.

Ejemplo:

Cree una máquina en espera virtual VirtualBox denominada ExportedMachine1 en una ubicación especificada:

```
>New-VMVirtualStandby -protectedserver 10.10.10.4 -volumes C:\ -vmname ExportedMachine1 -
usesourceram -targetpath I:\VMExport
```

New-VMVirtualStandby

El comando `New-VMVirtualStandby` PowerShell le permite crear una nueva máquina en espera virtual VMware Workstation mediante Rapid Recovery.

Uso

El uso del comando es el siguiente:

```
New-VMVirtualStandby -core [host name] -user [login] -password [password] -protectedserver
[name | IP address] -volumes [volumes names] -vmname [virtual machine name] [-ram [total
megabytes] | -usesourceram] -targetpath [location] -pathusername [login] -pathpassword
[password] -initialexport
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `New-VMVirtualStandby`:

Tabla 263. Opciones del comando New-VMVirtualStandby

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Muestra los trabajos de un equipo protegido específico, indicado por dirección IP.
-volumes	Opcional. Enumere los nombres de los volúmenes que desee exportar. Si no se especifica, se exportarán todos los volúmenes de los puntos de recuperación. Los valores deben estar entre comillas dobles y separados por espacios; por ejemplo, "c:", "d:".  NOTA: No utilice barras finales en nombres de volúmenes.
-vmname	Nombre de Microsoft Windows de la máquina virtual.

Opción	Descripción
-ram	Asignar una cantidad específica de RAM en el servidor virtual.
-usesourceram	Opcional. Asigna la misma cantidad de RAM en el servidor virtual que la que tiene el equipo protegido de origen.
-pathusername	El nombre de usuario para iniciar sesión en el equipo de red. Solo se necesita cuando se especifica una ubicación de red de la ruta de acceso de destino.
-pathpassword	La contraseña para iniciar sesión en el equipo de red. Solo se necesita cuando se especifica una ubicación de red de la ruta de acceso de destino.
-initialexport	Opcional. Especifique esta opción si tiene que iniciar la exportación de una máquina virtual a petición inicial después de configurar la espera virtual.

Ejemplo:

Crear un nuevo servidor en espera virtual VMware Workstation:

```
>New-VMVirtualStandby -protectedserver 10.10.10.4 -volumes C:\ -vmname ExportedMachine1 -
usesourceram -targetpath I:\VMExport
```

La secuencia de comandos se pausa, lo que requiere que el usuario especifique un número de índice de la estación de trabajo adecuada. Introduzca el número de índice de la secuencia de comandos que desee completar (en este caso, 2). El ejemplo continúa:

```
2
Verify location ...
Virtual Standby successfully configured
PS C:\Users\Administrator>
```

Push-Replication

El comando `Push-Replication` fuerza la replicación de uno o más equipos protegidos.

Uso

El uso del comando es el siguiente:

```
Push-Replication -core [host name] -user [user name] -password [password] -targetcore [host
name] -all | -protectedserver [machine name | IP address]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `Push-Replication` :

Tabla 264. Opciones del comando Push-Replication

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-all	Fuerza la replicación en todos los equipos que se están replicando en el Core de destino.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.

Opción	Descripción
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Nombre del equipo protegido en el Core de destino donde se va a forzar la replicación.
-user	Opcional. Inicio de sesión en el equipo host del Core remoto. Si especifica un inicio de sesión, deberá proporcionar también una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.

Ejemplo:

Distribuir la replicación en un único equipo protegido:

```
>Push-Replication -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd
-targetcore 10.10.10.20:8006 -protectedserver 10.10.5.22
```

Distribuir la replicación en todos los equipos protegidos:

```
>Push-Replication -all
```

Push-Rollup

El comando `Push-Rollup` fuerza una consolidación de un equipo protegido.

Uso

El uso del comando es el siguiente:

```
Push-Rollup -core [host name] -user [user name] -password [password] -protectedserver [machine
name | IP address]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `Push-Rollup` :

Tabla 265. Opciones del comando Push-Rollup

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-all	Fuerza todos los equipos protegidos.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Forzado para el nombre de del equipo protegido actual.

Opción	Descripción
-user	Opcional. Inicio de sesión en el equipo host del Core remoto. Si especifica un inicio de sesión, deberá proporcionar también una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.

Ejemplo:

Distribuir la consolidación en un único equipo protegido:

```
>Push-Rollup -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22
```

Distribuir la consolidación en todos los equipos protegidos:

```
>Push-Rollup -all
```

Remove-Agent

El comando de PowerShell `Remove-Agent` permite quitar un equipo de la protección del Core de Rapid Recovery.

Uso

El uso del comando es el siguiente:

```
Remove-Agent -core [host name] -user [login] -password [password] -protectedserver [name | IP address] -deleterecoverypoints -all
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `Remove-MountAgent`:

Tabla 266. Opciones del comando `Remove-Agent`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Desmonta todos los puntos de recuperación montados para el equipo protegido actual.
-deleterecoverypoints	Opcional. Elimina todos los puntos de recuperación del equipo protegido.

Opción	Descripción
-all	Opcional. Elimina todos los equipos protegidos del Core.

Ejemplo:

Desmonta todos los equipos protegidos y sus puntos de recuperación:

```
>Remove-Agent -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -
deleterecoverypoints -all
```

Remove-Mount

El comando `Remove-Mount` desmonta un punto de recuperación montado especificado por `/Path`. Desmontar los puntos para el equipo seleccionado mediante el parámetro `-protectedserver` o desmontar los puntos para todos los puntos de recuperación montados con el parámetro `-all`.

Uso

El uso del comando es el siguiente:

```
Remove-Mount -core [host name] -user [user name] -password [password] [-
protectedserver [machine name] | -path [mount path]]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `Remove-Mount`:

Tabla 267. Opciones del comando `Remove-Mount`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-all	Desmonta todos los puntos de recuperación montados.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-path	Desmonta el punto de montaje seleccionado.
-protectedserver	Desmonta todos los puntos de recuperación montados para el equipo protegido actual.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.

Ejemplo:

Desmontar un punto de recuperación especificado mediante la ruta de acceso:

```
>Remove-Mount -core 10.10.10.10:8006 -user administrator -password 23WE@#sdd -path C:\mountedRecoveryPoint
```

Remove-Mounts

El comando `Remove-Mounts` desmonta todos los puntos de recuperación montados.

Uso

El uso del comando es el siguiente:

```
Remove-Mounts -core [host name] -user [user name] -password [password]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `Remove-Mounts`:

Tabla 268. Opciones del comando `Remove-Mounts`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.

Ejemplo:

Desmontar todos los puntos de recuperación en el Core especificado:

```
>Remove-Mounts -core 10.10.10.10:8006 -user administrator -password 23WE@#sdd
```

Remove-RecoveryPoints

El comando `Remove-RecoveryPoints` PowerShell permite eliminar puntos de recuperación de un equipo específico.

Uso

El uso del comando es el siguiente:

```
Remove-RecoveryPoints -core [host name] -user [login] -password [password] -[range | chain | all] -protectedserver [name | IP address] -rpn [number | numbers] | -time [time string | time interval specified by two time strings]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Remove-RecoveryPoints`:

Tabla 269. Opciones del comando `Remove-RecoveryPoints`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Desmonta todos los puntos de recuperación montados para el equipo protegido actual.
-rpn	Opcional. Solo para eliminación en cadena (imagen base con cadena de puntos incrementales o huérfanos). Número secuencial de un punto de recuperación que se va a eliminar (utilice el comando <code>Get-RecoveryPoints</code> para obtener los números). Especifique varios números separados por espacios para eliminar múltiples puntos de recuperación con un único comando.
-time	Utilice esta opción para eliminar una cadena de puntos de recuperación. Opcional. Para eliminar un único punto de recuperación, seleccione el punto de recuperación por su hora de creación. Especifique el momento exacto con el formato "mm/dd/yyyy hh:mm tt" (por ejemplo, "2/24/2012 09:00 AM"). Tenga en cuenta que debe especificar los valores de fecha y hora de la zona horaria establecida en su equipo. Obligatorio. Para un rango de fechas, especifique un intervalo de tiempo mediante dos cadenas separadas por una coma y un espacio para seleccionar el rango de los puntos de recuperación que hay que eliminar.
-range	Opcional. El rango de puntos de recuperación que hay que eliminar por intervalo de tiempo.
-chain	Opcional. Una imagen base con incrementaciones secuenciales o un conjunto secuencial de puntos huérfanos para eliminar los seleccionados por número de punto de recuperación o tiempo de creación del punto de recuperación.
-all	Opcional. Eliminar todos los equipos protegidos del Core.

Ejemplo:

Eliminar un punto de recuperación especificado por la fecha:

```
>Remove-RecoveryPoints -core 10.10.10.10:8006 -user administrator -password 23WE@#sdd -time "2/24/2012 09:00 AM"
```

Eliminación del repositorio

El comando PowerShell `Remove-Repository` elimina un repositorio Rapid Recovery y su contenido del Core.

Uso

El uso del comando es el siguiente:

```
Remove-Repository -core [host name] -user [login] -password [password] -name [repository name] -all
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `Remove-Repository`:

Tabla 270. Opciones del comando `Remove-Repository`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-name	El nombre de repositorio que desea eliminar.
-all	Elimine todos los repositorios asociados con este Core.

Ejemplo:

Elimine todos los repositorios del Core local:

```
>Remove-repository -all
```

Remove-ScheduledArchive

Si programó Rapid Recovery para que archive puntos de recuperación de forma regular en un equipo específico, puede utilizar el comando `Remove-ScheduledArchive` PowerShell para eliminar ese archivo comprimido programado del Core.

Uso

El uso del comando es el siguiente:

```
Remove-ScheduledArchive -core [host name] -user [login] -password [password] -all -ids [id | id1 id2]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Remove-ScheduledArchive`:

Tabla 271. Opciones del comando `Remove-ScheduledArchive`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-all	Elimine todos los archivos asociados con este Core.
-id	El identificador del archivo que desea eliminar. Para visualizar más de un archivo, separe cada Id. con un espacio.

Ejemplo:

Eliminar varias archivaciones programadas del Core local:

```
>Remove-ScheduledArchive -ids 799138c8-3dfc-4398-9711-1823733c2a31, 26c29bb7-b320-47f5-b5a8-dffc49f50e25
```

Remove-VirtualStandby

Si programó Rapid Recovery para que exporte datos de forma continua a una máquina virtual, puede utilizar el comando `Remove-VirtualStandby` PowerShell para cancelar y eliminar este trabajo programado.

Uso

El uso del comando es el siguiente:

```
Remove-VirtualStandby -core [host name] -user [login] -password [password] -all | -  
protectedserver [name(s) | IP address]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Remove-VirtualStandby`:

Tabla 272. Opciones del comando `Remove-VirtualStandby`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-all	Elimine todos los trabajos en espera virtual asociados con este Core.
-protectedserver	El nombre o la dirección IP del equipo protegido para el que quiere eliminar el estado en espera virtual.

Ejemplo:

Eliminar todos los trabajos en espera virtual asociados con este Core:

```
>Remove-VirtualStandby -all
```

Resume-Replication

El comando `Resume-Replication` le permite reanudar la replicación. Consulte [Suspend-Replication](#) para obtener más información.

Uso

El uso del comando es el siguiente:

```
Resume-Replication -core [host name] -user [user name] -password [password] -all | -  
protectedserver [machine name | IP address] -incoming [host name] | -outgoing [host name]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `Resume-Replication`:

Tabla 273. Opciones del comando `Resume-Replication`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-all	Todos los servidores protegidos.
-protectedserver	Reanuda la replicación para el equipo especificado.
-incoming	Nombre de host del Core remoto que se replica en el equipo Core. La replicación se reanuda para todos los equipos protegidos en el Core remoto.
-outgoing	Nombre de host del Core de destino remoto en el que se están replicando los datos. La replicación se reanuda para todos los equipos protegidos en el Core remoto.

Ejemplo:

Reanude la replicación del equipo protegido con IP 10.10.10.128 del Core local y especifique el repositorio que se está utilizando:

```
>Resume-Replication replicationname Replication1 -targetserver 10.10.10.128,Administrator,123asdQ -protectedserver 10.10.10.4
```

```
# Repository
- -----
```

```
1 Repository A
2 Repository B
```

Please, input number of Repository from the list above or type 'exit' to exit:

Se pausa la secuencia de comandos y se requiere que el usuario especifique un número de índice del repositorio adecuado. Introduzca el número de índice de la secuencia de comandos que desee completar (en este caso, 2). El ejemplo continúa:

```
2
Replication job was started.
True
PS C:\Users\Administrator>
```

Resume-Snapshot

Un administrador puede reanudar las instantáneas, exportar a máquinas virtuales y realizar replicaciones. Consulte [Start-VMExport](#) para obtener más información.

Uso

El uso del comando es el siguiente:

```
Resume-Snapshot -core [host name] -user [user name] -password [password] -all | -  
protectedserver [name | IP address]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Resume-Snapshot`:

Tabla 274. Opciones del comando Resume-Snapshot

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-all	Todos los servidores protegidos.
- protectedserver	Reanudar la instantánea para el equipo especificado.

Ejemplo:

Reanudar las instantáneas para el equipo protegido con IP 10.10.10.4 para el core local:

```
>Resume-Snapshot -protectedserver 10.10.10.4
```

Resume-VirtualStandby

El comando de PowerShell `Resume-VirtualStandby` permite reanudar la exportación de datos suspendida en un servidor en espera virtual de Rapid Recovery.

Uso

El uso del comando es el siguiente:

```
Resume-VirtualStandby -core [host name] -user [login] -password [password] -all | -  
protectedserver [name(s) | IP address]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `Resume-VirtualStandby`:

Tabla 275. Opciones del comando `Resume-VirtualStandby`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-all	Reanudar las exportaciones de todas las máquinas en espera virtual.
- protectedserver	El nombre o los nombres (separados por una coma y un espacio) de los equipos protegidos con máquinas en espera virtual que quiere reanudar.

Ejemplo:

Reanude las exportaciones en espera virtual de un equipo protegido:

```
>Resume-VirtualStandby -core 10.10.10.10:8006 -user administrator -password 23WE@#sdd -  
protectedserver 10.10.5.22
```

Resume-VMExport

El comando `Resume-VMExport` permite a un administrador exportar a máquina virtual. Consulte [Suspend-VMExport](#) para obtener más información.

Uso

El uso del comando es el siguiente:

```
Resume-VMExport -core [host name] -user [user name] -password [password] -all | -  
protectedserver [name | IP address]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `Resume-VMExport`:

Tabla 276. Opciones del comando `Resume-VMExport`

Opción	Descripción
<code>-?</code>	Muestra el mensaje de ayuda.
<code>-core</code>	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
<code>-password</code>	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
<code>-user</code>	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
<code>-all</code>	Todos los servidores protegidos.
<code>-protectedserver</code>	Reanudar la instantánea para el equipo especificado.

Ejemplo:

Reanudar la exportación a una máquina virtual para cada equipo protegido en el Core local:

```
>Resume-VMExport -all
```

Start-Archive

Las empresas suelen utilizar almacenamiento a largo plazo para archivar tanto los datos de conformidad como los de no conformidad. La función de archivado de Rapid Recovery se utiliza para ayudar a retener durante más tiempo los datos exigidos por ley y de no conformidad. El administrador puede guardar un archivo en la ubicación de red o de almacenamiento local especificado las credenciales y el comando `/Path`.

Uso

El uso del comando es el siguiente:

```
Start-Archive -path -startdate -enddate [-all] | -protectedserver [machine name] or [IP]] -core [host name] -user [user name] -password [password]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `Start-Archive`:

Tabla 277. Opciones del comando Start-Archive

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-path	Ruta de acceso de la ubicación. Ejemplo de ruta de acceso: "D:\trabajo\archivocomprimido" o ruta de acceso a la red: "\\nombreServidor\nombreRecursoCompartido".
-all	Archivar todos los puntos de recuperación para todos los equipos en el Core.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-startdate	Fecha inicial del intervalo de fechas de puntos de recuperación creados. Deberá indicarse con el formato especificado por el SO del PC actual.
-enddate	Fecha final del intervalo de fechas. De manera predeterminada es la fecha actual.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Archivar puntos de recuperación para el equipo especificado.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-archiveusername	Opcional. Solo es requerido para la ruta de red.
-archivepassword	Opcional. Solo es requerido para la ruta de red.
-comment	Opcional. Ejemplo:-comment 'Before install new application'.

Ejemplo:

Archivar todos los puntos de recuperación para todos los equipos del Core:

```
>Start-Archive -path D:\work\archive -startdate 'Example 04/30/2012' -all
```

Start-AttachabilityCheck

El comando `Start-AttachabilityCheck` fuerza una comprobación de conectabilidad para todas las bases de datos de SQL Server protegidas por el Core.

Uso

El uso del comando es el siguiente:

```
Start-AttachabilityCheck -core [host name] -user [username] - password [password]
- protectedserver [machine name | IP address] -rpn [number | numbers] | -time [time string]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Start-AttachabilityCheck`:

Tabla 278. Opciones del comando `Start-AttachabilityCheck`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	El equipo protegido en el que realizar la comprobación de conectabilidad de SQL.
-rpn	Opcional. El número secuencial de un punto de recuperación en el que realizar la comprobación de conectabilidad de SQL. Puede utilizar el comando <code>GetRecoveryPoints</code> para obtener los números de los puntos de recuperación. Puede especificar varios números separados por espacios para realizar las comprobaciones en múltiples puntos de recuperación con un único comando. NOTA: Si no es específica ni la opción <code>'time'</code> ni <code>'rpn'</code> en este comando, se utiliza el punto de recuperación más reciente para la prueba de conectabilidad.
-time	Opcional. Determina el punto de recuperación que debe seleccionarse para la comprobación de conectabilidad de SQL. Debe especificar la hora exacta en el formato "MM/DD/AAAA hh:mm tt" (por ejemplo, "04/24/2015 09:00 AM"). Especifique los valores de hora y fecha de la zona horaria establecida en su equipo local. NOTA: Si no es específica ni la opción <code>'time'</code> ni <code>'rpn'</code> en este comando, se exportará el punto de recuperación más reciente.

