Dell PowerStore

Protección de sus datos

Versión 4.4

Es posible que este contenido se haya traducido con IA. Para obtener más información, consulte el siguiente enlace.

Marzo 2026
Rev. A10

DELL Technologies

Notas, avisos y advertencias

NOTA: NOTE indica información importante que lo ayuda a hacer un mejor uso de su producto.

PRECAUCIÓN: CAUTION indica la posibilidad de daños en el hardware o la pérdida de datos y le informa cómo evitar el problema.

AVISO: WARNING indica la posibilidad de daños en la propiedad, lesiones personales o la muerte.

Tabla de contenido

Recursos adicionales

Como parte de un esfuerzo por mejorar, se lanzan periódicamente revisiones de software y hardware. Algunas funciones que se describen en este documento no son compatibles con todas las versiones del software o el hardware actualmente en uso. Las notas de la versión del producto proporcionan la información más actualizada acerca de las características del producto. Póngase en contacto con el proveedor de servicio si un producto no funciona correctamente o como se describe en este documento.

Dónde obtener ayuda

La información sobre soporte, productos y licenciamiento puede obtenerse de la siguiente manera:

- **Información del producto**: para obtener documentación o notas de la versión sobre productos y características, visite el Centro de información de PowerStore.
- **Solución de problemas**: para obtener información sobre productos, actualizaciones de software, licenciamiento y servicio, vaya al soporte de Dell y busque la página de soporte del producto correspondiente.
- **Soporte técnico**: Para realizar solicitudes de servicio y de soporte técnico, vaya al Soporte de Dell y busque la página **Solicitudes de servicio**. Para abrir una solicitud de servicio, debe contar con un acuerdo de soporte técnico válido. Póngase en contacto con el representante de ventas para recibir información sobre cómo obtener un acuerdo de soporte técnico válido o para aclarar cualquier tipo de duda en relación con su cuenta.

Comentarios del cliente

Hay un botón de comentarios en el lado derecho de PowerStore Manager. Si selecciona **Comentarios** , se abre una ventana del navegador en la que puede completar y enviar una encuesta de comentarios.

1

Introducción

Este capítulo contiene la siguiente información:

Temas:

Protección de datos

En PowerStore, se proporcionan diversos medios para proteger sus datos:

- Local protection: crea instantáneas (copias de un punto en el tiempo) de volúmenes, Grupos de volúmenesmáquinas virtuales o sistemas de archivos en el PowerStore sistema.
- Protección remota: replicación de datos a un sistema remoto o espejeado de estos mediante volúmenes metro con fines de redundancia en caso de un desastre.
- Respaldo remoto: respaldo de volúmenes y Grupos de volúmenes directamente desde PowerStore a PowerProtect DD.

PowerStore permite crear políticas de protección personalizadas, que son conjuntos de reglas para la creación de instantáneas, la replicación y el respaldo remoto, y asignarlas a recursos de almacenamiento. Las políticas de protección aplican las reglas definidas en el recurso de almacenamiento, lo que le brinda protección local, protección remota y respaldo remoto.

NOTA: Las reglas de respaldo remoto solo se pueden aplicar a volúmenes y Grupos de volúmenes.

NOTA: Las políticas de protección que incluyen una regla de replicación no se pueden asignar a volúmenes metro. Consulte Uso de políticas de protección con metro.

NOTA: En PowerStoreOS 3.x y versiones posteriores, las políticas de protección no se pueden aplicar a máquinas virtuales basadas en volúmenes virtuales (vVols). Consulte Replicación de volúmenes virtuales.

PowerStore también le permite configurar el respaldo estándar para los servidores NAS mediante NDMP. Para obtener detalles, consulte Habilitar el respaldo NDMP.

Instantáneas

Las instantáneas son copias de solo lectura, de un punto en el tiempo, de los datos de un volumen,Grupo de volúmenes, máquina virtual o sistema de archivos. Cuando se crea una instantánea, se guarda el estado del recurso de almacenamiento de un punto en el tiempo. Con el uso de instantáneas, puede proteger sus datos de manera local y restaurar un recurso de almacenamiento a un estado anterior.

Puede crear instantáneas de forma manual en cualquier momento. También es posible configurar reglas de instantánea como parte de una política de protección y asignarlas a recursos de almacenamiento. El sistema crea automáticamente instantáneas del recurso pertinente según el calendario especificado en la política de protección.

A partir dePowerStore3.5, puede crear instantáneas seguras que un administrador o un intruso no pueden eliminar manualmente y que se eliminan automáticamente solo cuando alcanzan su fecha de vencimiento. Las instantáneas seguras proporcionan un medio adicional de protección contra ataques de ransomware.

Si se producen daños en los datos o se eliminan accidentalmente, puede recuperar los datos de las instantáneas o restaurar el volumen oGrupo de volúmeneshasta el momento en que se creó la instantánea.

En los sistemas de archivos, puede crear dos tipos de acceso para las instantáneas de archivos de solo lectura: protocol y .snapshot. El tipo de acceso predeterminado es protocol, que se puede exportar como un recurso compartido de SMB, una exportación

NFS, o ambos. Puede compartir y montar la instantánea en un cliente como cualquier otro sistema de archivos. En el caso de los tipos de acceso .snapshot, puede acceder a los archivos en la instantánea desde el sistema de archivos de producción en el subdirectorio `.snapshot` de cada directorio.

También puede crear instantáneas de volúmenes coherentes con el orden de escritura y con las aplicaciones:

- Instantáneas coherentes con el orden de escritura:PowerStoreContiene todas las escrituras en elGrupo de volúmenesmiembros para proporcionar una copia uniforme de un punto en el tiempo y garantizar una protección coherente en todos los volúmenes miembro. Puede generar instantáneas coherentes con el orden de escritura a partir dePowerStore Manager.
- Instantáneas coherentes con las aplicaciones: puede crear instantáneas coherentes con las aplicaciones de un volumen o unGrupo de volúmenesmediante AppSync. Cuando usted crea una instantánea coherente con las aplicaciones, todas las I/O entrantes de una aplicación determinada se ponen en modo inactivo mientras se crea la instantánea.

Para verificar si una instantánea es coherente con el orden de escritura o con las aplicaciones, consulte las columnas **Write-Order Consistent** y **Application Consistent** en las tablas de instantáneas de un volumen oGrupo de volúmenesenPowerStore Manager.

NOTA: Si no puede ver estas columnas, puede agregarlas mediante la opción **Mostrar/ocultar columnas de tabla**.

El mapeo de instantáneas a hosts no es compatible conPowerStore. Para permitir que un host conectado acceda a una instantánea, puede crear un clon delgado, una copia de la instantánea con capacidad de escritura y uso eficiente del espacio, y mapearlo a un host. Puede actualizar el clon delgado de diferentes instantáneas con la operación de actualización.

Para obtener detalles sobre las posibles operaciones relacionadas con instantáneas, puede realizar mediantePowerStore Manager, consulte el capítulo Instantáneas .

NOTA: Para obtener más información sobre los límites de instantáneas paraPowerStoreconsulte *la matriz de soporte simple de Dell Technologies PowerStore*

Replicación

La replicación de datos es un proceso en el cual los datos se duplican en un sistema remoto, lo que proporciona una redundancia mejorada en caso de que falle el sistema de producción principal. La replicación minimiza los costos de una falla del sistema asociados con el tiempo de inactividad y simplifica el proceso de recuperación ante un desastre natural o un error humano.

PowerStore Es compatible con la replicación remota asíncrona y síncrona de volúmenes Grupos de volúmenes, servidores NAS y volúmenes virtuales.

NOTA: Si el clúster de replicación tiene varios dispositivos, se recomienda que la capacidad de los dispositivos remotos sea lo más similar posible. Las variaciones significativas en la capacidad de los dispositivos remotos pueden dar lugar a una asignación desequilibrada de sesiones de replicación entre estos, lo que puede afectar el rendimiento del clúster. Para equilibrar una asignación desequilibrada de sesiones de replicación entre dispositivos remotos, se recomienda realizar una migración de volúmenes de destino.

Para configurar la replicación de volúmenes y Grupos de volúmenes:

1. Cree una conexión remota entre los sistemas de origen y destino.
2. Cree una política de protección con una regla de replicación que satisfaga de mejor manera las necesidades del negocio.
3. Asigne una política de protección al volumen o Grupos de volúmenes.

Para configurar la replicación para servidores NAS:

1. Configure y mapee la red de movilidad de archivos.
2. Cree una conexión remota entre los sistemas de origen y destino.
3. Cree una política de protección con una regla de replicación que satisfaga de mejor manera las necesidades del negocio.
4. Asigne una política de protección al servidor NAS.

NOTA: No se recomienda modificar la red de movilidad de archivos cuando no se puede acceder al sistema par. Cuando el sistema par vuelve a estar activo, el resultado puede ser que ambos servidores NAS estén en modo de producción.

Para configurar la replicación para volúmenes virtuales (vVols):

1. Cree una conexión remota entre los sistemas de origen y destino.
2. La creación de políticas de protección y su asignación a volúmenes virtuales se realizan en vSphere. Consulte Replicación de volúmenes virtuales.

Para la replicación de archivos y volúmenes, PowerStore le permite conmutar por error el control al sistema remoto e invertir la dirección de una sesión de protección remota. Es posible que la conmutación por error sea necesaria en los siguientes casos:

- Si desea migrar datos a un nuevo sistema y, a continuación, comenzar a trabajar desde él sin perder datos. En este caso, puede realizar una conmutación por error sin pérdida de datos.
- Cuando no hay acceso a los datos en el sistema de origen, puede pasar al sistema remoto y continuar trabajando con la copia de protección remota del punto en el tiempo más reciente. Sin embargo, es posible que se produzca una pérdida de datos en esta situación debido a que la copia más reciente en el sistema remoto no incluye los cambios de datos realizados entre el momento en que se creó esta copia y el momento en que los datos del sistema se volvieron inaccesibles.
- Cuando se puede acceder a los datos en el sistema de origen, pero su integridad puede verse afectada. En este caso, debe volver a la copia de protección de un punto en el tiempo más reciente creada antes de que se dañen los datos.
- Puede realizar una prueba de conmutación por error en el recurso de almacenamiento de destino para probar la preparación de la recuperación ante desastres del sistema.

Para obtener información detallada sobre los procedimientos relacionados con la replicación que puede realizar, consulte el capítulo Replicación.

Para obtener información detallada sobre los límites de replicación sincronizada y no sincronizada, consulte la *Matriz de soporte simple de Dell Technologies PowerStore* en la página Documentación de PowerStore.

Políticas de protección

Una política de protección consta de reglas de instantánea, reglas de replicación y reglas de respaldo remoto, las que usted puede crear para establecer una protección de datos coherente en todos los recursos de almacenamiento. Después de configurar una política de protección, puede asignarla a los recursos de almacenamiento nuevos o existentes.

Una política de protección puede incluir una regla de replicación, una regla de respaldo remoto y hasta cuatro reglas de instantánea. Todos los tipos de regla pueden estar en varias políticas.

Las políticas de protección administran la creación de instantáneas, las sesiones de replicación y el respaldo remoto según las reglas que contienen. Puede crear políticas con diversas reglas que proporcionan distintos niveles de protección para satisfacer las necesidades de protección locales y remotas, y asignar una política a múltiples recursos de almacenamiento para proporcionar una protección idéntica a esos recursos.

Puede crear o modificar reglas y políticas pertinentes en función de sus privilegios de usuario.

Si desea crear una regla, asegúrese de revisar los parámetros y los requisitos del negocio con un administrador antes de continuar. Esto ayuda a establecer y mantener políticas coherentes en todo el sistema.

Para obtener información detallada sobre los procedimientos relacionados con las políticas de protección que puede realizar, consulte el capítulo Políticas de protección.

Protección de metro

Metro proporciona replicación síncrona bidireccional (activa/activa) en dosPowerStoresistemas. Un volumen metro se expone con el uso de dos sistemas distintos, los que generalmente están en dos centros de datos diferentes, a una distancia de hasta 96 km (o 60 millas), o en dos ubicaciones lejanas dentro del mismo centro de datos. Los dos sistemas colaboran para exponer un único volumen metro a hosts de aplicaciones proporcionando la misma imagen y datos de SCSI. Los hosts y la aplicación perciben los dos volúmenes físicos alojados por los dos sistemas como un único volumen con múltiples rutas.

La protección de metro permite una mayor disponibilidad y prevención de desastres, balanceo de recursos entre centros de datos y migración del almacenamiento entre dosPowerStoresistemas.

Cuando configura un volumen metro, su contenido se replica en el sistema remoto. Se utilizan políticas de protección para configurar medidas adicionales de protección, como instantáneas locales.

Una sesión metro requiere dosPowerStoresistemas y, opcionalmente, un servicio testigo que se ejecuta en un host o una VM independientes.

Cuando configura un recurso metro, el sistema desde el que está configurado el recurso metro se establece automáticamente como preferido y el otro se configura como no preferido. Cuando no hay ningún servicio testigo configurado o cuando el servicio testigo no está disponible, estas funciones ayudan a guiar el comportamiento del sistema en situaciones de falla. Cuando se produce una falla (ya sea en uno de los sistemas o en la conexión entre estos), la sesión metro se “fractura” y el sistema no preferido deja de gestionar I/O mientras que el sistema preferido proporciona acceso de host.

El servicio testigo es un tercero pasivo que se instala en un host independiente.

NOTA: El servicio del testigo se debe implementar en un tercer dominio de falla, que esté separado de los dosPowerStoreSistemas que forman parte de la sesión de Metro. La instalación del servicio testigo en un sistema independiente garantiza su disponibilidad si se produce una falla de alimentación en los sistemas metro.

El testigo observa el estado de los dos sistemas. Cuando se produce una falla, el testigo determina qué sistema permanece accesible para los hosts y continúa gestionando I/O. Un testigo instalado en un tercer sitio proporciona protección contra escenarios de una única falla.

Metro cambia entre el uso del testigo y el uso de la función del sistema como medio para la recuperación tras situaciones de una única falla (cuando el testigo no está configurado o no está disponible, la recuperación tras una única falla se realiza manualmente).

Para obtener un resumen de los atributos de metro y una comparación con la replicación síncrona y asíncrona, consulte Resumen de la replicación.

Respaldo remoto

El respaldo remoto le permite respaldar volúmenes y grupos de volúmenes directamente desde PowerStore a un sistema PowerProtect DD.

PowerStore es compatible con el respaldo en un dispositivo PowerProtect físico o en PowerProtect DD Virtual Edition (DDVE).

Un respaldo remoto crea una instantánea de un volumen o un grupo de volúmenes en el sistema PowerProtect. Las instantáneas creadas son coherentes con fallas generales y no hay integración de las aplicaciones.

Una vez que se encuentran en PowerProtect DD, los respaldos se pueden recuperar en un clúster de PowerStore nuevo o existente. También puede buscar el contenido de un respaldo en el sistema DD mediante el acceso instantáneo y obtener acceso temporal rápido a las instantáneas respaldadas sin recuperarlas en el clúster de PowerStore.

Cuando se respalda un recurso por primera vez, se crea una copia completa. Los siguientes respaldos son incrementales: solo se copian los cambios del último respaldo para mejorar la eficiencia.

Cuando asigna una política de protección que incluye una regla de respaldo remoto a un volumen o grupo de volúmenes, se crea una sesión de respaldo remoto. Solo se puede crear una sesión de respaldo remoto por recurso. Las sesiones de respaldo remoto se muestran en la pestaña **Sesiones de respaldo** de la página **Respaldo remoto**.

El respaldo remoto se inicia desde PowerStore. El flujo de trabajo de respaldo remoto se describe en Flujo de trabajo básico de respaldo remoto.

Una sesión remota rastrea cada una de las operaciones (respaldo, recuperación y acceso instantáneo). Puede monitorear el progreso de las sesiones y realizar acciones desde las páginas de las sesiones remotas.

2

Sistemas remotos

Este capítulo incluye la siguiente información:

Temas:

Descripción general

En la tabla Sistemas remotos (en **Protección**), se muestran las conexiones de sistema remoto configuradas. En la tabla Sistemas remotos puede:

- Ver información de sistemas remotos, como el nombre y la IP del sistema remoto, el tipo de sistema (sistema de almacenamiento o PowerProtect DD), las funcionalidades compatibles (visibles solo si ambos sistemas las admiten) y el estado de la conexión de datos. En la vista detallada, se proporciona el estado de conectividad IP de todos los iniciadores.
- Monitoree el estado de la administración y la conexión de datos para fines de solución de problemas.
- Seleccione un sistema remoto y, a continuación, seleccione **Modificar** para editar sus atributos. Puede cambiar la dirección IP de administración y la descripción. Para el tipo de conexión TCP, también puede cambiar la latencia de red de una conexión de sistema remoto.
- Seleccione un sistema remoto y, a continuación, seleccione **Eliminar** para eliminarlo. No puede eliminar un sistema remoto en los siguientes casos:
  - Cuando hay sesiones de replicación activas asociadas con el sistema remoto.
  - Cuando hay sesiones de respaldo remoto activas asociadas con el sistema remoto.
  - Cuando hay una regla de replicación asociada con el sistema remoto.
  - Cuando hay una regla de respaldo remoto asociada con el sistema remoto.
  - Cuando hay sesiones metro.
- Seleccione un sistema remoto y haga clic en **Más acciones** > **Verificar y actualizar** para verificar y actualizar la conexión al sistema remoto. La verificación y la actualización detectan cambios en los sistemas locales y remotos, restablecen las conexiones de datos y, a la vez, toman en cuenta los ajustes del protocolo de autenticación por desafío mutuo (CHAP).
- Para sistemas con el tipo de conexión TCP, seleccione un sistema remoto y haga clic en **Más acciones** > **Administrar grupo de red** para agregar, modificar o eliminar grupos de red.
- Para sistemas remotos PowerProtect DD:
  - Si hay una pérdida de conexión durante menos de diez minutos, el sistema remoto se recupera automáticamente cuando se restaura la conectividad de red. Si la pérdida de conexión dura más de diez minutos, seleccione **Más acciones** > **Verificar y actualizar** una vez que se restaura la conectividad para cambiar el estado del sistema remoto a Correcto.
  - Seleccione un sistema remoto y, a continuación, seleccione **Más acciones** > **Ver detalles de capacidad** para ver el uso y las métricas históricas de ese sistema durante un período seleccionado.
  - Si se renovó el certificado de un sistema remoto, seleccione el sistema remoto y, a continuación, seleccione **Más acciones** > **Actualizar certificado** para ver y confirmar la actualización del certificado del sistema remoto.
  - Puede comprobar si hay problemas de conectividad en las columnas Estado de administración/archivo y Conexión de datos de la tabla Sistemas **remotos** .

Consideraciones para replicación y metro

Configure conexiones de sistemas remotos para la replicación y la protección metro entre dos sistemas, lo que garantiza la compatibilidad de versiones y tipos de conexión.

La replicación y la protección metro requieren una conexión de sistema remoto entre dosPowerStoresistemas. Debe crear una conexión de sistema remoto antes de configurar la protección remota. Para la replicación, la conexión de sistema remoto está asociada con la regla

de replicación. Si está utilizandoPowerStoreManager, puede crear una conexión de sistema remoto mientras crea una regla de replicación. También es posible crear un sistema remoto cuando se configura metro en un volumen o grupo de volúmenes.

Es posible crear una conexión remota entre sistemas que ejecutan diferentes versiones (3.x, 4.x). Las versiones de los sistemas determinan las funcionalidades compatibles (tipos de replicación y funcionalidad de protección remota). Ambos sistemas deben ejecutar el programaPowerStoreversion para que se admita una funcionalidad en esta versión. Se deben cumplir las siguientes condiciones para la replicación de objetos de almacenamiento:

Tabla 1. Replicación de almacenamiento: requisitos

Tipo de replicación	Versiones permitidas	Tipo de conexión	Latencia de red	Propósito de la red de almacenamiento (para el tipo de conexión TCP)
Asíncrono: volumen	1.x o posterior	• TCP • FC: compatible con las versiones 4.2 y posteriores	-	Replicación
Asíncrono: archivo	3.x o superior	• TCP • FC: compatible con las versiones 4.3 y posteriores	-	Replicación
Asíncrono: volumen virtual	3.x o superior	TCP	-	Replicación
Metro	3.x o posterior para compatibilidad con volúmenes, 4.x o posterior para compatibilidad con grupos de volúmenes	• TCP (consulte Requisitos y limitaciones de Metro) • FC: compatible con las versiones 4.4 y posteriores	Baja (menos de 5 ms)	Replicación
Síncrono: volumen	4.x o superior	• TCP • FC: compatible con las versiones 4.3 y posteriores	Baja (menos de 5 ms)	Replicación
Síncrono: archivo	4.x o superior	• TCP • La replicación síncrona de archivos mediante la replicación metro (con falla automática cuando se configura el testigo) es compatible con las versiones 4.3 y posteriores. • FC: compatible con las versiones 4.4 y posteriores.	Baja (menos de 5 ms)	Replicación

- Para el tipo de conexión TCP, asegúrese de que se cumplan las siguientes condiciones:
  - Las redes de almacenamiento deben configurarse con el propósito de replicación.
  - La red debe estar asignada a al menos un puerto.
  - Cada puerto debe contar con al menos dos direcciones IP.
- Para la replicación mediante la conexión FC (incluido metro), todas las conexiones FC deben utilizar switches FC (la conexión directa o punto a punto no son compatibles).
- No se admite la modificación del tipo de conexión de datos en un sistema remoto. Para modificar el tipo de conexión de datos, elimine el sistema remoto y cree un nuevo sistema remoto con el nuevo tipo de conexión de datos.

NOTA: Después de eliminar y volver a generar el sistema remoto, todos los datos NAS que se replicaron en este dejan de ser válidos. Como resultado, todos los datos NAS existentes se copian en el sitio remoto. Para la replicación de bloques, los datos del sitio remoto se reutilizan y solo se copian datos incrementales en el sistema remoto.

- Los tipos de conexión TCP y FC no se pueden usar simultáneamente para replicar datos entre dosPowerStoresistemas. Es posible replicar datos del sistema A al sistema B mediante el tipo de conexión TCP, y del sistema A al sistema C mediante el tipo de conexión FC.

NOTA: Para sistemas remotos con el tipo de conexión TCP, asegúrese de haber configurado la red de almacenamiento con la replicación como propósito (consulte Establecer el propósito del sistema remoto) y haberla asignado a al menos un puerto.

Consideraciones para el respaldo remoto

El respaldo remoto requiere una conexión de sistema remoto entre un sistema PowerStore y un sistema PowerProtect DD. La conexión remota está asociada con una regla de respaldo remoto y el sistema PowerProtect DD se puede configurar durante la creación de la regla.

Para el respaldo remoto, se deben cumplir las siguientes condiciones:

- Las redes de almacenamiento deben configurarse con el propósito de replicación.
- La red debe estar asignada a al menos un puerto.
- El sistema PowerStore debe ejecutar la versión 3.x o superior.
- Para obtener información sobre las versiones de PowerProtect DDOS compatibles, consulte *Matriz de soporte simple de PowerStore de Dell Technologies*.
- La red de almacenamiento de PowerStore debe poder comunicarse con la red de transferencia de datos de PowerProtect DD.
- El propósito de la red de almacenamiento debe establecerse en Replicación.

Cuando hay varias redes de almacenamiento con fines de replicación, el sistema selecciona una red de almacenamiento con la máxima conectividad con el sistema remoto PowerProtect DD en los siguientes escenarios:

- Se agrega un sistema remoto.
- Se realiza la verificación y actualización en el sistema remoto.
- La red de almacenamiento se reconfigura de una manera que afecta al sistema remoto PowerProtect DD.

NOTA: Para el respaldo remoto, se recomienda configurar una red de almacenamiento simétrica escalada en todos los dispositivos del clúster.

Agregar una conexión de sistema remoto para replicación y metro

Configurar una conexión de sistema remoto entre el origen y el destinoPowerStoreSistemas para permitir la replicación síncrona y asíncrona, y la protección metro.

