Protección de datos y recuperación ante desastres

ONTAP 9

NetApp
April 24, 2024

Tabla de contenidos

Protección de datos y recuperación ante desastres

Protección de datos con System Manager

Información general sobre la protección de datos con System Manager

Los temas de esta sección muestran cómo configurar y gestionar la protección de datos con System Manager en ONTAP 9.7 y versiones posteriores.

Si utiliza System Manager en ONTAP 9.7 o una versión anterior, consulte "Documentación clásica de System Manager de ONTAP"

Proteja sus datos mediante la creación y la gestión de copias Snapshot, reflejos, almacenes y relaciones de mirroring y almacén.

SnapMirror es la tecnología de recuperación ante desastres diseñada para la conmutación al nodo de respaldo del almacenamiento principal al secundario en un sitio geográficamente remoto. Como su nombre indica, SnapMirror crea una réplica, o réplica, de sus datos de trabajo en almacenamiento secundario desde la cual puede seguir proporcionando datos en caso de catástrofe en el centro principal.

Un *vault* está diseñado para la replicación de copias snapshot disco a disco con el fin de cumplir con los estándares y otros fines relacionados con la gobernanza. A diferencia de la relación de SnapMirror, en la que el destino normalmente solo contiene las copias Snapshot que actualmente se encuentran en el volumen de origen, un destino de almacén normalmente conserva las copias Snapshot puntuales creadas durante un período mucho más largo.

A partir de ONTAP 9.10.1, se pueden crear relaciones de protección de datos entre bloques de S3 mediante SnapMirror S3. Los bloques de destino pueden estar en sistemas ONTAP locales o remotos, o en sistemas que no sean ONTAP, como StorageGRID y AWS. Para obtener más información, consulte "Información general de SnapMirror de S3".

Cree políticas de protección de datos personalizadas

Puede crear políticas de protección de datos personalizadas con System Manager cuando las políticas de protección existentes no son apropiadas para sus necesidades. A partir de ONTAP 9.11.1, puede usar System Manager para crear políticas de mirroring y almacén personalizadas para mostrar y seleccionar políticas heredadas. Esta función también está disponible en ONTAP 9.8P12 y en parches posteriores de ONTAP 9.8.

Cree políticas de protección personalizadas en los clústeres de origen y destino.

Pasos

1. Haga clic en **Protección > Configuración de directiva local**.
2. En **Directivas de protección**, haga clic en →.
3. En el panel **Directivas de protección**, haga clic en + Add .
4. Escriba el nombre de la nueva política y seleccione el alcance de la misma.
5. Elija un tipo de política. Para agregar una directiva sólo de almacén o sólo de duplicación, seleccione

asíncrona y haga clic en **utilizar un tipo de directiva heredada**.

6. Complete los campos obligatorios.
7. Haga clic en **Guardar**.
8. Repita estos pasos en el otro clúster.

Configure las copias Snapshot

Puede crear políticas de copia de Snapshot para especificar el número máximo de copias de Snapshot que se crean automáticamente y la frecuencia con la que se crean. La política especifica cuándo crear copias Snapshot, cuántas copias se retendrán y cómo nombrarlas.

Este procedimiento crea una política de copias de Snapshot únicamente en el clúster local.

Pasos

1. Haga clic en **Protección > Descripción general > Configuración de directivas locales**.
2. En **Directivas de instantánea**, haga clic en →y, a continuación, haga clic en + Add .
3. Escriba el nombre de la directiva, seleccione el ámbito de la directiva y, en **programaciones**, haga clic en + Add para introducir los detalles de la programación.

Calcule el espacio que se puede reclamar antes de eliminar las copias snapshot

A partir de ONTAP 9.10.1, puede usar System Manager para seleccionar las copias de Snapshot que desea eliminar y calcular el espacio que puede reclamarse antes de eliminarlas.

Pasos

1. Haga clic en **almacenamiento > volúmenes**.
2. Seleccione el volumen desde el que desea eliminar copias de Snapshot.
3. Haga clic en **copias Snapshot**.
4. Seleccione una o más copias de Snapshot.
5. Haga clic en **calcular espacio recuperable**.