Ejemplo:

Realizar una comprobación de conectabilidad de SQL en el punto de recuperación más reciente para el servidor SQL protegido especificado:

```
>Start-AttachabilityCheck - protectedserver 10.10.9.120
```

Start-ChecksumCheck

El comando `Start-ChecksumCheck` PowerShell permite forzar una comprobación de la suma de comprobación de los puntos de recuperación de Exchange Server.

Uso

El uso del comando es el siguiente:

```
Start-ChecksumCheck -core [host name] -user [login] -password [password] -protectedserver [name  
| IP address] -rpn [number | numbers] | -time [time string]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Start-ChecksumCheck`:

Tabla 279. Opciones del comando Start-ChecksumCheck

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	El nombre del equipo protegido.
-rpn	Opcional. Solo para eliminación en cadena (imagen base con cadena de puntos incrementales o huérfanos). El número secuencial de un punto de recuperación para comprobar (utilice el comando <code>Get-RecoveryPoints</code> para obtener los números). Especifique varios números separados por espacios para eliminar múltiples puntos de recuperación con un único comando.
-time	Opcional. Seleccione el punto de recuperación para controlar por su hora de creación, en lugar de su número secuencial. Especifique el momento exacto con el formato "mm/dd/yyyy hh:mm tt" (por ejemplo, "2/24/2012 09:00 AM"). Tenga en cuenta que debe especificar los valores de fecha y hora de la zona horaria establecida en su equipo.

Ejemplo:

Iniciar una comprobación de la suma de comprobación en dos puntos de recuperación:

```
> Start-ChecksumCheck -core 10.10.10.10 -user administrator -password 23WE@#$sdd -  
protectedserver 10.10.5.22 -rpn 5 7
```

Start-EsxiExport

El comando `Start-EsxiExport PowerShell` inicia la ejecución de una exportación virtual desde el punto de recuperación seleccionado de Rapid Recovery en una máquina virtual de servidor ESX(i).

Los parámetros requeridos incluyen el nombre del equipo protegido que contiene los puntos de recuperación que hay que exportar; el nombre de la máquina virtual a la que se está exportando; la cantidad de RAM que hay que asignar en la máquina virtual; el nombre de host y el puerto del host del servidor Linux, y la ruta de acceso a la carpeta local, de red, o de Linux donde se almacenarán los archivos resultantes de la máquina virtual.

Uso

El uso del comando es el siguiente:

```
Start-EsxiExport -core [host name] -user [user name] -password [password] -protectedserver [machine name | IP address] -volumes [volume names] -rpn [number | numbers] | -time [time string] -vmname [virtual machine name] -hostname [virtual host name] -hostport [virtual host port number] -hostusername [virtual host user name] hostpassword [virtual host password] [-ram [total megabytes] | -usesourceram] -diskprovisioning [thin | thick] -diskmapping [automatic | manual | withvm]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Start-EsxiExport`:

Tabla 280. Opciones del comando Start-EsxiExport

Opción	Descripción
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Equipo protegido con puntos de recuperación que se deben exportar.
-volumes	Opcional. Lista de nombres de volumen que deben exportarse. Si no se especifica, todos los volúmenes en los puntos de recuperación especificados se exportarán. Los valores deben estar entre comillas dobles y separados por un espacio. No utilice barras finales en nombres de volúmenes. Por ejemplo, especifique "C:" no "C:/"
-rpn	Opcional. El número secuencial de un punto de recuperación que hay que exportar. (Puede utilizar el comando <code>Get-RecoveryPoints</code> para obtener los números de los puntos de recuperación).
	NOTA: Si no es específica ni la opción 'time' ni 'rpn' en este comando, se exportará el punto de recuperación más reciente.
-time	Opcional. Determina el punto de recuperación que debe seleccionarse para la exportación. Debe especificar la hora exacta en el formato "MM/DD/AAAA hh:mm tt" (por ejemplo, "04/24/2015 09:00 AM"). Especifique los valores de hora y fecha de la zona horaria establecida en su equipo local.
	NOTA: Si no es específica ni la opción 'time' ni 'rpn' en este comando, se exportará el punto de recuperación más reciente.
-vmname	Nombre de Windows de la máquina virtual.
-hostname	Nombre de host del servidor virtual.

Opción	Descripción
-hostport	Número de puerto del servidor virtual.
-hostusername	Nombre de usuario para el host del servidor virtual.
-hostpassword	Contraseña del host del servidor virtual.
-ram	Asigna una cantidad de RAM específica al servidor virtual.
-usesourceram	Opcional. Asigna la misma cantidad de RAM en el servidor virtual que en el equipo protegido de origen.
-diskprovisioning	Opcional. La cantidad de espacio en disco que se asignará en la máquina virtual. Especifique 'thick' para crear el disco virtual del tamaño de la unidad original en el servidor protegido o 'thin' para asignar la cantidad de espacio en disco real en la unidad original, además de algunos megabytes adicionales. La opción seleccionada de forma predeterminada es 'thin'.
-diskmapping	Opcional. Seleccione 'auto,' 'manual' o 'withvm'. El modo habilitado de forma predeterminada es el de asignación automática.
-resetup	Opcional. Vuelve a crear la máquina virtual si ya se ha presentado en la ubicación especificada.
-datacenter	Opcional. Especifica qué centro de datos se va a utilizar.
-resourcepool	Opcional. Especifica qué grupo de recursos se va a utilizar.
-datastore	Opcional. Especifica qué almacén de datos se va a utilizar.
-computeresource	Opcional. Especifica qué recursos de cálculo se van a utilizar.
-version	Opcional. Especifica qué versión de ESXi se va a utilizar.

Start-HypervExport

El comando PowerShell `Start-HypervExport` inicia la ejecución de una exportación virtual desde el punto de recuperación de Rapid Recovery seleccionado en una máquina virtual de servidor Hyper-V.

Uso

El uso del comando es el siguiente:

```
Start-HypervExport -core [host name] -user [user name] -password [password] -protectedserver [[machine name] or [IP address]] -volumes [volume names] -rpn [number | numbers] | -time [time string] [-vmname [uselocalmachine] | -hostname [virtual host name] -hostport [virtual host port number] -hostusername [virtual host user name] -hostpassword [virtual host password] -vmlocation [location]] [-ram [total megabytes] | -usesourceram] -diskformat [VHD | VHDX]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Start-HypervExport`:

Tabla 281. Opciones del comando Start-HypervExport

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Equipo protegido con puntos de recuperación que se deben exportar.
-volumes	Opcional. Lista de nombres de volumen que deben exportarse. Si no se especifica, todos los volúmenes en los puntos de recuperación especificados se exportarán. Los valores deben estar entre comillas dobles y separados por un espacio. No utilice barras finales en nombres de volúmenes. Por ejemplo, especifique "C:" no "C:/"
-rpn	Opcional. El número secuencial de un punto de recuperación que hay que exportar. (Puede utilizar el comando <code>Get-RecoveryPoints</code> para obtener los números de los puntos de recuperación).
	NOTA: Si no es especifica ni la opción 'time' ni 'rpn' en este comando, se exportará el punto de recuperación más reciente.
-time	Opcional. Determina el punto de recuperación que debe seleccionarse para la exportación. Debe especificar la hora exacta en el formato "MM/DD/AAAA hh:mm tt" (por ejemplo, "04/24/2015 09:00 AM"). Especifique los valores de hora y fecha de la zona horaria establecida en su equipo local.
	NOTA: Si no es especifica ni la opción 'time' ni 'rpn' en este comando, se exportará el punto de recuperación más reciente.
-vmname	Nombre de Windows de la máquina virtual.
-gen2	Opcional. Especifique utilizar la segunda generación de VM. Si no se especifica, se utiliza la generación 1. Rapid Recovery admite la generación 2 de Windows Server 2012 R2 a través de Windows 8.1.
-usevhdx	Opcional. Si especifica esta opción, Rapid Recovery utiliza el formato de disco VHDX para crear la VM. Si no lo hace, se utiliza el formato de disco VHD. La generación 2 solo utiliza el formato VHDX.
-uselocalmachine	Opcional. Conecta el servidor Hyper-V local. Si se utiliza este parámetro, se ignoran las siguientes opciones: hostname, host port, host username, host password.
-hostname	Nombre de host del servidor virtual.
-hostport	Número de puerto del servidor virtual.
-hostusername	Nombre de usuario para el host del servidor virtual.
-hostpassword	Contraseña del host del servidor virtual.
-vmlocation	Ruta de acceso local o de red a la carpeta donde quiere guardar los archivos de la máquina virtual.
-ram	Asigna una cantidad de RAM específica al servidor virtual.
-usesourceram	Opcional. Asigna la misma cantidad de RAM en el servidor virtual que en el equipo protegido de origen.

Start-LogTruncation

El comando `Start-LogTruncation` fuerza un truncamiento del registro para el servidor SQL protegido o el servidor Microsoft Exchange especificados.

Uso

El uso del comando es el siguiente:

```
Start-LogTruncation -core [host name] -user [user name] -password [password] -protectedserver [[machine name] or [IP address]] -target [sql | exchange]
```

Opciones de comando

En la tabla siguiente se describen las opciones disponibles para el comando `Start-LogTruncation`:

Tabla 282. Opciones del comando Start-LogTruncation

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Archivo de puntos de recuperación para el equipo especificado.
-target	Especifica el tipo de truncado de registro ("sql" o "exchange"). Si no se especifica, se truncan los registros en todas las bases de datos.

Ejemplo:

Truncar registros SQL:

```
>Start-LogTruncation -protectedserver SQL1 -target sql
```

Truncar los registros de servidor Exchange: todos los puntos de recuperación para todos los equipos del Core:

```
> start-LogTruncation -protectedserver ExServer2 -target exchange
```

Start-MountabilityCheck

El comando `Start-MountabilityCheck` fuerza una comprobación de la capacidad de montaje para los almacenes de correo de Microsoft Exchange protegidos.

Uso

El uso del comando es el siguiente:

```
Start-MountabilityCheck -core [host name] -user [user name] -password [password] -protectedserver [[machine name] or [IP address]] -rpn [number | numbers] | -time [time string]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Start-MountabilityCheck`:

Tabla 283. Opciones del comando Start-MountabilityCheck

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Archivo de puntos de recuperación para el equipo especificado.
-rpn	Opcional. El número secuencial de un punto de recuperación que hay que exportar. (Puede utilizar el comando <code>GetRecoveryPoints</code> para obtener los números de los puntos de recuperación). ❗ NOTA: Si no es especifica ni la opción 'time' ni 'rpn' en este comando, se exportará el punto de recuperación más reciente.
-time	Opcional. Determina el punto de recuperación que debe seleccionarse para la exportación. Debe especificar la hora exacta en el formato "MM/DD/AAAA hh:mm tt" (por ejemplo, "04/24/2015 09:00 AM"). Especifique los valores de hora y fecha de la zona horaria establecida en su equipo local. ❗ NOTA: Si no es especifica ni la opción 'time' ni 'rpn' en este comando, se exportará el punto de recuperación más reciente.

Ejemplo:

Iniciar una comprobación de capacidad de montaje de todos los puntos de recuperación para todos los equipos del Core:

```
> Start-MountabilityCheck -protected EX01
```

Start-Protect

El comando `Start-Protect` permite a un administrador agregar un servidor bajo la protección de un Core.

Uso

```
Start-Protect -core [host name] -user [user name] -password [password] -repository [repository name] -agent [name | IP address] -agentusername [user name] -agentpassword [password] -agentport [port] -volumes [volume names]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Start-Protect`:

Tabla 284. Opciones del comando Start-Protect

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-repository	Nombre de un repositorio del Core donde están almacenados los datos del equipo protegido.
-agentname	Dirección IP o nombre del equipo protegido.
-agentusername	Inicie sesión en el servidor para estar protegido.
-agentpassword	Establezca una contraseña en el servidor para estar protegido.
-agentport	Número de puerto de servidor protegido.
-volumes	Lista de volúmenes para proteger. Los valores deben estar entre comillas dobles y separados por un espacio. No utilice barras finales en nombres de volúmenes. Por ejemplo, "c:" o "d".

Ejemplo:

Poner volúmenes de un servidor bajo protección:

```
>Start-Protect -repository "Repository 1" -agentname 10.10.9.120 -agentusername administrator -agentpassword 12345 -agentport 5002 -volumes "c:" "d:"
```

Start-ProtectCluster

El comando `Start-ProtectCluster` permite a un administrador agregar un clúster de servidores bajo protección por un Core.

Uso

El uso del comando es el siguiente:

```
Start-ProtectCluster -core [host name] -user [user name] -password [password] -repository [repository name] -clustername [name | IP address] -clusterusername [user name for cluster] -clusterpassword [password for cluster] -clusterport [port] -clustervolumes [volume names] -clusternodes [cluster nodes names and volumes]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Start-ProtectCluster`:

Tabla 285. Opciones del comando Start-ProtectCluster

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-repository	Nombre de un repositorio del Core donde están almacenados los datos del equipo protegido. El nombre se debe poner entre comillas dobles.
-clustername	El nombre del clúster que se debe proteger.
-clusterusername	Nombre de usuario para el clúster que se debe proteger.
-clusterpassword	Contraseña para el clúster que se debe proteger.
-clusterport	Número de puerto para el clúster que se debe proteger.

Opción	Descripción
-clustervolumes	Lista de volúmenes para proteger. Los valores deben estar entre comillas dobles y separados por un espacio. No utilice barras finales en nombres de volúmenes. Por ejemplo, "c:", "d".
-clusternodes	Enumera los nodos de clúster con sus volúmenes para proteger. Primero especifique la etiqueta "nodename" y luego introduzca el nombre del nodo. A continuación, especifique la etiqueta "volumes" y luego introduzca una lista de volúmenes para el nodo. Por ejemplo: "nodename", "10.10.10.10", "volumes", "c:", "e:", "nodename", "10.10.10.11", "volumes", "c:"

Ejemplo:

Poner volúmenes de un servidor bajo protección:

```
>Start-ProtectCluster -repository "Repository 1" -clustername 10.10.9.120 -clusterusername administrator -clusterpassword 12345 -clusterport 5002 -clustervolumes "c:" "d:" -clusternodes nodename 10.10.10.10 volumes "c:" "e:"
```

Start-RepositoryCheck

El comando `Start-RepositoryCheck` PowerShell permite comprobar la integridad de un repositorio.

Uso

El uso del comando es el siguiente:

```
Start-RepositoryCheck -name [repository name] | -all [check all repositories] -password [password] -force
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Start-RepositoryCheck`:

Tabla 286. Opciones del comando Start-RepositoryCheck

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-repository	Obligatorio. El nombre del repositorio que desea comprobar.

Opción	Descripción
-all	Opcional. Comprobar todos los repositorios asociados con este Core.
-force	Opcional. Realizar la comprobación de repositorio sin confirmación.

Ejemplo:

Iniciar la comprobación de un repositorio:

```
>Start-RepositoryCheck -repository newRepository1 -core 10.10.10.10:8006 -user administrator -password 23WE@#sdd
```

Start-RestoreArchive

Las empresas suelen utilizar almacenamiento a largo plazo para archivar tanto los datos de conformidad como los de no conformidad. La función de archivado de Rapid Recovery se utiliza para ayudar a retener durante más tiempo los datos exigidos por ley y de no conformidad. El administrador puede guardar un archivo en la ubicación de red o de almacenamiento local especificado las credenciales y el comando-Path.

Uso

El uso del comando es el siguiente:

```
Start-RestoreArchive -core [host name] -user [login] -password [password] -all | -protectedserver [name | IP address | "[name1 | IP address1]" "[name2 | IP address2]"] -repository [name] -archiveusername [name] -archivepassword [password] -path [location] -cloudaccountname [name] -cloudcontainer [name]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comandoStart-RestoreArchive:

Tabla 287. Opciones del comando Start-RestoreArchive

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-all	Archivar puntos de recuperación para todos los equipos protegidos.

Opción	Descripción
-protectedserver	El equipo protegido con los puntos de recuperación que desea archivar. Puede especificar varios nombres de equipo entre comillas dobles y separados por comas.
-repository	El nombre del repositorio en el que quiere colocar los puntos de recuperación restaurados. El nombre debe ir entre comillas dobles; por ejemplo, "Repository1".
-archiveusername	Opcional. El nombre de usuario para iniciar sesión en el equipo remoto. Solo es necesario para la ruta de red.
-archivepassword	Opcional. La contraseña para iniciar sesión en el equipo remoto. Solo es necesario para la ruta de red.
-path	La ruta de acceso en la que quiere guardar los datos archivados. Por ejemplo: - Equipo local: "d:\work\archive" - Ruta de red: "\\servername\sharename" - Carpeta de una cuenta de la nube: "Folder Name" NOTA: El número de símbolos no debe ser mayor de 100 para las ubicaciones locales y de red, ni mayor de 150 para una ubicación de la nube.
-cloudaccountname	Opcional. Solo se utiliza para la archivación de la nube. El nombre de la cuenta de la nube donde quiere guardar el archivo.
-cloudcontainer	Opcional. Solo se utiliza para la archivación de la nube. El nombre del contenedor de la nube de la cuenta de nube elegida, donde se guardará el archivo. Cuando se utiliza esta opción, debe especificar también el parámetro "-cloudaccountname".
-manifestcore	Opcional. Especifique el Core que desea utilizar del manifiesto del archivo restaurado.