Requisitos previos

Antes de crear una conexión de sistema remoto, asegúrese de obtener los siguientes detalles del sistema remoto:

- Dirección IP del sistema
- Credenciales de autenticación de usuario o credenciales temporales para conectarse al sistema

Pasos

1. Seleccionar **Protección** > **Sistemas remotos**.
2. En la ventana **Sistemas remotos**, haga clic en **Agregar**.
3. En el panel deslizable **Agregar sistema remoto**, configure los siguientes campos:
   - Tipo de sistema remoto: seleccionar **PowerStore**.
   - Dirección IP de administración
   - Descripción (opcional)
   - Tipo de conexión de datos
     - TCP: seleccionar latencia de red

       NOTA: Si el sistema remoto se utiliza para la replicación metro o síncrona, la latencia de red se debe configurar en Baja.

     - Fibre Channel (SCSI)

NOTA: Para configurar la replicación mediante FC, asegúrese de lo siguiente:

- Los puertos para la replicación están configurados en ambosPowerStore(determine qué puertos están disponibles para la replicación y zonifique la red FC.
- La conectividad de red se establece entre elPowerStoresistemas en las interfaces de administración.

- Nombre de usuario o ID temporal

4. Haga clic en **Agregar**.
5. En el panel **Autorización de usuarios**, verifique el certificado del sistema remoto y haga clic en **Confirmar**.

Resultados

La nueva conexión de sistema remoto se agrega a la tabla **Sistemas remotos**. Puede pasar el cursor sobre la columna **Funcionalidad** para ver las funcionalidades de protección remota de la nueva conexión.

NOTA: Las funcionalidades que se muestran se derivan de las configuraciones de red y las versiones de software que se ejecutan en los sistemas locales y remotos.

Genere credenciales temporales para la autenticación

Sobre esta tarea

Cuando CAC/PIV está habilitado en PowerStore, la autenticación basada en un nombre de usuario y una contraseña está deshabilitada. Si debe proporcionar un nombre de usuario y una contraseña para la autenticación (como cuando crea una conexión de sistema remoto), puede crear una ID temporal y un secreto mediante PowerStore Manager o una API REST.

NOTA: Las credenciales temporales caducan después de 10 minutos.

NOTA: Para utilizar la API REST a fin de crear las credenciales temporales, ejecute el comando generate_temp_credentials.

Para obtener detalles, consulte la *Guía de configuración de seguridad de PowerStore* en la página Documentación de PowerStore.

Pasos

1. Desde PowerStore Manager, seleccione **Configuración**.
2. En Seguridad, seleccione **Autenticación**.
3. Seleccione la pestaña **Credenciales temporales**.
4. Haga clic en **Generar ID temporal y secreto**.
   Se muestran una ID y un secreto temporales.

Establecer el propósito de la red de almacenamiento

PowerStoreEs compatible con la configuración de puertos dedicados o compartidos para la conectividad y la replicación del host.

Cuando crea una red de almacenamiento, puede establecer el propósito de red en el paso **Detalles de red** del asistente **Crear red de almacenamiento** (**Configuración** > **Redes** > **IP de red** > **Almacenamiento** > **Crear**).

NOTA: Puede seleccionar cualquiera de los propósitos disponibles o todos ellos:

- Almacenamiento (iSCSI)
- Almacenamiento (NVMe/TCP)
- Replicación

Para habilitar la protección de replicación o metro entre dosPowerStoresistemas, seleccione la opción **Replicación** .

Para habilitar el respaldo en PowerProtect mediante TCP, seleccione la opción **Replicación** .

NOTA: Cuando se configuran varias redes de almacenamiento con múltiples IP con el propósito de replicación, la protección remota puede consumir más recursos del sistema. Para configuraciones de red complejas, se recomienda revisar los requisitos de red de protección remota antes de asignar el propósito de replicación.

Para agregar un propósito a una red, seleccione la red y, a continuación, seleccione **Más acciones** > **Reconfigurar**. A continuación, puede asignar el propósito agregado a puertos específicos asignados a la red.

Si un propósito está habilitado para uno o más puertos asignados a una red, no puede eliminar el propósito de esa red. Si desea eliminar un propósito de una red, primero deshabilítelo en todos los puertos asignados a la red.

Para modificar el propósito de un puerto, seleccione **Hardware** > **Puertos** > **[puerto]** > **Más acciones** > **Modificar propósitos asignados**. Seleccione la red pertinente y, a continuación, seleccione o desmarque los propósitos para agregarlos o eliminarlos del puerto, respectivamente.

NOTA: No puede quitar el propósito de replicación de un puerto mapeado a una red de almacenamiento cuando hay un sistema remoto TCP que utiliza esa red.

Cuando se selecciona la red de almacenamiento para una asignación de puertos (en el paso **Asignación para dispositivo** del asistente **Crear red de almacenamiento**), el propósito se muestra en la columna Propósitos asignados al puerto.

Una vez finalizada la configuración, la red de almacenamiento se agrega a la tabla Redes disponibles y el propósito se muestra en la columna Propósitos.

Para ver las redes de almacenamiento mapeadas de un puerto y sus propósitos, seleccione **Hardware** > **Puertos**. La red de almacenamiento asignada para cada puerto se muestra en la columna Red asignada. Si hay más de una red asignada, se muestra la cantidad de redes asignadas. Seleccione el nombre de red o el número que se muestra en la columna Red asignada para mostrar la lista de las redes asignadas al puerto.

Grupos de redes de replicación

Cada sistema remoto puede utilizar diferentes redes y puertos de replicación definidos en un grupo de redes de replicación. Un par de sistemas remotos puede utilizar uno o varios grupos de redes de replicación para el tráfico de datos de replicación. Cuando crea una conexión remota, se crea automáticamente un grupo de redes de replicación predeterminado para el par de sistemas remotos. El grupo predeterminado incluye todas las redes que tienen un propósito de replicación. Puede agregar, modificar y eliminar grupos de redes de replicación según sus necesidades.

Para agregar, modificar y eliminar grupos de redes de replicación, seleccione **Protección** > **Sistemas remotos**. Seleccione un sistema remoto de la lista y, a continuación, elija **Más acciones** > **Administrar grupos de redes**.

Para ver los detalles de los grupos de redes configurados para un par de sistemas remotos, seleccione el nombre del sistema remoto en la lista **Sistemas remotos** (**Protección** > **Sistemas remotos**) con el fin de abrir la ventana **Propiedades** del sistema remoto. En la pestaña Conectividad, se muestra información detallada sobre la red de datos de replicación que se basa en la configuración del grupo de redes de replicación.

Agregar un grupo de red de replicación

Sobre esta tarea

Cuando crea un grupo de red de replicación, se crea la misma configuración de grupo de red en ambos miembros del par de sistemas remotos.

NOTA: Es posible que el grupo de red demore algunos minutos en configurarse en los dos sistemas PowerStore.

Para agregar un grupo de red:

Pasos

1. Seleccione **Protección** > **Sistemas remotos** > **[sistema remoto]**.
2. En el menú **Más acciones**, seleccione **Administrar grupos de red** > **Crear**.
3. En la ventana **Crear grupo de redes**, especifique el nombre del grupo y seleccione las redes locales y remotas de las listas respectivas.
4. Seleccione **Aplicar** para crear el grupo.

Modificar un grupo de red de replicación

Sobre esta tarea

Se recomienda transferir una o más redes del grupo predeterminado y formar un grupo de redes de replicación independiente según sus necesidades

Para modificar un grupo de red de replicación:

Pasos

1. Seleccione **Protección** > **Sistemas remotos** > **[sistema remoto]**.
2. En el menú **Más acciones**, seleccione **Administrar grupos de redes**. En la ventana **Administrar grupos de redes**, se muestran los grupos de red creados para el par de sistemas remotos.
3. Seleccione el grupo que desee modificar y, luego seleccione **Modificar**.
4. En la ventana **Modificar grupo de red**, puede cambiar el nombre del grupo y agregar o eliminar redes locales y remotas del grupo.
5. Cuando haya terminado, seleccione **Modificar** para aplicar los cambios.

Eliminar un grupo de red de replicación

Sobre esta tarea

Para eliminar un grupo de red de replicación:

Pasos

1. Seleccione **Protección** > **Sistemas remotos** > **[sistema remoto]**.
2. En el menú **Más acciones**, seleccione **Administrar grupos de redes**. En la ventana **Administrar grupos de redes**, se muestran los grupos de red creados para el par de sistemas remotos.
3. Seleccione el grupo que desee eliminar y, luego **Eliminar**.
4. Seleccione **Eliminar** para confirmar la selección.

Uso de tramas jumbo con sistemas remotos

Si utiliza tramas jumbo, asegúrese de que estas estén configuradas en ambos lados de la conexión de sistema remoto (puertos y puertos de switch de PowerStore) y en todos los puertos entre los dos arreglos de almacenamiento. La falta de coincidencia en el tamaño de MTU genera una advertencia en los siguientes casos:

- Configuración de una conexión de sistema remoto.
- Modificación de ajustes de la conexión de sistema remoto.
- Uso de la opción **Verificar y actualizar**.

NOTA: No se recomienda cambiar el tamaño de MTU de una red de almacenamiento cuando una sesión de replicación está activa.

NOTA: Si se cambia el tamaño de MTU después de la creación del sistema remoto, es necesario deshabilitar y, a continuación, habilitar (rehabilitar) los puertos de red del switch que está conectado a los puertos etiquetados para replicación de PowerStore con el fin de aplicar el cambio en el sistema remoto.

Para cambiar el tamaño de MTU:

1. Ponga en pausa la sesión de replicación.
2. Cambie el tamaño de la MTU de la red de almacenamiento (**Ajustes de configuración** > **Redes** > **MTU del clúster**).
3. Ejecute **Verificar y actualizar** en el sistema remoto para confirmar que no se emita ninguna advertencia.
4. Reanude la sesión de replicación.

Agregar una conexión de sistema remoto para el respaldo remoto

Configure una conexión de sistema remoto entre un sistema PowerStore y un sistema PowerProtect DD para habilitar el respaldo remoto.

Requisitos previos

Antes de agregar la conexión remota, asegúrese de haber obtenido los siguientes detalles del sistema PowerProtect DD:

- Dirección IP del dispositivo PowerProtect DD
- Nombre de la unidad de almacenamiento
- Parámetros de transferencia de datos

NOTA: La creación de un sistema remoto con información de identificación de unidad de almacenamiento no válida da lugar a una pérdida de la conexión de datos. En ese caso, en la columna Estado en **Protección** > **Sistema remoto** > **[PowerProtect DD]** > **Conectividad** se muestra Error de autenticación. Seleccione **Modificar** para PowerProtect DD y corrija las credenciales no válidas. Para obtener más información, consulte el artículo de la base de conocimientos de Dell 000208506 (Si se cambia la contraseña de la cuenta de usuario de PowerProtect DD...).

Sobre esta tarea

NOTA: Puede agregar un único dispositivo PowerProtect DD al mismo clúster de PowerStore varias veces utilizando un ID de unidad de almacenamiento diferente cada vez. De esa manera, puede respaldar diferentes recursos en diferentes ubicaciones dentro de un único sistema PowerProtect DD.

NOTA: Si la unidad de almacenamiento se quita del sistema DD, se produce una pérdida de conexión de datos completa y se deben limpiar las sesiones remotas y las instantáneas. Para obtener más información, consulte el artículo de la base de conocimientos de Dell 000208497 (Si se extrae una unidad de almacenamiento de DD...).

Pasos

1. Seleccione **Protección** > **Sistemas remotos**.
2. En la ventana **Sistemas remotos**, haga clic en **Agregar**.
3. En el panel deslizable **Agregar sistema remoto**, configure los siguientes campos:
   - Tipo de sistema remoto: seleccione **PowerProtect DD**.
   - Dirección IP de administración
   - Descripción (opcional)
   - Nombre de usuario y contraseña de administración
   - Nombre de la unidad de almacenamiento
   - Dirección IP, nombre de usuario y contraseña de transferencia de datos
4. Configure la opción Habilitar cifrado.
   - Cuando el cifrado está deshabilitado, la conexión con PowerStore no utiliza TLS ni autenticación.
   - Cuando el cifrado está habilitado, la conexión con PowerStore utiliza el modo de autenticación de contraseña bidireccional de DD Boost y negocia el nivel de cifrado que se basa en los ajustes de seguridad globales de DD Boost.

     NOTA: Se recomienda habilitar el cifrado cuando el sistema remoto es DDVE en la nube.
5. Haga clic en **Agregar**.
6. En el panel **Autorización de usuarios**, verifique el certificado del sistema remoto y haga clic en **Confirmar** para crear la conexión remota.

Resultados

El nuevo sistema se agrega a la lista **Sistemas remotos**. El tipo del sistema es PowerProtect DD y la funcionalidad es Respaldo remoto.

3

Instantáneas

Este capítulo contiene la siguiente información:

Temas:

Crear una instantánea

Cree una instantánea para guardar el estado de un recurso de almacenamiento en un determinado punto en el tiempo, lo que permite la restauración a un estado anterior.

Cuando crea una instantánea, se guarda el estado del recurso de almacenamiento y todos los archivos y los datos que contiene en un momento dado. Puede usar instantáneas para restaurar todo el recurso de almacenamiento a un estado anterior. Puede crear una instantánea de un volumen, Grupo de volúmenesun sistema de archivos o una máquina virtual.

Antes de crear una instantánea, tenga en cuenta lo siguiente:

- Las instantáneas no son copias completas de los datos originales. No confíe en instantáneas en el caso de operaciones de duplicación, recuperación ante desastres ni herramientas de alta disponibilidad. Debido a que las instantáneas provienen parcialmente de datos en tiempo real de los recursos de almacenamiento, pueden volverse inaccesibles si el recurso de almacenamiento también lo está.
- A pesar de que las instantáneas son eficientes en cuanto a uso del espacio, consumen la capacidad general de almacenamiento del sistema. Asegúrese de que el sistema tenga capacidad suficiente para alojar las instantáneas.
- Cuando configure instantáneas, revise la política de retención de instantáneas asociada con el recurso de almacenamiento. Es conveniente cambiar la política de retención en las reglas asociadas o configurar manualmente una política de retención diferente, según el propósito de la instantánea.
- Las instantáneas manuales que se crean con PowerStore Manager se conservan durante una semana después de su creación (a menos que se configure de otro modo).
- Si se alcanza el número máximo de instantáneas, no se pueden crear más. En este caso, para habilitar la creación de nuevas instantáneas, debe eliminar las instantáneas existentes.

  NOTA: Para obtener información sobre los límites de instantáneas, consulte *la Matriz de soporte simple de Dell Technologies PowerStore* en la página PowerStore Documentation.

- Para configurar instantáneas seguras (especialmente cuando se configuran como parte de una política de protección local), se recomienda revisar los requisitos del negocio con un administrador antes de continuar. Las instantáneas seguras no se pueden eliminar hasta el final del período de retención y es necesario planificar con anticipación para evitar alcanzar el límite máximo de instantáneas. Para obtener detalles sobre las instantáneas seguras, consulte Instantáneas seguras.

Si no puede ver las instantáneas que se crearon para un objeto de almacenamiento, agregue la columna Instantáneas a la tabla mediante **Mostrar/ocultar columnas de tabla**. En la columna Instantáneas, se muestra la cantidad de instantáneas que se crearon para cada objeto. Si se hace clic en el número, se abre la ventana **Instantáneas**, en la que se proporciona información detallada sobre cada instantánea.

Crear una instantánea de un volumen

Sobre esta tarea

Si desea crear una única instantánea de un volumen (y no como parte de una política de protección asignada), utilice la opción **Crear instantánea**.

NOTA: Puede utilizar el mismo procedimiento para crear una instantánea de un grupo de volúmenes.

Pasos

1. Para abrir la ventana **Volúmenes**, seleccione **Almacenamiento** > **Volúmenes**.
2. Haga clic en la casilla de verificación junto al volumen pertinente para elegirlo y, a continuación, seleccione **Proteger** > **Crear instantánea**.
3. En el panel deslizable **Crear instantánea de volumen**, ingrese un nombre único para la instantánea y establezca la **Política de retención local**.

   NOTA: El período de retención se establece en una semana de manera predeterminada. Puede establecer un período de retención diferente o seleccionar **Sin eliminación automática** para que la retención sea indefinida.

4. Si desea crear una instantánea segura, configure un período de retención y seleccione la opción **Instantánea segura**.
5. Haga clic en **Crear instantánea**.

Crear una instantánea de un sistema de archivos

Sobre esta tarea

Si desea crear una única instantánea de un sistema de archivos (y no como parte de una política de protección asignada), utilice la opción **Crear instantánea**.

Pasos

1. Para abrir la ventana **Sistemas de archivos**, seleccione **Almacenamiento** > **Sistemas de archivos**.
2. Haga clic en la casilla de verificación junto al sistema de archivos pertinente para elegirlo y, a continuación, seleccione **Proteger** > **Crear instantánea**.
3. En el panel deslizable **Crear instantánea de sistema de archivos**, ingrese un nombre único para la instantánea y configure la **Política de retención local**.

   NOTA: El período de retención se establece en una semana de manera predeterminada. Puede establecer un período de retención diferente o seleccionar **Sin eliminación automática** para que la retención sea indefinida.

4. Seleccione el Tipo de acceso a instantánea de archivos.
5. Si la publicación de eventos se configuró en el servidor NAS, puede optar por habilitarla.
6. Haga clic en **Crear instantánea**.

Crear una instantánea de una máquina virtual

Sobre esta tarea

Si desea crear una única instantánea de una máquina virtual (y no como parte de una política de protección asignada), utilice la opción **Crear instantánea**.

Pasos

1. Para abrir la ventana **Máquinas virtuales**, seleccione **Computación** > **Máquinas virtuales**.
2. Haga clic en la casilla de verificación junto a la máquina virtual pertinente para elegirla y, a continuación, seleccione **Proteger** > **Crear instantánea**.
3. En el panel deslizable **Crear instantánea de máquina virtual**, ingrese un nombre único para la instantánea.
4. De manera opcional, ingrese una descripción breve.
5. Haga clic en **Crear instantánea**.

Crear un clon delgado

Los clones delgados son copias con capacidad de escritura de una instantánea, un volumen,Grupo de volúmeneso el sistema de archivos al que puede acceder un host. A diferencia de un clon completo, un clon delgado es una copia con uso eficiente del espacio que comparte

bloques de datos con su objeto primario y no un respaldo completo del recurso original. Se puede crear un clon delgado directamente como una copia del objeto primario o con una de sus instantáneas.

Los clones delgados conservan el acceso de lectura completo al recurso original. Puede modificar los datos dentro del clon delgado y conservar la instantánea original.

Con clones delgados, puede establecer puntos jerárquicos en el tiempo para conservar los datos en diferentes etapas de modificación de datos. Si se elimina, se migra o se replica el recurso primario, el clon delgado no se ve afectado.

NOTA: Si un volumen primario se migra de un dispositivo a otro, los clones delgados del volumen también se migran.

Crear un clon delgado de un volumen oGrupo de volúmenes

Sobre esta tarea

Puede realizar las siguientes acciones en clones delgados de volúmenes y grupos de volúmenes:

- Asignar clones delgados a diferentes hosts.
- Actualice el clon delgado.
- Restaurar el clon delgado desde un respaldo.
- Aplicar políticas de protección a clones delgados.

Pasos

1. Seleccionar **Almacenamiento** > **Volúmenes** o **Almacenamiento** > **Grupos de volúmenes** para abrir la ventana de recursos pertinente.
2. Haga clic en la casilla de verificación junto al volumen correspondiente oGrupo de volúmenesy, a continuación, seleccione **Replanificación** > **Crear clon delgado**.
3. En la ventana deslizable **Create Thin Clone** , realice lo siguiente:
   - Ingrese un nombre de clon delgado.
   - Ingrese una descripción.
   - Establezca una política de QoS.
   - Establezca una política de rendimiento (solo para clones delgados creados a partir de volúmenes).
   - Configure la conectividad de host (solo para los clones delgados que se crean a partir de volúmenes).
   - Establezca una política de protección.
4. Haga clic en **Clonar**.

Crear un clon delgado de un sistema de archivos

Sobre esta tarea

Puede realizar las siguientes acciones en clones delgados de volúmenes y grupos de volúmenes:

- Asignar clones delgados a diferentes hosts.
- Restaurar el clon delgado desde un respaldo.
- Aplicar políticas de protección a clones delgados.

Pasos

1. Seleccione **Almacenamiento** > **Sistemas de archivos** para abrir la ventana **Sistemas de archivos**.
2. Haga clic en la casilla de verificación junto al sistema de archivos pertinente y, a continuación, seleccione **Proteger** > **Clonar sistema de archivos**
3. En la ventana deslizable **Crear clon delgado**, configure el nombre del clon delgado y, opcionalmente, una descripción
4. Si la publicación de eventos se configuró en el servidor NAS, puede optar por habilitarla.
5. Haga clic en **Clonar**.

Crear un clon delgado de una instantánea

Sobre esta tarea

Puede crear un clon delgado de una instantánea creada para un volumen, un grupo de volúmenes o un sistema de archivos.

Pasos

1. Abra la ventana del recurso de almacenamiento pertinente.
2. Haga clic en un recurso para abrir su ventana Visión general.
3. Haga clic en la pestaña **Protección**.
4. Haga clic en **Instantáneas** para ver la lista de instantáneas creadas para el recurso.
5. Seleccione una instantánea de la tabla y, a continuación, seleccione **Más acciones** > **Crear un clon delgado usando una instantánea**.

Uso de clones para acceder a instantáneas de solo lectura desde los hosts

El mapeo y la anulación del mapeo de instantáneas de bloques a hosts no se admite en PowerStore. Para permitir que un host conectado acceda a una instantánea, cree un clon delgado de la instantánea y asígnela a un host. Una vez que crea el clon delgado, puede usar la operación de actualización para actualizarlo a partir de diferentes instantáneas. Para obtener más información, consulte Actualizar un recurso de almacenamiento.

Las instantáneas de archivos se pueden montar directamente en hosts (para permitir el acceso de solo lectura) o mediante la creación de un clon delgado (para permitir el acceso de lectura y escritura). Para montar el sistema de archivos directamente, las instantáneas se pueden exportar como exportaciones NFS o recursos compartidos de SMB.

Puede exportar instantáneas con uno de los siguientes tipos de acceso:

- Protocolo: la instantánea se exporta con un nuevo nombre de recurso compartido.
- .snapshot: puede ver la instantánea en Unix/Linux en el directorio .snapshot del sistema de archivos y, en Windows, si hace clic con el botón secundario en el sistema de archivos y selecciona la opción **Versión anterior**.

Actualizar un recurso de almacenamiento

La operación de actualización se usa para reemplazar el contenido de un recurso de almacenamiento con el contenido de un recurso relacionado (un clon o una instantánea secundaria indirecta). Puede crear un duplicado del entorno de producción que se usará con distintos propósitos (como prueba y desarrollo, generación de informes, etc.). Para garantizar que el entorno duplicado permanezca actualizado, se debe actualizar con un recurso de almacenamiento que incluya los cambios recientes.

Puede usar la operación de actualización en los siguientes escenarios:

- Actualizar un clon delgado a partir del volumen base.
- Actualizar un recurso de almacenamiento o un clon delgado a partir de otro clon delgado en la familia.
- Actualizar un recurso de almacenamiento o un clon delgado a partir de una instantánea de un volumen de base o clon delgado relacionado.

En el caso de los sistemas de archivos, puede actualizar una instantánea de un sistema de archivos con el sistema de archivos primario directo.

Si actualiza el clon delgado de una instantánea que tiene instantáneas derivadas, estas permanecen sin cambios y la jerarquía de la familia se mantiene intacta. Si actualiza un Grupo de volúmenes, también se actualiza la imagen de un punto en el tiempo en todos los volúmenes miembros.

Cuando actualice un recurso a partir de una instantánea que se replicó desde un sistema remoto, compruebe los valores de tiempo de creación y datos de origen para asegurarse de usar la instantánea correcta. El valor **Hora de datos de origen** de las instantáneas replicadas refleja la hora original de los datos de origen y el valor **Hora de creación** se actualiza a la hora de la replicación.

NOTA: Dado que, mediante la operación de actualización, se reemplaza el contenido de un recurso de almacenamiento, se recomienda tomar una instantánea del recurso antes de actualizarlo. La creación de un respaldo le permite volver a un momento dado previo.