Habilitar o deshabilitar el acceso de los clientes al directorio de copia Snapshot

A partir de ONTAP 9.10.1, se puede usar System Manager para habilitar o deshabilitar los sistemas cliente para acceder a un directorio de copia de Snapshot en un volumen. Al habilitar el acceso, el directorio de copia Snapshot resulta visible para los clientes y permite que los clientes de Windows asignen una unidad al directorio de copias Snapshot para ver y acceder a su contenido.

Puede habilitar o deshabilitar el acceso al directorio de copias Snapshot de un volumen mediante la edición de la configuración del volumen o la edición de la configuración de recursos compartidos del volumen.

Habilitar o deshabilitar el acceso de los clientes al directorio de copia de Snapshot mediante la edición de un volumen

De forma predeterminada, los clientes pueden acceder al directorio de copia Snapshot de un volumen.

Pasos

1. Haga clic en **almacenamiento > volúmenes**.
2. Seleccione el volumen que contiene el directorio copias de Snapshot que desea mostrar u ocultar.
3. Haga clic en ⋮ Y seleccione **Editar**.
4. En la sección **Configuración de copias Snapshot (local)**, seleccione o anule la selección de **Mostrar el directorio de copias Snapshot a clientes**.
5. Haga clic en **Guardar**.

Habilitar o deshabilitar el acceso de los clientes al directorio de copia de Snapshot mediante la edición de un recurso compartido

De forma predeterminada, los clientes pueden acceder al directorio de copia Snapshot de un volumen.

Pasos

1. Haga clic en **almacenamiento > Recursos compartidos**.
2. Seleccione el volumen que contiene el directorio copias de Snapshot que desea mostrar u ocultar.
3. Haga clic en ⋮ Y seleccione **Editar**.
4. En la sección **Propiedades de recurso compartido**, seleccione o anule la selección de **permitir a los clientes acceder al directorio copias Snapshot**.
5. Haga clic en **Guardar**.

Prepare el mirroring y el almacenamiento

Puede proteger los datos replicando en un clúster remoto con fines de recuperación ante desastres y backup de datos.

Existen varias políticas de protección predeterminadas disponibles. Debe haber creado las políticas de protección si desea usar políticas personalizadas.

Pasos

1. En el clúster local, haga clic en **Protección > Descripción general**.
2. Expanda **Configuración de interconexión de clústeres**. Haga clic en **Add Network interfaces** y añada interfaces de red de interconexión de clústeres para el clúster.

   Repita este paso en el clúster remoto.

3. En el clúster remoto, haga clic en **Protección > Descripción general**. Haga clic en ⋮ En la sección Cluster peers y haga clic en **Generate Passphrase**.
4. Copie la clave de acceso generada y péguela en el clúster local.
5. En el clúster local, en Cluster peers, haga clic en **Peer Clusters** y pare los clústeres locales y remotos.
6. De manera opcional, en Storage VM peers, haga clic en ⋮ Posteriormente **Peer Storage VMs** para poner en la misma conexión los equipos virtuales de almacenamiento.
7. Haga clic en **proteger volúmenes** para proteger sus volúmenes. Para proteger sus LUN, haga clic en **almacenamiento > LUN**, seleccione una LUN que proteger y, a continuación, haga clic en Protect.

   Seleccione la política de protección según el tipo de protección de datos que necesite.

8. Para comprobar que los volúmenes y LUN están protegidos correctamente desde el clúster local, haga clic en **almacenamiento > volúmenes** o **almacenamiento > LUN** y expanda la vista volumen/LUN.

Otras maneras de hacerlo en ONTAP

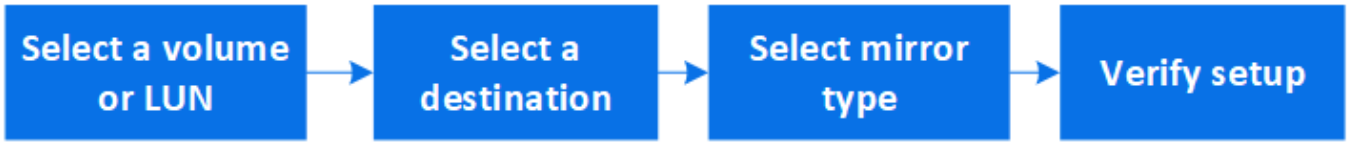
Para ejecutar estas tareas con…	Ver este contenido…
System Manager Classic (disponible con ONTAP 9.7 y versiones anteriores)	"Información general de preparación para la recuperación ante desastres de volúmenes"
La interfaz de línea de comandos de ONTAP	"Cree una relación de paridad entre clústeres"