Ejemplo:

Archivar todos los puntos de recuperación de todos los equipos del Core y guardarlos en el equipo local:

```
>Start-RestoreArchive -path D:\work\archive -startdate 'Example 04/30/2012' -all
```

Start-ScheduledArchive

El comando `Start-ScheduledArchive` PowerShell permite forzar una archivación programada de Rapid Recovery para que sea a petición, independientemente del programa preestablecido.

Uso

El uso del comando es el siguiente:

```
Start-ScheduledArchive -core [host name] -user [login] -password [password] -all -ids [id | id1 id2]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Start-ScheduledArchive`:

Tabla 288. Opciones del comando Start-ScheduledArchive

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-all	Fuerza todas las archivaciones programadas.
-id	El número de identificación o los identificadores separados por espacios de las archivaciones programadas que quiere forzar.

Ejemplo:

Iniciar varias tareas de archivación programada:

```
>Start-ScheduledArchive -ids 799138c8-3dfc-4398-9711-1823733c2a31, 26c29bb7-b320-47f5-b5a8-dffc49f50e25
```

Start-VBExport

El comando `start-VBExport` inicia la ejecución de una exportación virtual desde el punto de recuperación seleccionado en una máquina virtual de servidor Oracle VirtualBox.

Los parámetros requeridos incluyen el nombre del equipo protegido que contiene los puntos de recuperación que hay que exportar; el nombre de la máquina virtual a la que se está exportando; la cantidad de RAM que hay que asignar en la máquina virtual; el nombre de host y el puerto del host del servidor Linux, y la ruta de acceso a la carpeta local, de red, o de Linux donde se almacenarán los archivos resultantes de la máquina virtual.

Uso

El uso del comando es el siguiente:

```
Start-VBExport -core -user [user name] -password [password] -protectedserver [machine name] or [IP address] -volumes [volume names] -rpn [number | numbers] |  
-time [time string] -vmname [virtual machine name] [-ram [total megabytes] |  
-usesourceram] -linuxhostname [linux hostname] -hostport [linux port] -targetpath [location]  
pathusername [user name] - pathpassword [password]
```

Opciones de comando

En la siguiente tabla se describen las opciones disponibles para el comando `Start-VBExport`:

Tabla 289. Opciones del comando Start-VBExport

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Equipo protegido con puntos de recuperación que se deben exportar.
-volumes	Opcional. Lista de nombres de volumen que deben exportarse. Si no se especifica, todos los volúmenes en los puntos de recuperación especificados se exportarán. Los valores deben estar entre comillas dobles y separados por un espacio. No utilice barras finales en nombres de volúmenes. Por ejemplo, especifique "C:" no "C:/"
-rpn	Opcional. El número secuencial de un punto de recuperación que hay que exportar. (Puede utilizar el comando <code>Get-RecoveryPoints</code> para obtener los números de los puntos de recuperación.)  NOTA: Si no es especifica ni la opción 'time' ni 'rpn' en este comando, se exportará el punto de recuperación más reciente.
-time	Opcional. Determina el punto de recuperación que debe seleccionarse para la exportación. Debe especificar la hora exacta en el formato "MM/DD/AAAA hh:mm tt" (por ejemplo, "04/24/2015 09:00 AM"). Especifique los valores de hora y fecha de la zona horaria establecida en su equipo local.  NOTA: Si no es especifica ni la opción 'time' ni 'rpn' en este comando, se exportará el punto de recuperación más reciente.
-vmname	Nombre de Windows de la máquina virtual.
-ram	Asigna una cantidad de RAM específica al servidor virtual.
-usesourceram	Opcional. Asigna la misma cantidad de RAM en el servidor virtual que en el equipo protegido de origen.
-linuxhostname	Nombre de host del servidor VirtualBox Linux.
-hostport	Puerto del servidor VirtualBox Linux.
-targetpath	Ruta de acceso local, de red o Linux a la carpeta donde almacenarán los archivos de la máquina virtual.
-pathusername	Nombre de usuario para el equipo de red. Solo se requiere cuando especifica una ruta de red en el parámetro <code>-targetpath</code> .
-pathpassword	Contraseña para equipo de red. Solo se requiere cuando especifica una ruta de red en el parámetro <code>-targetpath</code> .
-accountusername	Opcional. Utilícelo si puede especificar una cuenta de usuario en la que registrar la máquina virtual exportada. Solo para equipo local o de red.
-accountpassword	Opcional. Utilícelo únicamente si especifica una cuenta de usuario en la que registrar la máquina virtual exportada mediante el parámetro <code>-accountusername</code> . (Solo para equipos locales o de red).

Ejemplo:

Exportar todos los volúmenes desde el último punto de recuperación del equipo 10.10.12.97 a una máquina virtual denominada NuevaVMVirtualBox:

```
>Start-VBExport -protectedserver 10.10.12.97 -vmname NewVirtualBoxVM -ram usesourceram -targetpath D:/exports
```

Start-VirtualStandby

El comando `Start-VirtualStandby` PowerShell permite forzar una exportación de datos de Rapid Recovery a una máquina virtual en espera. Esta exportación a petición se puede producir fuera de las exportaciones en espera virtual programadas de forma regular.

Uso

El uso del comando es el siguiente:

```
Start-VirtualStandby -core [host name] -user [login] -password [password] -all | -protectedserver [name(s) | IP address]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Start-VirtualStandby`:

Tabla 290. Opciones del comando Start-VirtualStandby

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-all	Forzar una exportación para todas las máquinas en espera virtual.
-protectedserver	El nombre o nombres (separados por una coma y un espacio) de los equipos protegidos que quiere forzar para exportar.

Ejemplo:

Forzar una exportación en espera virtual para un equipo protegido:

```
>Start-VirtualStandby -core 10.10.10.10:8006 -user administrator -password 23WE@#sdd -  
protectedserver 10.10.5.22
```

Start-VMExport

El comando `Start-VMExport` inicia la ejecución de una exportación virtual desde el punto de recuperación seleccionado en una máquina virtual del servidor VMWare Workstation.

Los parámetros requeridos incluyen el nombre del equipo protegido que contiene los puntos de recuperación que hay que exportar; el nombre de la máquina virtual a la que se está exportando; la cantidad de RAM que hay que asignar en la máquina virtual, y la ruta de acceso a la carpeta local o de red donde se almacenarán los archivos resultantes de la máquina virtual.

Uso

El uso del comando es el siguiente:

```
Start-VMExport -core -user [user name] -password [password] -protectedserver [machine name] or  
[IP address] -volumes [volume names] -rpn [number | numbers] |  
-time [time string] -vmname [virtual machine name] [-ram [total megabytes] |  
-usesourceram] -linuxhostname [linux hostname] -hostport [linux port] -targetpath [location]  
pathusername [user name] - pathpassword [password]
```

Opciones de comando

En la siguiente tabla se describen las opciones disponibles para el comando `Start-VMExport`:

Tabla 291. Opciones del comando Start-VMExport

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Equipo protegido con puntos de recuperación que se deben exportar.
-volumes	Opcional. Lista de nombres de volumen que deben exportarse. Si no se especifica, todos los volúmenes en los puntos de recuperación especificados se exportarán. Los valores deben estar entre comillas dobles y separados por un espacio. No utilice barras finales en nombres de volúmenes. Por ejemplo, especifique "C:" no "C:/"

Opción	Descripción
-rpn	Opcional. El número secuencial de un punto de recuperación que hay que exportar. (Puede utilizar el comando <code>Get-RecoveryPoints</code> para obtener los números de los puntos de recuperación). NOTA: Si no es especifica ni la opción 'time' ni 'rpn' en este comando, se exportará el punto de recuperación más reciente.
-time	Opcional. Determina el punto de recuperación que debe seleccionarse para la exportación. Debe especificar la hora exacta en el formato "MM/DD/AAAA hh:mm tt" (por ejemplo, "04/24/2015 09:00 AM"). Especifique los valores de hora y fecha de la zona horaria establecida en su equipo local. NOTA: Si no es especifica ni la opción 'time' ni 'rpn' en este comando, se exportará el punto de recuperación más reciente.
-vmname	Nombre de Windows de la máquina virtual.
-ram	Asigna una cantidad de RAM específica al servidor virtual.
-usesourceram	Opcional. Asigna la misma cantidad de RAM en el servidor virtual que en el equipo protegido de origen.
-targetpath	Ruta de acceso local, de red o Linux a la carpeta donde almacenarán los archivos de la máquina virtual.
-pathusername	Nombre de usuario para el equipo de red. Solo se requiere cuando especifica una ruta de red en el parámetro <code>-targetpath</code> .
-pathpassword	Contraseña para equipo de red. Solo se requiere cuando especifica una ruta de red en el parámetro <code>-targetpath</code> .
-version	Versión de VMware Tools que hay que utilizar. Las versiones válidas son: 7, 8, 9 y 10.

Ejemplo:

Exportar todos los volúmenes desde el último punto de recuperación del equipo 10.10.12.97 a una máquina virtual denominada NuevaVMVMWare:

```
>Start-VBExport -protectedserver 10.10.12.97 -vmname NewVMWareVM -ram usesourceram -targetpath D:/exports
```

Stop-ActiveJobs

El comando `Stop-ActiveJobs` cancela los trabajos activos en un equipo protegido especificado.

Uso

El uso del comando es el siguiente:

```
Stop-ActiveJobs [-protectedserver [machine name | IP address]] [-core [host name]] -user [user name] -password [password] -jobtype [jobtype]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Stop-ActiveJobs`:

Tabla 292. Opciones del comando Stop-ActiveJobs

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-all	Selecciona y cancela eventos del tipo especificado para todos los equipos protegidos.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Determina el equipo protegido en el que deben cancelarse los trabajos.
-jobtype	Opcional. Especifica el filtro del tipo de trabajo. Los valores disponibles son: 'transfer' (transferencia de datos), 'repository' (mantenimiento de repositorio), 'replication' (replicaciones locales y remotas), 'backup' (restauración y copia de seguridad), 'bootcdbuilder' (crear CD de inicio), 'diagnostics' (cargar registros), 'exchange' (comprobación de archivos de Exchange Server), 'export' (exportación de punto de recuperación), 'pushinstall' (implementar software Agent en equipos protegidos), 'rollback' (restaurar datos desde un punto de recuperación), 'rollup' (despliegues de puntos de recuperación), 'sqlattach' (comprobaciones de la conectabilidad de Agent) y 'mount' (no de repositorio). De forma predeterminada, todos los trabajos del tipo especificado se cancelan.

Ejemplo:

Detener el trabajo de transferencia en el equipo protegido:

```
>Stop-ActiveJobs -protectedserver 10.10.1.76 -jobtype transfer
```

Detener todos los trabajos para un equipo protegido específico:

```
>Stop-ActiveJobs -protectedserver 10.10.1.76 -all
```

Suspend-Replication

El comando `Suspend-Replication` permite a un administrador pausar la replicación.

Los usuarios pueden pausar las replicaciones de tres modos:

- Pausar la replicación en el Core principal para todos los equipos protegidos (`-outgoing parameter`)

El administrador debe especificar el nombre del equipo remoto emparejado con la replicación saliente para pausar la replicación saliente en el Core principal.

```
>Suspend-replication -outgoing 10.10.12.10
```

- Pausar la replicación en el Core principal para un único equipo protegido (parámetro `-protectedserver`)

```
>Suspend-replication -protectedserver 10.10.12.97
```

- Pausar la replicación en el Core de destino (`-incoming parameter`)

Si el Core local es un Core de destino, el administrador puede pausar la replicación especificando el Core de principal mediante el parámetro `-incoming` (entrante).

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Suspend-Replication`:

Tabla 293. Opciones del comando Suspend-Replication

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-all	Realiza una pausa en todos los equipos protegidos en el Core seleccionado.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-pause	[snapshots],[replication] o [vmexport].
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-protectedserver	Pausa el servidor protegido actual.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-incoming	Nombre de host del Core remoto que se replica en el equipo Core. La replicación se suspende para todos los equipos protegidos en el Core remoto.
-outgoing	Nombre de host del Core de destino remoto en el que se están replicando los datos. La replicación se suspende para todos los equipos protegidos en el Core remoto.

Ejemplo:

Pausar la replicación saliente en el Core remoto con la dirección IP: 10.10.1.15, para el único equipo protegido con la dirección IP: 10.10.1.76:

```
>Suspend-replication -core 10.10.1.15 -protectedserver 10.10.1.76
```

Pausar la replicación saliente desde el Core local al Core de destino remoto con la dirección IP: 10.10.1.63 para todos los equipos protegidos:

```
>Suspend-replication -outgoing 10.10.1.63
```

Pausar la replicación entrante desde 10.10.1.82 en el Core remoto con la dirección IP: 10.10.1.15 (El administrador puede pausar la replicación entrante solo para todo el equipo):

```
>Suspend-replication -core 10.10.1.15 -incoming 10.10.1.82
```

Suspend-RepositoryActivity

El comando `Suspend-RepositoryActivity` PowerShell permite pausar actividades para un repositorio de Rapid Recovery. Al suspender actividades, se coloca un candado en el repositorio, lo que evita que se introduzcan o se dejen datos.

Uso

El uso del comando es el siguiente:

```
Suspend-RepositoryActivity -core [host name] -user [login] -password [password] -all | -repository ["name" | "name1 " "name2"]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Suspend-RepositoryActivity`:

Tabla 294. Opciones del comando Suspend-RepositoryActivity

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-all	Suspender las actividades de todos los repositorios asociados con este Core.
-repository	El nombre del repositorio que desea bloquear. El nombre se debe poner entre comillas dobles. Puede especificar varios repositorios separados por espacios.

Ejemplos:

Suspender las actividades para varios repositorios:

```
>Suspend-RepositoryActivity -repository "repository1" "repository2"
```

Suspender las actividades en todos los repositorios:

```
>Suspend-RepositoryActivity -all
```

Suspend-ScheduledArchive

El comando `Suspend-ScheduledArchive` PowerShell permite pausar un archivo programado de Rapid Recovery. Este comando evita que se produzca el archivo como programado hasta que vuelva a activarlo..

Uso

El uso del comando es el siguiente:

```
Suspend-ScheduledArchive -core [host name] -user [login] -password [password] -all -ids [id | id1 id2]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Suspend-ScheduledArchive`:

Tabla 295. Opciones del comando `Suspend-ScheduledArchive`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-all	Pausa todas las archivaciones programadas.
-id	El número de identificación o los números separados por espacios de las archivaciones programadas que hay que suspender.

Ejemplo:

Suspender varias archivaciones programadas:

```
>Suspend-ScheduledArchive -ids 799138c8-3dfc-4398-9711-1823733c2a31, 26c29bb7-b320-47f5-b5a8-dffc49f50e25
```

Suspend-Snapshot

El comando `Suspend-Snapshot` permite a un administrador realizar una pausa en las instantáneas.

Uso

El uso del comando es el siguiente:

```
Suspend-Snapshot -core [host name] -user [user name] -password [password] -all |  
-protectedserver [name | IP address] -time [time string]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Suspend-Snapshot`:

Tabla 296. Opciones del comando `Suspend-Snapshot`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-all	Realiza una pausa en todos los equipos protegidos en el Core seleccionado.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-time	La hora, en formato 'Day-Hours-Minutes', a la que se reanudarán las instantáneas (solo para pausa de instantáneas).

Ejemplo:

Pausar las instantáneas del equipo protegido con IP 10.10.10.4 del Core local e indicar que se reanuden a una hora determinada:

```
>Suspend-Snapshot -protectedserver 10.10.10.4 -time 3-20-50
```

Suspend-VirtualStandby

El comando `Suspend-VirtualStandby` PowerShell permite pausar la exportación de datos en una máquina en espera virtual de Rapid Recovery.

Uso

El uso del comando es el siguiente:

```
Suspend-VirtualStandby -core [host name] -user [login] -password [password] -all | -  
protectedserver [name(s) | IP address]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Suspend-VirtualStandby`:

Tabla 297. Opciones del comando `Suspend-VirtualStandby`

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de inicio de sesión. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-all	Pausar las exportaciones de todas las máquinas en espera virtual.
-protectedserver	El nombre o los nombres (separados por una coma y un espacio) de los equipos protegidos con máquinas en espera virtual que quiere suspender.

Ejemplo:

Suspender las exportaciones en espera virtual de un equipo protegido:

```
>Suspend-VirtualStandby -core 10.10.10.10:8006 -user administrator -password 23WE@#sdd -protectedserver 10.10.5.22
```

Suspend-VMExport

El comando `Suspend-VMExport` permite a un administrador realizar una pausa en las exportaciones a máquinas virtuales.

Uso

```
Suspend-VMExport -core [host name] -user [user name] -password [password] -all | -protectedserver [name | IP address]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Suspend-VMExport`:

Tabla 298. Opciones del comando Suspend-VMExport

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-all	Realiza una pausa en todos los equipos protegidos en el Core seleccionado.
-protectedserver	Pausa el servidor protegido actual.