Antes de actualizar una instantánea, es obligatorio apagar la aplicación y desmontar el volumen o el sistema de archivos que se ejecuta en el host de producción y, a continuación, vaciar la caché del host para evitar daños en los datos durante la operación de actualización.

Actualizar un volumen mediante una instantánea

Sobre esta tarea

Para actualizar un volumen mediante una instantánea:

Pasos

1. Abra la ventana de la lista de volúmenes.
2. Haga clic en el volumen desde el que se tomó la instantánea para abrir su ventana Visión general.
3. Haga clic en la pestaña **Protección** y, a continuación, en **Instantáneas**.
4. En la lista de instantáneas, seleccione la instantánea que desea usar para la operación de actualización.
5. Haga clic en **Más acciones** > **Actualizar usando instantánea**.
6. En el panel deslizable **Actualizar usando instantánea**, seleccione el volumen o clon que desea actualizar en la lista desplegable **Volumen que se está actualizando**.
7. Seleccione si desea crear una instantánea de respaldo para el volumen actualizado (la opción se selecciona de manera predeterminada).
8. Haga clic en **Actualizar**

Actualizar un volumen desde un volumen relacionado

Sobre esta tarea

Puede actualizar un volumen mediante un volumen relacionado (un clon o una instantánea secundaria indirecta).

Pasos

1. Abra la ventana de la lista de volúmenes
2. Seleccione un volumen y, a continuación, seleccione **Replanificar** > **Actualizar usando un volumen relacionado**.
3. En el panel deslizable **Actualizar usando un volumen relacionado**, haga clic en **Seleccionar el volumen desde el cual actualizar** y seleccione el volumen de origen.
4. Haga clic en **Actualizar**.

Actualizar una instantánea de un sistema de archivos

Sobre esta tarea

Puede actualizar una instantánea de un sistema de archivos con su sistema de archivos primario directo.

Pasos

1. Abra la ventana de la lista de sistemas de archivos.
2. Haga clic en el sistema de archivos desde el que se tomó la instantánea para abrir su ventana Visión general.
3. Haga clic en la pestaña **Protección** y, a continuación, en **Instantáneas**.
4. En la lista de instantáneas, seleccione la instantánea que desea usar para la operación de actualización.
5. Haga clic en **Más acciones** > **Actualizar usando instantánea**.
6. Haga clic en **Actualizar**.

Actualizar un clon de servidor NAS

Actualice el servidor NAS clonado con los datos más actualizados del origen sin necesidad de crear un clon.

Requisitos previos

Cuando un servidor NAS de origen experimenta cambios significativos en la configuración y en los datos, el servidor NAS clonado se debe actualizar con los cambios. A partir de PowerStore 4.4, puede actualizar un clon de servidor NAS con los cambios realizados en el servidor de origen.

Un clon de servidor NAS no se puede actualizar en los siguientes casos:

- El clon no tiene un origen válido (puede localizar el origen del clon mediante el**Origen del servidor NAS**en la tabla **NAS Servers** .
- El clon contiene uno o más sistemas de archivos que no existen en el host (sistemas de archivos huérfanos).
- El origen o el clon contiene sistemas de archivos habilitados para FLR.
- El servidor NAS es parte de un proceso activo de transferencia de NAS.

Si se creó un nuevo sistema de archivos en el origen, se duplica en el destino durante la actualización.

Si se elimina un sistema de archivos del servidor NAS de origen o se crea un nuevo sistema de archivos en el servidor NAS de clon, la actualización del clon falla. Para actualizar el clon, es necesario eliminar los sistemas de archivos huérfanos y reiniciar la operación de actualización. Para localizar los sistemas de archivos huérfanos, seleccione el servidor NAS clonado en la tabla **NAS Servers** y, a continuación, seleccione**Replanificación** > **Ver sistemas de archivos huérfanos**.

NOTA: Los cambios en la configuración que no sean nombres e IP de SMB y NFS no se sobrescriben como parte de la operación de actualización.

NOTA: Las políticas de QoS no se actualizan desde el origen al clon.

Sobre esta tarea

Para actualizar un clon de servidor NAS:

Pasos

1. Abra la ventana **NAS Servers** .
2. Seleccione un clon de servidor NAS y, a continuación, seleccione**Replanificación** > **Actualizar clon**.

Resultados

El servidor NAS clonado se actualiza con datos del servidor NAS de origen y la fecha y hora de actualización se actualizan en el**Última actualización**en la tabla **NAS Servers** .

Restaurar un recurso de almacenamiento a partir de una instantánea

La operación de restauración se usa para reconstruir un entorno después de un evento que puede haber puesto en riesgo sus datos. Puede usar la operación de restauración para reemplazar el contenido de un recurso de almacenamiento primario por datos de una instantánea secundaria directa. La restauración restablece los datos del recurso de almacenamiento primario al punto en el tiempo en el que se tomó la instantánea.

Antes de restaurar una instantánea, es obligatorio apagar la aplicación y desmontar el sistema de archivos que se ejecuta en el host de producción y, a continuación, vaciar la caché del host para evitar daños en los datos durante la operación de restauración.

Si restaura un Grupo de volúmenes, todos los volúmenes miembros se restauran al punto en el tiempo asociado con la instantánea de origen.

Cuando restaure un recurso a partir de una instantánea que se replicó con un sistema remoto, compruebe el valor de tiempo de los datos de origen para garantizar que usa la instantánea correcta.

Restaurar un volumen o un grupo de volúmenes desde una instantánea

Sobre esta tarea

NOTA: Para evitar problemas de integridad de datos, antes de restaurar un volumen, es obligatorio apagar las aplicaciones que lo utilizan y colocar el volumen offline en el host.

Pasos

1. Seleccione la casilla de verificación junto al volumen o el grupo de volúmenes que desea restaurar.
2. Seleccione **Proteger** > **Restaurar desde instantánea**.
3. En el panel deslizable **Restaurar volumen desde instantánea**, seleccione la instantánea que se usará para la operación de restauración.
4. Elija si desea crear una instantánea de respaldo del volumen o el grupo de volúmenes restaurado (la opción se selecciona de manera predeterminada).
5. Haga clic en **Restaurar**.

Restaurar un sistema de archivos desde una instantánea

Sobre esta tarea

Antes de continuar con la operación de restauración, las aplicaciones que usan el sistema de archivos se deben apagar y el sistema de archivos se debe colocar offline en los hosts para impedir problemas de integridad de datos.

Pasos

1. Seleccione la casilla de verificación junto al sistema de archivos que desea restaurar.
2. Seleccione **Proteger** > **Restaurar desde instantánea**.
3. En el panel deslizable **Restaurar sistema de archivos desde instantánea**, seleccione la instantánea que se usará para la operación de restauración.
4. Elija si desea crear una instantánea de respaldo del sistema de archivos restaurado (la opción se selecciona de manera predeterminada).
5. Haga clic en **Restaurar**.

Instantáneas seguras

Las instantáneas seguras no se pueden eliminar antes de su fecha de vencimiento. Utilice instantáneas seguras para proteger sus datos de ataques maliciosos.

NOTA: Las instantáneas seguras son compatibles con las instantáneas de bloques que se crean para volúmenes o grupos de volúmenes y para las instantáneas del sistema de archivos (tanto de protocolo como .snapshot).

PowerStore le permite generar instantáneas seguras. A diferencia de las instantáneas normales, las instantáneas seguras no se pueden eliminar manualmente y se eliminan solo cuando alcanzan su fecha de vencimiento.

NOTA: Si desea usar instantáneas seguras, se recomienda revisar los requisitos del negocio con un administrador antes de continuar para evitar alcanzar el límite máximo de instantáneas.

Las instantáneas seguras proporcionan protección contra la eliminación accidental o maliciosa de datos de respaldo y son eficaces contra ataques en los que se exige rescate. La generación de instantáneas seguras garantiza la capacidad de restaurar los datos a un punto en el tiempo anterior.

Para generar manualmente una instantánea segura de un volumen, un grupo de volúmenes o un sistema de archivos, seleccione la opción **Instantánea segura** en el panel **Crear instantánea**. Para generar instantáneas seguras como parte de una política de protección local, cree una regla de instantánea y seleccione la opción **Instantánea segura** en el panel **Crear regla de instantánea**. Agregue la columna **Instantáneas seguras habilitadas** a la tabla **Reglas de instantáneas** para ver qué reglas generan instantáneas seguras.

NOTA: Asegúrese de configurar un período de retención para las instantáneas seguras. La opción de instantánea segura no está disponible cuando se selecciona **Sin eliminación automática**.

NOTA: Cuando una instantánea de un grupo de volúmenes se configura como segura, todos los miembros del grupo se configuran como seguros.

Puede ver y monitorear instantáneas seguras agregando la columna Instantáneas seguras a la tabla Instantáneas. También puede filtrar las listas de instantáneas para ver las instantáneas seguras.

Es posible convertir instantáneas no seguras existentes en instantáneas seguras seleccionando la opción **Instantánea segura** en el panel **Detalles de la instantánea**. De manera similar, puede convertir una regla de instantánea no segura en segura seleccionando la opción **Instantánea segura** en el panel **Propiedades** de la regla de instantánea.

NOTA: Solo las instantáneas que crea la regla después de modificarla como segura son instantáneas seguras. Las instantáneas creadas antes de la modificación permanecen como no seguras.

Cuando una regla de instantánea segura se elimina o se quita de una política, o cuando se cancela la asignación de una política que incluye una regla de instantánea segura de un recurso, las instantáneas seguras que creó la regla permanecen seguras y no se pueden eliminar hasta que vencen. Los objetos de almacenamiento que tienen instantáneas seguras no se pueden eliminar hasta que las instantáneas caduquen.

La fecha de vencimiento de las instantáneas seguras no se puede reducir, pero se puede modificar a una fecha y hora posteriores.

Instantánea segura y replicación:

- Para los clústeres en los que se ejecuta PowerStoreOS 3.5 y versiones superiores, todas las instantáneas seguras que se generan en el sistema local se replican como seguras en el clúster remoto.
- Si en el clúster de destino se ejecuta una versión de PowerStoreOS anterior a 3.5, las instantáneas seguras se replican como instantáneas normales en ese clúster. En ese caso, la regla de instantánea en el clúster de destino no es segura. Si se produce una conmutación por error en un clúster en el que se ejecuta una versión de PowerStoreOS anterior a 3.5, no se crean instantáneas seguras para el recurso de almacenamiento.
- Puede restaurar una instantánea segura.
- No puede actualizar una instantánea segura.

Después de la actualización de PowerStore a la versión 3.5, las instantáneas y las reglas de instantánea no seguras existentes se pueden modificar a seguras.

Si debe eliminar una instantánea segura que no ha alcanzado su fecha de vencimiento, póngase en contacto con el soporte de Dell.

4

Políticas de protección

Este capítulo incluye la siguiente información:

Temas:

Reglas de instantánea

Puede crear reglas de instantánea para controlar parámetros, como la frecuencia de creación y el período de retención de instantáneas. También puede crear reglas de instantánea para generar instantáneas seguras. Las reglas de instantánea, junto con las reglas de replicación y las reglas de respaldo remoto, permiten configurar y aplicar políticas de protección de datos coherentes a los recursos de almacenamiento según los requisitos de protección de datos.

Si desea crear una regla de instantánea además de las reglas existentes, se recomienda revisar los requisitos del negocio con un administrador antes de continuar. Es posible que esto permita lograr y mantener políticas coherentes en todo el sistema.

Crear una regla de instantáneas

Pasos

1. Seleccione **Protección** > **Políticas de protección**.
2. En la ventana **Políticas de protección**, haga clic en **Reglas de instantáneas** en la barra **Protección**.
3. En la ventana **Reglas de instantáneas**, haga clic en **Crear**.
4. En el panel deslizable **Crear regla de instantáneas**, ingrese un nombre para la nueva regla.
5. Establezca los siguientes valores:
   - Seleccione los días en los que se creará una instantánea.
   - Configure la frecuencia y la hora de inicio:
     - Para que una instantánea se cree en un intervalo fijo, seleccione esta opción y establezca la cantidad de horas después de la cual se creará una instantánea.
     - Para que se cree una instantánea en un momento específico de los días seleccionados, seleccione la opción **Hora del día** y establezca la hora y la zona horaria.
   - Configure el período de retención.
   - Para crear instantáneas seguras, seleccione la opción **Instantánea segura**. Para obtener detalles sobre las instantáneas seguras, consulte Instantáneas seguras.

     NOTA: Se recomienda revisar los requisitos del negocio con un administrador antes de continuar para evitar alcanzar el límite máximo de instantáneas.

   - En el caso de las instantáneas de archivos, seleccione el tipo de acceso de la instantánea de archivos.
6. Haga clic en **Crear**.

Reglas de replicación

Una regla de replicación es un conjunto de parámetros que el sistema usa para sincronizar los datos en una sesión de replicación. Los parámetros incluyen la selección de un destino de replicación, el tipo de replicación y la configuración de un objetivo de punto de recuperación (RPO).

Una vez que haya configurado una regla de replicación, puede optar por usarla en una política de protección nueva o existente, con lo cual los parámetros de la sesión de replicación cambian o se aplican automáticamente para cualquier recurso de almacenamiento que utilice la política de protección.

No puede cambiar una política de protección de modo que use una regla de replicación diferente con un sistema remoto diferente. Para cambiar una política de protección con una regla de replicación usando un sistema remoto diferente, elimine la política anterior antes de asignar una nueva.

NOTA: El cambio de un sistema remoto requiere una sincronización completa.

Si desea crear una regla de replicación además de las reglas existentes, se recomienda revisar los parámetros y los requisitos del negocio con un administrador antes de continuar. Es posible que esto permita lograr y mantener políticas coherentes en todo el sistema.

Crear una regla de replicación

Pasos

1. Seleccione **Protección** > **Políticas de protección**.
2. En la ventana **Políticas de protección**, haga clic en **Reglas de replicación** en la barra **Protección**.
3. En la ventana **Reglas de replicación**, haga clic en **Crear**.
4. En el panel deslizable **Crear regla de replicación**, ingrese un nombre para la nueva regla.
5. Establezca los siguientes valores:
   - Cree un nombre de regla.
   - Seleccione un destino de replicación existente o configure un destino nuevo.
   - Seleccione el tipo de replicación (asíncrona o síncrona).

     NOTA: La selección del tipo de replicación síncrona establece los valores de RPO y umbral de alerta en cero. Estos valores no se pueden modificar.

   - Si seleccionó el tipo de replicación asíncrona:
     - Establezca el valor de RPO.
     - Establezca el valor de Umbral de alerta.
6. Haga clic en **Crear**.

Objetivo de punto de recuperación

El objetivo de punto de recuperación (RPO) indica la cantidad aceptable de datos, medida en unidades de tiempo, que se pueden perder en caso de una falla. Cuando configura una regla de replicación, puede establecer la sincronización automática de acuerdo con el RPO. Los posibles valores de RPO varían de 5 minutos a 24 horas. El valor predeterminado de RPO es una hora.

NOTA: Un intervalo de RPO más pequeño proporciona más protección y consume menos espacio. Sin embargo, tiene un impacto más alto en el rendimiento, lo que genera más tráfico de red. Un intervalo de RPO mayor puede aumentar el consumo de espacio, lo cual puede afectar a los programas de instantáneas y los umbrales de espacio.

Umbral de alerta

Cuando configura una regla de replicación asíncrona, puede especificar un umbral de alerta, que es la cantidad de tiempo que espera el sistema antes de generar una alerta de cumplimiento si una sesión de replicación no cumple con el RPO. Si se establecer el umbral de alerta en cero, se generarán alertas si el tiempo de sincronización real supera el RPO.

Reglas de respaldo remoto

Cree una regla de respaldo remoto y agréguela a una política para habilitar el respaldo remoto.

Una regla de respaldo remoto es un conjunto de parámetros que permiten que el sistema PowerStore respalde volúmenes y grupos de volúmenes en un dispositivo PowerProtect DD. La regla especifica el sistema de destino en el que se crean los respaldos, su tiempo de retención y la frecuencia de la operación de respaldo.

NOTA: Las reglas de respaldo remoto no son compatibles con instantáneas seguras.

Una vez que se genere la regla de respaldo remoto, agréguela a una política de protección existente o genere una nueva política.

NOTA: Una política de protección puede incluir solo una regla de respaldo remoto.

Crear una regla de respaldo remoto

Pasos

1. Seleccione **Protection** > **Protection Policies**.
2. En la ventana **Políticas de protección**, haga clic en **Reglas de respaldo remoto** en la barra **Protección**.
3. En la ventana **Reglas de respaldo remoto**, seleccione **Crear**.
4. Establezca los siguientes valores:
   - Nombre de la regla
   - Destino: seleccione un sistema PowerProtect DD en la lista desplegable o configure un nuevo sistema (consulte Agregar una conexión remota para respaldo remoto).
   - Días de la semana en los que se crea el respaldo.
   - Frecuencia/hora de inicio: cuando se selecciona **Cada**, la frecuencia de respaldo se establece en horas o días. Cuando se selecciona **Hora del día**, la frecuencia de respaldo se establece en días.
   - Período de retención: seleccione la unidad de tiempo (horas, días, meses o años) y establezca el período para conservar los respaldos generados.

     NOTA: La retención máxima es de 70 años.
5. Haga clic en **Create**.

Crear una política de protección

Sobre esta tarea

Cree una política de protección para proporcionar protección local o remota para los recursos de almacenamiento. Cada política de protección puede incluir una regla de replicación, una regla de respaldo remoto y hasta cuatro reglas de instantánea. Una regla puede estar en varias políticas.

Pasos

1. Seleccionar **Protección** > **Política de protección**.
2. En la ventana **Políticas de protección**, haga clic en **Crear**.
3. En el panel deslizable **Crear política de protección**, ingrese un nombre para la nueva política.
4. De manera opcional, seleccione las reglas de instantánea que desea incluir en la política o cree una regla de instantánea (consulte Crear una regla de instantánea).
5. De manera opcional, seleccione las reglas de replicación que desea incluir en la política o cree una regla de replicación (consulte Crear una regla de replicación).
6. De manera opcional, seleccione la regla de respaldo remoto que desea incluir en la política o cree una regla de respaldo remoto (consulte Crear una regla de respaldo remoto).
7. Haga clic en **Create**.

Resultados

Cuando crea una política de protección que incluye una regla de replicación, la política se replica automáticamente en el sistema remoto y se asigna a los recursos de destino que crea la política. La política replicada y los nombres de reglas asociados constan de los nombres de políticas y reglas en el sistema de origen y se agregan con el nombre del sistema remoto. Los cambios que se realizan en la política original o en las reglas incluidas se replican en el sistema remoto para garantizar la sincronización. Tras una conmutación por error de replicación, la política replicada se activa en el sistema de destino.

El sistema administra las políticas y las reglas replicadas y no se muestran en las tablas de políticas y reglas del sistema de destino. Sin embargo, puede ver los detalles de las reglas en la pestaña **Protección** de los volúmenes de replicación o los grupos de volúmenes si pasa el puntero sobre el nombre de la política replicada. Para las políticas de protección asignadas a volúmenes metro, se crea una política idéntica de solo lectura en el sistema remoto y se puede ver en la ventana **Políticas de protección** del sistema remotoPowerStoreDirector.

Modificar la política de protección

Puede modificar una política de protección agregando y quitando reglas de instantánea, replicación y respaldo remoto.

Sobre esta tarea

NOTA: El cambio de los ajustes de una política de protección aplica los nuevos ajustes a todos los objetos a los que se asigna la política de protección. Si desea cambiar la política de protección de un recurso, se recomienda crear otra política de protección y asignarla a ese recurso.

No puede cambiar el destino de replicación en una regla de replicación que se usa en políticas de protección asignadas a uno o más recursos de almacenamiento. Para volver a configurar la replicación en un sistema remoto diferente, cancele la asignación de la política de protección y asigne una nueva con una regla de replicación diferente. Si cancela la asignación de una política de protección con una regla de replicación, se elimina la sesión de replicación asociada, y si asigna una nueva política de protección, se crea una sesión, lo que requiere una sincronización completa en el destino nuevo.

Puede cambiar una sesión de replicación asíncrona a replicación síncrona (para recursos de bloques) o viceversa (recursos de bloques y archivos) modificando la regla de replicación que se utiliza en la política de protección.

Pasos

1. Seleccione **Protección** > **Políticas de protección**.
2. Seleccione la casilla de verificación junto a la política pertinente y haga clic en **Modificar**.
3. En el panel deslizable **Propiedades**, puede modificar los siguientes parámetros:
   - Nombre de la política
   - Reglas de instantánea seleccionadas
   - Reglas de replicación seleccionadas
   - Reglas de respaldo remoto seleccionadas
4. Haga clic en **Aplicar**.

Asignar una política de protección

Asigne una política de protección a uno o más recursos de almacenamiento para aplicar las reglas de instantánea, replicación y respaldo remoto incluidas en la política a los recursos de almacenamiento. La política de protección realiza automáticamente operaciones de instantáneas, replicación y respaldo remoto en función de los parámetros especificados.

Si está disponible una política de protección que cumple con los requisitos de protección de datos, puede asignarla a un recurso de almacenamiento en cualquier momento.

Puede asignar una política de protección a un recurso de almacenamiento durante la creación del recurso o en una etapa posterior.

Para la protección del almacenamiento de bloques:

- Asigne políticas de protección que contengan reglas de instantáneas, replicación y respaldo remoto a volúmenes yGrupos de volúmenes.
- Cuando asigna una nueva política de protección que contiene una regla de replicación al recurso de almacenamiento, se requiere una sincronización inicial completa.
- Con el respaldo remoto, cuando se asigna una política que incluye una regla de respaldo remoto a un volumen o grupo de volúmenes, se crea automáticamente una sesión de respaldo remoto en estado Inactivo.

- Si se asigna una política que incluye una regla de respaldo remoto a un recurso que no es compatible con el respaldo remoto, no se hace caso de la regla.
- Con los volúmenes metro, solo puede asignar políticas de protección que incluyan reglas de instantáneas. Una política que incluye una regla de replicación no se puede asignar a un volumen metro. Después de asignar la política de protección al volumen metro o al grupo de volúmenes, la política y las reglas de instantáneas se copian en el sistema remoto y se muestran en las tablas Protection Policies y Snapshot Rules con un icono de candado, lo que indica que son de solo lectura.

Para la protección del almacenamiento de archivos:

- PowerStoreadmite la protección local (instantáneas) en el nivel del sistema de archivos y la protección remota (replicación) en el nivel del servidor NAS.
- Puede asignar una política de protección a un servidor NAS solo si incluye una regla de replicación. La regla de replicación se aplica a todos los sistemas de archivos en el servidor NAS y no se hace caso de las reglas de instantánea (si existen).
- Puede asignar una política de protección a un sistema de archivos solo si incluye una regla de instantáneas. La regla de instantánea se aplica al sistema de archivos y no se hace caso de una regla de replicación (si existe).
- Puede asignar diferentes políticas de protección a un servidor NAS y a los sistemas de archivos que incluye.

Asignar una política de protección a un objeto de almacenamiento

Sobre esta tarea

Asigne una política de protección a un volumen, un grupo de volúmenes, un sistema de archivos o un servidor NAS.

Pasos

1. Seleccione la casilla de verificación del recurso de almacenamiento al que desea asignar una política de protección.
2. Para volúmenes, grupos de volúmenes y sistemas de archivos, seleccione **Proteger** > **Asignar política de protección**. Para los servidores NAS, seleccione **Más acciones** > **Asignar política de protección**.

   NOTA: Si seleccionó un recurso no válido, la opción de asignación queda inactiva. Si pasa el cursor sobre **Asignar política de protección**, se muestra información sobre herramientas en la que se explica por qué no es válido para esta acción.

3. En el panel deslizable **Asignar política de protección**, seleccione la política de protección.
4. Haga clic en **Aplicar**.

Asignar una política de protección a varios objetos de almacenamiento

Sobre esta tarea

Asigne una política de protección a varios objetos de almacenamiento del mismo tipo (volúmenes, grupos de volúmenes, sistemas de archivos o servidores NAS).