Configure los reflejos y almacenes

Cree un mirror y almacén de un volumen para proteger los datos en caso de desastre y disponer de varias versiones archivadas de los datos a las que se puede revertir. A partir de ONTAP 9.11.1, se puede usar System Manager para seleccionar políticas de mirroring y almacén predefinidas y personalizadas, para mostrar y seleccionar políticas heredadas, y para anular las programaciones de transferencia definidas en una política de protección al proteger volúmenes y máquinas virtuales de almacenamiento. Esta función también está disponible en ONTAP 9.8P12 y en parches posteriores de ONTAP 9.8.

> Si utiliza la versión de revisión de ONTAP 9.8P12 o posterior de ONTAP 9.8 y configuró SnapMirror con System Manager, debe utilizar ONTAP 9.9.1P13 o posterior y ONTAP 9.10.1P10 o versiones de revisión posteriores si tiene pensado actualizar a las versiones de ONTAP 9.9.1 o ONTAP 9.10.1.

Este procedimiento crea una política de protección de datos en un clúster remoto. Los clústeres de origen y destino utilizan interfaces de red de interconexión de clústeres para intercambiar datos. En el procedimiento se asume el "se crean interfaces de red de interconexión de clústeres y los clústeres que contienen los volúmenes tienen una relación entre iguales" (emparejado). También es posible establecer una relación entre iguales de máquinas virtuales de almacenamiento para la protección de datos; sin embargo, si las máquinas virtuales de almacenamiento no tienen una relación entre iguales, pero los permisos están habilitados, las máquinas virtuales de almacenamiento se establecen una relación entre iguales automáticamente cuando se crea la relación de protección.



Pasos

1. Seleccione el volumen o LUN que desea proteger: Haga clic en **almacenamiento > volúmenes** o **almacenamiento > LUN** y, a continuación, haga clic en el volumen o nombre de LUN que desee.
2. Haga clic en Protect.
3. Seleccione el clúster de destino y la máquina virtual de almacenamiento.
4. De forma predeterminada, la política asíncrona está seleccionada. Para seleccionar una directiva síncrona, haga clic en **más opciones**.
5. Haga clic en **proteger**.
6. Haga clic en la ficha **SnapMirror (local o remoto)** del volumen o LUN seleccionados para verificar que la protección está configurada correctamente.

Información relacionada

- "Crear y eliminar volúmenes de prueba de conmutación al nodo de respaldo de SnapMirror".

Otras maneras de hacerlo en ONTAP

Para ejecutar estas tareas con…	Ver este contenido…
System Manager Classic (disponible con ONTAP 9.7 y versiones anteriores)	"Información general sobre backup de volúmenes mediante SnapVault"
La interfaz de línea de comandos de ONTAP	"Cree una relación de replicación"

Resincronice una relación de protección

Cuando el volumen de origen original vuelva a estar disponible después de un desastre, puede volver a sincronizar los datos del volumen de destino y restablecer la relación de protección.

Este procedimiento reemplaza los datos del volumen de origen original en una relación asíncrona para poder empezar a proporcionar datos del volumen de origen original de nuevo y reanudar la relación de protección original.

Pasos

1. Haga clic en **Protección > Relaciones** y, a continuación, haga clic en la relación de desconexión que desea volver a sincronizar.
2. Haga clic en ⋮ Y, a continuación, seleccione **Resync**.
3. En **Relaciones**, supervise el progreso de la resincronización comprobando el estado de la relación. El estado cambia a "reflejado" cuando se completa la resincronización.

Restaurar un volumen de una copia de Snapshot anterior

Si se pierden o se dañan datos de un volumen, es posible revertir los datos mediante la restauración a partir de una copia de Snapshot anterior.