Ejemplo:

Suspender la exportación de máquina virtual para el equipo protegido con IP 10.10.10.4 para el Core local:

```
>Suspend-VMExport -protectedserver 10.10.12.25
```

Update-Repository

El comando `Update-Repository` agrega una extensión a un repositorio DVM existente. El tamaño especificado debe estar comprendido entre 250 MB y 16 TB.

Uso

```
Update-Repository -name [repository name] -size [size] [[[-datapath [datapath]
-metadatapath [metadata path]] | [-uncpath [UNC path] -shareusername [share user name] -
sharepassword [share password]]] -core [host name] -user [user name]
-password [password]
```

Opciones de comando

La siguiente tabla describe las opciones disponibles para el comando `Update-Repository`:

Tabla 299. Opciones del comando Update-Repository

Opción	Descripción
-?	Muestra el mensaje de ayuda.
-core	Opcional. Dirección IP del equipo host del Core remoto (con número de puerto opcional). De forma predeterminada, la conexión se realiza con el Core instalado en el equipo local.

Opción	Descripción
-user	Opcional. Nombre de usuario para el equipo host de Core remoto. Si especifica un nombre de usuario, también deberá proporcionar una contraseña. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-password	Opcional. Contraseña para el equipo host de Core remoto. Si especifica una contraseña, también deberá proporcionar un nombre de usuario. Si no especifica ninguno, se utilizarán las credenciales del usuario que ha iniciado sesión.
-name	Nombre del repositorio DVM.
-size	Tamaño de extensión del repositorio DVM. Las unidades disponibles son b, Kb, MB, GB, TB y PB.
-datapath	Solo para la ubicación local. Determina la ruta de acceso a los datos de la extensión del repositorio DVM.
-metadatapath	Solo para la ubicación local. Determina la ruta de acceso a los metadatos de la extensión del repositorio DVM.
-uncpath	Solo para la ubicación compartida. Determina las rutas de acceso a los datos y metadatos de la extensión del repositorio DVM.
-shareusername	Solo para la ubicación compartida. Determina el inicio de sesión para la ubicación compartida.
-sharepassword	Solo para la ubicación compartida. Determina la contraseña para la ubicación compartida.

Ejemplo:

Agregar una extensión al repositorio DVM del tamaño mínimo:

```
>Update-Repository -name Repository1 -size 250Mb -datapath C:\Repository\Data -metadatapath C:\repository\Metadata
```

Localización

Cuando se ejecuta en el mismo equipo en el que Rapid Recovery Core está instalado, el módulo PowerShell de Rapid Recovery basa su idioma de visualización en el conjunto de idiomas para el Core. Las versiones de Rapid Recovery localizadas como esta admiten inglés, chino (simplificado), francés, coreano, alemán, japonés, portugués (Brasil) y español.

Si el módulo PowerShell de Rapid Recovery está instalado en un equipo separado, el inglés es el único idioma admitido.

Calificadores

La siguiente tabla describe los calificadores disponibles para el módulo Rapid Recovery PowerShell.

Tabla 300. Calificadores del módulo Rapid Recovery PowerShell

Calificador	Uso
-core <Rapid Recovery Core Name>	Nombre del host del Core. Predeterminado: Localhost
-ProtectedServer <Protected Server Name>	Nombre de host/dirección IP de Rapid Recovery Agent. Predeterminado: Localhost si hay varios servidores protegidos; de lo contrario, el único servidor protegido.

Calificador	Uso
-Mode <READ, READWRITE, WRITE>	Modo de montaje del punto de recuperación. Predeterminado: Read.
-Volumes <Snapshot Volume Letter>	Letra de volumen de la instantánea de Rapid Recovery Agent. Predeterminado: All.
-User <User Name>	Nombre de usuario conectado al Core de Rapid Recovery. Suele ser el usuario del servicio.
-Domain <Domain Name>	Dominio al que pertenece el usuario definido en /User.
-Password <Password>	Contraseña del usuario definida en /User.
-Path <Target path to mount, dismount recovery points or archive location>	Por ejemplo: C:\RapidRecoveryMount.

Extensión de trabajos de Rapid Recovery mediante secuencias de comandos

Rapid Recovery permite a los administradores automatizar la administración y la gestión de recursos en algunas apariciones a través de la ejecución de comandos y secuencias de comandos. El software Rapid Recovery admite el uso de las secuencias de comandos de PowerShell para Windows y secuencias de comandos de Bourne Shell para Linux.

Los trabajos del Core se crean automáticamente siempre que inicia operaciones en el Core de Rapid Recovery como la replicación, la exportación virtual o una instantánea de copia de seguridad. Puede ampliar estos trabajos ejecutando una secuencia de comandos antes o después de estos. Se conocen como pre y post secuencias de comandos.

Este apéndice describe las secuencias de comandos que pueden utilizar los administradores en las apariciones indicadas en Rapid Recovery para Windows y Linux.

⚠ PRECAUCIÓN: Las secuencias de comandos de muestra de PowerShell y Bourne que proporciona este documento funcionarán cuando se ejecuten según hayan diseñado administradores cualificados. Tome precauciones al modificar secuencias de comandos que estén en uso para mantener versiones que funcionen. Cualquier modificación en las secuencias de comandos de muestra incluidas aquí, así como cualquier secuencia de comandos que cree, se consideran personalizaciones, que no están cubiertas por el servicio de asistencia de Dell.

Temas:

- [Uso de secuencias de comandos PowerShell en Rapid Recovery](#)
- [Parámetros de entrada para las secuencias de comandos de PowerShell](#)
- [Secuencias de comandos de PowerShell de prueba](#)
- [Uso de las secuencias de comandos de Bourne Shell en Rapid Recovery](#)
- [Parámetros de entrada para las secuencias de comandos de Bourne Shell](#)
- [Secuencias de comandos de muestra de Bourne Shell](#)

Uso de secuencias de comandos PowerShell en Rapid Recovery

Windows PowerShell es un entorno conectado con el framework .NET de Microsoft diseñado para automatización administrativa. Rapid Recovery incluye kits de desarrollo de software (SDK) de cliente globales para la creación de secuencias de comandos de PowerShell que permite a los usuarios administrativos ejecutar secuencias de comandos de PowerShell proporcionadas por el usuario en las apariciones indicadas; por ejemplo, antes o después de una instantánea, conectabilidad, comprobaciones de capacidad de montaje, etc. Los administradores pueden ejecutar secuencias de comandos desde el Core Rapid Recovery y desde el equipo protegido. Las secuencias de comandos pueden aceptar parámetros, y la salida de una secuencia de comandos se graba en los archivos de registro del Core y del equipo protegido.

ⓘ NOTA: Para los trabajos nocturnos, conserve un archivo de secuencia de comandos y el parámetro de entrada JobType para distinguir entre los trabajos nocturnos.

Los archivos de secuencia de comandos se encuentran en la carpeta `%ALLUSERSPROFILE%\AppRecovery\Scripts`.

- En Windows 7, la ruta de acceso para localizar la carpeta `%ALLUSERSPROFILE%` es: `C:\ProgramData`.
- En Windows 2003, la ruta de acceso para localizar la carpeta es: `Documents and Settings\All Users\Application Data\`.

NOTA: Windows PowerShell es necesario y debe instalarse y configurarse antes de ejecutar secuencias de comandos de Rapid Recovery.

Para obtener más información acerca del uso de secuencias de comandos de PowerShell, consulte [Secuencias de comandos de PowerShell de prueba](#), [Parámetros de entrada para las secuencias de comandos de PowerShell](#), [Parámetros de entrada para las secuencias de comandos de Bourne Shell](#) y [Secuencias de comandos de muestra de Bourne Shell](#).

Requisitos previos para las secuencias de comandos de PowerShell

Para poder ejecutar secuencias de comandos de PowerShell para Rapid Recovery, debe tener instalado Windows PowerShell 2.0 o posteriores. Debido a las nuevas funciones introducidas en PowerShell 3.0, que incluyen un acceso más sencillo a las propiedades de objetos, acceso Web de PowerShell, así como compatibilidad con llamadas REST, Dell recomienda el uso de PowerShell 3.0 o posterior.

NOTA: Coloque el archivo `powershell.exe.config` en el directorio de inicio de PowerShell. Por ejemplo, `C:\WindowsPowerShell\powershell.exe.config`.

powershell.exe.config

```
<?xml version="1.0"?>
<configuration>
  <startup useLegacyV2RuntimeActivationPolicy="true">
    <supportedRuntime version="v4.0.30319"/>
    <supportedRuntime version="v2.0.50727"/>
  </startup>
</configuration>
```

Prueba de las secuencias de comandos de PowerShell

Si quiere probar las secuencias de comandos que planifica ejecutar, puede hacerlo usando el editor gráfico de PowerShell, `powershell_ise`. También debe agregar el archivo de configuración, `powershell_ise.exe.config` a la misma carpeta del archivo de configuración, `powershell.exe.config`.

NOTA: El archivo de configuración, `powershell_ise.exe.config` debe tener el mismo contenido que el archivo `powershell.exe.config`.

PRECAUCIÓN: Si la secuencia de comandos previa o posterior de PowerShell falla, el trabajo también fallará.

Localización

Quando se ejecuta en el mismo equipo en el que el Core de Rapid Recovery está instalado, el módulo PowerShell de Rapid Recovery basa su idioma de visualización en el conjunto de idiomas para el Core. Las versiones de Rapid Recovery localizadas como esta que admiten inglés, chino (simplificado), francés, coreano, alemán, japonés, portugués (Brasil) y español.

Si el módulo Rapid Recovery PowerShell está instalado en un equipo separado, el inglés es el único idioma admitido.

Calificadores

La siguiente tabla describe los calificadores disponibles para el módulo Rapid Recovery PowerShell.

Tabla 301. Calificadores del módulo Rapid Recovery PowerShell

Calificador	Uso
-core <Rapid Recovery Core Name>	Nombre del host del Core. Predeterminado: Localhost
-ProtectedServer <Protected Server Name>	Nombre de host/dirección IP de Rapid Recovery Agent. Predeterminado: Localhost si hay varios servidores protegidos; de lo contrario, el único servidor protegido.
-Mode <READ, READWRITE, WRITE>	Modo de montaje del punto de recuperación. Predeterminado: Read.
-Volumes <Snapshot Volume Letter>	Letra de volumen de la instantánea de Rapid Recovery Agent. Predeterminado: All.
-User <User Name>	Nombre de usuario conectado al Core de Rapid Recovery. Suele ser el usuario del servicio.
-Domain <Domain Name>	Dominio al que pertenece el usuario definido en /User.
-Password <Password>	Contraseña del usuario definida en /User.
-Path <Target path to mount, dismount recovery points or archive location>	Por ejemplo: C:\RapidRecoveryMount.

Parámetros de entrada para las secuencias de comandos de PowerShell

Todos los parámetros de entrada se utilizan en secuencias de comandos de ejemplo. Los parámetros se describen en las tablas siguientes.

NOTA: Los archivos de secuencias de comandos deben tener el mismo nombre que los archivos de secuencias de comandos de ejemplo.

AgentProtectionStorageConfiguration (espacio de nombres Replay.Common.Contracts.Agents)

La siguiente tabla presenta los objetos disponibles para el parámetro AgentProtectionStorageConfiguration.

Tabla 302. Objetos para el parámetro de AgentProtectionStorageConfiguration

Método	Descripción
public Guid RepositoryId { get; set; }	Obtiene o establece la Id. del repositorio en el que se almacenan los puntos de recuperación del Agent.
public string EncryptionKeyId { get; set; }	Obtiene o establece la Id. de la clave de cifrado para los puntos de recuperación de este Agent. Una cadena vacía indica que no hay cifrado.

AgentTransferConfiguration (espacio de nombres Replay.Common.Contracts.Transfer)

La siguiente tabla presenta los objetos disponibles para el parámetro AgentTransferConfiguration.

Tabla 303. Objetos para el parámetro de AgentTransferConfiguration

Método	Descripción
public uint MaxConcurrentStreams { get; set; }	Obtiene o establece el número máximo de conexión TCP simultáneas que el Core establece para el Agent, para la transferencia de datos.
public uint MaxTransferQueueDepth { get; set; }	Obtiene o establece el número máximo de extensiones de bloques que se pueden poner en cola para la escritura. Cuando se lee un rango de bloques desde una secuencia de transferencia, el rango se coloca en una cola productor o consumidor en la que la hebra de consumidor lee y escribe en el objeto epoch (época). Si el repositorio escribe más lento de lo que la red es capaz de leer, esta cola se llena. El punto en el que la cola esté llena y la lectura se detenga, es la profundidad máxima de cola de transferencia.
public uint MaxConcurrentWrites { get; set; }	Obtiene o establece el número máximo de operaciones pendientes de escritura de bloques en una época en un momento dado. Si los bloques adicionales se reciben por encima del número máximo de operaciones de escritura especificadas en este parámetro, dichos bloques adicionales se ignoran hasta que terminen las escrituras pendientes.
public ulong MaxSegmentSize { get; set; }	Obtiene o establece el número máximo de bloques contiguos para la transferencia en una única solicitud. Según las pruebas que se realicen, los valores óptimos podrían ser más altos o más bajos.
public Priority Priority { get; set; }	Obtiene o establece la prioridad para la solicitud de transferencia.
public uint GetChangedBlocksRetries { get; set; }	Obtiene o establece el recuento de reintentos si la recuperación inicial de los bloques cambiados desde el agente ha fallado.
public int MaxRetries { get; set; }	Obtiene o establece el número máximo de veces que una transferencia errónea se debería intentar, antes de considerarla como incorrecta.
public bool UseDefaultMaxRetries { get; set; }	Si está incluido, se utilizará el número máximo predeterminado de reintentos (que se especifica en la configuración de transferencia).
public Guid ProviderId { get; set; }	Obtiene o establece el GUID del proveedor de VSS a usar para las instantáneas en este host. Normalmente, los administradores aceptan el valor predeterminado.
public Collection<ExcludedWriter> ExcludedWriterIds { get; set; }	Obtiene o establece el conjunto de las Id. de escritor de VSS que se deberán excluir de esta instantánea. La Id. se determina por el nombre del escritor. Este nombre es solo por motivos de documentación y no es necesario proporcionar una coincidencia exacta con el nombre real del escritor.

Método	Descripción
public ushort TransferDataServerPort { get; set; }	Obtiene o establece un valor que contiene el puerto TCP sobre el que aceptar conexiones desde el Core para la transferencia real de los datos desde el equipo protegido hasta el Core. El Agente intenta escuchar en este puerto, pero si el puerto está en uso, el equipo protegido puede utilizar en su lugar un puerto distinto. El Core deberá utilizar el número de puerto especificado en las propiedades BlockHashesUri y BlockDataUri del objeto VolumeSnapshotInfo para cada volumen de retén.
public TimeSpan CleanSnapshotTimeout { get; set; }	Obtiene o establece el tiempo de espera para la limpieza de la instantánea después de que finalice la transferencia.
public TimeSpan SnapshotTimeout { get; set; }	Obtiene o establece el tiempo de espera para que se complete una operación de instantánea de VSS, antes de abandonar y considerar que ha superado el tiempo de espera máximo.
public TimeSpan TransferTimeout { get; set; }	Obtiene o establece el tiempo de espera para contacto posterior desde el Core antes de abandonar la instantánea.
public TimeSpan NetworkReadTimeout { get; set; }	Obtiene o establece el tiempo de espera para las operaciones de lectura de red relacionadas con esta transferencia.
public TimeSpan NetworkWriteTimeout { get; set; }	Obtiene o establece el tiempo de espera para las operaciones de escritura de red relacionadas con esta transferencia.
public uint InitialQueueSize { get; set; }	Obtiene o establece un tamaño de cola inicial o solicitudes.
public uint MinVolumeFreeSpacePercents { get; set; }	Obtiene o establece una cantidad mínima de espacio libre en un volumen medido en porcentaje. Si el espacio libre es menor que la cantidad especificada en este parámetro, se eliminan todos los registros de cambio y se fuerza una imagen de base.
public uint MaxChangeLogsSizePercents { get; set; }	Obtiene o establece un tamaño máximo de registros de cambio del controlador como parte de la capacidad de volumen medido en porcentaje. Si parte de los registros de cambio son mayores que este valor, se eliminan todos los registros de cambio y se fuerza una imagen de base.
public bool EnableVerification { get; set; }	Obtiene o establece un valor indicando si se ha realizado la verificación del diagnóstico de cada bloque enviado al Core.

BackgroundJobRequest (espacio de nombres Replay.Core.Contracts.BackgroundJobs)

La siguiente tabla presenta los objetos disponibles para el parámetro BackgroundJobRequest.

Tabla 304. Objetos para el parámetro de BackgroundJobRequest

Método	Descripción
public AgentIdsCollection AgentIds { get; set; }	Obtiene o establece la Id. de los equipos protegidos.
public bool IsNightlyJob { get; set; }	Obtiene o establece el valor indicando si el trabajo de fondo es un trabajo nocturno.
public Guid NightlyJobTransactionId { get; set; }	Obtiene o establece la Id. de la transacción de trabajos nocturnos.
public Guid JobId { get; set; }	Obtiene o establece la Id. del trabajo en segundo plano.
public bool Force { get; set; }	Obtiene o establece el valor que indica si un trabajo se ha forzado o no.

Método	Descripción
public uint JobStartsCount { get; set; }	Obtiene o establece el número de intentos para iniciar un trabajo.
public virtual bool InvolvesAgentId(Guid agentId)	Determine el valor indicando si el Agent concreto está implicado en un trabajo.