Pasos

1. Seleccione **Protección** > **Políticas de protección**.
2. Seleccione la casilla de verificación de una política en la lista y, a continuación, seleccione **Más acciones** > **Asignar política de protección**.

   En el panel deslizable **Asignar política de protección**, se proporciona un resumen de todos los recursos de almacenamiento que ya tienen una política de protección asignada.
3. En el panel deslizable **Asignar política de protección**, seleccione el tipo de recurso y, a continuación, seleccione los objetos pertinentes en la lista de recursos.
4. Repita el paso 3 si desea asignar la política seleccionada a tipos de recurso adicionales.
5. Haga clic en **Asignar**.

Cambiar la política de protección asignada a un objeto de almacenamiento

Sobre esta tarea

Tenga en cuenta las siguientes pautas relacionadas con reglas de replicación:

- El reemplazo de una política de protección que incluye una regla de replicación por una política sin una regla de replicación elimina la replicación de todos los recursos asignados con esa política.
- El reemplazo de una política de protección que incluye una regla de replicación por una política que tiene la misma regla de replicación le permite volver a configurar la protección local sin interrumpir la replicación.
- Es posible reemplazar una política de protección que incluye una regla de replicación por una política con una regla de replicación diferente solo si ambas políticas tienen configurado el mismo sistema remoto.

  NOTA: Para cambiar la asignación de una política de protección con una regla de replicación a un sistema remoto diferente, elimine la política anterior antes de asignar una nueva.

- El reemplazo de una política de protección que incluye una regla de replicación asíncrona por una política que incluye una regla de replicación síncrona puede afectar el rendimiento de las sesiones de replicación de volúmenes y grupos de volúmenes.

Tenga en cuenta las siguientes pautas relacionadas con reglas de respaldo remoto:

- El reemplazo de una política de protección que incluye una regla de respaldo remoto por una política sin una regla de respaldo remoto elimina la protección remota del sistema remoto DD.
- El reemplazo de una política de protección que incluye una regla de respaldo remoto por una política que tiene la misma regla de respaldo remoto hace que el siguiente respaldo sea un respaldo completo (y no incremental).
- El reemplazo de una política de protección que incluye una regla de respaldo remoto por una política con una regla de respaldo remoto diferente y el mismo sistema remoto hace que el siguiente respaldo sea un respaldo completo (y no incremental).

Pasos

1. Seleccione el recurso de almacenamiento pertinente para abrir su ventana **Visión general**.
2. Haga clic en la pestaña **Protección**.
3. Junto al nombre de la política de protección asignada, haga clic en **Cambiar**.
4. En el panel deslizable **Cambiar política de protección**, seleccione una política de protección diferente.
5. Haga clic en **Aplicar**.

Cancelar asignación de una política de protección

Sobre esta tarea

La eliminación de la política de protección de un recurso de almacenamiento da lugar a lo siguiente:

- Las instantáneas y la replicación programadas, según las reglas asociadas con la política, se detienen.
- Las instantáneas existentes permanecen y se conservan en el sistema de acuerdo con los ajustes de la regla de instantánea en el momento de su creación.
- El recurso de almacenamiento de destino permanece en modo de solo lectura. Puede clonar el recurso de almacenamiento de destino para obtener una copia de lectura/escritura o cambiar el atributo **destino de replicación** en la página **Propiedades** del recurso de almacenamiento.

NOTA: No puede cancelar la asignación de una política de protección cuando la importación está en curso.

NOTA: La cancelación de la asignación de una política de protección que incluye una regla de replicación síncrona solo se puede realizar desde el sistema que tiene la política de lectura/escritura (y no la copia de solo lectura de la política).

Pasos

1. Seleccione la casilla de verificación del recurso de almacenamiento al que desea asignar una política de protección.
2. Para volúmenes, grupos de volúmenes y sistemas de archivos, seleccione **Proteger** > **Cancelar asignación de política de protección**. Para servidores NAS, seleccione **Más acciones** > **Cancelar asignación de política de protección**.
3. Haga clic en **Cancelar asignación** para confirmar.

5

Replicación

Este capítulo contiene la siguiente información:

Temas:

Replicación asíncrona

La replicación asíncrona es un modo de replicación en el que las actualizaciones al sistema de destino (como los cambios en el contenido, el tamaño y la membresía) se producen en un intervalo establecido que se basa en el RPO definido. Durante la sincronización, el sistema de destino se actualiza con todos los cambios de datos que se produjeron desde el último ciclo de sincronización.

PowerStore Es compatible con la replicación remota asíncrona de volúmenes, grupos de volúmenes, servidores NAS y Virtual Volumes.

NOTA: La sincronización de volúmenes virtuales solo es compatible con instantáneas de solo lectura.

Para aplicar replicación asíncrona a un recurso de almacenamiento, asigne al recurso una política de protección que incluya una regla de replicación asíncrona. La asignación de una política de protección crea una sesión de replicación que se agrega a la lista de sesiones de replicación (**Protección** > **Replicación**) y en la columna Tipo de replicación se muestra Asíncrona.

La sincronización se produce de manera automática, de acuerdo con un programa definido, o manualmente. Las instantáneas se sincronizan desde el sistema de origen al sistema de destino y mantienen la eficiencia del uso compartido de bloques.

NOTA: La sincronización de instantáneas no es compatible con la replicación de archivos.

Puede iniciar manualmente la sincronización de una sesión de replicación en cualquier momento seleccionando la sesión de replicación y, a continuación, **Sincronizar**. La sesión de replicación debe estar en uno de los siguientes estados:

- Funcionando normalmente
- Sistema en pausa

Durante la sincronización de una sesión de replicación, puede realizar las siguientes acciones:

- Realizar una conmutación por error planificada desde el sistema de origen.
- Realizar una conmutación por error desde el sistema de destino.
- Poner en pausa las sesiones de replicación desde el sistema de origen o de destino.
- Eliminar una sesión de replicación mediante la eliminación de una política de protección.

NOTA: La conmutación por error (planificada o no planificada) solo es posible después de que se escribe una copia de datos de base en el sistema de destino, lo que se indica mediante un estado OK de la sesión de replicación.

Para obtener un resumen de los atributos de la replicación asíncrona y la comparación con la replicación síncrona y metro, consulte Resumen de la replicación.

Replicación asíncrona de bloques

Lo siguiente se aplica a la replicación asíncrona de bloques:

- Cuando se crea una sesión de replicación asíncrona, se crea un recurso de solo lectura coincidente en el sistema de destino. También se crea una definición de solo lectura de la política de protección en el sistema de destino. Esta política se utiliza si se realiza una conmutación por error de la sesión de replicación.
- Cuando se agregan volúmenes a un Grupo de volúmenes o se cambia el tamaño del Grupo de volúmenes durante una sesión de replicación asíncrona, los cambios no aparecen inmediatamente en el destino. Puede realizar una sincronización manual o esperar hasta que se produzca la sincronización según el RPO.
- Puede cambiar de replicación asíncrona a síncrona modificando la regla de replicación en la política de protección asignada.

NOTA: El cambio de la replicación asíncrona a la replicación síncrona puede afectar el rendimiento de las sesiones de replicación de volúmenes y grupos de volúmenes.

Replicación asíncrona de archivos

Lo siguiente se aplica a la replicación asíncrona de archivos:

- La política de protección se asigna al servidor NAS y, de manera predeterminada, todos los sistemas de archivos en un servidor NAS protegido se sincronizan desde el sistema de origen al de destino.
- Puede optar por agregar sistemas de archivos o eliminarlos del servidor NAS, incluso cuando forma parte de una sesión de replicación.
- Cuando los sistemas de archivos se modifican durante una sesión de replicación asíncrona, los cambios se reflejan en el sistema de destino en el siguiente ciclo de sincronización.
- No se admite el cambio de replicación asíncrona a síncrona.
- La replicación de instantáneas no es compatible.

Replicación síncrona

La replicación síncrona es un modo de replicación en el que las actualizaciones de datos en el sistema de origen se replican en el sistema de destino de inmediato cuando se producen (replicación de RPO cero). El uso de la replicación síncrona garantiza que ambos sistemas estén completamente sincronizados en cualquier momento. La replicación síncrona garantiza cero pérdida de datos, pero puede causar latencia, según la distancia entre los sistemas de origen y destino.

NOTA: No se garantiza ninguna pérdida de datos cuando la replicación no funciona con normalidad, como durante pausas de la sesión de replicación o interrupciones de la red.

PowerStore Es compatible con la replicación remota síncrona de volúmenes, grupos de volúmenes, clones delgados, instantáneas de bloques y servidores NAS.

Para aplicar la replicación síncrona a un recurso de almacenamiento, asigne al recurso una política de protección que incluya una regla de replicación síncrona. La asignación de una política de protección crea una sesión de replicación que se agrega a la lista de sesiones de replicación (**Replicación** > **de protección**) y la columna Tipo de replicación muestra Síncrona.

Cuando se crea una sesión de replicación, el recurso de almacenamiento se replica en el sistema de destino. Cuando se realizan actualizaciones en el recurso, solo estas se replican en el sistema de destino.

Puede conmutar por error una sesión de replicación síncrona mediante una conmutación por error planificada o no planificada. Para obtener detalles, consulte la sección Conmutación por error.

La cancelación de la asignación de la política de protección del recurso de almacenamiento elimina la sesión de replicación. Cuando la sesión de replicación funciona con normalidad, la cancelación de la asignación de la política solo se puede realizar en el sistema de origen.

Cuando asigna una política de protección que incluye una regla de replicación síncrona, el sistema de origen tiene una política de lectura/escritura, mientras que el sistema de destino tiene una copia de solo lectura de la política. Solo se puede modificar o eliminar la política de lectura/escritura. Si el sistema que tiene la política de lectura/escritura está inactivo, la realización de una conmutación por error cambia las funciones de los sistemas y le permite administrar la política de protección de lectura/escritura desde el sistema de destino.

Para habilitar la replicación síncrona, el par de sistemas debe configurarse con baja latencia de red (menos de cinco milisegundos). La latencia de red configurada no se puede cambiar mientras están configuradas sesiones de replicación síncrona para estos sistemas.

Para obtener un resumen de los atributos de la replicación síncrona y la comparación con la replicación asíncrona y metro, consulte Resumen de la replicación.

Replicación síncrona de bloques

- Cuando se crea una sesión de replicación síncrona, se crea un recurso de solo lectura coincidente en el sistema de destino. También se crea una definición de solo lectura de la política de protección en el sistema de destino. Esta política se utiliza si se realiza una conmutación por error de la sesión de replicación.
- Instantáneas de usuario:
  - Las instantáneas del recurso que se crearon antes de la creación de la sesión se sincronizan con el sistema de destino.
  - Una vez creada la sesión de replicación, las instantáneas de usuario se ejecutan simultáneamente en los sistemas de origen y destino con contenido casi idéntico.
  - Las instantáneas de usuario que se crean cuando la sesión de replicación está en pausa no se replican en el sistema de destino después de la reanudación o la recuperación.
- Para cambiar los parámetros de un recurso (como el nombre, el tamaño y la política de rendimiento), debe pausar la sesión de replicación.
- Puede cambiar de replicación síncrona a asíncrona modificando la regla de replicación en la política de protección asignada.

Durante la replicación síncrona de bloques, puede realizar lo siguiente:

- Migración dentro del clúster: durante la transferencia, el estado de la sesión de replicación cambia a En pausa para migración. La sesión de replicación reanuda su estado cuando la migración finaliza. Las sesiones que se pausaron cuando se inició la migración permanecen en pausa.
- NDU: las sesiones de replicación cuyo estado es Funcionando normalmente cuando se inicia la NDU continúan activas durante esta. El estado de las sesiones de replicación en pausa cambia a En pausa para NDU.
- Reconfiguración del clúster: puede volver a configurar la red de replicación del clúster, expandir o reducir el clúster o reubicarlo. La replicación se reanuda una vez finalizada la reconfiguración.

Cuando se mapea un volumen en el sistema de destino a un host, el sistema configura la afinidad del nodo para este volumen y, en consecuencia, todas las I/O se dirigen automáticamente al nodo seleccionado. No es necesario pausar y reanudar la sesión de replicación para que la redirección de I/O surta efecto. La configuración de la afinidad del nodo para los volúmenes en el sistema de destino proporciona balanceo de carga e impide la latencia de la replicación. Puede configurar la afinidad del nodo manualmente mediante la API REST.

NOTA: Si no puede ver la columna de afinidad del nodo en la tabla Volúmenes, agréguela mediante **Mostrar/ocultar columnas de tabla**.

Lo siguiente se aplica a la replicación síncrona del grupo de volúmenes:

- Todos los miembros deben residir en el mismo dispositivo.
- Solo los grupos de volúmenes con coherencia con el orden de escritura configurada se pueden asignar con una política de protección que incluya una regla de replicación síncrona.
- Una política de protección asignada a un grupo de volúmenes se aplica a todos los miembros del grupo. Una política de protección no puede proteger volúmenes individuales en un grupo de volúmenes.
- Para cambiar los parámetros de un grupo de volúmenes (como el nombre, la política de rendimiento y la coherencia con el orden de escritura), debe pausar la sesión de replicación que tiene asignada.

Replicación síncrona de archivos

Lo siguiente se aplica a la replicación de archivos:

- La política de protección se asigna al servidor NAS y, de manera predeterminada, todos los sistemas de archivos en un servidor NAS protegido se sincronizan desde el sistema de origen al de destino.
- Puede optar por agregar sistemas de archivos o eliminarlos del servidor NAS, incluso cuando forma parte de una sesión de replicación.
- Cuando se crea una sesión de replicación síncrona, se crean un servidor NAS y sistemas de archivos vacíos en el sistema de destino. También se replican la configuración del servidor de archivos y una política de protección de solo lectura.
- El servidor NAS en el sistema de destino se configura sin la configuración de IP habilitada y todos los sistemas de archivos están disponibles sin recursos compartidos habilitados
- Cuando se crea una sesión de replicación, los sistemas de archivos se replican en el destino. Los cambios posteriores se replican en el destino cuando se producen.
- Para la replicación síncrona, el aumento del tamaño de un sistema de archivos que se está replicando requiere que, en primer lugar, la sesión de replicación se ponga en pausa. La reducción del tamaño de un sistema de archivos no requiere que la sesión de replicación se ponga en pausa.
- Para la replicación síncrona, no es posible cambiar la latencia de red del par de sistemas de replicación a un valor superior a cinco milisegundos cuando se definen sesiones de replicación síncrona.
- El cambio entre la replicación síncrona y asíncrona no se admite para la replicación de archivos.

- A partir de PowerStore 4.1, el intervalo de sondeo de los objetos de replicación aumentó a dos minutos. El aumento se realizó para mejorar el rendimiento cuando hay varias solicitudes de sondeo. Permita tiempo adicional para que el estado del objeto se actualice en PowerStore Manager.
- A partir de PowerStore 4.3, la replicación síncrona de archivos utiliza la tecnología metro para la conmutación por error automática, lo que requiere la configuración de un servicio testigo.

Pausar una sesión de replicación

Cuando se pausa una sesión de replicación, los cambios realizados en el recurso en el sistema de origen no se replican en el sistema de destino.

Puede pausar una sesión de replicación desde el sistema de origen o de destino. Para pausar un sistema de destino, seleccione **Protection** > **Replication** > **[sesión de replicación]** y, a continuación, seleccione **Pause**.

Cuando se pausa una sesión de replicación síncrona, se crea una instantánea de recuperación que se utilizará como la base común más reciente cuando se reanude la sesión.

A partir de 4.3, la replicación síncrona de PowerStore archivos utiliza metro para la conmutación por error automática. La pausa de una sesión de replicación desactiva la interacción del testigo y deshabilita la conmutación por error automática.

Mientras una sesión de replicación está en pausa, puede realizar lo siguiente:

- Reanude la sesión de replicación.
- Eliminar la sesión de replicación mediante la eliminación de la política de protección en el recurso de almacenamiento.
- Cambiar el tamaño o el nombre del recurso de almacenamiento.
- Cambiar la membresía de un grupo de volúmenes.
- Iniciar la migración a otro dispositivo del clúster.

Reanudar una sesión de replicación

Cuando reanuda una sesión de replicación, los cambios realizados en el recurso en el sistema de origen durante la pausa se sincronizan con el sistema de destino.

Puede reanudar una sesión de replicación desde el sistema de origen o destino. Para reanudar un sistema de destino, seleccione **Protección** > **Replicación** > **[sesión de replicación en pausa]** y, a continuación, seleccione **Reanudar**.

Cuando se reanuda una sesión de replicación síncrona, los cambios en el recurso de almacenamiento en el sistema de origen se sincronizan con el recurso en el sistema de destino en función de la instantánea de recuperación que se creó cuando se puso en pausa la sesión. Los datos del host escritos en el recurso durante la pausa se sincronizan con el destino. La replicación continua se reanuda para mantener la sincronización entre el origen y el destino.

NOTA: Las instantáneas que se crearon con la sesión de replicación síncrona en pausa no se sincronizan con el destino.

A partir de 4.3, la replicación síncrona de PowerStore archivos utiliza metro para la conmutación por error automática. Después de reanudar una sesión de replicación, el estado del servicio testigo tarda aproximadamente cinco minutos en cambiar a Engaged.

Cuando se reanuda una sesión de replicación asíncrona, la sincronización se realiza en el siguiente RPO. Puede optar por sincronizar manualmente los recursos si selecciona la sesión de replicación y, a continuación, **Sincronizar**.

Conmutación por error

La conmutación por error de una sesión de replicación incluye el cambio de funciones entre los sistemas de origen y de destino, y la inversión de la dirección de la sesión de replicación.

Existen dos tipos de conmutación por error:

- Conmutación por error planificada: iniciada por el usuario. Incluye sincronización entre el origen y el destino para evitar la pérdida de datos.
- Conmutación por error no prevista: se inicia desde el sistema de destino en respuesta a una falla en el sistema de origen.

Durante una conmutación por error de sesión de replicación, el sistema realiza las siguientes acciones:

- Detener las operaciones de I/O en el objeto de origen.
- Sincronizar los objetos de almacenamiento de origen y destino (se produce solo en una conmutación por error prevista).

- Detener la sesión de replicación.
- Invertir funciones entre los sistemas de origen y destino.
- Promover la versión del objeto más reciente en el nuevo origen.
- Reanudar las tareas de I/O en el nuevo origen (iniciadas por el usuario).
- Para una conmutación por error planificada, si así lo especifica el usuario, volver a proteger.

Después de una conmutación por error, puede acceder a las aplicaciones del nuevo sistema de origen para recuperar los datos.

Realizar una prueba de conmutación por error

Después de configurar una sesión de replicación, puede probar la conexión para asegurarse de que los sitios se hayan configurado y estén preparados correctamente para la recuperación ante desastres.

NOTA: Una prueba de conmutación por error solo se puede realizar en el sistema de destino.

Durante una prueba de conmutación por error, el sistema realiza una conmutación por error y se proporciona acceso de producción al sitio de destino mediante el uso de datos replicados o una instantánea de un punto en el tiempo. El recurso de almacenamiento de destino está disponible en el modo de lectura/escritura, y el acceso de producción se habilita para los hosts y las aplicaciones. Puede verificar su configuración de recuperación ante desastres mientras la replicación continúa ejecutándose en segundo plano.

Para detener la prueba de conmutación por error, seleccione una de las siguientes acciones:

- Failover to the current test data: si realizó cambios en los datos durante la prueba de conmutación por error, puede usar los datos de prueba actualizados. Esta opción permitirá detener la prueba y conservar los datos de prueba. Todos los datos que se replican desde el origen durante la prueba se descartan y el sistema de destino se convierte en el origen.

  NOTA: Debe confirmar estos cambios antes de realizar una conmutación por error a los datos de prueba.

- Stop the failover test: cuando detenga la prueba, se deshabilitará el acceso de producción al destino para los hosts y las aplicaciones, y el recurso de almacenamiento de destino se actualizará con los datos más recientes sincronizados con el sistema de origen. Puede crear una instantánea de respaldo de los datos de prueba antes de detener la prueba de conmutación por error.

Restricciones

Solo se puede ejecutar una prueba de conmutación por error bajo las siguientes condiciones:

- LasPowerStoreLa versión en los sistemas de origen y destino es 2.x o posterior.
- La sesión de replicación está en un estado correcto.

  NOTA: También se puede realizar una prueba de conmutación por error cuando el estado de la sesión de replicación es System Paused o Paused si se completó la sincronización inicial.

Durante la prueba de conmutación por error, no puede realizar las siguientes acciones en el sistema de destino:

- Cambiar la membresía de un grupo de volúmenes
- Aumentar el tamaño de un grupo de volúmenes
- Cambiar el nombre de un grupo de volúmenes
- Iniciar una migración
- Quitar una política de protección

NOTA: Aún puede realizar estas acciones en el sistema de origen.

No puede realizar una conmutación por error prevista mientras haya una prueba de conmutación por error en curso. Detenga la prueba de conmutación por error para realizar una conmutación por error prevista. Sin embargo, las conmutaciones por error no previstas pueden continuar produciéndose sin interrupción en respuesta a un desastre. Si es posible, se recomienda detener la prueba de conmutación por error antes de una conmutación por error no planificada para evitar la pérdida de datos que se replican en el destino después de que se inicia la prueba de conmutación por error.

También puede pausar y reanudar las sesiones de replicación durante una prueba de conmutación por error. Si elimina una sesión de replicación durante una prueba de conmutación por error, la prueba se cancela.

Iniciar una prueba de conmutación por error

Puede iniciar una prueba de conmutación por error a partir de los datos de destino actuales o una instantánea.

Existen dos maneras de iniciar una prueba de conmutación por error:

- Desde **Protección** > **Replicación**, seleccione la sesión de replicación que desea probar y, a continuación, seleccione **Start Failover Test**.
- En la pestaña **Protección** del recurso, seleccione **Replicación** y, a continuación, **Iniciar prueba de conmutación por error**.

Una vez que se inicia la prueba de conmutación por error, se genera una alerta en la sesión de replicación. La alerta se borra después de que se detiene la prueba.

Detener una prueba de conmutación por error

Antes de detener la prueba de conmutación por error, se recomienda desmontar los sistemas de archivos y detener todas las aplicaciones en ejecución en el recurso de destino para evitar daños en los datos.

Existen dos maneras de detener una prueba de conmutación por error:

- Desde **Protección** > **Replicación**, seleccione la sesión de replicación que tiene una prueba en curso y, a continuación, seleccione **Stop Failover Test**.
- En la pestaña **Protección** del recurso con una prueba en curso, elija **Replicación** y, a continuación, seleccione **Detener prueba de conmutación por error**.

También puede crear una instantánea para guardar los datos de prueba que se crearon durante la prueba de conmutación por error.

Conmutación por error planificada

Cuando realiza una conmutación por error prevista, la sesión de replicación se conmuta por error de forma manual desde el sistema de origen al sistema de destino. Antes del inicio de la conmutación por error, el sistema de destino se sincroniza con el sistema de origen para impedir la pérdida de datos.

Antes de realizar una conmutación por error planificada, asegúrese de detener las operaciones de I/O de todas las aplicaciones y los hosts. No puede poner en pausa una sesión de replicación que está experimentando una conmutación por error planificada.

Durante una conmutación por error planificada, puede realizar las siguientes acciones:

- Realizar una conmutación por error no prevista.
- Eliminar la sesión de replicación mediante la eliminación de la política de protección en el recurso de almacenamiento.

No puede iniciar una conmutación por error prevista cuando haya una prueba de conmutación por error en curso.

Puede iniciar una prueba de conmutación por error prevista en los datos de origen actuales o a partir de una instantánea.

Existen dos maneras de iniciar una conmutación por error prevista:

- En **Protección** > **Replicación**, seleccione la sesión de replicación pertinente y, a continuación, seleccione **Conmutación por error planificada**.
- En la pestaña **Protección** del recurso, seleccione **Replicación** y **Conmutación por error planificada**.

Para la replicación síncrona, la conmutación por error planificada se puede iniciar desde el sistema de origen cuando la sesión de replicación se encuentra en el estado Funcionando normalmente. Debido a que los datos están completamente sincronizados entre los sistemas, la conmutación por error no causa pérdida de datos. Sin embargo, se recomienda detener las operaciones de I/O de las aplicaciones y los hosts antes de iniciar la conmutación por error.