Este procedimiento reemplaza los datos actuales del volumen de origen con datos de una versión de copia Snapshot anterior. Debe realizar esta tarea en el clúster de destino.

Pasos

1. Haga clic en **Protección > Relaciones** y, a continuación, haga clic en el nombre del volumen de origen.
2. Haga clic en ⋮ Y, a continuación, seleccione **Restaurar**.
3. En **Fuente**, el volumen de origen está seleccionado de forma predeterminada. Haga clic en **otro volumen** si desea elegir un volumen distinto al de origen.
4. En **destino**, elija la copia Snapshot que desea restaurar.
5. Si su origen y destino se encuentran en diferentes clústeres, en el clúster remoto, haga clic en **Protección > Relaciones** para supervisar el progreso de la restauración.

Otras maneras de hacerlo en ONTAP

Para ejecutar estas tareas con…	Ver este contenido…
System Manager Classic (disponible con ONTAP 9.7 y versiones anteriores)	"Información general sobre la restauración de volúmenes mediante SnapVault"
La interfaz de línea de comandos de ONTAP	"Restaure el contenido de un volumen a partir de un destino de SnapMirror"

Recuperar desde copias Snapshot

Es posible recuperar un volumen a un momento específico anterior mediante la restauración desde una copia Snapshot.

Este procedimiento restaura un volumen a partir de una copia Snapshot.

Pasos

1. Haga clic en **almacenamiento** y seleccione un volumen.
2. En **copias Snapshot**, haga clic en ⋮ Junto a la copia Snapshot que desea restaurar y seleccione **Restaurar**.

Restaurar en un nuevo volumen

A partir de ONTAP 9.8, se puede usar System Manager para restaurar los datos de los que se ha realizado un backup en el volumen de destino a un volumen distinto al de origen.

Cuando se restaura a otro volumen, es posible seleccionar un volumen existente o crear un volumen nuevo.

Pasos

1. Seleccione la relación de protección deseada: Haga clic en **Protección > Relaciones**.
2. Haga clic en ⋮ Y haga clic en **Restaurar**.
3. En la sección **Fuente**, seleccione **otro volumen** y seleccione el clúster y Storage VM.
4. Seleccione **volumen existente** o **Crear un nuevo volumen**.
5. Si va a crear un volumen nuevo, introduzca el nombre del volumen.

6. En la sección **destino**, seleccione la copia Snapshot que desea restaurar.
7. Haga clic en **Guardar**.
8. En **Relaciones**, supervise el progreso de la restauración visualizando **Estado de transferencia** para la relación.

Resincronización inversa de una relación de protección

A partir de ONTAP 9.8, es posible usar System Manager para realizar una operación de resincronización inversa a fin de eliminar una relación de protección existente y revertir las funciones de los volúmenes de origen y de destino. A continuación, se utilizará el volumen de destino para suministrar datos mientras se repara o se sustituye el origen, se actualiza el origen y se establece la configuración original de los sistemas.

> System Manager no admite la resincronización inversa con relaciones dentro del clúster. Puede usar la CLI de ONTAP para realizar operaciones de resincronización inversa con relaciones entre clústeres.

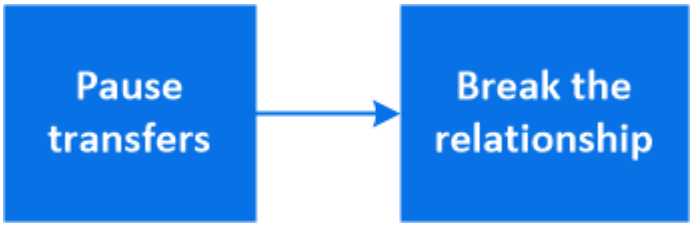
Cuando se realiza una operación de resynch inversa, se eliminan todos los datos del volumen de origen más recientes que los datos de la copia Snapshot común.

Pasos

1. Seleccione la relación de protección deseada: Haga clic en **Protección > Relaciones**.
2. Haga clic en ⋮ Y haga clic en **Reverse Resync**.
3. En **Relaciones**, supervise el progreso de la resincronización inversa visualizando **Estado de transferencia** para la relación.