ChecksumCheckJobRequest (espacio de nombres Replay.Core.Contracts.Exchange.ChecksumChecks)

Hereda sus valores del parámetro, DatabaseCheckJobRequestBase.

DatabaseCheckJobRequestBase (espacio de nombres Replay.Core.Contracts.Exchange)

Hereda sus valores del parámetro, BackgroundJobRequest.

Tabla 305. Objetos para el parámetro de DatabaseCheckJobRequestBase

Método	Descripción
public string RecoveryPointId { get; set; }	Obtiene o establece la Id. del punto de recuperación para la que se comprobarán las bases de datos.

ExportJobRequest (espacio de nombres Replay.Core.Contracts.Export)

Hereda sus valores del parámetro, BackgroundJobRequest.

La siguiente tabla presenta los objetos disponibles para el parámetro ExportJobRequest.

Tabla 306. Objetos para el parámetro de ExportJobRequest

Método	Descripción
public uint RamInMegabytes { get; set; }	Obtiene o establece el tamaño de memoria para la VM exportada. Establecer en cero (0) para utilizar el tamaño de memoria del equipo de origen.
public ushort CpuCount { get; set; }	Obtiene o establece el número de CPU para la VM exportada. Establecer en 0 para utilizar el número de CPU del equipo de origen.
public ushort CoresPerCpu { get; set; }	Obtiene o establece los Cores por número de CPU para la VM exportada. Establecer en 0 para utilizar los Cores por número de CPU del equipo de origen.
public VirtualMachineLocation Location { get; set; }	Obtiene o establece la ubicación de destino para esta exportación. Es una clase base abstracta.
public VolumeImageIdsCollection VolumeImageIds { get; private set; }	Obtiene o establece las imágenes de volumen a incluir en la exportación de la VM.
public ExportJobPriority Priority { get; set; }	Obtiene o establece la prioridad para la solicitud de exportación.

NightlyAttachabilityJobRequest (espacio de nombres Replay.Core.Contracts.Sql)

Hereda sus valores del parámetro, BackgroundJobRequest.

Tabla 307. Objetos para el parámetro de NightlyAttachabilityJobRequest

Método	Descripción
public int SimultaneousJobsCount { get; set; }	Obtiene o establece el número de trabajos que se pueden ejecutar simultáneamente.

RollupJobRequest (espacio de nombres Replay.Core.Contracts.Rollup)

Hereda sus valores del parámetro, BackgroundJobRequest.

TakeSnapshotResponse (espacio de nombres Replay.Agent.Contracts.Transfer)

La siguiente tabla presenta los objetos disponibles para el parámetro TakeSnapshotResponse.

Tabla 308. Objetos para el parámetro de TakeSnapshotResponse

Método	Descripción
public Guid SnapshotSetId { get; set; }	Obtiene o establece el GUID asignado por VSS a esta instantánea.
public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }	Obtiene o establece la recopilación de información de instantánea para cada volumen incluido en el retén.

TransferJobRequest (espacio de nombres Replay.Core.Contracts.Transfer)

Hereda sus valores del parámetro, BackgroundJobRequest.

La siguiente tabla presenta los objetos disponibles para el parámetro TransferJobRequest.

Tabla 309. Objetos para el parámetro de TransferJobRequest

Método	Descripción
public VolumeNameCollection VolumeNames { get; set; }	Obtiene o establece la recopilación de los nombres para transferencia.

Método	Descripción
	VolumeNames es una estructura de datos que contiene los siguientes datos: • GuidName. La guía asociada con el volumen, utilizada como el nombre si no se establece un DisplayName. • DisplayName. El nombre del volumen que aparece.
public VolumeNameCollection TransferredVolumes { get; set; }	Obtiene o establece la recopilación de los volúmenes transferidos.
public VolumeNameCollection DependentVolumeNames { get; set; }	Obtiene o establece la recopilación de los volúmenes dependientes.
public QuotaSettingsCollection EnabledDiskQuotas { get; set; }	Obtiene o establece las cuotas que se han activado en un volumen.
public ShadowCopyType ShadowCopyType { get }	Obtiene el tipo de copia para transferencia. Los valores disponibles son: • Copiar • Completo
public AgentTransferConfiguration TransferConfiguration { get; set; }	Obtiene o establece la configuración de transferencia. AgentTransferConfiguration es un objeto que incluirá los siguientes datos: • MaxConcurrentStreams. El número máximo de conexión TCP simultáneas que el Core establecerá para el Agent, para la transferencia de datos. • MaxTransferQueueDepth. El número máximo de extensiones de bloques que se pueden poner en cola para la escritura • MaxConcurrentWrites. El número máximo de operaciones pendientes de escritura de bloques en una época en un momento dado. Si los bloques adicionales se reciben cuando queda pendiente esta cantidad de bloques de escritura, dichos bloques adicionales se ignorarán hasta que se escriban los bloques pendientes. • MaxSegmentSize. El número máximo de bloques contiguos para la transferencia en una única solicitud. • Priority. Un objeto que tendrá los siguientes datos: • Sin definir • Uno • Dos • Tres • Cuatro • Cinco • Seis • Siete • Ocho • Nueve • Diez • Más alto (que es igual a Uno) • Más bajo (que es igual a Diez) • Predeterminado (que es igual a Cinco) • MaxRetries. El número máximo de veces que una transferencia errónea se debería intentar, antes de considerarla como incorrecta. • UseDefaultMaxRetries. Un valor indicando que el número máximo de reintentos es el valor predeterminado. • ProviderId. El GUID del proveedor de VSS a usar para las instantáneas en este host. Los usuarios utilizan normalmente la configuración predeterminada.

Método	Descripción
public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }	Obtiene o establece la configuración de almacenamiento.
public string Key { get; set; }	Genera una clave pseudoaleatoria (aunque no criptográficamente segura) que se puede utilizar como contraseña de un solo uso para autenticar solicitudes de transferencia.
public bool IsBaseImage { get; set; }	Obtiene o establece el valor que indica si se tomará la imagen base.
public bool IsForced { get; set; }	Obtiene o establece el valor que indica si se ha forzado la transferencia.
public Guid ProtectionGroupId { get; set; }	Obtiene o establece la Id. del grupo de protección.
public TargetComponentTypes LogTruncationTargets { get; set; }	Obtiene o establece el valor que indica para qué bases de datos el truncamiento del registro se llevará a cabo (SQL o Exchange).
public bool ForceBaseImage { get }	Obtiene el valor que indica si la imagen base se ha forzado o no.
public bool IsLogTruncation { get }	Obtiene el valor que indica si el trabajo de truncamiento del registro se está realizando o no.

TransferPrescriptParameter (espacio de nombres Replay.Common.Contracts.PowerShellExecution)

Hereda sus valores del parámetro TransferScriptParameterBase.

TransferPostscriptParameter (espacio de nombres Replay.Common.Contracts.PowerShellExecution)

La siguiente tabla presenta los objetos disponibles para el parámetro TransferPostscript. Hereda sus valores del parámetro TransferScriptParameterBase.

Tabla 310. Objetos para el parámetro de TransferPostscript

Método	Descripción
public VolumeNameCollection VolumeNames { get; set; }	Obtiene o establece la recopilación de los nombres de volumen para transferencia. VolumeNames es una estructura de datos que contiene los siguientes datos: - GuidName. La guía asociada con el volumen, utilizada como el nombre si no se establece un DisplayName. - DisplayName. El nombre del volumen que aparece.
public ShadowCopyType ShadowCopyType { get; set; }	Obtiene o establece el tipo de copia para transferir. ShadowCopyType es una enumeración con valores. Los valores disponibles son: - Desconocido - Copiar - Completo
public AgentProtectionStorageConfigurationCom mon StorageConfiguration { get; set; }	Obtiene o establece la configuración de almacenamiento.

Método	Descripción
<pre>public AgentTransferConfiguration TransferConfiguration { get; set; }</pre>	Obtiene o establece la configuración de transferencia. AgentTransferConfiguration es un objeto que incluirá los siguientes datos: • MaxConcurrentStreams. El número máximo de conexión TCP simultáneas que el Core establecerá para el Agent, para la transferencia de datos. • MaxTransferQueueDepth. El número máximo de extensiones de bloques que se pueden poner en cola para la escritura • MaxConcurrentWrites. El número máximo de operaciones pendientes de escritura de bloques en una época en un momento dado. Si los bloques adicionales se reciben cuando queda pendiente esta cantidad de bloques de escritura, dichos bloques adicionales se ignorarán hasta que se escriban los bloques pendientes. • MaxSegmentSize. El número máximo de bloques contiguos para la transferencia en una única solicitud. • Priority. Un objeto que tiene los siguientes datos: • "Sin definir • "Uno • "Dos • "Tres • "Cuatro • "Cinco • "Seis • "Siete • "Ocho • "Nueve • "Diez • "Más alto (que es igual a Uno) • "Más bajo (que es igual a Diez) • "Predeterminado (que es igual a Cinco) • MaxRetries. El número máximo de veces que una transferencia errónea se debería intentar, antes de considerarla como incorrecta. • UseDefaultMaxRetries. Un valor indicando que el número máximo de reintentos es el valor predeterminado. • ProviderId. El GUID del proveedor de VSS a usar para las instantáneas en este host. Normalmente, los administradores aceptan el valor predeterminado.
<pre>public AgentTransferConfiguration TransferConfiguration { get; set; } (cont.)</pre>	• ExcludedWriterIds. Conjunto de los Id. de escritor de VSS que se deberán excluir de esta instantánea. El Id. está codificado por el nombre del escritor. Este nombre es sólo por motivos de documentación, y no es necesario que coincida exactamente con el nombre real del escritor. • TransferDataServerPort. Un valor que contiene el puerto TCP sobre el que aceptar conexiones desde el Core para la transferencia real de los datos desde el Agent hasta el Core. • SnapshotTimeout. El tiempo de espera para que se complete una operación de instantánea de VSS, antes de abandonar y considerar que ha superado el tiempo de espera máximo. • TransferTimeout. El tiempo de espera para contacto posterior desde el Core antes de abandonar la instantánea. • NetworkReadTimeout. El tiempo de espera para las operaciones de lectura de red relacionadas con esta transferencia. • NetworkWriteTimeout. El tiempo de espera para las operaciones de escritura de red relacionadas con esta transferencia. • InitialQueueSize. Un tamaño de cola inicial de solicitudes. • MinVolumeFreeSpacePercents. Una cantidad mínima de espacio libre en un volumen en porcentaje. • MaxChangeLogsSizePercents. Un tamaño máximo de registros de cambio del controlador como parte de la capacidad de volumen medida en porcentaje.

Método	Descripción
	· EnableVerification. Un valor indicando si se ha realizado la verificación del diagnóstico de cada bloque enviada al Core.
public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }	Obtiene o establece la configuración de almacenamiento. El objeto AgentProtectionStorageConfiguration contiene los siguientes datos: · RepositoryId. El nombre del repositorio donde se almacenarán los puntos de recuperación de este Agent · EncryptionKeyId. El Id. de la clave de cifrado para los puntos de recuperación de este Agent. Una cadena vacía indica que no hay cifrado.
public string Key { get; set; }	El método clave genera una clave pseudoaleatoria (aunque no criptográficamente segura) que se puede utilizar como contraseña de un solo uso para autenticar solicitudes de transferencia.
public bool ForceBaseImage { get; set; }	Obtiene o establece el valor que indica si la transferencia era una captura de imagen base forzada.
public bool IsLogTruncation { get; set; }	Obtiene o establece el valor que indica si se ha truncado el registro.
public uint LatestEpochSeenByCore { get; set; }	Obtiene o establece el valor de época más reciente. El método LatestEpochSeenByCore es el número ordinal de la instantánea tomada más recientemente por el Core. Este es el 'número de tiempo' asignado por el controlador del filtro a esta instantánea concreta en el momento en que se tomó con VSS.
public Guid SnapshotSetId { get; set; }	Obtiene o establece el GUID asignado por VSS a esta instantánea.
public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }	Obtiene o establece la recopilación de información de instantánea para cada volumen incluido en la instantánea.

TransferScriptParameterBase (namespace Replay.Common.Contracts.PowerShellExecution)

La siguiente tabla presenta los objetos disponibles para el parámetro TransferScriptParameterBase.

Tabla 311. Objetos para el parámetro de TransferScriptParameterBase

Método	Descripción
public AgentTransferConfiguration TransferConfiguration { get; set; }	Obtiene o establece la configuración de transferencia.
public AgentProtectionStorageConfigurationCommon StorageConfiguration { get; set; }	Obtiene o establece la configuración de almacenamiento.

VirtualMachineLocation (espacio de nombres Replay.Common.Contracts.Virtualization)

La siguiente tabla presenta los objetos disponibles para el parámetro VirtualMachineLocation.

Tabla 312. Objetos para el parámetro de VirtualMachineLocation

Método	Descripción
public string Description { get; set;}	Obtiene o establece una descripción de esta ubicación que el usuario puede entender.
public string Name { get; set;}	Obtiene o establece el nombre de la VM.

VolumelimgeldsCollection (espacio de nombres Replay.Core.Contracts.RecoveryPoints)

Hereda su valor del parámetro, System.Collections.ObjectModel.Collection<string>.

VolumeName (espacio de nombres Replay.Common.Contracts.Metadata.Storage)

La siguiente tabla presenta los objetos disponibles para el parámetro VolumeName.

Tabla 313. Objetos para el parámetro de VolumeName

Método	Descripción
public string GuidName { get; set;}	Obtiene o establece la Id. del volumen.
public string DisplayName { get; set;}	Obtiene o establece el nombre del volumen.
public string UrlEncode()	Obtiene una versión codificada de URL del nombre que se puede pasar de forma limpia en un URL.
NOTA: Hay un problema conocido en WCF de .NET 4.0 (https://connect.microsoft.com/VisualStudio/feedback/ViewFeedback.aspx?FeedbackID=413312), que impide que los caracteres de escape de la ruta de acceso funcionen correctamente en una plantilla de URI. Como un nombre de volumen contiene los caracteres '\ ' y '?', debe reemplazar los caracteres especiales '\ ' y '? ' por otros caracteres especiales.	
public string GetMountName()	Devuelve un nombre para este volumen, que es válido para montar la imagen del volumen en la misma carpeta.

VolumeNameCollection (espacio de nombres Replay.Common.Contracts.Metadata.Storage)

Hereda su valor del parámetro, System.Collections.ObjectModel.Collection<VolumeName>.

La siguiente tabla presenta los objetos disponibles para el parámetro VolumeNameCollection.

Tabla 314. Objetos para el parámetro de VolumeNameCollection

Método	Descripción
public override bool Equals(object obj)	Determina si la instancia y un objeto especificado, que también debe ser un objeto VolumeNameCollection, tienen el mismo valor. (Overrides Object.Equals(Object).)
public override int GetHashCode()	Devuelve el código hash para esta VolumeNameCollection. (Overrides Object.GetHashCode().)

VolumeSnapshotInfo (namespace Replay.Common.Contracts.Transfer)

La siguiente tabla presenta los objetos disponibles para el parámetro VolumeSnapshotInfo.

Tabla 315. Objetos para el parámetro de VolumeSnapshotInfo

Método	Descripción
public Uri BlockHashesUri { get; set; }	Obtiene o establece el URI en el que los fragmentos (hash) MD5 de los bloques de volumen se pueden leer.
public Uri BlockDataUri { get; set; }	Obtiene o establece el URI en el que los bloques de datos de volumen se pueden leer.

VolumeSnapshotInfoDictionary (espacio de nombres Replay.Common.Contracts.Transfer)

Hereda sus valores del parámetro, System.Collections.Generic.Dictionary<VolumeName, VolumeSnapshotInfo>.

Secuencias de comandos de PowerShell de prueba

Las secuencias de comandos de ejemplo siguientes se proporcionan para ayudar a los usuarios administrativos en la ejecución de dichas secuencias de PowerShell.

Vínculos relacionados

[PreTransferScript.sh](#)
[PostTransferScript.ps1](#)
[PreExportScript.ps1](#)
[PostExportScript.ps1](#)
[PreNightlyJobScript.ps1](#)
[PostNightlyJobScript.ps1](#)

PreTransferScript.ps1

PreTransferScript se ejecuta en el equipo protegido antes de transferir una instantánea.

Sample PreTransferScript

```
# receiving parameter from transfer job
param([object]$TransferPrescriptParameter)
```

```
# building path to Agent's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Agent 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
# Converting input parameter into specific object
$TransferPrescriptParameterObject = $TransferPrescriptParameter -as
[Replay.Common.Contracts.PowerShellExecution.TransferPrescriptParameter];
# Working with input object. All echo's are logged
if($TransferPrescriptParameterObject -eq $null) {
    echo 'TransferPrescriptParameterObject parameter is null'
}
else {
    echo 'TransferConfiguration:' $TransferPrescriptParameterObject.TransferConfiguration
    echo 'StorageConfiguration:' $TransferPrescriptParameterObject.StorageConfiguration
}
```

PostTransferScript.ps1

PostTransferScript se ejecuta en el equipo protegido después de transferir una instantánea.