Después de una conmutación por error planificada, la sesión de replicación queda inactiva. Para sincronizar el recurso de almacenamiento de destino y reanudar la sesión de replicación, utilice la acción **Volver a proteger**. También puede seleccionar la opción Volver a proteger antes de realizar la conmutación por error, lo que inicia automáticamente la sincronización en la dirección opuesta (en el siguiente RPO) después de que se completa la conmutación por error y devuelve el sistema de origen y de destino a un estado normal.

NOTA: Cuando los datos se sincronizan como parte de la acción de reprotección, en el gráfico de rendimiento del sistema de origen se muestra un punto único. Dado que el siguiente punto en el tiempo se registra en el gráfico cuando se produce la siguiente sincronización, el gráfico aparece vacío. Para ver los valores de rendimiento, pase el cursor sobre el gráfico.

Desconexión de red durante una DRT

Cuando se realiza una DRT, no se recomienda simular una falla de red entre los sistemas local y remoto y, a continuación, realizar una conmutación por error no planificada al sistema de destino para habilitar el acceso al servidor NAS de DR. Dado que no hay comunicación entre los sistemas, PowerStore no puede garantizar que ambos servidores NAS estén en un estado compatible. Una vez que se restaura la conexión, ambos servidores NAS están en modo de producción (desconexión entre sitios). Como resultado, ambos sistemas cambian al modo de destino para evitar que los datos se escriban en ambas ubicaciones.

Para resolver este estado, se requiere la intervención del soporte técnico.

Para obtener más información, consulte el artículo de la base de conocimientos 000215482 de Dell (Interrupción de la conexión de red entre sitios... [en inglés]).

Conmutación por error no planificada

La conmutación por error no planificada se produce después de eventos del sistema de origen, como una falla en el sistema de origen o eventos que generan tiempo de inactividad para el acceso de producción. La conmutación por error no planificada se inicia desde el sistema de destino y proporciona acceso de producción al recurso de destino original a partir de una instantánea de un punto en el tiempo.

NOTA: A partir dePowerStore4.3, la replicación síncrona de archivos utiliza metro para la conmutación por error automática. Si se configura un servicio testigo, la conmutación por error automática está disponible para todas las sesiones de replicación síncrona de archivos. Consulte Testigo metro para obtener detalles sobre la configuración del testigo.

Cuando usted inicia una conmutación por error no planificada, puede optar por usar la copia de datos más reciente o una instantánea de los datos (si está disponible) como origen de datos.

Cuando se restablece la conexión al sistema de origen, el recurso de origen inicial se coloca en modo de destino. Utilice la opción **Volver a proteger** para sincronizar el recurso de almacenamiento de destino y, a continuación, reanude la sesión de replicación.

NOTA: Antes de realizar una conmutación por error no planificada, apague el servidor NAS en el sitio de producción. No se recomienda desactivar el vínculo de replicación para probar la funcionalidad de conmutación por error no planificada, ya que puede provocar una falta de disponibilidad de datos. A partir dePowerStore4.3, es necesario apagar el clúster antes de la conmutación por error no planificada.

NOTA: Cuando se realiza la replicación de archivos, no se recomienda modificar la red de movilidad de archivos después de realizar una conmutación por error no planificada. Una vez que se restaura la conexión entre los sistemas de origen y de destino, el resultado puede ser que ambos servidores NAS estén en modo de producción.

NOTA: Para habilitar el acceso no disruptivo a los datos en el entorno SMB, se recomienda configurar la disponibilidad continua para los recursos compartidos de SMB y volver a montarlos después de restablecer la conexión.

Conmutación por error automática para la replicación síncrona de archivos

La replicación síncrona de archivos utiliza la tecnología metro para la conmutación por error automática, lo que requiere que una tecnología de servicio testigo realice una conmutación por error automáticamente al sistema de destino cuando el sistema de origen está inactivo.

A partir de 4.3, la replicación síncrona de PowerStore archivos utiliza la tecnología metro para la conmutación por error automática. Se debe configurar un servicio testigo para habilitar la conmutación por error automática.

El sistema identifica cuando el sistema de origen está inactivo y conmuta por error automáticamente la sesión de replicación al sistema de destino.

En la tabla de sesiones de replicación (**Replicación** > **con protección**), el **Estado de conmutación por error automático** indica si la sesión de replicación está habilitada para la conmutación por error automática. Los estados posibles son:

- No aplicable: la sesión de replicación no es una sesión de replicación síncrona de archivos.
- Actualización necesaria: la versión de software del sistema remoto para la sesión de replicación no es compatible con el servicio de testigo de archivos (FWS). Es necesario actualizar el sistema a una versión compatible con FWS para habilitar la conmutación por error automática.
- Manual Enable Required: los sistemas locales y remotos admiten la conmutación por error automática basada en testigos. Para habilitar manualmente la conmutación por error automática para la sesión de replicación heredada, seleccione la casilla de verificación junto a la sesión y, a continuación, seleccione **Habilitar conmutación por error automática**.
- Habilitada para la interacción del testigo: la sesión de replicación está habilitada para la conmutación por error automática basada en testigos.

NOTA: El estado de conmutación por error automática también se muestra en la ventana de detalles de la sesión de replicación.

La replicación se produce en el nivel del servidor NAS, pero las operaciones de replicación sincronizada metro de archivos se realizan en el nivel de grupo del sistema de archivos, que incluye todos los pares de sistemas de archivos sincronizados.

Durante una sesión de replicación síncrona metro de archivos, si alguno de los pares de sistemas de archivos no está en estado sincronizado (por ejemplo, después de pausar y reanudar la sesión de replicación) y la pérdida de conexión desencadena una conmutación por error automática, los sistemas de archivos no sincronizados no realizan una conmutación por error al sistema de destino, mientras que todos los sistemas de archivos que están en estado sincronizado se conmutan por error y se gestionan las I/O desde el nuevo sistema de origen. Como resultado, el estado de la sesión de replicación cambia a **Conmutación por error parcial**.

Si hace clic en la flecha junto al nombre del servidor NAS en la tabla **Replicación** , se expande su lista de sistemas de archivos y se muestra el estado de cada sistema de archivos.

Puede seleccionar cualquiera de las opciones siguientes:

- Espere a que el sistema de origen se recupere y la sesión de replicación se sincronice por completo, y luego vuelva a intentar la conmutación por error.

  NOTA: Para asegurarse de que todos los sistemas de archivos estén sincronizados, compruebe que el estado de la sesión de replicación (columna **Estado de la sesión de replicación** >) haya cambiado a **Conmutado por error**. A partir de PowerStore 4.3, también puede usar la API REST para comprobar el estado de sincronización de una sesión de replicación. Para las sesiones de replicación síncrona metro de archivos, compruebe el estado en el sistema de destino. En el caso de las sesiones de replicación heredadas, compruebe el estado en el sistema de origen.

- Reintente la conmutación por error mediante la opción Forzar: seleccione la sesión de replicación y, a continuación, seleccione **Conmutación por error**. En el aviso **Failover Replication** que se muestra, seleccione la opción **Force failover en el recurso de destino** .

  NOTA: La conmutación por error forzada se puede iniciar mediante o la PowerStore Manager API REST.

  NOTA: El uso de conmutación por error forzada puede provocar la pérdida de datos.

Recuperar un servidor NAS

Puede resolver escenarios de múltiples fallas en los sistemas a través de acciones de conmutación por error o recuperación para mantener la accesibilidad y la funcionalidad del servidor NAS.

Pueden producirse escenarios de múltiples fallas en los que los sistemas de origen y destino no pueden comunicarse entre sí, y uno de los sistemas o ambos no pueden comunicarse con el servicio testigo. Cuando ocurren estos escenarios, los servidores NAS en los sistemas local y remoto están offline y el servicio testigo no puede determinar qué sistema debe permanecer accesible para el host.

Para resolver los siguientes escenarios de falla, inicie una conmutación por error al sistema de destino:

- La conexión entre el sistema de destino y el servicio testigo deja de funcionar y, a continuación, el sistema de origen se desactiva.
- El servicio del testigo deja de funcionar y, a continuación, el sistema de origen.

Para resolver los siguientes escenarios de falla, utilice la opción **Recuperar** (**Servidores NAS** > **de almacenamiento** > **[servidor NAS]** > **Más acciones** > **de recuperación**):

- La conexión entre el sistema de origen y el servicio testigo deja de funcionar y, a continuación, el sistema de destino se desactiva.
- El servicio del testigo deja de funcionar y, a continuación, el sistema de destino se desactiva.
- La conexión entre el sistema de destino y el servicio testigo, seguida de la conexión entre el sistema de origen y el sistema testigo, deja de funcionar y, a continuación, la conexión entre los sistemas de origen y destino.
- El servicio del testigo deja de funcionar y, a continuación, la conexión entre los sistemas de origen y destino.

Después de seleccionar **Recover**, el servidor NAS recuperado pasa al modo de producción.

NOTA: No utilice la opción **Recuperar** para situaciones distintas a las especificadas anteriormente.

NOTA: La recuperación del servidor NAS también se puede iniciar mediante la API REST.

Consideraciones adicionales de replicación

Durante la replicación de bloques, cuando el sistema de origen se pone en pausa para una NDU y el sistema de destino está activo, el estado del sistema de destino cambia a *System_Paused*. Si el sistema de destino está inactivo durante la NDU del sistema de origen, cuando vuelve a estar activo, su estado permanece en *OK*.

Durante la replicación de archivos, cuando el sistema de origen está en pausa para una NDU, el sistema de destino permanece en el estado *OK* independientemente de su estado de conectividad.

A partir de 4.3, la replicación síncrona de PowerStore archivos utiliza metro para la conmutación por error automática. Se recomienda conmutar por error la sesión de replicación al sitio remoto antes de iniciar la NDU para evitar la conmutación por error automática durante los reinicios del clúster del sitio de origen.

Prueba de recuperación ante desastres para servidores NAS en replicación

Una prueba de recuperación ante desastres ejecuta un plan de recuperación ante desastres que le permite comprobar que el sistema pueda recuperarse y restaurar datos y operaciones en caso de producirse un desastre.

En PowerStore, se proporcionan varias opciones para probar la capacidad del sistema de recuperarse de un desastre y recobrar la funcionalidad:

- Clonar un servidor NAS para pruebas de recuperación ante desastres mediante direcciones IP únicas.
- Clonar un servidor NAS para pruebas de recuperación ante desastres mediante una red aislada con direcciones IP duplicadas.
- Conmutación por error planificada (consulte la sección anterior).

Clonar un servidor NAS para pruebas de recuperación ante desastres mediante direcciones IP únicas

Sobre esta tarea

La clonación de un servidor NAS es la opción recomendada para probar la DR. Puede clonar el servidor NAS mediante PowerStore Manager y probarlo sin afectar la producción. Para habilitar el acceso al servidor NAS recientemente clonado, es necesario configurar una nueva interfaz de red única. La dirección IP configurada no puede estar en uso en los servidores NAS de origen o destino. También se requieren ajustes únicos para unir el servidor a un dominio de AD.

Los cambios que se hacen en los sistemas de archivos clonados no afectan a los que se hacen en los sistemas de archivos de producción y viceversa. Cuando se completa la prueba de DR, el servidor clonado se puede eliminar.

Puede elegir cualquiera de las siguientes opciones:

- Clonar el servidor NAS en el sistema de origen, replicarlo en el destino y realizar una conmutación por error planificada al sistema de destino.
- Clonar el servidor NAS en el sistema de destino y acceder a los datos (la conmutación por error no es necesaria porque los recursos clonados ya están accesibles en el sistema de destino).

Pasos

1. En PowerStore Manager, seleccione **Almacenamiento** > **Servidores NAS**.
2. Seleccione el servidor NAS que desea clonar y, a continuación, elija **Replanificar** > **Clonar servidor NAS**.
3. En la ventana **Crear clon**, proporcione un nombre para el clon y seleccione los sistemas de archivos que desea clonar.
4. Seleccione **Crear**.
   El servidor NAS clonado se agrega a la lista de servidores.
5. Seleccione el nombre del servidor NAS clonado para abrir la ventana de detalles del servidor.
6. Para agregar una interfaz de archivos:
   a. Seleccione la pestaña **Red**.
   b. En **Interfaz de archivos**, seleccione **Agregar**.
   c. Proporcione la información de la interfaz y seleccione **Agregar**.
7. Para establecer el protocolo de uso compartido:

a. Seleccione la pestaña **Protocolos de uso compartido**.
b. Seleccione el protocolo pertinente (SMB, NFS o FTP).
c. Configure la información necesaria y seleccione **Aplicar**.

8. Si clonó el servidor NAS de origen:
   a. Replique el servidor NAS en el sistema de destino. Para obtener detalles, consulte Replicación.
   b. Realice una conmutación por error planificada al destino. Para obtener detalles, consulte Conmutación por error planificada.
   c. Compruebe si el host puede acceder a los datos.
9. Si clonó el servidor de producción replicado en el sistema de destino, no se requiere la conmutación por error. Verifique el acceso de host.

Clonar un servidor NAS para pruebas de recuperación ante desastres mediante una red aislada con direcciones IP duplicadas

Es posible probar la recuperación ante desastres usando la misma configuración que la producción. El uso de ajustes idénticos puede reducir el riesgo y aumentar la reproducibilidad en un escenario de falla. Sin embargo, el uso de direcciones IP duplicadas crea conflictos. La ejecución de la prueba de DR en un entorno aislado del entorno de producción le permite evitar estos conflictos.

En PowerStoreOS 3.6 y versiones posteriores, puede crear un entorno de pruebas de recuperación ante desastres (DRT) aislado como ayuda para estar preparado ante un desastre.

La creación de un entorno aislado le permite usar la misma dirección IP y el mismo nombre de host que el sistema de producción y realizar una DRT para un servidor NAS en replicación sin ningún impacto en la producción.

Para crear un entorno de DRT, debe configurar una red aislada con un enrutador de DRT independiente y crear agregaciones de enlaces con los puertos de I/O de red.

Mediante la PSTCLI o la API REST, cree un entorno de red dedicado en el servidor de destino clonando el servidor NAS en replicación al sistema PowerStore de destino. El clon es una copia completa del entorno de producción y un entorno de pruebas dedicado, que está aislado de la producción. Puede crear un entorno de red aislado y configurar el entorno de pruebas con la misma dirección IP y el mismo nombre de host que el sistema de producción. El servidor NAS de DRT no tiene ningún impacto en el entorno de producción y se puede ejecutar sin conflictos de dirección IP cuando se produce una conmutación por error y una conmutación por recuperación en el servidor NAS de replicación.

Para probar la DR con el uso de un entorno de pruebas aislado:

1. Cree el clon del servidor NAS en el destino. Utilice la marca `is_dr_test`.
2. Cree una interfaz de vinculación de usuario para NAS con la misma dirección IP que el servidor NAS de origen.
3. Una el clon a AD (si es necesario).
4. Verifique que los hosts puedan acceder a los datos.

NOTA: También puede usar la DRT en servidores NAS independientes.

Requisitos y limitaciones

Para crear un entorno de DRT, asegúrese de que se cumplan los siguientes requisitos:

- Adquiera la información de la red privada:
  - Gateway
  - Máscara de red
  - ID de VLAN (opcional)
- Identifique los puertos de red de la red aislada y los de la red de producción.

Tenga en cuenta las siguientes limitaciones al crear un entorno de DRT:

- La interfaz de vinculación dedicada a DRT no se puede utilizar para crear ningún otro servidor NAS de producción.
- Un servidor NAS configurado como producción no se puede reconfigurar como parte de la DRT.
- Un servidor NAS configurado como parte de la DRT no se puede reconfigurar como producción.
- Un servidor NAS que ya no forma parte de una DRT no se puede reconfigurar y se debe eliminar.
- Después de que un servidor NAS está activo y configurado con información de red, la configuración adicional (como DNS, CAVA y Kerberos) se debe realizar manualmente.
- El servidor NAS habilitado para DRT no se puede replicar.
- La modificación y la eliminación del servidor NAS se pueden realizar mediante PowerStore Manager.

Configurar el entorno de pruebas de recuperación ante desastres mediante PSTCLI

Pasos

1. Adquiera el nombre del servidor NAS en el sitio de destino (que se clonará):

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> nas_server show
# | id | name | operational_status |  current_node_id  | file_interfaces.ip_addre~
--+-------------+--------+--------------------+-------------------
1 |647f545a-4b11-5cdd-4d4c-eeeba81eb143 | File80| Started | R2C4-appliance-1-node~|
127.1.1.1
```

2. Clone el servidor NAS proporcionando un nuevo nombre para el clon y utilizando el switch `-is_dr_test true`:

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> nas_server -name File80
clone -name File80_c -is_dr_test true
Success
```

3. Busque el ID del puerto IP para la vinculación de archivos NAS que está conectada a la red aislada:

   NOTA: Si la vinculación de archivos NAS no se creó, puede crearla mediante PSTCLI o PowerStore Manager.

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> ip_port_show -output nvp
8:  id =IP_PORT23
    current_usages =
    ip_pool_addresses =
    bond:
    name=BaseEnclosure-NodeA-bond1
```

4. Cree la interfaz de archivos para el servidor NAS clonado:

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> file_interface create
-nas_server_name File80_c -ip_address "10.10.10.10" -prefix_length 24 -gateway
"10.10.10.1" -vlan_id 5
-ip_port_id IP_PORT23
Created
# |     id
--+------------------------------------
1 |64830ae5-2760-59ce-4c90-82772509648e
```