Sirva datos desde un destino de SnapMirror

Para servir datos desde un destino de mirroring cuando un origen deja de estar disponible, detenga las transferencias programadas hacia el destino y, a continuación, rompa la relación de SnapMirror para hacer que el destino sea editable.



Pasos

1. Seleccione la relación de protección deseada: Haga clic en **Protección > Relaciones** y, a continuación, haga clic en el nombre de volumen deseado.
2. Haga clic en ⋮.
3. Detener transferencias programadas : haga clic en **Pausa**.
4. Haga que el destino sea editable: Haga clic en **romper**.
5. Vaya a la página principal **Relaciones** para verificar que el estado de la relación se muestra como "roto".

Siguientes pasos:

Cuando el volumen de origen deshabilitado se vuelve a disponibilidad, debe volver a sincronizar la relación para copiar los datos actuales en el volumen de origen original. Este proceso sustituye los datos del volumen de origen original.

Otras maneras de hacerlo en ONTAP

Para ejecutar estas tareas con…	Ver este contenido…
System Manager Classic (disponible con ONTAP 9.7 y versiones anteriores)	"Información general sobre la recuperación ante desastres de volúmenes"
La interfaz de línea de comandos de ONTAP	"Activar el volumen de destino"

Configurar la recuperación ante desastres de los equipos virtuales de almacenamiento

Mediante System Manager, es posible crear una relación de recuperación ante desastres (DR de VM de almacenamiento) para replicar una configuración de VM de almacenamiento a otra. En caso de desastre en el sitio principal, puede activar rápidamente la máquina virtual de almacenamiento de destino.

Complete este procedimiento desde el destino. Si necesita crear una nueva política de protección, por ejemplo, cuando su máquina virtual de almacenamiento de origen tiene SMB configurado, debe usar System Manager para crear la política y seleccionar la opción **Identity preserve** en la ventana **Add Protection Policy**.
Para obtener más información, consulte "Cree políticas de protección de datos personalizadas".

Pasos

1. En el clúster de destino, haga clic en **Protección > Relaciones**.
2. En **Relaciones**, haga clic en proteger y elija **Storage VMs (DR)**.
3. Seleccione una política de protección. Si creó una política de protección personalizada, selecciónela, elija el clúster de origen y la máquina virtual de almacenamiento que desea replicar. También puede crear una máquina virtual de almacenamiento de destino introduciendo un nuevo nombre de máquina virtual de almacenamiento.
4. Haga clic en **Guardar**.

Proporcione datos desde un destino de recuperación ante desastres de SVM

A partir de ONTAP 9.8, es posible utilizar System Manager para activar una máquina virtual de almacenamiento de destino después de un desastre. Si activa la máquina virtual de almacenamiento de destino, es posible escribir en los volúmenes de destino de SVM y proporcionar datos a los clientes.

Pasos

1. Si se puede acceder al clúster de origen, compruebe que la SVM está detenida: Vaya a **almacenamiento > Storage VMs** y compruebe la columna **Estado** de la SVM.
2. Si el estado de la SVM de origen es "en ejecución", deténgase: Seleccione ⋮ Y seleccione **Detener**.
3. En el clúster de destino, localice la relación de protección deseada: Vaya a **Protección > Relaciones**.

4. Haga clic en ⋮ Y seleccione **Activar destino almacenamiento VM**.

Reactivar una máquina virtual de almacenamiento de origen

A partir de ONTAP 9.8, podrá utilizar System Manager para reactivar un equipo virtual de almacenamiento de origen después de un desastre. Volver a activar la máquina virtual de almacenamiento de origen detiene la máquina virtual de almacenamiento de destino y vuelve a habilitar la replicación desde el origen al destino.

Acerca de esta tarea

Cuando se reactiva la máquina virtual de almacenamiento de origen, System Manager realiza las siguientes operaciones en segundo plano:

- Crea una relación de recuperación ante desastres de SVM inversa del destino original al origen con una resincronización de SnapMirror
- Detiene la SVM de destino
- Actualiza la relación de SnapMirror
- Rompe la relación de SnapMirror
- Reinicia la SVM original
- El problema realiza una resincronización de SnapMirror del origen original del destino original
- Borra las relaciones de SnapMirror

Pasos

1. Seleccione la relación de protección deseada: Haga clic en **Protección > Relaciones**.
2. Haga clic en ⋮ Y haga clic en **reactivar almacenamiento de origen VM**.
3. En **Relaciones**, supervise el progreso de reactivación de la fuente visualizando **Estado de transferencia** para obtener información sobre la relación de protección.