Sample PostTransferScript

```
# receiving parameter from transfer job
param([object] $TransferPostscriptParameter)
# building path to Agent's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Agent 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
# Converting input parameter into specific object
$TransferPostscriptParameterObject = $TransferPostscriptParameter -as
[Replay.Common.Contracts.PowerShellExecution.TransferPostscriptParameter];
# Working with input object. All echo's are logged
if($TransferPostscriptParameterObject -eq $null) {
    echo 'TransferPostscriptParameterObject parameter is null'
}
else {
    echo 'VolumeNames:' $TransferPostscriptParameterObject.VolumeNames
    echo 'ShadowCopyType:' $TransferPostscriptParameterObject.ShadowCopyType
    echo 'ForceBaseImage:' $TransferPostscriptParameterObject.ForceBaseImage
    echo 'IsLogTruncation:' $TransferPostscriptParameterObject.IsLogTruncation
}
```

PreExportScript.ps1

PreExportScript se ejecuta en el Core antes de cualquier trabajo de exportación.

Sample PreExportScript

```
# receiving parameter from export job
param([object]$ExportJobRequest)
# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
```

```
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
# Converting input parameter into specific object
$ExportJobRequestObject = $ExportJobRequest -as [Replay.Core.Contracts.Export.ExportJobRequest]
# Working with input object. All echo's are logged
if($ExportJobRequestObject -eq $null) {
    echo 'ExportJobRequestObject parameter is null'
}
else {
    echo 'Location:' $ExportJobRequestObject.Location
    echo 'Priority:' $ExportJobRequestObject.Priority
}
```

PostExportScript.ps1

PostExportScript se ejecuta en el Core después de cualquier trabajo de exportación.

NOTA: No hay parámetros de entrada para PostExportScript cuando se utiliza para su ejecución una vez en el equipo protegido exportado tras el arranque inicial. El equipo protegido normal debería tener esta secuencia de comandos en una carpeta de secuencias de comandos de PowerShell como PostExportScript.ps1.

Sample PostExportScript

```
# receiving parameter from export job
param([object]$ExportJobRequest)
# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
$regVal2 = $regLM.GetValue('InstallLocation')
$regVal2 = $regVal2 + 'CoreService\Common.Contracts.dll'
# Converting input parameter into specific object
$ExportJobRequestObject = $ExportJobRequest -as [Replay.Core.Contracts.Export.ExportJobRequest]
# Working with input object. All echo's are logged
if($ExportJobRequestObject -eq $null) {
    echo 'ExportJobRequestObject parameter is null'
}
else {
    echo 'VolumeImageIds:' $ExportJobRequestObject.VolumeImageIds
    echo 'RamInMegabytes:' $ExportJobRequestObject.RamInMegabytes
}
```

PreNightlyJobScript.ps1

PreNightlyJobScript se ejecuta antes de cada trabajo nocturno, en el lado del Core. Contiene el parámetro \$JobClassName, que ayuda a administrar los trabajos secundarios de forma separada.

Sample PreNightlyJobScript

```
# receiving parameters from Nightlyjob
param([System.String]$JobClassMethod, [object]$NightlyAttachabilityJobRequest, [object]
$RollupJobRequest, [object]$Agents, [object]$ChecksumCheckJobRequest, [object]
$TransferJobRequest, [int]$LatestEpochSeenByCore)
```

```

# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
# Nightlyjob has four child jobs: NightlyAttachability Job, Rollup Job, Checksum Check Job and
Log Truncation Job. All of them are triggering the script, and $JobClassMethod (contain job
name that calls the script) helps to handle those child jobs separately
switch ($JobClassMethod) {
# working with NightlyAttachability Job
    NightlyAttachabilityJob {
        $NightlyAttachabilityJobRequestObject = $NightlyAttachabilityJobRequest -as
[Replay.Core.Contracts.Sql.NightlyAttachabilityJobRequest];
        echo 'Nightly Attachability job results: ';
        if($NightlyAttachabilityJobRequestObject -eq $null) {
            echo 'NightlyAttachabilityJobRequestObject parameter is null';
        }
        else {
            echo 'AgentIds:' $NightlyAttachabilityJobRequestObject.AgentIds;
            echo 'IsNightlyJob:' $NightlyAttachabilityJobRequestObject.IsNightlyJob;
        }
        break;
    }
# working with Rollup Job
    RollupJob {
        $RollupJobRequestObject = $RollupJobRequest -as
[Replay.Core.Contracts.Rollup.RollupJobRequest];
        echo 'Rollup job results: ';
        if($RollupJobRequestObject -eq $null) {
            echo 'RollupJobRequestObject parameter is null';
        }
        else {
            echo 'SimultaneousJobsCount:' $RollupJobRequestObject.SimultaneousJobsCount;
            echo 'AgentIds:' $RollupJobRequestObject.AgentIds;
            echo 'IsNightlyJob:' $RollupJobRequestObject.IsNightlyJob;
        }
        $AgentsCollection = $Agents -as "System.Collections.Generic.List`1[System.Guid]"
        if($AgentsCollection -eq $null) {
            echo 'AgentsCollection parameter is null';
        }
        else {
            echo 'Agents GUIDs:'
            foreach ($a in $AgentsCollection) {
                echo $a
            }
        }
        break;
    }
# working with Checksum Check Job
    ChecksumCheckJob {
        $ChecksumCheckJobRequestObject = $ChecksumCheckJobRequest -as
[Replay.Core.Contracts.Exchange.ChecksumChecks.ChecksumCheckJobRequest];
        echo 'Exchange checksumcheck job results: ';
        if($ChecksumCheckJobRequestObject -eq $null) {
            echo 'ChecksumCheckJobRequestObject parameter is null';
        }
        else {
            echo 'RecoveryPointId:' $ChecksumCheckJobRequestObject.RecoveryPointId;
            echo 'AgentIds:' $ChecksumCheckJobRequestObject.AgentIds;
            echo 'IsNightlyJob:' $ChecksumCheckJobRequestObject.IsNightlyJob;
        }
        break;
    }
# working with Log Truncation Job
    TransferJob {
        $TransferJobRequestObject = $TransferJobRequest -as
[Replay.Core.Contracts.Transfer.TransferJobRequest];

```



```

echo 'Transfer job results: ';
if($TransferJobRequestObject -eq $null) {
    echo 'TransferJobRequestObject parameter is null';
}
else {
    echo 'TransferConfiguration:' $TransferJobRequestObject.TransferConfiguration;
    echo 'StorageConfiguration:' $TransferJobRequestObject.StorageConfiguration;
}
echo 'LatestEpochSeenByCore:' $LatestEpochSeenByCore;
break;
}
}

```

PostNightlyJobScript.ps1

PostNightlyJobScript se ejecuta después de cada trabajo nocturno en el Core. Contiene el parámetro \$JobClassName, que ayuda a administrar los trabajos secundarios de forma separada.

Sample PostNightlyJobScript

```

# receiving parameters from Nightlyjob
param([System.String]$JobClassMethod , [object]$NightlyAttachabilityJobRequest, [object]
$RollupJobRequest, [object]$Agents, [object]$ChecksumCheckJobRequest, [object]
$TransferJobRequest, [int]$LatestEpochSeenByCore, [object]$TakeSnapshotResponse)
# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
$regVal2 = $regLM.GetValue('InstallLocation')
$regVal2 = $regVal2 + 'CoreService\Core.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal2) | out-null
# Nightlyjob has four child jobs: NightlyAttachability Job, Rollup Job, Checksum Check Job and
Log Truncation Job. All of them are triggering the script, and $JobClassMethod (contain job
name that calls the script) helps to handle those child jobs separately
switch ($JobClassMethod) {
# working with NightlyAttachability Job
    NightlyAttachabilityJob {
        $NightlyAttachabilityJobRequestObject = $NightlyAttachabilityJobRequest -as
[Replay.Core.Contracts.Sql.NightlyAttachabilityJobRequest];
        echo 'Nightly Attachability job results: ';
        if($NightlyAttachabilityJobRequestObject -eq $null) {
            echo 'NightlyAttachabilityJobRequestObject parameter is null';
        }
        else {
            echo 'AgentIds:' $NightlyAttachabilityJobRequestObject.AgentIds;
            echo 'IsNightlyJob:' $NightlyAttachabilityJobRequestObject.IsNightlyJob;
        }
        break;
    }
# working with Rollup Job
    RollupJob {
        $RollupJobRequestObject = $RollupJobRequest -as
[Replay.Core.Contracts.Rollup.RollupJobRequest];
        echo 'Rollup job results: ';
        if($RollupJobRequestObject -eq $null) {
            echo 'RollupJobRequestObject parameter is null';
        }
        else {
            echo 'AgentIds:' $RollupJobRequestObject.AgentIds;
            echo 'IsNightlyJob:' $RollupJobRequestObject.IsNightlyJob;
        }
    }
}

```

```

$AgentsCollection = $Agents -as "System.Collections.Generic.List`1[System.Guid]"
if($AgentsCollection -eq $null) {
    echo 'AgentsCollection parameter is null';
}
else {
    echo 'Agents GUIDs:'
    foreach ($a in $AgentsCollection) {
        echo $a
    }
    break;
}
}
# working with Checksum Check Job
ChecksumCheckJob {
    $ChecksumCheckJobRequestObject = $ChecksumCheckJobRequest -as
[Replay.Core.Contracts.Exchange.ChecksumChecks.ChecksumCheckJobRequest];
    echo 'Exchange checksumcheck job results: ';
    if($ChecksumCheckJobRequestObject -eq $null) {
        echo 'ChecksumCheckJobRequestObject parameter is null';
    }
    else {
        echo 'RecoveryPointId:' $ChecksumCheckJobRequestObject.RecoveryPointId;
        echo 'AgentIds:' $ChecksumCheckJobRequestObject.AgentIds;
        echo 'IsNightlyJob:' $ChecksumCheckJobRequestObject.IsNightlyJob;
    }
    break;
}
# working with Log Truncation Job
TransferJob {
    $TransferJobRequestObject = $TransferJobRequest -as
[Replay.Core.Contracts.Transfer.TransferJobRequest];
    echo 'Transfer job results: ';
    if($TransferJobRequestObject -eq $null) {
        echo 'TransferJobRequestObject parameter is null';
    }
    else {
        echo 'TransferConfiguration:' $TransferJobRequestObject.TransferConfiguration;
        echo 'StorageConfiguration:' $TransferJobRequestObject.StorageConfiguration;
    }
    echo 'LatestEpochSeenByCore:' $LatestEpochSeenByCore;
    $TakeSnapshotResponseObject = $TakeSnapshotResponse -as
[Replay.Agent.Contracts.Transfer.TakeSnapshotResponse];
    if($TakeSnapshotResponseObject -eq $null) {
        echo 'TakeSnapshotResponseObject parameter is null';
    }
    else {
        echo 'ID of this transfer session:' $TakeSnapshotResponseObject.SnapshotSetId;
        echo 'Volumes:' $TakeSnapshotResponseObject.VolumeSnapshots;
    }
    break;
}
}
}

```

Uso de las secuencias de comandos de Bourne Shell en Rapid Recovery

El shell Bourne (sh) es un lenguaje de shell o un intérprete de línea de comandos para sistemas operativos basados en Unix. Bourne Shell se utiliza en Rapid Recovery con Linux para personalizar entornos y especificar que se produzcan ciertas operaciones en una secuencia predeterminada. .sh es la extensión de archivo y la convención de asignación de nombres para los archivos Bourne shell.

Bourne Again Shell (BASH) es un lenguaje de shell parecido que implementa la misma gramática, parámetros y ampliación de variables, redireccionamiento y citado. BASH también utiliza la misma extensión de archivo .sh. La información que aquí aparece también se aplica del mismo modo a BASH.

Utilizando los ganchos de exportación y transferencia previa y posterior, puede realizar operaciones del sistema antes y después de una transferencia o exportación. Por ejemplo, es posible que desee desactivar un cronjob mientras se produce una transferencia y activarlo una vez acabada la transferencia. Como ejemplo adicional, es posible que necesite ejecutar comandos para limpiar datos específicos de aplicaciones del disco. El contenido se escribe en un archivo temporal y se ejecuta utilizando `exec`. La secuencia de comandos se ejecuta utilizando el intérprete definido en la primera línea de la secuencia de comandos, por ejemplo, `(#!/usr/bin/env bash)`. Si el intérprete especificado no está disponible, la secuencia de comandos utiliza el shell predeterminado definido en la variable de entorno `$SHELL`.

Puede sustituir y utilizar cualquier intérprete. Por ejemplo, en la línea `# !` de la secuencia de comandos, puede sustituir `"bash"` por `"zsh"` (shell Z), `"tcsh"` (shell tee), etcétera, basándose en su preferencia.

Puede agregar objetos disponibles desde el parámetro `TransferPrescript` o agregar sus propios comandos a las secuencias de comandos `PreTransferScript.sh` y `PostTransfer.sh` para personalizarlas.

Este apéndice describe las secuencias de comandos que se pueden utilizar por los administradores en las apariciones indicadas en Rapid Recovery para Windows y Linux. Incluye los siguientes temas:

- [Parámetros de entrada para las secuencias de comandos de Bourne Shell](#)
- [Secuencias de comandos de muestra de Bourne Shell](#)

Requisitos previos para las secuencias de comandos de Bourne Shell

Rapid Recovery proporciona la posibilidad de ejecutar secuencias de comandos de Bourne Shell en el equipo del Agent de Linux antes y después de una transferencia. Las secuencias de comandos siguientes son compatibles con los equipos de Linux protegidos con el software Rapid Recovery Agent.

NOTA: Tenga en cuenta que, si una secuencia de comandos no es ejecutable, fallará el trabajo de transferencia.

- `PreTransferScript.sh`
- `PostTransferScript.sh`
- `PostExportScript.sh`

Para utilizar estas secuencias de comandos, asegúrese de que se encuentran en el directorio `/opt/apprecovery/scripts/`.

Parámetros compatibles de secuencias de comandos de transferencia y transferencia posterior

Se admiten los siguientes parámetros en Linux para las secuencias de comandos de transferencia. Para obtener más información, consulte [Secuencias de comandos de muestra de Bourne Shell](#).

- `TransferPrescriptParameter_VolumeNames=$TransferPrescriptParameter_VolumeNames`
- `TransferPrescriptParameter_ShadowCopyType=$TransferPrescriptParameter_ShadowCopyType`
- `TransferPrescriptParameter_TransferConfiguration=$TransferPrescriptParameter_TransferConfiguration`
- `TransferPrescriptParameter_StorageConfiguration=$TransferPrescriptParameter_StorageConfiguration`
- `TransferPrescriptParameter_Key=$TransferPrescriptParameter_Key`
- `TransferPrescriptParameter_ForceBaseImage=$TransferPrescriptParameter_ForceBaseImage`
- `TransferPrescriptParameter_IsLogTruncation=$TransferPrescriptParameter_IsLogTruncation`
- `TransferPrescriptParameter_LatestEpochSeenByCore=$TransferPrescriptParameter_LatestEpochSeenByCore`

Se admiten los siguientes parámetros en Linux para las secuencias de comandos de transferencia posterior.

- `TransferPostscriptParameter_VolumeNames=$TransferPostscriptParameter_VolumeNames`
- `TransferPostscriptParameter_ShadowCopyType=$TransferPostscriptParameter_ShadowCopyType`
- `TransferPostscriptParameter_TransferConfiguration=$TransferPostscriptParameter_TransferConfiguration`
- `TransferPostscriptParameter_StorageConfiguration=$TransferPostscriptParameter_StorageConfiguration`
- `TransferPostscriptParameter_Key=$TransferPostscriptParameter_Key`
- `TransferPostscriptParameter_ForceBaseImage=$TransferPostscriptParameter_ForceBaseImage`
- `TransferPostscriptParameter_IsLogTruncation=$TransferPostscriptParameter_IsLogTruncation`
- `TransferPostscriptParameter_LatestEpochSeenByCore=$TransferPostscriptParameter_LatestEpochSeenByCore`

Prueba de secuencias de comandos de Bourne Shell

Puede probar las secuencias de comandos que desea ejecutar utilizando el editor para los archivos (.sh) de secuencias de comandos.

NOTA: Si la secuencia de comandos previa o posterior de Bourne Shell falla, el trabajo también fallará. Hay información disponible acerca del trabajo en el archivo `/var/log/apprecovery/apprecovery.log`. Las secuencias de comandos correctas devuelven el código de salida 0.

Parámetros de entrada para las secuencias de comandos de Bourne Shell

Los parámetros para las secuencias de comando de Bourne Shell en Rapid Recovery se describen en las siguientes tablas.

TransferPrescriptParameters_VolumeNames

La siguiente tabla presenta los objetos disponibles para el parámetro `TransferPrescript`.

Tabla 316. Objetos de TransferPrescript

Método	Descripción
<code>public VolumeNameCollection</code> <code>VolumeNames { get; set; }</code>	Obtiene o establece la recopilación de los nombres de volumen para transferencia. <code>VolumeNames</code> es una estructura de datos que contiene los siguientes datos: • <code>GuidName</code>. La guía asociada con el volumen, utilizada como el nombre si no se establece un <code>DisplayName</code>. • <code>DisplayName</code>. El nombre del volumen que aparece.
<code>public ShadowCopyType ShadowCopyType</code> <code>{ get; set; }</code>	Obtiene o establece el tipo de copia para transferencia. <code>ShadowCopyType</code> es una enumeración con valores. Los valores disponibles son: • Desconocido • Copiar • Completo
<code>public string Key { get; set; }</code>	El método clave genera una clave pseudoaleatoria (aunque no criptográficamente segura) que se puede utilizar como contraseña de un solo uso para autenticar solicitudes de transferencia.