5. Vea la interfaz de archivos:

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> file_interface_show
# |id | nas_server_id | ip_address | prefix_length | gateway | is_disabled
--+-------------+--------+--------------------+-------------------
  1 |647f5509-11f4-a52d-ee1f-82772509648e | 647f545a-4b11-5cdd-4d4c-eeeba81eb143 |
10.10.10.10 |24 | 10.10.10.1 | no
  2 |64830ae5-2760-59ce-4c90-82772509648e | 6483092f-3e71-8a92-0a0b-82772509648e |
10.10.10.10 |24 | 10.10.10.1 | no
```

Configurar un servidor NAS en un entorno de DRT mediante la API REST

Sobre esta tarea

NOTA: Si no utiliza la API REST, omita esta sección.

Pasos

1. Para clonar el servidor NAS en el espacio de nombres especificado, ejecute `/nas_server/{id}/clone` y especifique `is_dr_test` como true.
2. Para crear una interfaz de red, ejecute `/file_interface` y especifique los parámetros de la red privada.

NOTA: En este paso, se crea la interfaz de archivos del servidor NAS clonado con la misma dirección IP, máscara de red y gateway que el servidor NAS de producción. Utilice la interfaz de vinculación/IP_Port asociada con la red privada.

Resultados

El servidor NAS está activo y se puede utilizar para la DRT en la red aislada.

Replicación de volúmenes virtuales

PowerStore Se integra con VMware Live Site Recovery para admitir la replicación asíncrona de Virtual Volume.

La protección remota de máquinas virtuales se configura mediante la administración basada en políticas de almacenamiento de vSphere (SPBM). Para la recuperación desde fallas, la conmutación por error de máquinas virtuales se configura mediante VMware Live Site Recovery.

VMware Live Site Recovery es una solución de recuperación ante desastres que automatiza la recuperación o la migración de máquinas virtuales entre un sitio protegido y un sitio de recuperación.

Las reglas de instantánea y replicación que se crean en PowerStore están expuestos a vSphere y se pueden agregar a las políticas de protección. vSphere proporciona una política de almacenamiento para PowerStore durante la creación de vVol.

Un grupo de replicación que incluye volúmenes virtuales que se deben replicar juntos es la unidad de replicación y conmutación por error que se configura en vSphere.

Se pueden generar instantáneas de solo lectura y de lectura/escritura para vVols. La sincronización, manual o de acuerdo con el programa configurado, se aplica solo a las instantáneas de solo lectura.

Para ver los detalles de una sesión de replicación de volúmenes virtuales:

1. Seleccione **Protección** > **Replicación**.
2. Haga clic en el estado de la sesión de replicación para ver sus detalles.

En el gráfico en la ventana de detalles de la sesión de replicación, se indica que vSphere administra la sesión de replicación.

En la ventana de detalles de la sesión de replicación, puede realizar lo siguiente:

- Ver los detalles de la sesión de replicación.
- Cambiar el nombre del grupo de replicación.
- Poner en pausa y reanudar la sesión de replicación.
- Sincronizar la sesión de replicación.

Requisitos previos

Antes de configurar la replicación de volúmenes virtuales, asegúrese de que se cumplan los siguientes requisitos:

- Tanto el sistema local como el remoto deben estar conectados y deben tener funcionalidad de vVol (consulte Sistemas remotos).
- Debe haber contenedores de almacenamiento definidos en ambos sistemas (**Almacenamiento** > **Contenedores de almacenamiento** > **Crear**) de modo que se puedan emparejar. Si hay un único contenedor de almacenamiento en cada sistema, los contenedores de almacenamiento se emparejan automáticamente. De lo contrario, es necesario especificar manualmente el destino del contenedor de almacenamiento (**Almacenamiento** > **Contenedores de almacenamiento** > **[contenedor de almacenamiento]** > **Protección** > **Crear**).

Crear una sesión de replicación de volúmenes virtuales

Sobre esta tarea

Para obtener información sobre la configuración necesaria en vSphere, consulte la documentación del usuario de VMware SRM.

Pasos

1. En PowerStore, cree una regla de replicación.
   La regla de replicación se expone a vCenter como una funcionalidad de replicación.
2. En vSphere, cree una política mediante la regla expuesta.

Se agrega una copia de solo lectura de la política de protección a PowerStore con un nombre idéntico (visible en la tabla **Políticas de protección**) y se marca con un icono de bloqueo.

NOTA: También puede agregar reglas de instantáneas para habilitar la protección local.

NOTA: No es posible crear, modificar ni eliminar una política de protección de solo lectura ni asignar la política a máquinas virtuales o cancelar la asignación de estas mediante PowerStore. Para realizar esta acción, utilice la actualización de la política de almacenamiento en vSphere.

3. En vSphere, cree una máquina virtual, asígnele una política de almacenamiento con una regla de replicación y asóciela a un grupo de replicación.

Resultados

El grupo de replicación y la sesión de replicación se crean automáticamente en PowerStore (visible en **Protección** > **Replicación** > **[sesión de grupo de replicación]**).

Monitoreo del rendimiento de grupos de replicación

Cuando en VMware se crea una política de almacenamiento que incluye una regla de replicación de PowerStore y se asigna a una VM basada en vVol, se crea una sesión de replicación en PowerStore para los recursos de vVol en el mismo grupo de recursos. VMware Live Site Recovery utiliza estos grupos de recursos de VMware para administrar las VM protegidas en grupos de replicación.

Puede monitorear el rendimiento de un grupo de replicación desde PowerStore. Seleccione **Protección** > **Replicación** y haga clic en el estado de una sesión de replicación de vVol para mostrar los detalles de la sesión (el **Tipo de recurso** debe ser *Grupo de replicación*). Haga clic en la pestaña **Rendimiento del grupo de replicación** para mostrar los datos de rendimiento del grupo de replicación. Puede optar por ver gráficos de los siguientes datos:

- Datos de replicación restantes
- Ancho de banda de replicación (normalizado)
- Tiempo de transferencia de replicación

También puede configurar la línea de tiempo de los datos mostrados.

Recuperación de máquinas virtuales

Site Recovery Manager (SRM) es una solución de recuperación ante desastres de VMware que automatiza la recuperación de máquinas virtuales durante estados de falla.

Para habilitar la recuperación de máquinas virtuales, es necesario configurar un plan de recuperación mediante SRM. Un plan de recuperación ejecuta pasos de recuperación predefinidos en grupos de replicación seleccionados. Los pasos de recuperación incluyen la conmutación por error, la reprotección y la prueba de conmutación por error.

Se crea un grupo de protección en vSphere, el que incluye uno o más grupos de replicación y un plan de recuperación. Si se produce una falla, SRM ejecuta el plan de recuperación en los volúmenes virtuales de los grupos de replicación.

En PowerStore, puede monitorear el estado de la sesión de replicación durante la recuperación.

Para obtener detalles adicionales, consulte *la Guía de VMware Site Recovery Manager*.

6

Protección de metro

Este capítulo incluye la siguiente información:

Temas:

Requisitos y limitaciones

Antes de configurar la protección metro, tenga en cuenta las siguientes limitaciones:

- La compatibilidad con Metro solo está disponible conModelo PowerStore TyPowerStoreDispositivos modelo Q.
- La protección metro está habilitada para volúmenes y grupos de volúmenes.
- La protección metro admite hosts de Windows, Linux y VMware ESXi con conexión FC/SCSI o iSCSI.

NOTA: Los hosts de Windows y Linux son compatibles a partir dePowerStoreSistema operativo 4.x.

Cuando se establece una conexión a un sistema remoto, el sistema detecta automáticamente la configuración y habilita para él las funcionalidades compatibles. Para habilitar la funcionalidad metro de bloques, asegúrese de que se cumplan las siguientes condiciones en ambosPowerStoreSistemas:

- Los dos sistemas están ejecutandoPowerStoreOS 3.x o posterior.
- La latencia en el sistema remoto es baja.
- Tipo de conexión de datos:
  - TCP: cuando es local y remotoPowerStoreSi se instalan sistemas que ejecutan la versión 3.x (o posterior), la conexión TCP se admite automáticamente. Sin embargo, cuando uno o ambos de losPowerStoreLos sistemas ejecutan la versión 2.x; debe actualizar los sistemas a la versión 3.x para habilitar metro. Después de la actualización, se muestra una alerta en la que se le solicita actualizar el tipo de conexión del sistema remoto. Haga clic en el enlace incluido en la alerta que se muestra para abrir la ventana **Actualizar transporte del sistema remoto**. A continuación, haga clic en **Actualizar transporte**.

    NOTA: La alerta se borra solo después de que se actualiza el transporte.

  - FC - A partir dePowerStoreversión 4.4, el tipo de conexión FC es compatible con metro.

Para implementar un servicio testigo, asegúrese de que se cumplan los siguientes requisitos previos:

- El servicio testigo debe estar instalado en un host Linux independiente (virtual o físico).
- El servicio del testigo se debe implementar en un tercer dominio de falla, que esté separado de los dosPowerStoreSistemas que forman parte de la sesión de Metro. La instalación del servicio testigo en un sistema independiente garantiza su disponibilidad si se produce una falla de alimentación en los sistemas metro.

- Sistemas operativos compatibles: consulte la *Matriz de soporte simple de Dell Technologies PowerStore* en la página Documentación de PowerStore.
- Dependencias (necesarias en el host de Linux):
  - Java 11 o Java 17 (paraPowerStoreversión 4.2 y posteriores)
  - SQLite

  NOTA: Las dependencias enumeradas se instalan automáticamente cuando se usa un administrador de paquetes (como yum o zypper).
- Hardware:
  - El sistema operativo debe ejecutarse en una arquitectura de CPU x64.
  - Un mínimo de 4 GB de RAM.
  - Un mínimo de 5 GB de espacio disponible en disco.
- Puertos:
  - El puerto 443/tcp debe estar abierto en el host testigo antes de instalar el testigo.
  - Los firewalls del centro de datos deben permitir el tráfico en el puerto 443 para habilitarsePowerStorepara enviar solicitudes al servicio testigo.
- Latencia de red: latencia máxima de 100 milisegundos en la red de administración entrePowerStorey el servicio de testigos.
- Acceso a cuenta de usuario: se requiere acceso raíz o sudo para instalar el servicio testigo en el host.
- Garantice la conectividad con elPowerStoreRed de administración.
- En el caso de un testigo virtual, se recomienda utilizar una dirección IP estática para la VM testigo. Sin embargo, si utiliza DHCP, agregue el testigo aPowerStoremediante el nombre de dominio calificado (FQDN).

NOTA: Para obtener más información sobre los límites de metro, consulte la *Matriz de soporte simple de Dell Technologies PowerStore* en la página Documentación de PowerStore.

Configurar la conectividad del host

NOTA: Se proporciona compatibilidad de host para el clúster de almacenamiento metro de VMware vSphere. Se soporta la conectividad de Fibre Channel e iSCSI.

NOTA: A partir de la versión 4.x del sistema PowerStore, se proporciona soporte para hosts Windows y Linux.

La conectividad metro del host está configurada en sistemas PowerStore locales y remotos y permite que los hosts y las aplicaciones perciban los volúmenes físicos de los dos sistemas como un único volumen. Cuando configure la conectividad metro para el host, seleccione el arreglo preferido a fin de determinar qué sistema conserva el acceso al almacenamiento si se produce una falla.

Se debe definir un host (ESXi, Windows o Linux) en los sistemas local y remoto para habilitar la conectividad metro del host.

Cuando crea un host, el asistente **Agregar host** permite configurar la conectividad del host:

NOTA: Las opciones de conectividad de host se muestran gráficamente en el asistente **Agregar host**.

- **Conectividad local**: proporciona acceso de host solo al sistema local.

  NOTA: La conectividad local también se puede utilizar con volúmenes metro.
- **Conectividad metro**: proporciona acceso de host a sistemas locales y remotos. Si selecciona esta opción, configure el acceso del sistema:
  - **El host está coubicado con este sistema**: la latencia de la ruta del host es menor para el sistema local y mayor para el sistema remoto. El host siempre intenta enviar I/O al sistema local (excepto cuando está inactivo).
  - **El host está coubicado con el sistema remoto**: la latencia de la ruta del host es menor para el sistema remoto. El host siempre intenta enviar I/O al sistema remoto (excepto cuando está inactivo).
  - **Coubicado con ambos sistemas**: la latencia y el rendimiento de la ruta del host son iguales para los sistemas local y remoto. El host envía I/O a los sistemas local o remoto en función de sus consideraciones de múltiples rutas.

NOTA: Independientemente de la conectividad configurada, todos los hosts ESXi deben estar configurados en el mismo clúster de vCenter.

NOTA: Para un host ESXi mapeado a un volumen metro, se recomienda utilizar el plug-in de selección de rutas (PSP) round robin con el modo de latencia habilitado.

NOTA: En caso de que uno de los sistemas quede offline, el host ESXi ingresa a una condición todas las rutas inactivas (APD). Para resolver esta condición, se recomienda configurar vSphere HA. Esta configuración permite que las máquinas virtuales en los hosts ESXi disponibles se reinicien y resuelvan la condición APD.

Testigo metro

En PowerStoreOS 3.6 y versiones posteriores, puede agregar un servicio testigo a la protección metro para proporcionar protección contra escenarios de falla únicos.

El servicio testigo es un tercero pasivo que se instala en un host independiente.

NOTA: El servicio del testigo se debe implementar en un tercer dominio de falla, que está separado de los dos PowerStore sistemas que forman parte de la sesión metro. La instalación del servicio testigo en un sistema independiente garantiza su disponibilidad si se produce una falla de alimentación en los sistemas metro.

Cuando se produce una falla, los sistemas local y remoto PowerStore se comunican con el servicio testigo y solicitan fracturar la sesión metro. A continuación, el testigo determina qué sistema permanece accesible para los hosts y continúa gestionando I/O. Si es posible, el testigo da prioridad al sistema PowerStore que se asignó con la función de preferencia. La adición del servicio de testigo a una sesión metro proporciona protección contra escenarios de falla única, incluidas las fallas del sistema preferidas que no se manejan sin un testigo.

El servicio del testigo es simple y no mantiene datos cruciales que no se pueden volver a crear. Por lo tanto, no es necesario respaldar, guardar ni recuperar el testigo y este se puede quitar y reinstalar cada vez que se requiera realizar una recuperación.

Implementar el testigo metro

Si se cumplen los requisitos previos, puede usar RPM para instalar directamente el servicio testigo. De lo contrario, puede usar un administrador de paquetes (yum o zypper) para instalar automáticamente las dependencias. Puede descargar el paquete de instalación desde la página de soporte de Dell.

Para instalar el servicio del testigo en un host de Linux, ejecute el siguiente comando:

```
sudo rpm -i <rpm_file>
```

NOTA: Puede utilizar un administrador de paquetes o RPM para desinstalar el servicio testigo.

NOTA: El servicio de testigo solo está disponible conModelo PowerStore TyPowerStoreDispositivos modelo Q.

Configurar el testigo metro

Sobre esta tarea

- Solo el administrador, el administrador de seguridad y el administrador de almacenamiento están autorizados para configurar el servicio testigo.
- Puede configurar el servicio de testigo antes o después de configurar metro.
- Solo se puede configurar un servicio testigo por clúster.
- El servicio testigo configurado se utiliza para todas las sesiones metro y no se puede deshabilitar para sesiones específicas.
- El estado del servicio testigo cambia a Engaged solo después de que se configura para los sistemas locales y remotos PowerStore .
- Para acceder a las herramientas de instalación del servicio de testigo (generador de token seguro y huella digital), utilice la ruta:

```
sles15:~ # ls /opt/dell-witness-service/scripts
```

NOTA: Realice los siguientes pasos para los sistemas PowerStore local y remoto.

Pasos

1. En Manager PowerStore , seleccione **Protection** > **Metro Witness**.
2. En la ventana **Testigo metro**, seleccione **Agregar**.
3. En la ventana **Agregar testigo**, configure los siguientes campos:
   - Name
   - Dirección IP/FQDN

- Token de seguridad: para generar un token de seguridad, ejecute el script generate_token.sh. Para obtener detalles, consulte la *Guía de configuración de seguridad de PowerStore* en la página Documentación de PowerStore.

  NOTA: El token vence en diez minutos.

- Descripción (opcional)

4. Verifique los requisitos de instalación que se muestran y seleccione la casilla de verificación para confirmar.
5. Seleccione **Agregar**.
6. En la ventana **Autorización de usuarios**, revise la huella digital del certificado del testigo y seleccione **Confirmar** para aceptar.

   NOTA: Para obtener detalles, consulte la *Guía de configuración de seguridad de PowerStore* en la página Documentación de PowerStore.

   El certificado se guarda en el sistema PowerStore.

Resultados

El testigo se crea y todos los volúmenes y los grupos de volúmenes metro existentes se asignan automáticamente a este. Los volúmenes y grupos de volúmenes metro recién creados se asignan automáticamente al testigo. En la columna **Recursos metro** de la ventana **Testigo metro**, se muestra la cantidad de recursos asignados al testigo.

Modificación y recuperación del testigo

El servicio del testigo es simple y no mantiene datos cruciales que no se pueden volver a crear. Por lo tanto, no es necesario respaldar, guardar ni recuperar el testigo y este se puede quitar y reinstalar cada vez que se requiera una recuperación.

Modificar los parámetros del testigo

Sobre esta tarea

En la ventana **Propiedades del testigo**, puede modificar el nombre y la descripción del testigo.

NOTA: Si desea cambiar la dirección IP o el FQDN del testigo, debe quitar y reinstalar el testigo.

Pasos

1. Seleccione **Protección** > **Testigo metro**.
2. Seleccione la casilla de verificación junto al testigo y elija **Modificar**.
3. Modifique los campos necesarios y seleccione **Aplicar**.

Reemplazar el testigo

Sobre esta tarea

Para reemplazar el servicio testigo, quítelo de los PowerStore sistemas y agréguelo. Es necesario quitar y agregar el testigo incluso si no se cambia el nombre de host o la dirección IP, ya que el nuevo testigo tiene un certificado diferente que se debe agregar a los PowerStore sistemas.

Pasos

1. Quite el servicio testigo de cada uno de los PowerStore sistemas. Para obtener detalles, consulte Quitar el testigo.
2. Agregue el servicio testigo a cada uno de los PowerStore sistemas. Para obtener detalles, consulte Configurar el testigo metro.

Modificar la configuración del host testigo

Si se debe modificar el host en el que está instalado el servicio testigo, puede realizar una de las siguientes acciones:

- Cree un host con la configuración necesaria e instale el testigo. A continuación, elimine el testigo existente de los PowerStore sistemas y reemplácelo por el nuevo testigo.

- Modifique el host existente:
  - Quite el testigo existente de los PowerStore sistemas. Para obtener detalles, consulte Quitar el testigo.
  - Desinstale el testigo del host existente.
  - Realice los cambios en la configuración necesarios en el host.
  - Reinstale el testigo en el host. Para obtener detalles, consulte Implementar el testigo metro.
  - Agregue el testigo a los PowerStore sistemas. Para obtener detalles, consulte Configurar el testigo metro.

Monitorear el testigo

Si selecciona **Protección** > **Testigo metro** > **[witness]**, se muestran las propiedades del testigo.

El servicio testigo mantiene la comunicación con cada nodo en cada dispositivo.

La ventana **Properties** del testigo muestra el estado de conexión de cada nodo y el estado de conexión general del servicio testigo.

Los posibles estados de conexión son los siguientes:

- Inicializando: todos los nodos están inicializando la conexión con el testigo.
- Correcto: todos los nodos pueden comunicarse con el testigo.
- Eliminando: el testigo se está eliminando del clúster.
- Parcialmente conectado: algunos nodos en algunos dispositivos pueden comunicarse con el testigo o el mismo testigo no está registrado en el sistema par.
- Desconectado: ningún nodo puede comunicarse con el testigo.

Una vez configurado el testigo, cada sesión metro intenta conectarse a él de manera independiente. Cada sesión metro tiene un estado que indica si puede usar el testigo cuando se produce una falla. Posibles estados del testigo para una sesión metro:

- Inicializando: el testigo se está inicializando, pero no está conectado.
- Desconectado: la sesión metro está en pausa o fracturada.
- Conectado: todos los nodos de todos los dispositivos están conectados al testigo y pueden usarlo si se produce una falla.
- Disengaged Invalid Configuration o Unavailable: la configuración del testigo no es válida (por ejemplo, el testigo está configurado solo en un sistema PowerStore o dos testigos diferentes están configurados en los sistemas local y remoto) o el testigo no está disponible.
- Desconectado, no se pudo inicializar: el testigo no se pudo inicializar con la sesión metro.
- Unconfigure in Progress: el testigo se está eliminando del PowerStore sistema.

Cuando el clúster tiene varios dispositivos, algunos de ellos pueden estar conectados al testigo, mientras que otros no. En consecuencia, es posible que el testigo no esté conectado para todas las sesiones metro existentes.

Quitar el testigo

Puede eliminar el servicio testigo de PowerStore en cualquier momento, independientemente de si está asignado a sesiones metro.

Para quitar el testigo, seleccione **Protección** > **Testigo metro** y, a continuación, marque la casilla junto al testigo y seleccione **Eliminar**.

Cuando se elimina el testigo, este se quita de todas las sesiones metro, las que se revierten al uso de reglas de preferencia como medio para determinar el comportamiento del sistema si se produce una falla.

Si ocurre un error durante la eliminación del testigo, este permanece en estado Anulación de configuración en curso hasta que se resuelve y, a continuación, la eliminación se reanuda.

Testigo: escenarios de falla

Cuando se produce una falla en un entorno metro con un servicio testigo, el sistema se comporta de la siguiente manera:

Cuando se pierde la conexión entre los sistemas local y remoto, la sesión metro se fractura. Ambos sistemas solicitan fracturar la sesión del testigo. El testigo responde con Operación exitosa a la primera solicitud y con Error a la segunda. El sistema que recibió Operación exitosa como respuesta mantiene el acceso de I/O de host al volumen metro, mientras que el que recibió Error se degrada a sí mismo.

El sistema no preferido envía la solicitud al testigo unos segundos después que el sistema preferido. Como resultado, si el sistema preferido está activo, recibe la respuesta Operación correcta y se selecciona para mantener el acceso de I/O de host.

Si el sistema preferido está inactivo, no envía una solicitud al testigo y el sistema no preferido recibe la respuesta Operación correcta.

Cuando uno de los sistemas pierde la conexión con el host, no hay impacto, ya que ambos continúan activos y el host puede acceder a ellos. Si se produce una pérdida de conexión entre los sistemas, el sistema que aún tiene conexión con el testigo recibe una respuesta de operación correcta y mantiene el acceso de I/O del host.

Configurar un volumen metro

Sobre esta tarea

La habilitación de la configuración metro para un volumen hace que sea visible para los hosts desde dosPowerStoreSistemas con una conexión de sistema remota.

Metro se puede configurar para volúmenes y clones de volúmenes que no son miembros de un grupo de volúmenes.

Los siguientes volúmenes no se pueden configurar como metro:

- Un volumen asignado con una política de protección que incluye una regla de replicación
- Un volumen o un clon de volumen que es miembro de un grupo de volúmenes
- Un volumen con una política de protección de solo lectura
- Un volumen que se está migrando o importando
- Un volumen que es un destino de replicación de solo lectura, el cual permanece una vez que se quita la replicación

NOTA: Si se configuró un testigo para estoPowerStoresistema, el volumen metro se asigna automáticamente al testigo.

Pasos

1. Seleccionar **Almacenamiento** > **Volumen** y seleccione la casilla de verificación de un volumen.
2. Seleccionar **Protección** > **Configuración del volumen metro**.
   Se muestra el panel deslizable **Configurar volumen metro**.
3. Seleccione un sistema remoto o configure un nuevo sistema remoto.
4. Si el sistema remoto tiene varios dispositivos, puede seleccionar la ubicación del volumen en el sistema remoto.
5. Haga clic en **Configure**.
6. En el sistema remoto, asigne el volumen metro configurado a un host.

Configurar un grupo de volúmenes metro

Sobre esta tarea

La habilitación de la configuración metro para un grupo de volúmenes hace que sea visible para los hosts desde dosPowerStoreSistemas con una conexión de sistema remota.

NOTA: Todos los volúmenes de un grupo de volúmenes se tratan como una sola instancia y todas las acciones en el grupo de volúmenes se aplican a todos sus miembros.

Los siguientes grupos de volúmenes no se pueden configurar como metro:

- Un grupo de volúmenes vacío
- Un clon de grupo de volúmenes
- Un grupo de volúmenes con un miembro clon
- Un grupo de volúmenes sin coherencia con el orden de escritura
- Un grupo de volúmenes que incluye volúmenes que no son locales.
- Un grupo de volúmenes asignado con una política de protección que incluye una regla de replicación.
- Un grupo de volúmenes con una política de protección de solo lectura
- Un grupo de volúmenes que se está migrando o importando
- Un grupo de volúmenes que es un destino de replicación de solo lectura

NOTA: Si se configuró un testigo para estoPowerStoresistema, el grupo de volúmenes metro se asigna automáticamente al testigo.

Pasos

1. Seleccionar **Almacenamiento** > **Grupo de volúmenes** y seleccione la casilla de verificación de un grupo de volúmenes.
2. Seleccionar **Protección** > **Configurar un grupo de volúmenes metro**.
   Se muestra el panel deslizable **Configurar grupo de volúmenes metro**.

3. Seleccione un sistema remoto o configure un nuevo sistema remoto.
4. Haga clic en **Configure**.
5. En el sistema remoto, mapee el grupo de volúmenes metro configurado a un host.

Configurar la función metro

NOTA: La función metro se puede configurar para volúmenes individuales, clones de volúmenes individuales o grupos de volúmenes. No puede configurar una función metro para volúmenes o clones que son miembros de un grupo de volúmenes.

Tras la configuración del recurso metro, el sistema desde el cual se configuró el recurso metro (volumen, clon de volumen o grupo de volúmenes) se establece automáticamente como preferido. Cuando el recurso metro está fracturado o en pausa y si no está configurado un testigo metro, el sistema preferido mantiene el acceso de host y producción y una asociación activa con una política de protección.

Cuando el estado del recurso metro es Funcionando normalmente (activo/activo), puede cambiar la función del recurso metro de preferido a no preferido o viceversa mediante las siguientes opciones:

- **Modificar función preferida**: utilice esta opción para cambiar la función actual de un recurso metro seleccionado. Esta opción se puede utilizar desde el sistema preferido o no preferido.

  NOTA: Puede acceder a esta opción seleccionando **Protección** > **Metro** y, a continuación, haga clic en el estado metro del recurso correspondiente para abrir la ventana Detalles del recurso metro.

- **Establecer función local en preferida** : utilice esta opción para establecer en preferido la función de varios recursos metro no preferidos seleccionados. Esta opción se debe utilizar antes de apagar el sistema preferido para realizar mantenimiento planificado. La configuración en preferido de los recursos metro no preferidos permite mantener el acceso de host y producción durante el apagado.

Monitorear recursos metro

Sobre esta tarea

Puede ver todos los recursos metro en el sistema, monitorear su estado y realizar acciones en un volumen, clon o grupo de volúmenes metro seleccionados.

Pasos

1. Seleccionar**Protección** > **Metro**para abrir la lista de recursos y detalles de metro.
2. Seleccione la casilla de verificación de un recurso metro para ver las posibles acciones que puede realizar en ese recurso.
3. Para ver información detallada sobre un recurso metro específico, haga clic en el estado del recurso en el**Estado de metro**columna.

   También puede ver información detallada sobre un recurso metro desde la**Almacenamiento** > **Volúmenes**o el**Almacenamiento** > **Grupos de volúmenes**Página:

   a. Haga clic en el nombre de un recurso metro en el**Almacenamiento** > **Volúmenes**o el**Almacenamiento** > **Grupos de volúmenes**para mostrar la página de información del recurso.
   b. Seleccione la**Protección**y, a continuación, seleccione la tarjeta**Volumen metro**o el**Grupo de volúmenes metro**para mostrar la información de metro para el recurso seleccionado.

Pausar un recurso metro

Sobre esta tarea

NOTA: Puede pausar volúmenes metro, clones o grupos de volúmenes individuales. No es posible pausar un volumen metro o un clon metro que son miembros de un grupo de volúmenes.

Es necesario pausar temporalmente un recurso metro en los siguientes escenarios:

- Cuando se requieren cambios en la configuración que no se pueden realizar con el recurso en normal funcionamiento, como el cambio de sus propiedades.
- Cuando los sistemas preferidos o no preferidos requieren mantenimiento, como el reemplazo de componentes de hardware defectuosos o cambios en la infraestructura de red.

- Cuando hay una falla en el sistema preferido que requiere la promoción del sistema no preferido para permitir una recuperación controlada.

La pausa se puede iniciar desde el sistema preferido o no preferido. Cuando un recurso metro está en pausa, la sincronización entre los sistemas se detiene temporalmente. Las políticas de acceso de producción y protección permanecen activas en el sistema preferido.

Cuando un recurso metro está fracturado y no hay conexión entre el sistema local y el remoto, la pausa se implementa solo en el sistema local (donde se inició):

- Cuando se inicia una pausa desde el sistema preferido:
  - El acceso de host y producción permanece habilitado en un recurso metro preferido pausado.
  - El acceso de host y producción permanece sin cambios en el recurso metro no preferido.
- Cuando se inicia una pausa desde el sistema no preferido:
  - El acceso de host y producción permanece deshabilitado, a menos que el recurso metro se haya promovido.
  - Dado que no hay conectividad de red, la pausa no modifica el estado del recurso metro preferido.
- Cuando se resuelve la conectividad, la pausa también se debe iniciar desde el sistema remoto.

Pasos

1. Seleccionar **Protección** > **Metro**.
2. Seleccione la casilla de verificación del recurso metro que desea pausar y haga clic en **Pausar**.
   Se muestra el panel deslizable **Pausar volumen/grupo de volúmenes metro**.
3. Haga clic en **Pausar** para confirmar.

Reanudar un recurso metro

Sobre esta tarea

NOTA: Puede reanudar volúmenes metro, clones o grupos de volúmenes individuales. No es posible reanudar un volumen metro o un clon metro que son miembros de un grupo de volúmenes.

La reanudación se puede iniciar desde el sistema preferido o desde el sistema no preferido.

Cuando reanuda un recurso metro preferido en pausa, el sistema preferido comienza a sincronizar los datos con el sistema no preferido. Una vez que finaliza la sincronización, el recurso metro regresa a un estado activo/activo.

Cuando reanuda un recurso metro promovido en pausa (anteriormente no preferido), el sistema no preferido comienza a sincronizarse con el preferido (estado Volviendo a proteger) para regresar a un estado activo/activo.

NOTA: Si un recurso metro estuvo en pausa durante mucho tiempo, la sincronización puede tardar debido a la acumulación de datos en el sistema preferido.

Si el sistema no preferido se promovió, la reanudación del recurso metro desde el sistema no preferido promovido sincroniza los datos de este sistema al preferido.

Pasos

1. Seleccionar**Protección** > **Metro**.
2. Seleccione la casilla de verificación del recurso metro que desea reanudar y haga clic en**Reanudar**.
   Se muestra el cuadro de diálogo **Reanudar volumen/grupo de volúmenes metro**.
3. Haga clic**Reanudar**para confirmar.

Promover un recurso metro

Requisitos previos

- Puede promover volúmenes metro, clones o grupos de volúmenes individuales. No es posible promover un volumen metro o un clon metro que sean miembros de un grupo de volúmenes.
- La promoción de un recurso metro se permite en un estado `Fractured` o `Paused`.

Sobre esta tarea

Cuando el enlace entre los dos sistemas de almacenamiento falla o cuando el sistema no preferido está inactivo, la sincronización entre los sistemas se detiene y el recurso metro se fractura. El sistema preferido permanece activo y continúa gestionando I/O. Si el usuario se encuentra en el sistema preferido, no se necesita realizar ninguna acción y los sistemas se sincronizan cuando se resuelve el problema.

Cuando se produce una falla en el sistema preferido, la sincronización entre los sistemas se detiene y el recurso metro se fractura. Ambos sistemas dejan de gestionar I/O. Para poder acceder al recurso metro, el usuario debe promoverlo en el sistema no preferido de manera de permitir el acceso de host y producción a él hasta que el sistema preferido se recupere.

Si el usuario verifica que el sistema preferido está disponible, el recurso metro en el sistema no preferido se puede promover sin consecuencias. Cuando el usuario se encuentra en el sistema no preferido, no es posible conocer el estado del sistema preferido (si el sistema está inactivo o si el enlace entre el sistema está inactivo). En este caso, la promoción del volumen metro en el sistema no preferido puede dar lugar a una situación en la que ambos sistemas continúan gestionando I/O, pero no se sincronizan.

Pasos

1. Seleccionar**Protección** > **Metro**.

   En la página Metro, se enumeran todos los recursos metro y se le permite evaluar todos los recursos afectados y priorizar la promoción de estos según sus consideraciones.

   NOTA: El estado de metro del recurso debe ser `Fractured`.

2. Seleccione el estado del recurso metro para mostrar la página de detalles del recurso metro y, a continuación, seleccione**Promover**.
   Se muestra el panel deslizable **Promover volumen/grupo de volúmenes metro**.

   NOTA: Antes de que se lleve a cabo la promoción, se toma una instantánea del recurso metro.

3. Verifique que comprende la implicancia de promover el recurso metro en caso de que el sistema remoto esté gestionando I/O y, si es posible, compruebe que el sistema remoto esté inactivo.
4. Seleccione la casilla de verificación de confirmación en la parte inferior del panel deslizable **Promover volumen metro/grupo de volúmenes** y seleccione**Promover**.
   El estado promovido del recurso metro se indica en la página de detalles del recurso metro.

Degradar un recurso metro

Sobre esta tarea

NOTA: Puede degradar volúmenes metro, clones o grupos de volúmenes individuales. No es posible degradar un volumen metro o un clon metro que son miembros de un grupo de volúmenes.

Cuando el sistema preferido se queda sin espacio de almacenamiento, la sincronización entre los sistemas se detiene y el recurso metro se fractura. Ambos sistemas dejan de gestionar I/O. En ese caso, el recurso metro en el sistema no preferido se debe promover para permitir el acceso de host y producción a él hasta que el sistema preferido resuelva el problema. Para habilitar este estado, en primer lugar, el recurso metro en el sistema preferido se debe degradar.

Pasos

1. Seleccionar**Protección** > **Metro**.

   NOTA: En la página Metro, se enumeran todos los recursos metro y se le permite evaluar todos los volúmenes afectados y priorizar la degradación de recursos según sus consideraciones.

2. Seleccione el estado de un recurso metro para mostrar la página de detalles del recurso metro y, a continuación, seleccione**Degradar**.
   Se muestra el panel deslizable **Degradar volumen/grupo de volúmenes metro**.
3. Verifique que comprende la implicancia de degradar el recurso metro en caso de que el sistema remoto esté gestionando I/O y, si es posible, compruebe que el sistema remoto esté inactivo.
4. Seleccionar**Degradar**.
   El estado degradado del recurso se indica en la página de detalles del recurso metro.

Finalizar un recurso metro

Sobre esta tarea

NOTA: Puede finalizar volúmenes metro individuales, clones o grupos de volúmenes. No es posible finalizar un volumen metro o un clon metro que sean miembros de un grupo de volúmenes.

Cuando finaliza un recurso metro, la configuración de metro se quita, lo que da lugar a dos volúmenes o grupos de volúmenes independientes. Si el recurso remoto no se elimina, el sistema quita la política de protección que tiene asignada, anula el mapeo de los hosts y le asigna un WWN de SCSI nuevo diferente. Puede finalizar un recurso metro desde el sistema preferido o no preferido.

Pasos

1. Seleccionar**Protección** > **Metro**.
2. Seleccione el estado de un recurso metro para mostrar la página de detalles del recurso metro y, a continuación, seleccione**Finalizar metro**.
   Se muestra el panel deslizable **Finalizar volumen/grupo de volúmenes metro**.
3. Seleccione una de las siguientes opciones en el panel deslizable:
   - Finalizar metro y mantener los recursos tanto en el sistema local como en el sistema remoto.

     NOTA: El sistema remoto anula el mapeo de los hosts y asigna un WWN de SCSI diferente al recurso. Si finaliza un grupo de volúmenes metro, se asigna un WWN de SCSI diferente a cada miembro del grupo de volúmenes.

   - Finalizar metro y eliminar el recurso y las instantáneas asociadas en el sistema remoto.

     NOTA: Los volúmenes remotos y los grupos de volúmenes asociados con instantáneas seguras no vencidas no se pueden eliminar.
4. Haga clic**Fin**.

Resumen de acciones permitidas en un recurso de metro

En la siguiente tabla, se resumen las acciones permitidas que puede realizar en un recurso de metro según el estado actual de este y el sistema desde el cual se inicia la acción.

NOTA: En la tabla se abordan casos de uso comunes y no se incluyen escenarios de falla poco frecuentes.

Tabla 2. Acciones permitidas de metro

Ubicación	Estado de metro	Modificar función	Promover	Degradar	Pausar	Reanudar	Finalizar metro
En el sistema preferido	Funcionando normalmente	Sí	No	No	Sí	No	Sí
	En pausa	No	No	Sí	No	Sí	Sí
	Fracturado	No	No	Sí	Sí	No	Sí
	Cambiando a sincronización metro	No	No	No	Sí	No	Sí
En el sistema no preferido	Funcionando normalmente	Sí	No	No	Sí	No	Sí
	En pausa	No	Sí (si el otro sistema es inaccesible)	No	No	Sí	Sí

Tabla 2. Acciones permitidas de metro (continuación)

Ubicación	Estado de metro	Modificar función	Promover	Degradar	Pausar	Reanudar	Finalizar metro
	Fracturado	No	Sí (si el otro sistema es inaccesible)	No	Sí	No	Sí
	Cambiando a sincronización metro	No	No	No	Sí	No	Sí

Uso de políticas de protección con metro

Cuando se asigna un recurso metro existente con una política de protección o se configura un recurso con una política de protección para metro, se aplica la misma protección al recurso metro en ambos sistemas. La política de protección que se crea en el sistema remoto es de solo lectura. Los cambios en la política de protección y en las reglas de instantáneas solo se pueden realizar en la política creada por el usuario (independientemente del sistema de almacenamiento en el que se creó). La política de solo lectura se sincroniza con los cambios cada 15 minutos.

Las instantáneas iniciadas por el usuario que se crean en un sistema de almacenamiento también se generan en el otro.

NOTA: La replicación síncrona y asíncrona no es compatible con los recursos metro. Una política de protección que contiene una regla de replicación no se puede asignar a un recurso metro.

La asignación de una política de protección se puede realizar en el sistema local o en el remoto (ya sea preferido o no preferido).

La cancelación de la asignación de la política de protección se debe realizar en el sistema de almacenamiento en el que se asignó. Después de que se cancela la asignación de la política de protección del recurso en el sistema local, también se cancela la asignación del recurso en el otro sistema. Una vez que no haya recursos metro que utilicen la política de protección de solo lectura, esta se elimina automáticamente del sistema.

NOTA: Cuando no se puede cancelar la asignación de la política del sistema de almacenamiento en el que se asignó, debido a una falla del recurso metro, se permite lo siguiente:

- Se puede cancelar la asignación de una política de solo lectura de un recurso metro preferido o se puede intercambiar por una política de lectura/escritura cuando el recurso está fracturado.
- Se puede cancelar la asignación de una política de solo lectura de un recurso metro no preferido promovido o se puede intercambiar por una política de lectura/escritura.

NOTA: Cuando el recurso metro está fracturado o una sesión metro está en pausa, se generan instantáneas solo en el sistema activo. Cuando el recurso metro se autorrepara o la sesión se reanuda, las instantáneas no se copian en el sistema remoto y permanecen en el sistema local hasta que vencen o se eliminan.

Uso de QoS con metro

Cuando un volumen de metro o un grupo de volúmenes se configuran con una política de QoS, la política no se replica en el sistema remoto. Si utiliza una configuración de metro en la que se utiliza QoS, se recomienda configurar la misma política de QoS en ambos lados del recurso de metro.

Si una política de QoS se configura solo en un lado del recurso de metro, es posible que un host prefiera ciertas rutas para enviar I/O. Lo mismo puede ocurrir cuando se configura una política de QoS en ambos lados del recurso de metro, pero los límites de QoS no coinciden.

7

Respaldo remoto

Este capítulo incluye la siguiente información:

Temas:

Terminología

Tabla 3. Terminología de respaldo remoto

TÉRMINO	DESCRIPCIÓN
PowerProtect DD	Un dispositivo Data Domain de nueva generación diseñado principalmente para el respaldo de datos.
PowerProtect Data Manager	Una aplicación de administración centralizada para administrar uno o más PowerProtect DD físicos o en la nube.
Unidad de almacenamiento DD	Una unidad lógica en PowerProtect DD que se expone a aplicaciones de respaldo mediante el protocolo de DD Boost.
Sistema remoto PowerProtect DD	Una unidad de almacenamiento en el sistema PowerProtect DD.
Sesión remota	Una sesión de instantánea remota que refleja el estado y el progreso de una operación en un sistema remoto PowerProtect DD. El tipo de sesión puede ser de respaldo, recuperación o acceso instantáneo.
Instantánea remota	Una representación de los datos que se respaldan en PowerProtect DD y que se pueden recuperar o buscar mediante el acceso instantáneo.

Prerrequisitos y límites

Cuando utilice el respaldo remoto, tenga en cuenta las siguientes limitaciones:

- Solo se puede crear una sesión de respaldo remoto por recurso (volumen o grupo de volúmenes).
- Solo se puede crear una sesión de recuperación o acceso instantáneo por instantánea remota.
- Se pueden crear hasta dos sesiones de acceso instantáneo por nodo.
- Las sesiones de respaldo remoto y recuperación y las sesiones de acceso instantáneo son mutuamente excluyentes: cuando una sesión de acceso instantáneo está activa, las sesiones de respaldo remoto y recuperación no se pueden ejecutar y viceversa.
- Cuando una NDU o una reconfiguración de red están en curso, las sesiones de respaldo remoto, recuperación y acceso instantáneo no se pueden ejecutar.
- Se puede crear una sesión de acceso instantáneo para un grupo de volúmenes que consta de hasta cuatro volúmenes.

- Si el tamaño del volumen respaldado supera el límite de cuota máxima de la unidad de almacenamiento (SU) de Data Domain, el respaldo puede fallar. Se recomienda no establecer cuotas de SU cuando se utiliza el respaldo remoto. Consulte la documentación de PowerProtect DD para obtener más información.
- Para obtener un rendimiento óptimo del sistema, se recomienda respaldar hasta 125 volúmenes en PowerProtect DD por dispositivo.
- Para obtener un rendimiento óptimo del sistema, se recomienda crear hasta 125 sesiones de respaldo remoto por dispositivo.
- El respaldo remoto no soporta volúmenes metro.
- La compatibilidad con DDVE en la nube solo está disponible con el proveedor de servicio en la nube de AWS.
- La desduplicación está deshabilitada en el lado del cliente, pero está habilitada en el lado del dispositivo PowerProtect.
- La HA no es compatible con el acceso instantáneo. El acceso instantáneo falla si el clúster se reinicia o realiza una conmutación por error. Para obtener detalles, consulte el artículo de la base de conocimientos 000208509 de Dell (Las sesiones de acceso instantáneo muestran un estado fallido después del reinicio del nodo).

Recursos de documentación

Consulte los siguientes recursos para obtener información adicional:

Tabla 4. Recursos de documentación

Documento	Descripción	Ubicación
Guía del usuario y de administración de PowerProtect Data Manager	En este documento, se proporciona información de configuración para PowerProtect Data Manager.	Soporte de Dell
Dell PowerProtect Data Manager: protección de datos para Dell PowerStore Guía de arreglos de almacenamiento	Este documento se centra en el respaldo y la recuperación de datos de volúmenes de bloques en PowerStore arreglos de almacenamiento con PowerProtect Data Manager.	Centro de información de Dell
PowerStore Ayuda en pantalla	En la ayuda en línea, se proporciona información contextual para la página que se abre en PowerStore Manager.	Integrado en PowerStore Manager

Flujo de trabajo básico de respaldo remoto

El respaldo de recursos en un sistema PowerProtect DD es la acción básica que usted puede realizar. Cuando se crean respaldos en un sistema PowerProtect DD, puede buscarlos y recuperarlos. Cada acción de respaldo remoto está enlazada a una sesión de respaldo remoto que le permite rastrear su progreso.

Sobre esta tarea

Realice los siguientes pasos para crear una sesión de respaldo remoto:

Pasos

1. Agregar una conexión de sistema remoto para el respaldo remoto.
2. Crear una regla de respaldo remoto.
3. Crear una política de protección: solo se puede agregar una regla de respaldo remoto a una política de protección.
4. Asignar una política de protección: asigne una política que incluya una regla de respaldo remoto a un volumen o grupo de volúmenes. Se crea una sesión de respaldo remoto y se muestra en la pestaña **Sesiones de respaldo** de la página **Respaldo remoto**.

Estados de las sesiones

Las sesiones de respaldo remoto, recuperación y acceso instantáneo pasan por varios estados que indican el progreso de las sesiones y los posibles problemas.

Los posibles estados de las sesiones son los siguientes:

- **Inicializando**: la sesión se está creando. Una vez finalizada la creación, el estado cambia a Inactivo.
- **Inactivo**: no se transfieren datos al dispositivo remoto. La sesión permanece en estado Inactivo hasta que se activa la regla de respaldo remoto programada o si usted inicia un respaldo manual.

- **Preparar**: el sistema PowerStore se está preparando para realizar un respaldo. Si hay varias sesiones activas, la sesión puede permanecer en el estado Preparar hasta que llega a la parte superior de la cola.
- **Reenvío de I/O** (se aplica solo a sesiones de acceso instantáneo): la sesión está reenviando las I/O del host.
- **En curso**: el sistema crea el respaldo en el sistema remoto. Durante este estado, puede hacer clic en el enlace de estado para monitorear el progreso del respaldo y ver más detalles.
- **Finalizado** (se aplica solo a sesiones de recuperación): la sesión finalizó correctamente.
- **Sistema en pausa**: la actualización o la migración no disruptiva puso en pausa la sesión.
- **En pausa**: la sesión está en pausa.
- **Cancelando**: la sesión se está cancelando.
- **Cancelado**: la sesión se canceló explícitamente. Las sesiones en los estados Preparar, En curso y En pausa se pueden cancelar.
- **Eliminando**: la sesión se está eliminando.
- **Falló**: la sesión no pudo crear el respaldo.
- **Reversión en curso**: se produjo un error mientras la sesión estaba activa y los cambios se revirtieron.
- **Error, se requiere limpieza**: se produjo un error mientras se revertían los cambios (como resultado de un error anterior). El servicio de limpieza, que se ejecuta de manera periódica, resuelve automáticamente el problema y el estado de la sesión cambia a Falló. Para las sesiones de respaldo remoto, los respaldos programados no se pueden ejecutar mientras la sesión está en este estado.
- **Cancelar, se requiere limpieza**: se produjo un error durante la operación de cancelación de la sesión. El servicio de limpieza, que se ejecuta de manera periódica, resuelve automáticamente el problema y el estado de la sesión cambia a Cancelado. Para las sesiones de respaldo remoto, los respaldos programados no se pueden ejecutar mientras la sesión está en este estado.