Resincronizar una máquina virtual de almacenamiento de destino

A partir de ONTAP 9.8, es posible usar System Manager para volver a sincronizar los datos y los detalles de configuración de la máquina virtual de almacenamiento de origen con la máquina virtual de almacenamiento de destino en una relación de protección romada y restablecer la relación.

ONTAP 9.11.1 introduce una opción para omitir una reconstrucción completa del almacén de datos al realizar un ensayo de recuperación ante desastres, lo que permite volver a la producción más rápido.

La operación de resincronización solo se realiza desde el destino de la relación original. La resincronización elimina los datos del equipo virtual de almacenamiento de destino que son más nuevos que los de la máquina virtual de almacenamiento de origen.

Pasos

1. Seleccione la relación de protección deseada: Haga clic en **Protección > Relaciones**.
2. Opcionalmente, seleccione **realizar una resincronización rápida** para omitir una reconstrucción completa del almacén de datos durante un ensayo de recuperación ante desastres.
3. Haga clic en ⋮ Y haga clic en **Resync**.

4. En **Relaciones**, supervise el progreso de la resincronización visualizando **Estado de transferencia** para la relación.

Realice backups de datos en el cloud con SnapMirror

A partir de ONTAP 9.9.1, puede realizar backups de sus datos en el cloud y restaurar sus datos desde el almacenamiento en cloud a un volumen diferente mediante System Manager. Es posible usar StorageGRID o ONTAP S3 como almacén de objetos en el cloud.

Antes de usar la función SnapMirror Cloud, debe solicitar una clave de licencia de API de SnapMirror Cloud al sitio de soporte de NetApp: "Solicite la clave de licencia de SnapMirror Cloud API".
Siguiendo las instrucciones, debe proporcionar una descripción simple de su oportunidad de negocio y solicitar la clave API mediante el envío de un correo electrónico a la dirección de correo electrónico proporcionada. Debe recibir una respuesta por correo electrónico en un plazo de 24 horas con instrucciones adicionales sobre cómo adquirir la clave API.

Añadir un almacén de objetos en la nube

Antes de configurar backups en el cloud de SnapMirror, tiene que añadir un almacén de objetos en el cloud StorageGRID o ONTAP S3.

Pasos

1. Haga clic en **Protección > Descripción general > Tiendas de objetos en la nube**.
2. Haga clic en + Add .

Realice un backup con la política predeterminada

Puede configurar rápidamente un backup de SnapMirror Cloud para un volumen existente usando la política de protección de cloud predeterminada, DailyBackup.

Pasos

1. Haga clic en **Protección > Descripción general** y seleccione **copia de seguridad de volúmenes en la nube**.
2. Si es la primera vez que realiza un backup en el cloud, introduzca su clave de licencia de API de SnapMirror Cloud en el campo de licencia, como se indica.
3. Haga clic en **autenticar y continuar**.
4. Seleccione un volumen de origen.
5. Seleccione un almacén de objetos en la nube.
6. Haga clic en **Guardar**.

Cree una política de backup en el cloud personalizada

Si no quiere usar la política de cloud DailyBackup predeterminada para sus backups de SnapMirror Cloud, puede crear su propia política.

Pasos

1. Haga clic en **Protección > Descripción general > Configuración de directivas locales** y seleccione **Directivas de protección**.

2. Haga clic en **Agregar** e introduzca los nuevos detalles de la directiva.
3. En la sección **Tipo de directiva**, seleccione **copia de seguridad en la nube** para indicar que está creando una política de nube.
4. Haga clic en **Guardar**.

Cree una copia de seguridad desde la página Volumes

Puede usar la página System Manager **Volumes** a cuando desea seleccionar y crear backups en la nube para varios volúmenes a la vez, o bien cuando desea usar una política de protección personalizada.