Método	Descripción
public bool ForceBaselImage { get; set; }	Obtiene o establece el valor que indica si la transferencia era una captura de imagen base forzada.
public bool IsLogTruncation { get; set; }	Obtiene o establece el valor que indica si se ha truncado el registro.
public uint LatestEpochSeenByCore { get; set; }	Obtiene o establece el valor de época más reciente. El método LatestEpochSeenByCore es el número ordinal de la instantánea tomada más recientemente por el Core. Este es el 'número de tiempo' asignado por el controlador del filtro a esta instantánea concreta en el momento en que se tomó con VSS.

TransferPostscriptParameter

La siguiente tabla presenta los objetos disponibles para el parámetro TransferPostscript.

Tabla 317. Objetos de TransferPostscript

Método	Descripción
public VolumeNameCollection VolumeNames { get; set; }	Obtiene o establece la recopilación de los nombres de volumen para transferencia. VolumeNames es una estructura de datos que contiene los siguientes datos: - GuidName. La guía asociada con el volumen, utilizada como el nombre si no se establece un DisplayName. - DisplayName. El nombre del volumen que aparece.
public ShadowCopyType ShadowCopyType { get; set; }	Obtiene o establece el tipo de copia para transferir. ShadowCopyType es una enumeración con valores. Los valores disponibles son: - Desconocido - Copiar - Completo
public string Key { get; set; }	El método clave genera una clave pseudoaleatoria (aunque no criptográficamente segura) que se puede utilizar como contraseña de un solo uso para autenticar solicitudes de transferencia.
public bool ForceBaselImage { get; set; }	Obtiene o establece el valor que indica si la transferencia era una captura de imagen base forzada.
public bool IsLogTruncation { get; set; }	Obtiene o establece el valor que indica si se ha truncado el registro.
public uint LatestEpochSeenByCore { get; set; }	Obtiene o establece el valor de época más reciente. El método LatestEpochSeenByCore es el número ordinal de la instantánea tomada más recientemente por el Core. Este es el 'número de tiempo' asignado por el controlador del filtro a esta instantánea concreta en el momento en que se tomó con VSS.

Secuencias de comandos de muestra de Bourne Shell

Esta sección describe las secuencias de comandos de Bourne Shell disponibles para que los usuarios administrativos las ejecuten en equipos protegidos.

⚠ PRECAUCIÓN: Las secuencias de comandos de muestra de Bourne que proporciona este documento funcionarán cuando se ejecuten según hayan diseñado administradores cualificados. Tome precauciones al modificar secuencias de comandos que estén en uso para mantener versiones que funcionan. Cualquier modificación en las secuencias de comandos de muestra incluidas aquí, así como cualquier secuencia de comandos que cree, se consideran personalizaciones, que no están cubiertas por Dell Support.

📌 NOTA: Los equipos protegidos utilizan el comando 'exec' de shell para iniciar la secuencia de comandos. Puede indicar qué intérprete debe ejecutar la secuencia de comandos definiendo dicha información en la primera línea de la secuencia de comandos. Si no especifica el intérprete, el shell predeterminado interpreta la secuencia de comandos. Si selecciona algo diferente al shell predeterminado, deberá asegurarse de que el intérprete especificado está disponible en todos los equipos protegidos.

Las secuencias de comandos de muestra para equipos protegidos incluyen:

PreTransferScript.sh

PreTransferScript se ejecuta en el equipo protegido antes de transferir una instantánea.

La siguiente secuencia de comandos almacena los valores de parámetros de entrada en Pre(Post)TransferScriptResult.txt ubicado y almacenado en el directorio principal raíz.

Sample PreTransferScript

```
#!/bin/bash
echo "TransferPrescriptParameter_VolumeNames=$TransferPrescriptParameter_VolumeNames
TransferPrescriptParameter_ShadowCopyType=$TransferPrescriptParameter_ShadowCopyType
TransferPrescriptParameter_Key=$TransferPrescriptParameter_Key
TransferPrescriptParameter_ForceBaseImage=$TransferPrescriptParameter_ForceBaseImage
TransferPrescriptParameter_IsLogTruncation=$TransferPrescriptParameter_IsLogTruncation
TransferPrescriptParameter_LatestEpochSeenByCore=
$TransferPrescriptParameter_LatestEpochSeenByCore" > ~/PreTransferScriptResult.txt
exit 0
```

PostTransferScript.sh

PostTransferScript se ejecuta en el equipo protegido después de transferir una instantánea.

La siguiente secuencia de comandos almacena los valores de parámetros de entrada en Pre(Post)TransferScriptResult.txt ubicado y almacenado en el directorio principal raíz.

Sample PostTransferScript

```
#!/bin/bash
echo "TransferPostscriptParameter_VolumeNames=$TransferPostscriptParameter_VolumeNames
TransferPostscriptParameter_ShadowCopyType=$TransferPostscriptParameter_ShadowCopyType
TransferPostscriptParameter_Key=$TransferPostscriptParameter_Key
TransferPostscriptParameter_ForceBaseImage=$TransferPostscriptParameter_ForceBaseImage
TransferPostscriptParameter_IsLogTruncation=$TransferPostscriptParameter_IsLogTruncation
TransferPostscriptParameter_LatestEpochSeenByCore=
$TransferPostscriptParameter_LatestEpochSeenByCore" > ~/PostTransferScriptResult.txt
exit 0
```

PostExportScript.sh

PostExportScript se ejecuta en el equipo protegido después de la transferencia.

La siguiente secuencia de comandos almacena los valores de parámetros de entrada en Pre(Post)ExportScriptResult.txt ubicado y almacenado en el directorio principal raíz.

Sample PostExportScript

```
#!/bin/bash
echo
"$curr_name-exported" > /etc/hostname
exit 0
```

API de Rapid Recovery

El objetivo de esta sección es proporcionar una introducción y una descripción general de las interfaces de programación de aplicaciones (API) de transferencia de estado representativa (REST) de Rapid Recovery, su uso y su función.

Las API de servicio web de Rapid Recovery son RESTful y le permiten automatizar y personalizar ciertas funciones y tareas dentro de la solución de software de Rapid Recovery para ayudarle a alcanzar sus objetivos comerciales.

Se accede a estas API a través de la página **Descargas** del Dell Data Protection | Portal de licencias de Rapid Recovery.

Temas:

- [Público al que va dirigido](#)
- [Trabajar con las API de REST de Rapid Recovery](#)
- [Descargar y ver las API de Core y Agent](#)
- [Lectura adicional recomendada](#)

Público al que va dirigido

Las API de Rapid Recovery están pensadas para los desarrolladores de aplicaciones que desean integrar y ampliar Rapid Recovery en su aplicación, así como administradores que desean crear secuencias de comandos de interacciones con el servidor del Core de Rapid Recovery.

Trabajar con las API de REST de Rapid Recovery

Las API de Rapid Recovery son API de estilo REST, lo que significa que utilizan solicitudes HTTP para proporcionar acceso a recursos (entidades de datos) a través de rutas de acceso URI. Las API de Rapid Recovery utilizan métodos HTTP estándar como GET, PUT, POST y DELETE. Debido a que las API de REST están basadas en estándares abiertos, puede utilizar cualquier lenguaje o herramienta que admita llamadas HTTP.

Hay dos maneras con las que los desarrolladores de aplicaciones y administradores pueden trabajar con las API de Rapid Recovery. Estas son:

- Utilizando C# o cualquier otro lenguaje .NET para utilizar directamente los archivos de la DLL del cliente .NET de Rapid Recovery.
- Comunicarse directamente con el endpoint HTTP para generar su propio XML.

Se recomienda este primer enfoque. Las DLL de cliente se incluyen en el SDK de Rapid Recovery. El método para llamar a las API de Rapid Recovery es coherente con la forma en que utilizaría cualquier servicio .NET 4.5X Windows Communication Foundation (WCF).

Descargar y ver las API de Core y Agent

El *Dell Data Protection | Rapid Recovery Software Developer Kit (SDK)* (Kit de desarrollador de software de Dell Data Protection | Rapid Recovery) incluye las API de REST para los componentes del Core de Rapid Recovery y el Agent de Rapid Recovery y archivos compatibles y de pruebas. Este contenido figura en las carpetas siguientes y está comprimido como un archivo que incluye los componentes siguientes:

Tabla 318. Componentes incluidos en el archivo del SDK

Nombre de carpeta	Contenido	Descripción
Core.Contracts	Las API del Core de Rapid Recovery	Contiene las API para ayudar a los desarrolladores o administradores a crear funciones en el Core de Rapid Recovery. Existen 2 conjuntos de contratos de servicios. 1 Abra el archivo CoreWeb.Client HTML en un navegador web para ver información de los estándares de REST generales. Se enumeran los contratos de servicios. Al hacer clic en cualquier identificador de recursos uniforme (URI) correspondiente, el navegador muestra información en el directorio Core.Contracts/docWeb/. La página resultante muestra información de las operaciones de servicios de REST generales, incluidos los métodos y las descripciones. 2 Abra el archivo Core.Client HTML en un navegador web para ver información detallada de C#. Al hacer clic en cualquier contrato de servicios convertido en hipervínculo (clase), el navegador muestra información en el directorio Core.Contracts/doc/. La página resultante muestra información detallada de todos los métodos C# en la clase seleccionada.
Agent.Contracts	Las API Rapid Recovery Agent (obsoletas)	Contiene las API que los desarrolladores o los administradores pueden utilizar para manipular Rapid Recovery Agent en equipos protegidos.  PRECAUCIÓN: Las API del Agent están obsoletas y se eliminarán de las versiones futuras del SDK. No se recomienda la manipulación directa de las API del Agent. El uso de estas API se considera una personalización y no se admitirá. La información se proporciona en la documentación para fines históricos. 1 Abra el archivo HTML AgentWeb.Client en un explorador web para ver la información de los estándares de REST generales. 2 Abra el archivo HTML.Client Agent en un explorador de web para ver información detallada de C#.
AppRecoveryAPI Samples	Muestras de códigos y bibliotecas de vínculos dinámicos	AppRecoveryAPISamples contiene muestras de códigos que están escritas en el lenguaje de programación C#. Estos archivos son un buen punto de partida para ver los fragmentos de código si se utiliza la API para personalizar la GUI, los sistemas de administración, etc. AppRecoveryAPISamples\dependencias contiene archivos de la biblioteca de vínculos dinámicos (DLL) que utiliza el Core de Rapid Recovery. Las DLL contienen contratos de datos (tipos con los que el Core es familiar) y contratos de servicios (métodos y operaciones de administración que se pueden utilizar para forzar el Core a hacer algo). Si quiere personalizar la interfaz gráfica de usuario o utilizar un sistema de administración para trabajar con el Core de Rapid Recovery, son necesarias estas DLL.  NOTA: La versión de la DLL que se utiliza debe coincidir con la versión del Core.

Puede descargar el SDK como archivo (API-Reference-x.x.x-xxxx). Cada x representa un dígito del número de compilación para la versión pertinente.

Complete los pasos de este procedimiento para obtener el SDK, descárguelo en el destino especificado y descomprima los archivos en preparación para utilizar las API del Core y del Agent.

- 1 Inicie sesión en el Dell Data Protection | Portal de licencias de Rapid Recovery (Portal de licencias de Dell Data Protection | Rapid Recovery) en <https://licenseportal.com>.
- 2 En el menú de navegación izquierdo del portal de licencias, haga clic en **Descargas**. Aparece la página **Descargas** del portal de licencias.
- 3 En página **Descargas**, en la sección Aplicaciones basadas en Windows, desplácese hasta la descripción del SDK y haga clic en **Descargar**.

- 4 Guarde el archivo descargado en la ubicación que prefiera.
- 5 Descomprima el archivo.
En la nueva carpeta API-Reference-x.x.x-xxxx, puede ver los conjuntos independientes de archivos que se describen en la tabla anterior.
- 6 Abra los archivos clave HTML que se describen en la tabla anterior en un navegador web para ver información sobre las API.

Lectura adicional recomendada

La Installation and Upgrade Guide (Guía de instalación y actualización) de Dell Data Protection | Rapid Recovery proporciona una descripción general de la arquitectura de Rapid Recovery y describe los pasos necesarios para instalar los componentes de Rapid Recovery y para actualizar los componentes del Core o el Agent de versiones anteriores.

Puede ver o descargar esta guía desde <https://support.software.dell.com/rapid-recovery/release-notes-guides/>.

Dell escucha al cliente y proporciona tecnología innovadora, soluciones comerciales, servicios fiables y valor en todo el mundo. Para obtener más información, visite <http://software.dell.com>.

Cómo ponerse en contacto con Dell

Para tratar cuestiones relacionadas con las ventas u otro tipo de preguntas, visite <http://software.dell.com/company/contact-us.aspx> o bien llame al número + 1-949-754-8000.

Recursos de asistencia técnica

La asistencia técnica está disponible para los clientes que han adquirido software de Dell con un contrato de mantenimiento válido y para clientes con versiones de prueba. Para acceder al portal de asistencia, vaya a <https://support.software.dell.com>.

El portal de asistencia proporciona herramientas de autoayuda que puede utilizar para resolver problemas de forma rápida e independiente, 24 horas, 365 días al año. Además, el portal de asistencia permite acceder directamente a los técnicos de asistencia de productos mediante un sistema de solicitud de servicio en línea.

El portal de asistencia le permite:

- Crear, actualizar y administrar solicitudes de servicio (casos).
- Ver artículos de la base de conocimientos.
- Obtener notificaciones de productos.
- Descargar software. Para obtener un software de prueba, vaya a <http://software.dell.com/trials>.
- Participar en discusiones de comunidad.

Administrador de volúmenes

El Administrador de volúmenes de Rapid Recovery gestiona los objetos y los almacena y presenta como volumen lógico. Saca el máximo provecho de la arquitectura de canalización dinámica para ofrecer escalabilidad TruScale, paralelismo y modelo de entrada y salida (E/S) asíncrono para obtener un alto rendimiento con la mínima latencia de E/S.

Agent

Rapid Recovery Agent es un software instalado en un equipo físico o virtual que permite que se incorpore a la protección en el Core de Rapid Recovery.

API de REST

La transferencia de estado representativa (REST) es una arquitectura del software simple sin estado diseñada para la escalabilidad. Rapid Recovery utiliza esta arquitectura en sus interfaces de programación de aplicaciones (API) para automatizar y personalizar ciertas funciones y tareas. Hay un conjunto independiente de API de REST para la funcionalidad de CORE y de los equipos protegidos (Agent).

capacidad de montaje

La capacidad de montaje de Exchange es una función de detección de corrupción que alerta a los administradores de posibles errores y asegura que todos los datos en servidores Exchange se recuperan correctamente en el caso de un error.

caracteres prohibidos

Los caracteres prohibidos son caracteres que no deben utilizarse cuando se asigna un nombre a un objeto en la Core Console de Rapid Recovery. Por ejemplo, cuando se define un nombre de visualización para un equipo protegido, no utilice ninguno de los siguientes caracteres especiales:

Tabla 319. Caracteres prohibidos

Carácter	Nombre de carácter	Prohibido en
?	signo de interrogación	nombre de visualización de equipo, clave de cifrado, repositorio, descripción de ruta de acceso
	barra vertical	nombre de visualización de equipo, clave de cifrado, repositorio, descripción de ruta de acceso
:	dos puntos	nombre de visualización de equipo, clave de cifrado, repositorio El uso de este símbolo se admite cuando se especifica una ruta de acceso, como por ejemplo c:\data .
/	barra diagonal	nombre de visualización de equipo, clave de cifrado, repositorio, descripción de ruta de acceso
\	barra diagonal inversa	nombre de visualización de equipo, clave de cifrado, repositorio El uso de este símbolo se admite cuando se especifica una ruta de acceso local o de red, como, por ejemplo, c:\data o \\ComputerName\SharedFolder\
*	asterisco	nombre de visualización de equipo, clave de cifrado, repositorio, descripción de ruta de acceso
"	comillas dobles	nombre de visualización de equipo, clave de cifrado, repositorio, descripción de ruta de acceso
<	cuña o paréntesis angular de apertura	nombre de visualización de equipo, clave de cifrado, repositorio, descripción de ruta de acceso

Carácter	Nombre de carácter	Prohibido en
>	cuña o paréntesis angular de cierre	nombre de visualización de equipo, clave de cifrado, repositorio, descripción de ruta de acceso

cifrado

Los datos se cifran para que sólo sean accesibles a los usuarios autorizados que tengan la clave de descodificación adecuada. Los datos se cifran mediante AES de 256 bits en el modo Encadenamiento de bloques de cifrado (CBC). En CBC, a cada bloque de datos se le aplica la disyunción exclusiva (XOR) con el bloque de texto cifrado previo antes del cifrado, de modo que cada bloque de texto cifrado nuevo depende de todos los bloques de texto sin formato precedentes. Se utiliza una frase de contraseña como vector de inicialización.

clave de licencia

Una clave de licencia es un método que se utiliza para registrar su software o dispositivo de Rapid Recovery. (También puede usar un archivo de licencia). Puede obtener las claves o archivos de licencia al registrar una cuenta del Dell Data Protection | Portal de licencias de Rapid Recovery. Para obtener más información, consulte [Portal de Licencias](#).

clúster

Consulte [Clúster de failover de Windows](#).