- **Se requiere limpieza**: la sesión se completó correctamente, pero se produjo un error durante la fase de limpieza local. El servicio de limpieza, que se ejecuta de manera periódica, resuelve automáticamente el problema y el estado de la sesión cambia a Inactivo o Finalizado. Para las sesiones de respaldo remoto, los respaldos programados no se pueden ejecutar mientras la sesión está en este estado.
- **Limpieza en curso**: se está realizando una limpieza.

Administración de sesiones de respaldo remoto

Cuando asigna una política de protección que incluye una regla de respaldo remoto a un volumen o grupo de volúmenes, se crea una sesión de respaldo remoto y se muestra en la pestaña **Sesiones de respaldo** de la página **Respaldo remoto**.

En la pestaña **Sesiones de respaldo**, puede realizar las siguientes acciones en una sesión de respaldo remoto:

- **Respaldar**: puede realizar un respaldo manual según demanda cuando la sesión está inactiva. Esto se puede hacer, por ejemplo, si el recurso no se respaldó durante un período prolongado.

  NOTA: Un respaldo creado manualmente está sujeto a la política de retención configurada en la regla de respaldo remoto.

- **Pausar**: la pausa de una sesión en estado Inactivo hace que esta se pause de inmediato. Si pausa una sesión cuando se encuentra En curso, esta se pausa solo después de que se completa el respaldo en ejecución actual. Los respaldos subsiguientes no se realizan mientras la sesión está en pausa.
- **Reanudar**: utilice esta opción para reanudar una sesión de respaldo en pausa. El siguiente respaldo se produce de acuerdo con el programa configurado.
- **Eliminar**: puede utilizar esta opción solo para eliminar una sesión de un recurso protegido por una política externa. En el caso de los recursos protegidos por una política de PowerStore, puede eliminar la sesión de respaldo remoto asociada cancelando la asignación de la política del recurso o eliminando la regla de respaldo remoto de la política asignada.
- **Cancelar**: puede utilizar esta opción para cancelar una sesión de respaldo solo cuando está En curso. La cancelación de una sesión hace que se cancele el respaldo actual y que se eliminen los datos copiados.

  NOTA: Cuando la sesión se encuentra en estado Preparar, otras sesiones pueden agregarse a la cola antes que ella. Cuando hace clic en **Cancelar**, el estado de la sesión cambia a **Cancelando**, pero la sesión se cancela solo cuando llega a la parte superior de la cola y se activa (estado En curso).

Recursos

En la pestaña Recursos, se muestran todos los volúmenes y grupos de volúmenes que tienen instantáneas remotas asociadas.

Un recurso se agrega a la tabla **Recursos** después de que una sesión de respaldo remoto creada para él desencadena la creación de una instantánea remota.

Si se elimina de PowerStore un volumen o un grupo de volúmenes que tiene instantáneas remotas asociadas, las instantáneas remotas no se ven afectadas. El recurso eliminado permanece en la lista de la tabla Recursos hasta que vencen todas sus instantáneas remotas asociadas. Para ver si se eliminó un recurso, agregue la columna **Origen eliminado** a la tabla Recursos mediante la opción **Mostrar/ ocultar columnas de tabla**.

En la pestaña **Recursos**, puede realizar las siguientes acciones:

- Administrar instantáneas: si selecciona un recurso en la lista y hace clic en **Administrar instantáneas**, se muestran todas las instantáneas remotas creadas para este recurso:
  - La hora de vencimiento de las instantáneas creadas automática y manualmente se basa en el tiempo de retención que se configuró en la regla de respaldo remoto.
  - La hora de vencimiento de una instantánea remota no se puede cambiar. El cambio del período de retención en una regla de respaldo remoto no afecta a las instantáneas existentes.
  - Para las instantáneas generadas automáticamente, un nombre de instantánea remota incluye el nombre de la regla de respaldo remoto que la creó.
  - Si selecciona una instantánea de la lista y hace clic en **Recuperar**, se crea una sesión de recuperación para esta instantánea. Consulte Recuperar una instantánea remota en el mismo clúster de PowerStore para obtener detalles.
  - Si selecciona una o más instantáneas y hace clic en **Eliminar**, se eliminan las instantáneas.

  NOTA: También puede ver las instantáneas remotas de un recurso y realizar acciones relacionadas haciendo clic en el recurso y seleccionando la pestaña **Instantáneas remotas**.

- Acceso instantáneo: si selecciona un recurso de la lista y hace clic en **Acceso instantáneo**, se inicia el proceso de habilitación del acceso instantáneo para la instantánea remota seleccionada. Para obtener información detallada, consulteCrear una sesión de acceso instantáneo.
- Descubrir instantáneas remotas: utilice esta opción cuando desee recuperar una instantánea remota de un recurso en un clúster de PowerStore diferente. Para obtener información detallada, consulteRecuperar una instantánea remota en un clúster diferente.

Sesiones de recuperación

Las instantáneas de volúmenes y grupos de volúmenes que se respaldan en un sistema PowerProtect DD se pueden recuperar en el mismo clúster o en otro clúster de PowerStore.

Es posible que desee recuperar una instantánea remota para restaurar el recurso de origen o para crear un clon delgado.

Recuperar una instantánea remota en el mismo clúster de PowerStore:

- Si el volumen o el grupo de volúmenes de origen del respaldo recuperado aún existe en el sistema, se crea una instantánea local en el clúster de PowerStore. Si es posible, la recuperación es incremental.
- Si el volumen o el grupo de volúmenes de origen del respaldo recuperado ya no existe en el sistema, se crean un volumen nuevo y una instantánea local y el nuevo volumen se restaura con los datos de la instantánea.

Recuperar una instantánea remota en un clúster de PowerStore diferente:

- Dado que el volumen de origen nunca existió en ese clúster, se crean un volumen nuevo y una instantánea local. El volumen nuevo se restaura con los datos de la instantánea.

Para cada operación de recuperación, se crea una sesión de recuperación. El estado inicial de la sesión es Preparar. Una vez que la sesión comienza a copiar la instantánea, el estado cambia a En curso y, cuando se copia, cambia a Finalizado.

Puede ver y monitorear el progreso de las sesiones de recuperación en la pestaña **Sesiones de recuperación** (**Protección** > **Respaldo remoto**). También puede realizar las siguientes acciones:

- Eliminar: utilice esta opción para eliminar una sesión de recuperación en un estado **Finalizado**.
- Cancelar: utilice esta opción para cancelar una sesión de recuperación en un estado **En curso**.

  NOTA: Cuando el estado de la sesión es **En curso**, otras sesiones pueden agregarse a la cola antes que ella. Cuando hace clic en **Cancelar**, el estado de la sesión cambia a **Cancelando**, pero la sesión se cancela solo cuando llega a la parte superior de la cola y se activa.

Una vez que se recupera un respaldo, este funciona como cualquier instantánea local. Puede usar un respaldo recuperado para restaurar un volumen primario o para crear un clon. La instantánea recuperada se configura en Sin eliminación automática. Puede cambiar este ajuste mediante la configuración de un período de retención. También puede modificarlo a una instantánea segura.

Recuperar una instantánea remota en el mismo clúster de PowerStore

Sobre esta tarea

Es posible que desee recuperar una instantánea remota en el mismo clúster de PowerStore en el que reside el recurso de origen cuando debe restaurar el recurso primario o crear un clon delgado. Puede recuperar una instantánea remota de un recurso tanto si aún existe como si se eliminó.

Pasos

1. Haga clic en **Protección** > **Respaldo remoto** y seleccione la pestaña **Recursos**.

   En la pestaña **Recursos**, se muestran todos los recursos (volúmenes y grupos de volúmenes) que tienen instantáneas remotas asociadas.
2. En la lista Recursos, haga clic en la casilla de verificación junto al recurso y seleccione **Administrar instantáneas** para ver todos los respaldos creados para ese recurso.
3. En el panel **Administrar instantáneas**, seleccione la instantánea que desea recuperar y haga clic en **Recuperar**.
4. En el mensaje de confirmación, haga clic en **Recuperar**.
   Se crea una sesión de recuperación para la instantánea y se agrega a la tabla Sesiones de recuperación. Si el recurso de origen existe en el clúster, se crea en él una instantánea local y el respaldo recuperado se copia en ella. La recuperación puede ser una copia completa o incluir solo las diferencias entre el respaldo y el recurso (copia incremental), según el último respaldo. Si el recurso de origen ya no existe en el clúster, se crea un nuevo volumen o grupo de volúmenes en el clúster de PowerStore, así como una instantánea local en la que se copia la instantánea remota.

   Puede monitorear el progreso de la sesión de recuperación en **Protección** > **Respaldo remoto** > **Sesiones de recuperación**.

Recuperar una instantánea remota en un clúster diferente

Sobre esta tarea

Cuando recupera una instantánea remota en un clúster de PowerStore que no sea el clúster que tiene el recurso de origen, se crea un nuevo volumen o grupo de volúmenes en el clúster de PowerStore, así como una instantánea local en la que se copia la instantánea remota.

Pasos

1. Haga clic en **Protección** > **Respaldo remoto** y seleccione la pestaña **Recursos**.
2. Haga clic en **Descubrir instantáneas remotas**.
3. En el panel **Descubrir instantáneas remotas**, configure lo siguiente:
   - Sistema remoto PowerProtect DD: seleccione el sistema PowerProtect DD desde el que desea recuperar el respaldo.
   - ID global de PowerStore: especifique el Globally Unique Identifier del clúster de PowerStore desde el que se inició el respaldo. Puede ver el ID global del clúster en **Ajustes** > **Clúster** > **Propiedades**. Para obtener información adicional sobre cómo recuperar el ID global del clúster, consulte el artículo de la base de conocimientos 000226798 de Dell (Cómo obtener el ID global del clúster primario...).
   - Desde: especifique la fecha y la hora de inicio para buscar instantáneas remotas.
   - Hasta: especifique la fecha y la hora de finalización para buscar instantáneas remotas.
4. Haga clic en **Siguiente**.
5. En la lista de instantáneas descubiertas, seleccione la instantánea que desea recuperar y haga clic en **Siguiente**.

   NOTA: Solo puede seleccionar instantáneas que creó un clúster de PowerStore.
6. Revise el resumen de la información y haga clic en **Recuperar**.

Resultados

PowerStore crea una sesión de recuperación que se puede ver en la pestaña **Sesiones de recuperación**. Cuando se completa la sesión, se crea la instantánea recuperada y un nuevo volumen en el clúster local.

Recuperación: consideraciones adicionales

- Cuando el origen original de una instantánea de respaldo que se recupera de DD ya no existe (instantánea huérfana), los bloques en el volumen recién creado que no se escribieron cuando se respaldó el volumen original se asignan y se escriben con ceros. En consecuencia, las capacidades física y lógica son las mismas (cuando se observan los datos de capacidad de respaldo recuperados). Cuando el nuevo volumen se mapea a un host, el espacio utilizado y el espacio libre se muestran correctamente. Para obtener detalles, consulte el artículo de la base de conocimientos 000208504 de Dell (Después de recuperar PowerStore desde Data Domain...).
- Cuando ya no existe un volumen o un grupo de volúmenes de origen en el clúster de PowerStore, la recuperación del respaldo respectivo siempre da lugar a la creación de un nuevo origen junto con la instantánea recuperada.
- Si el tamaño de la instantánea recuperada no coincide con el del volumen de origen, la recuperación es completa (se copia la instantánea completa de PowerProtect a PowerStore).
- La recuperación incremental (que solo recupera los cambios que se produjeron desde el respaldo) se produce si se cumplen las siguientes condiciones:
  - El tamaño del volumen de origen no ha cambiado desde que se respaldó.
  - Tanto el volumen de origen como el respaldo remoto más reciente existen en el clúster de PowerStore.
- Es posible que la velocidad de transferencia promedio de una recuperación incremental no siempre sea precisa, aunque el porcentaje de progreso de la recuperación refleja con exactitud la cantidad de datos recuperados.

Sesiones de acceso instantáneo

El acceso instantáneo le permite acceder a instantáneas remotas en un sistema PowerProtect DD sin tener que recuperarlas en el clúster de PowerStore.

- Utilice la opción de acceso instantáneo para buscar una instantánea remota antes de decidir si desea recuperarla o para acceder a una instantánea de un recurso eliminado, dañado o modificado y copiarla en el host.
- Solo se permite una sesión de acceso instantáneo por instantánea remota.
- Se puede crear una sesión de acceso instantáneo para grupos de volúmenes que incluyen hasta cuatro miembros.
- Cuando se ejecuta una sesión de acceso instantáneo para un recurso de almacenamiento, el clúster de PowerStore no puede realizar operaciones de respaldo y recuperación para los recursos protegidos que se encuentran en el mismo dispositivo que ese recurso. Se recomienda finalizar la sesión de acceso instantáneo cuando sea posible para proporcionar protección continua para los recursos de almacenamiento.
- El acceso instantáneo falla cuando un clúster se reinicia o realiza una conmutación por error. Para reiniciar el acceso instantáneo en este caso, anule el mapeo del volumen de acceso instantáneo desde el host, elimine la sesión y vuelva a crearla.
- El sistema configura la afinidad de nodos para las sesiones de acceso instantáneo durante la creación. Si el host no puede acceder al nodo con el que tiene afinidad la sesión de acceso instantáneo, esta no realiza una conmutación por error al otro nodo y el host puede tener problemas para acceder a los datos del recurso de acceso instantáneo.

En la pestaña **Sesiones de acceso instantáneo**, se proporciona la siguiente información:

- Estado: el estado de la sesión es Reenvío de I/O.
- Recurso local: se muestra el nuevo volumen o grupo de volúmenes que se creó como parte de la sesión. Si hace clic en el hiperenlace del recurso local, se abre la página Detalles de este recurso, donde puede ver los detalles del volumen o los miembros del grupo de volúmenes. También puede ver datos de rendimiento, comprobar alertas emitidas y mapear hosts al recurso o anular su mapeo de este.

En la pestaña Sesiones de acceso instantáneo, puede finalizar una sesión de acceso instantáneo. Para finalizar la sesión, primero debe quitar todos los mapeos de host al recurso local.

Los volúmenes y los grupos de volúmenes que se crean como parte de las sesiones de acceso instantáneo también se muestran en **Almacenamiento** > **Volúmenes** > **Acceso instantáneo** y **Almacenamiento** > **Grupos de volúmenes** > **Acceso instantáneo**.

Crear una sesión de acceso instantáneo

El acceso instantáneo le permite obtener acceso a instantáneas remotas en PowerProtect DD sin tener que recuperarlas en el clúster de PowerStore.

Pasos

1. Seleccione **Protección** > **Respaldo remoto** > **Recursos**.
2. En la lista de recursos, marque la casilla de verificación junto al recurso y haga clic en **Acceso instantáneo**.

   En el panel **Habilitar acceso instantáneo**, se muestran todas las instantáneas remotas disponibles para el recurso seleccionado.

3. Seleccione la instantánea a la que desea acceder.

   NOTA: También puede seleccionar el recurso y, a continuación, seleccionar **Instantáneas remotas** > **instantáneas remotas** > **Habilitar acceso instantáneo**.

4. De manera opcional, puede mapear hosts al volumen que se crea cuando se inicia la sesión de acceso instantáneo. Haga clic en **Mapear hosts**, seleccione los hosts que desea mapear y haga clic en **Aplicar**.
   Los hosts mapeados se enumeran en la sección Conectividad del host.

   NOTA: Esta opción existe solo para volúmenes y no para grupos de volúmenes. El mapeo de hosts a miembros de un grupo de volúmenes solo es posible después de que usted crea la sesión de acceso instantáneo (consulte los detalles a continuación).

5. Haga clic en **Habilitar**.
   Se crea una sesión de acceso instantáneo y se agrega a la pestaña **Sesiones de acceso instantáneo**. Se crea un volumen o un grupo de volúmenes asociados locales para la sesión, los que se pueden ver en la pestaña **Acceso instantáneo** de la ventana **Volúmenes** o **Grupos de volúmenes**.

   NOTA: La pestaña **Acceso instantáneo** se muestra solo cuando PowerProtect DD se agrega como un sistema remoto.

   El recurso creado es de lectura/escritura. Los datos se escriben temporalmente en el dispositivo PowerProtect DD mientras la instantánea remota permanece sin cambios. Cuando se elimina la sesión, se pierden todas las escrituras.

Resultados

Después de crear un acceso instantáneo para un grupo de volúmenes, puede asignar hosts a miembros del grupo de volúmenes que se creó para la sesión:

1. Seleccione **Protección** > **Respaldo remoto** > **Sesiones de acceso instantáneo**.
2. Haga clic en el enlace del grupo de volúmenes en la columna **Recurso local** para ver sus miembros.
3. Seleccione los miembros que desea mapear y haga clic en **Mapear** para abrir el panel **Mapear hosts**.

Acceso instantáneo: consideraciones adicionales

- PowerStore soporta el acceso instantáneo para todos los recursos de bloques, excepto con los almacenes de datos VMware vStorage VMFS. Si debe acceder a datos dentro de una instantánea remota, recupérela y, a continuación, cree y monte un clon delgado.
- La HA no es compatible con el acceso instantáneo; consulte Alta disponibilidad y el artículo de la base de conocimientos 000208509 de Dell (Las sesiones de acceso instantáneo muestran un estado fallido después del reinicio del nodo).
- El acceso instantáneo no es compatible con DDVE en la nube.

Alta disponibilidad

La alta disponibilidad es compatible (pero no está garantizada) con sesiones de respaldo remoto y sesiones de recuperación, pero no con sesiones de acceso instantáneo:

- Cuando un nodo está inactivo o se reinicia:
  - Las sesiones de respaldo y recuperación conmutan por error al nodo par y continúan en este.
  - Las sesiones de acceso instantáneo son específicas del nodo. Cuando el nodo en el que se ejecuta la sesión es inaccesible o está inactivo, la sesión pasa al estado fallido. Anule el mapeo del volumen del host, elimine la sesión y, a continuación, vuelva a crearla.
- Cuando un dispositivo se apaga o se reinicia:
  - Todas las sesiones de respaldo y recuperación se reanudan cuando el dispositivo vuelve a estar activo.
  - Las sesiones de acceso instantáneo pasan a un estado fallido. Anule el mapeo del volumen del host, elimine la sesión y, a continuación, vuelva a crearla.

Alertas de respaldo remoto

En la pestaña **Alertas** (que se encuentra en **Monitoreo**), se muestran las alertas generales que se producen para las sesiones de respaldo remoto, como la creación y la finalización de sesiones, la adición o la eliminación de un sistema remoto, etc. Puede filtrar las alertas de respaldo remoto seleccionando **Sesión remota** y **Sistema remoto** como Tipo de recurso.

Las alertas también se emiten cuando se producen fallas. La cantidad de alertas se muestra en las pestañas **Sesiones de respaldo** y **Sesiones de recuperación**. Haga clic en el número para abrir la pestaña **Alertas**.

8

Respaldo de NDMP para servidores NAS

Este capítulo incluye la siguiente información:

Temas:

Habilitar el respaldo NDMP

Puede configurar el respaldo estándar para los servidores NAS mediante NDMP. El Network Data Management Protocol (NDMP) proporciona un estándar para respaldar servidores de archivos en una red. Cuando NDMP está habilitado, una aplicación de administración de datos (DMA) de otros fabricantes, como Dell Networker, puede detectar elPowerStoreNDMP mediante la dirección IP del servidor NAS.

Sobre esta tarea

La habilitación de NDMP se realiza después de la creación del servidor NAS.

PowerStoreadmite:

- NDMP de tres vías: los datos se transfieren mediante la DMA a través de una red de área local (LAN) o una red de área extendida (WAN).
- Respaldos completos e incrementales

Pasos

1. Seleccionar **Almacenamiento** > **Servidores NAS** > **[servidor NAS]** > **Protección**.
2. En **NDMP Backup**, si **Disabled** está activo, deslice el botón para seleccionar **Enabled**.
3. Ingrese una contraseña en **New Password**.
   El nombre de usuario siempre es `ndmp`.
4. Vuelva a ingresar la misma contraseña nueva en **Verificar contraseña**.
5. Haga clic en **Aplicar**.

Siguientes pasos

Salga de la página de NDMP y regrese a ella para validar que NDMP esté habilitado.

A

Resumen de replicación

En este apéndice se incluye la siguiente información:

Temas:

Resumen de replicación

En la siguiente tabla, se resumen los diversos atributos de replicación (síncrona y asíncrona) y metro.

Tabla 5. Replicación y metro: resumen

Atributo	Replicación asíncrona	Replicación síncrona	Metro
Tipo compatible	Bloque y archivo	Bloque y archivo	Bloque
Recursos de almacenamiento	Volúmenes, grupos de volúmenes, clones delgados, servidores NAS, vVols	Volúmenes, grupos de volúmenes, clones delgados, servidores NAS	Volúmenes y grupos de volúmenes
Tipo de replicación	Asíncrona	Síncrona	Síncrona
RPO de destino	Valor fijo de 5 min a 24 h	0	0
Acceso de host	Activo/pasivo. Requiere una conmutación por error	Activo/pasivo. Requiere una conmutación por error o RTO>0. En el caso de archivos, requiere conmutación por error automática.	Cambio de ruta de ALUA activo/activo
Protocolos de host	SCSI, NVMe	SCSI, NVMe	SCSI
WWN/NQN de bloque	Diferente	Diferente	El mismo WWN en ambos extremos
Testigo	No	Archivo: Sí Bloque: No	Sí
RTT/distancia	No se aplica	5 milisegundos	5 milisegundos*
Impacto del rendimiento en el acceso del host	Impacto mínimo según el dimensionamiento y la carga de trabajo	Agrega latencia adicional (tiempo de ida y vuelta en espejo)	Agrega latencia adicional (tiempo de ida y vuelta en espejo)
Replicación de instantáneas	Replicación de instantáneas de bloques en el origen. La replicación de instantáneas para archivos no es compatible.	Instantáneas de bloques casi idénticas. La replicación de instantáneas para archivos no es compatible.	Instantáneas casi idénticas
Prueba de conmutación por error	Sí (por ejemplo, archivo, mediante un clon)	Sí (por ejemplo, archivo, mediante un clon)	No se aplica
Conversión asíncrona <-> síncrona	Permitida para los recursos de bloques. No soportada con archivos.	Permitida para los recursos de bloques. No soportada con archivos.	No compatible
Instantánea de recuperación	Base común en cada ciclo de replicación	Se soporta cuando está en pausa	No compatible

Tabla 5. Replicación y metro: resumen (continuación)

Atributo	Replicación asíncrona	Replicación síncrona	Metro
NDU	La replicación se pausa durante la NDU	Las sesiones activas continúan	Las sesiones activas continúan

1

1 Es posible que algunas aplicaciones protegidas requieran menor RTT/distancia para la configuración de metro.

B

Casos de uso

Este capítulo contiene la siguiente información:

Temas:

Casos de uso de instantáneas y clones delgados

Puede utilizar instantáneas y clones delgados para restaurar volúmenes dañados y crear ambientes de pruebas.

Las instantáneas son copias de solo lectura que se pueden usar para guardar el estado actual de un objeto. Puede utilizar instantáneas para recuperar datos rápidamente en caso de que se produzcan daños o errores de usuario. Un host no puede acceder directamente a las instantáneas.

Los clones delgados son copias con capacidad de escritura de una instantánea, un volumen o un Grupo de volúmenes a los que puede acceder un host. Se pueden crear directamente como una copia del objeto primario o mediante una de sus instantáneas. Tanto las instantáneas como los clones delgados son copias con uso eficiente del espacio que comparten bloques de datos con su objeto primario.

Uso de instantáneas y clones delgados para la recuperación parcial de un volumen

Puede utilizar instantáneas y clones delgados para recuperar parte de un volumen, como archivos individuales o registros de la base de datos, desde un punto en el tiempo anterior. Primero, cree un clon delgado a partir de la instantánea que contiene los datos que necesita recuperar. Luego, proporcione acceso de host al clon y recupere los datos desde el host.

Uso de instantáneas para restaurar un volumen o un Grupo de volúmenes

Puede utilizar instantáneas para revertir un volumen a un punto en el tiempo anterior si hay daños. Para revertir un volumen o un Grupo de volúmenes a un punto en el tiempo anterior, utilice la operación de restauración de volúmenes y proporcione una instantánea anterior a los daños. La operación de restauración es inmediata. También puede crear una instantánea de respaldo para guardar el estado del volumen o del Grupo de volúmenes antes de utilizar la operación de restauración.

Uso de clones delgados para probar un parche antes de aplicarlo al volumen de producción

Antes de instalar un parche o una actualización de software de una aplicación crucial en un volumen, puede tomar un clon delgado del volumen y, a continuación, aplicar a este la actualización. Después de instalar la actualización y verificar que sea segura para el entorno, puede instalarla en los otros volúmenes.

Crear clones delgados para uso de desarrollo

En lugar de aprovisionar volúmenes o Grupos de volúmenes para cada desarrollador individual, puede crear clones delgados. La creación de clones delgados del volumen o del Grupo de volúmenes permite distribuir los mismos datos y la misma configuración a cada desarrollador. Además, los clones delgados ocupan menos espacio que si hubiera creado un clon completo del volumen o aprovisionado volúmenes o Grupos de volúmenes individuales. También puede tomar instantáneas de los clones delgados y replicarlas.

Casos de uso de replicación

Puede utilizar la replicación para el tiempo de inactividad planificado, como durante una migración entre clústeres, la instalación de una actualización de software importante y la recuperación ante desastres.

Migración entre clústeres

Si necesita migrar un objeto de almacenamiento a otro clúster de PowerStore, puede configurar una replicación única entre los dos clústeres, seguida de una conmutación por error planificada al clúster nuevo para completar la migración. Después de la migración, desmantele el objeto de origen para recuperar espacio en el clúster original.

Uso de la replicación para el tiempo de inactividad previsto

El tiempo de inactividad previsto es una situación en la que el sistema de origen se desconecta con fines de mantenimiento o prueba mientras las operaciones se realizan en el sistema de destino. Antes del tiempo de inactividad previsto, tanto el origen como el destino se ejecutan con una sesión de replicación activa. No se producen pérdidas de datos en el tiempo de inactividad previsto.

En este escenario, el sistema de origen, Boston, se desconecta para realizar mantenimiento, y el sistema de destino, Nueva York, se usa como sistema de producción durante el período de mantenimiento. Tras el mantenimiento, la producción vuelve al sistema en Boston.

Para iniciar el tiempo de inactividad previsto, seleccione **Planned Failover** en el sistema de origen en Boston. El sistema de destino en Nueva York se sincroniza por completo con el origen para garantizar que no se produzca una pérdida de datos. La sesión permanece en pausa mientras el sistema de origen en Boston se vuelve de solo lectura y el destino, de lectura/escritura. El recurso de almacenamiento de destino de Nueva York puede proporcionar acceso al host. En el recurso de almacenamiento de destino en Nueva York, seleccione **Reprotect** para reanudar la replicación en la dirección inversa.

Para reanudar las operaciones en el sistema en Boston después del mantenimiento, seleccione **Planned Failover** en el sistema en Nueva York. Tras la conmutación por error, seleccione **Reprotect** en el sistema en Boston.

NOTA: Para replicar los datos del destino al origen con la operación Reprotect, asegúrese de que haya una política de replicación en el sistema de destino con una regla de replicación que indique el sistema de origen. Por ejemplo, si la sesión de replicación normal se produce de un sitio en Boston a un sitio en Nueva York, la política de replicación en el recurso de almacenamiento de destino en Nueva York debe indicar a Boston.

Uso de la replicación para la recuperación ante desastres

En este escenario de recuperación ante desastres, el sistema de origen, Boston, no está disponible debido a un desastre natural o provocado por el hombre. Se creó un sistema de destino, Nueva York, que contiene una copia completa o una réplica de los datos de producción. El acceso a los datos se puede restaurar mediante una conmutación por error de Nueva York, ya que se configuró una sesión de replicación entre los sistemas en Boston y en Nueva York.

El uso de réplicas para la recuperación ante desastres reduce al mínimo la posible pérdida de datos. La réplica se actualiza con la versión correspondiente a la última vez que el destino se sincronizó con el origen, según se especifica en la regla de replicación asociada. La cantidad de pérdida de datos potencial se basa en el ajuste del objetivo de punto de recuperación (RPO) de la regla de replicación asociada. Se puede realizar una conmutación por error de la sesión de replicación en el sistema de destino en Nueva York con los datos más recientes que se replicaron desde Boston.

Una vez que se realiza una conmutación por error de la sesión en el sistema en Nueva York, se convierte en lectura/escritura. Cuando se establece originalmente una sesión de replicación entre los sistemas de origen y destino, el recurso de almacenamiento recibe los permisos de acceso correctos al host y al recurso compartido. La creación del acceso de host correcto en el sistema de destino con anticipación reduce el tiempo de inactividad en caso de que se produzca un desastre.

Para reanudar las operaciones en el sistema en Boston, cuando esté disponible:

1. En el sistema en Nueva York, seleccione la opción **Reprotect**, que inicia la reanudación de la sesión de replicación en la dirección inversa.
2. Cuando los sistemas estén sincronizados, seleccione la opción **Planned Failover** en el sistema en Nueva York.
3. Seleccione la casilla de verificación para volver a proteger automáticamente el sistema tras una conmutación por error. O, una vez finalizada la conmutación por error, en el sistema en Boston, seleccione **Reprotect**.

NOTA: Para replicar los datos del destino al origen con la operación Reprotect, asegúrese de que haya una política de replicación en el sistema de destino con una regla de replicación que indique el sistema de origen. Por ejemplo, si la sesión de replicación se produce de

un sitio en Boston a un sitio en Nueva York, la política de replicación en el recurso de almacenamiento de destino en Nueva York debe indicar a Boston.

Casos de uso de protección de metro

Utilice la protección de metro para garantizar la alta disponibilidad, el balanceo de carga y la migración de los datos.

Uso de metro para alta disponibilidad

Un volumen metro se expone con el uso de dos arreglos de almacenamiento distintos que colaboran para exponer un único volumen metro a hosts de aplicaciones proporcionando la misma imagen y datos de SCSI. Los hosts y las aplicaciones que se ejecutan en ellos perciben dos volúmenes físicos como un único volumen con múltiples rutas. En consecuencia, los hosts pueden acceder a ambos lados del volumen metro. Si hay una pérdida de enlace o una falla de uno de los sistemas, es posible mantener el acceso de host al sistema activo.

La protección de metro proporciona replicación síncrona bidireccional, en la que ambos lados del volumen metro pueden utilizarse para producción. En lugar de recuperación ante desastres (mediante la conmutación por error de una sesión de replicación a un sistema remoto), metro permite evitar desastres proporcionando sincronización automática entre los sistemas sin tiempo de inactividad.

Uso de metro para el balanceo de carga

Con el volumen metro de PowerStore, los centros de datos se pueden optimizar para utilizar al máximo los sistemas PowerStore a través de un entorno activo-activo que permite el balanceo de cargas de trabajo entre sistemas PowerStore. La transferencia de aplicaciones de manera no disruptiva entre sistemas PowerStore es simple y se puede realizar cuando sea necesario balancear la capacidad o el rendimiento.

Uso de metro para la migración

Puede utilizar volúmenes de metro cuando es necesario migrar cargas de trabajo entre sistemas de PowerStore. El uso de volúmenes de metro para la migración es simple y reduce el riesgo de pérdida de datos. Con la opción de volumen de metro, la migración no es disruptiva. Una vez que finalice la migración, el volumen de metro se puede quitar o mantener para permitir una recuperación rápida cuando se produce una falla del sistema o incluso una falla del sitio completo.