Cluster Continuous Replication (CCR)

Solución de clúster de failover de almacenamiento no compartido que utiliza la tecnología incluida de registro asíncrono incorporada para crear y mantener una copia de cada grupo de almacenamiento en un segundo servidor en un clúster de failover. CCR está diseñado para ser una solución de uno o dos centros de datos, proporcionando ambos alta disponibilidad y confianza del sitio. Es uno de los dos tipos de implementaciones de Servidor de buzón en clúster (CMS) disponibles en Exchange 2007.

clúster de copia única

Una solución de clúster de failover de almacenamiento, que utiliza una copia única de un grupo de almacenamiento en el almacenamiento que se comparte entre los nodos del clúster. Es uno de los dos tipos de implementaciones de Servidor de buzón en clúster (CMS) disponibles en Exchange 2007.

clúster de failover de Windows

Grupo de equipos independientes que funcionan de forma conjunta para aumentar la disponibilidad de las aplicaciones y servicios. Los servidores en clúster (denominados nodos) se conectan mediante cables físicos y también por software. Si falla uno de los nodos del clúster, otro nodo empezará a proporcionar servicio (este proceso se conoce como failover). El usuario detecta una serie de pequeñas caídas en el servicio. Rapid Recovery admite la protección de un número de tipos de clústeres de SQL Server y Exchange Server.

clúster de servidor

Consulte [Clúster de failover de Windows](#).

compresión

La Storage Networking Industry Association (SNIA) define la compresión como el proceso de cifrado de datos para reducir su tamaño.

conectabilidad SQL

La conectabilidad SQL es una ejecución de prueba dentro del Core de Rapid Recovery para asegurarse de que todos los puntos de recuperación de SQL están libres de errores y disponibles para la copia de seguridad en caso de error.

Consola de administración central

La Consola de administración central de Rapid Recovery es un componente opcional destinado para entornos con uno o más Core de Rapid Recovery. Este componente es un portal web que proporciona una interfaz central donde podrá agrupar, administrar y generar informes para varios Cores mediante una única interfaz basada en web.

consolidación

El proceso de consolidación es un procedimiento de mantenimiento interno que se realiza de noche y que ejecuta la política de retención al reducir y eliminar los puntos de recuperación antiguos. Rapid Recovery reduce la consolidación solo a operaciones de metadatos.

copia de seguridad de SharePoint

Una copia de seguridad de SharePoint es una copia de los datos que se utilizan para restaurar y recuperar los datos de un servidor SharePoint tras un fallo del sistema. Desde la copia de seguridad de SharePoint puede realizar la recuperación de la granja completa de SharePoint, o bien uno o más componentes de la granja.

copia de seguridad de SQL

Una copia de seguridad de SQL es una copia de los datos que se utilizan para restaurar y recuperar los datos de un servidor SQL tras un fallo del sistema. Desde la copia de seguridad de SQL puede realizar la recuperación de la base de datos completa de SQL, o bien uno o más componentes de la base de datos SQL.

copia de seguridad diferencial de SQL

Una copia de seguridad de la base de datos diferencial es una copia acumulativa de todos los cambios en los datos desde la última copia de seguridad completa de la base de datos SQL. Las copias de seguridad diferenciales son normalmente más rápidas de crear que las copias de seguridad completas de la base de datos, y reducen el número de registros de transacciones requeridos para recuperar la base de datos.

Core

El Core de Rapid Recovery es el componente central de la arquitectura de Rapid Recovery. El Core proporciona los servicios esenciales de copia de seguridad, recuperación, retención, replicación, archivado y administración. En el contexto de la replicación, el Core también se denomina source core (Core de origen). El Core de origen es el Core que origina, y el Core de destino es el destino (otro Core de Rapid Recovery en su propio servidor exclusivo, donde se replican equipos y clústeres protegidos).

Core Console

La Core Console de Rapid Recovery es una interfaz basada en web que permite administrar totalmente el Core de Rapid Recovery.

Core de destino

El Core de destino, que en ocasiones se denomina Core de réplica, es el Rapid Recovery Core que recibe los datos replicados (puntos de recuperación) desde el Core de origen.

Core remoto

Un Core remoto representa un Core de Rapid Recovery al que se puede acceder a través de un equipo que no es de Core mediante Local Mount Utility o la Consola de administración central.

desduplicación global

La Storage Networking Industry Association (SNIA) define la desduplicación de datos como la sustitución de varias copias de datos (en niveles variables de granularidad) con referencias a una copia compartida para ahorrar espacio de almacenamiento o ancho de banda. El Administrador de volúmenes de Rapid Recovery realiza la desduplicación global de datos en un volumen lógico. El nivel de granularidad de la desduplicación es de 8 KB. El ámbito de desduplicación de Rapid Recovery se limita a los equipos protegidos con el mismo repositorio y clave de cifrado.

en espera virtual

El estado de espera virtual es un proceso que crea una copia idéntica en una máquina virtual de un equipo protegido. El equipo de origen original puede ser físico o virtual, pero el producto siempre es virtual. Puede crear un estado en espera virtual único a petición o puede definir requisitos para crear la VM arrancable y, constantemente, actualizarla después de capturar cada instantánea en el equipo protegido original.

equipo con puntos de recuperación únicamente

Un equipo con puntos de recuperación únicamente es la representación en el Core de los puntos de recuperación de un equipo que anteriormente estaba protegido en el Core y se eliminó. Si quita la replicación, pero mantiene los puntos de recuperación, también da como resultado un equipo con puntos de recuperación únicamente. La información se puede ver y recuperar a nivel de archivos. No

puede utilizar un equipo con puntos de recuperación únicamente para realizar una BMR o restaurar volúmenes completos, ni puede agregar más datos a un equipo con puntos de recuperación únicamente.

equipo protegido

Un equipo protegido, también llamado Agent, es un ordenador físico o una máquina virtual que está protegido en el Core de Rapid Recovery. Los datos de la copia de seguridad se transmiten del equipo protegido al repositorio especificado en el Core mediante un intervalo de protección predefinido. La imagen base transmite todos los datos a un punto de recuperación (incluido el sistema operativo, las aplicaciones y las configuraciones). Cada instantánea incremental posterior confirma solo los bloques cambiados en los volúmenes de disco especificados en el equipo protegido. Los equipos protegidos basados en software tienen el software Rapid Recovery Agent instalado. Algunas máquinas virtuales también pueden protegerse sin agentes con algunas limitaciones.

etiquetado blanco

Rapid Recovery ofrece la posibilidad de que los proveedores de servicios de copia de seguridad y recuperación tras desastres utilicen Rapid Recovery como marca blanca o la personalicen con su propia identidad. De ese modo, pueden venderlo o distribuirlo como un producto o un servicio propio.

evento

Un evento es un proceso que el Core ha registrado. Los eventos se pueden ver en la Core Console haciendo clic en el icono 

(Eventos) de la barra de iconos. La vista predeterminada muestra la página **Tareas** cuando se hace clic en el icono  (Eventos). Esta vista muestra los eventos relacionados con un trabajo. Los eventos por los que recibe una notificación se pueden ver en la página **Alertas**. En la página **Diario** aparece un registro de todos los eventos. Puede personalizar la notificación de cualquier evento si configura o modifica los grupos de notificación existentes. Esta acción aumenta la prioridad del evento al mostrarla en la página de **Alertas**. A los miembros de un grupo de notificaciones se les notificará de los eventos con el método de notificación que se ha establecido en las opciones de notificación del grupo.

frase de contraseña

Una frase de contraseña es una clave que se utiliza en el cifrado de datos. Si se pierde la frase de contraseña, los datos no se pueden recuperar.

frases prohibidas

Las frases prohibidas son frases (o conjuntos de caracteres) que no deben utilizarse para el nombre de ningún objeto en la Core Console de Rapid Recovery porque están reservadas para el uso de sistemas operativos. La práctica recomendada es evitar el uso de estas frases siempre que sea posible. Por ejemplo, cuando se define un nombre de visualización para un equipo protegido, no utilice ninguna de las siguientes frases:

Tabla 320. Frases prohibidas

Frases	Uso general	Prohibido en
con	consola	nombre de visualización de equipo, clave de cifrado, repositorio, descripción de ruta de acceso
prn	puerto de impresora	nombre de visualización de equipo, clave de cifrado
aux	puerto auxiliar	nombre de visualización de equipo, clave de cifrado
nul	valor nulo	nombre de visualización de equipo, clave de cifrado
com1, com2... through com9	puerto de comunicación	nombre de visualización de equipo, clave de cifrado
lpt1, lpt2... through lpt9	puerto de terminal de impresión en línea	nombre de visualización de equipo, clave de cifrado, repositorio, descripción de ruta de acceso

grupo de disponibilidad de base de datos (DAG)

Un conjunto de hasta 16 servidores Microsoft Exchange Server 2010 Mailbox que proporcionan recuperación a nivel de base de datos, automática, a partir de una base de datos, servidor o error de red. Los DAG utilizan replicación continua y un subconjunto de tecnologías de clústering de failover en Windows para proporcionar alta disponibilidad y fiabilidad del sitio. Servidores Mailbox en un monitor DAG entre ellos para errores. Cuando se añade un servidor Mailbox a un DAG, funciona con los otros servidores del DAG para proporcionar recuperación automática a nivel de base de datos frente a errores de bases de datos.

imagen base

La primera transferencia de copia de seguridad guardada en el Core se denomina una instantánea de imagen base. Todos los datos de todos los volúmenes especificados (incluido el sistema operativo, las aplicaciones y la configuración) se guardan en el Core. Para obtener más información, consulte [Instantánea](#).

inicialización

En la replicación, la transferencia inicial de las imágenes base desduplicadas e instantáneas incrementales de Agents protegidos, que pueden formar hasta cientos o miles de gigabytes de datos. La replicación inicial se puede inicializar en el Core de destino usando medios externos, lo que es útil para grandes conjuntos de datos o sitios con enlaces lentos.

instantánea

Una instantánea es un término habitual en el sector para referirse a la función de capturar y almacenar el estado de un volumen de disco en un punto determinado, mientras las aplicaciones se están ejecutando. La instantánea es crítica si se necesita recuperar el sistema debido a un corte de conexión o a un error del sistema. Las instantáneas de Rapid Recovery ofrecen reconocimiento por parte de la aplicación, lo cual significa que todos los registros de transacciones abiertas y transacciones en marcha se completan y que las memorias caché se vacían antes de crear la instantánea. Rapid Recovery utiliza Microsoft Volume Shadow Services (VSS) (Servicios de instantáneas de volumen de Microsoft [VSS]) para facilitar instantáneas de la aplicación en estado coherente tras la interrupción.

instantánea incremental

Las instantáneas incrementales son copias de seguridad que constan únicamente de datos cambiados en el equipo protegido desde la última copia de seguridad. Se guardan en el Core de forma habitual, en base al intervalo definido (por ejemplo, cada 60 minutos). Para obtener más información, consulte [Instantánea](#).

Live Recovery

Live Recovery de Rapid Recovery es una tecnología de recuperación instantánea para máquinas virtuales o servidores. Proporciona acceso casi continuo a volúmenes de datos en un servidor virtual o físico, y permite recuperar un volumen completo con RTO cercanos a cero y unos RPO de minutos.

Local Mount Utility

Local Mount Utility (LMU) es una aplicación descargable que permite montar un punto de recuperación en un Core de Rapid Recovery desde cualquier equipo.

nodo de clúster

Un equipo individual es parte de un clúster de failover de Windows.

Portal de licencias

El Dell Data Protection | Portal de licencias de Rapid Recovery es una interfaz web donde los usuarios y socios puede descargar el software, registrar los dispositivos de Rapid Recovery y gestionar las suscripciones de licencias. Los usuarios del Portal de licencias pueden registrar cuentas, descargar el software de Core y Agent de Rapid Recovery, administrar grupos, seguir la actividad de grupos, registrar dispositivos integrados, registrar equipos, invitar a usuarios y generar informes. Para obtener más información, consulte la *guía del usuario del Dell Data Protection | Portal de licencias de Rapid Recovery*.

puntos de recuperación

Los puntos de recuperación son una colección de instantáneas de varios volúmenes de disco. Por ejemplo, C:, D: y E:.

quórum

Para un clúster de failover, el número de elementos debe estar en línea para que un clúster dado continúe la ejecución. Los elementos relevantes en este contexto son nodos de clúster. A este término también se le puede hacer referencia como recurso con capacidad para quórum seleccionado para mantener los datos de configuración necesarios para la recuperación del clúster. Estos datos contienen detalles de todos los cambios que se han aplicado a la base de datos de clústeres. El recurso de quórum suele ser accesible a otros recursos de clúster para que cualquier nodo de clúster tenga acceso a los cambios de base de datos más recientes. De forma predeterminada, sólo hay un recurso de quórum por clúster de servidor. Una configuración de quórum concreta (configuración para un clúster de failover) determina el punto en el que demasiados errores detendrán la ejecución del clúster.

Rapid Recovery

Rapid Recovery establece un nuevo estándar para la protección de datos unificada gracias a que combina la copia de seguridad, la replicación y la recuperación en una única solución que se ha diseñado para que sea la copia de seguridad más rápida y fiable de protección de máquinas virtuales (MV), así como equipos físicos y entornos de nube.

replicación

La replicación es el proceso de copiar puntos de recuperación de un Core de Rapid Recovery y transmitirlos a otro Core de Rapid Recovery con fines de recuperación tras desastres. El proceso requiere la existencia de una relación de emparejamiento origen-destino entre dos o más Cores. La replicación está gestionada por equipos protegidos. Se puede configurar cualquier equipo (o todos los equipos) protegido o replicado en un Core de origen para replicar en un Core de destino. Se trata de los puntos de recuperación que se copian al Core de destino.

repositorio

Un repositorio es una colección de imágenes base e instantáneas incrementales tomadas de los equipos protegidos de un Rapid Recovery Core. Los repositorios se deben crear en dispositivos de almacenamiento primarios rápidos. Los repositorios DVM se pueden almacenar en una ubicación local del equipo del Core, en cuyo caso solo está alojado en un sistema operativo Windows compatible. Se puede usar almacenamiento de conexión directa, una red de área de almacenamiento o un servidor conectado a la red con la capacidad adecuada.

restaurar

El proceso de restaurar uno o más volúmenes de almacenamiento en un equipo a partir de puntos de recuperación guardados en el Core de Rapid Recovery se conoce como realizar una restauración. Esto se conocía anteriormente como reversión.

retención

La retención define el tiempo durante el que las instantáneas de copia de seguridad de los equipos protegidos se almacenarán en el Core de Rapid Recovery. La política de retención se ejecuta en los puntos de recuperación mediante el proceso de consolidación.

roles de administración

La Consola de administración central de Rapid Recovery introduce un nuevo concepto de roles de administración que permiten dividir la responsabilidad administrativa entre datos de confianza y administradores de servicio junto con el control de acceso para permitir una delegación de la administración segura y eficaz.

secuencias de comandos de PowerShell

Windows PowerShell es un entorno conectado con el framework .NET de Microsoft diseñado para automatización administrativa. Rapid Recovery incluye los SDK de cliente completos para las secuencias de comandos de PowerShell que permiten a los administradores automatizar la administración de recursos de Rapid Recovery mediante la ejecución de comandos directamente o por medio de secuencias de comandos.

Sistema de archivos de objeto

El almacén de objetos adaptable de Rapid Recovery es un componente de sistema de archivos de objeto. Trata a todos los bloques de datos, de los que se derivan las instantáneas, como objetos. Almacena, recupera, mantiene y replica esos objetos. Se ha diseñado para ofrecer rendimiento ampliable de entrada/salida (E/S) junto con deduplicación global de datos, cifrado y administración de retención. El Sistema de archivos de objeto interactúa directamente con tecnologías de almacenamiento estándar del sector.

Smart Agent

El Rapid Recovery Smart Agent se instala en los equipos protegidos por el Core de Rapid Recovery. El Smart Agent realiza el seguimiento de bloques cambiados en el volumen de discos y hace instantáneas de los bloques cambiados en un intervalo predefinido de protección.

suma de comprobación

Una suma de comprobación es una función que crea bloques de datos que se utilizan para detectar errores accidentales que se crean durante la transmisión o almacenamiento.

Transport Layer Security

Transport Layer Security (TLS) es un moderno protocolo de red criptográfico diseñado para garantizar la seguridad de las comunicaciones a través de Internet. Este protocolo, definido por Internet Engineering Task Force, es el sucesor de Secure Sockets Layer (SSL). El término SSL sigue utilizándose de manera general, y los protocolos son interoperables (un cliente TLS puede degradar su nivel para comunicarse con un servidor SSL).

True Scale

True Scale es la arquitectura adaptable de Rapid Recovery.

truncamiento del registro

El truncamiento del registro es una función que elimina registros del registro de transacciones. Para un equipo SQL Server, cuando fuerza el truncamiento de los registros de SQL Server, este proceso identifica el espacio libre en el servidor SQL. Para un equipo Exchange Server, cuando fuerza el truncamiento de los registros de Exchange, esta acción libera espacio en el servidor Exchange.

Universal Recovery

La tecnología Rapid Recovery Universal Recovery ofrece una flexibilidad ilimitada para restaurar equipos. Permite realizar la recuperación monolítica para y desde cualquier plataforma física o virtual de su elección, así como actualizaciones de recuperación incrementales en máquinas virtuales desde cualquier origen físico o virtual. También permite realizar recuperaciones en el nivel de aplicación, elemento y objeto de archivos individuales, carpetas, correo electrónico, elementos de calendario, bases de datos y aplicaciones.

Verified Recovery

La tecnología Verified Recovery se utiliza para llevar a cabo pruebas automatizadas de recuperación y la verificación de copias de seguridad. Admite varios sistemas de archivos y servidores.