Pasos

1. Haga clic en **almacenamiento > volúmenes**.
2. Seleccione los volúmenes de los que desea realizar una copia de seguridad en la nube y haga clic en **proteger**.
3. En la ventana **proteger volumen**, haga clic en **más opciones**.
4. Seleccionar una política.

   Puede seleccionar la política predeterminada, DailyBackup o una política de cloud personalizada que haya creado.

5. Seleccione un almacén de objetos en la nube.
6. Haga clic en **Guardar**.

Restaure desde el cloud

Puede usar System Manager para restaurar datos con backups del almacenamiento de cloud a otro volumen en el clúster de origen.

Pasos

1. Haga clic en **almacenamiento > volúmenes**.
2. Seleccione la ficha **copia de seguridad en la nube**.
3. Haga clic en ⋮ Junto al volumen de origen que desea restaurar y seleccione **Restaurar**.
4. En **Source**, seleccione una VM de almacenamiento y, a continuación, escriba el nombre del volumen en el que desea restaurar los datos.
5. En **destino**, seleccione la copia Snapshot que desea restaurar.
6. Haga clic en **Guardar**.

Eliminar una relación de SnapMirror Cloud

Puede usar System Manager para eliminar una relación de cloud.

Pasos

1. Haga clic en **almacenamiento > volúmenes** y seleccione el volumen que desea eliminar.
2. Haga clic en ⋮ Junto al volumen de origen y seleccione **Eliminar**.
3. Seleccione **Eliminar el extremo del almacén de objetos en la nube (opcional)** si desea eliminar el extremo del almacén de objetos en la nube.
4. Haga clic en **Eliminar**.

Quitar un almacén de objetos en la nube

Puede usar System Manager para quitar un almacén de objetos en cloud si no forma parte de una relación de backup en el cloud. Cuando un almacén de objetos en cloud forma parte de una relación de backup en el cloud, no se puede eliminar.

Pasos

1. Haga clic en **Protección > Descripción general > Tiendas de objetos en la nube**.
2. Seleccione el almacén de objetos que desea eliminar; haga clic en ⋮ Y seleccione **Eliminar**.

Realice backups de datos con Cloud Backup

A partir de ONTAP 9.9.1, se puede usar System Manager para realizar backups de datos en el cloud con Cloud Backup.

> Cloud Backup admite volúmenes de lectura y escritura de FlexVol y volúmenes de protección de datos (DP). No se admiten los volúmenes de FlexGroup y SnapLock.

Antes de empezar

Debe realizar los siguientes procedimientos para establecer una cuenta en BlueXP. Para la cuenta de servicio, debe crear la función como "Administrador de cuentas". (Otros roles de cuenta de servicio no tienen los privilegios necesarios para establecer una conexión desde System Manager).

1. "Cree una cuenta en BlueXP".
2. "Cree un conector en BlueXP" con uno de los siguientes proveedores de cloud:
   - Microsoft Azure
   - Amazon Web Services (AWS)
   - Google Cloud Platform (GCP)
   - StorageGRID (ONTAP 9.10.1)

   > A partir de ONTAP 9.10.1, puede seleccionar StorageGRID como proveedor de backup en cloud, pero solo si BlueXP está implementado en las instalaciones. El conector BlueXP debe instalarse en las instalaciones y estar disponible a través de la aplicación de software como servicio (SaaS) BlueXP.

3. "Suscríbase a Cloud Backup Service en BlueXP" (requiere la licencia adecuada).
4. "Genere una clave de acceso y una clave secreta con BlueXP".

Registre el clúster con BlueXP

Puede registrar el clúster en BlueXP usando BlueXP o System Manager.

Pasos

1. En System Manager, vaya a **Descripción general de la protección**.
2. En **Cloud Backup Service**, proporcione los siguientes detalles:
   - ID del cliente
   - Clave secreta de cliente

3. Seleccione **Registrar y continuar**.

Habilite Cloud Backup

Después de registrar el clúster en BlueXP, necesitará habilitar Cloud Backup e iniciar el primer backup en el cloud.

Pasos

1. En el Administrador del sistema, haga clic en **Protección > Descripción general** y, a continuación, desplácese a la sección **Cloud Backup Service**.
2. Introduzca **ID de cliente** y **Secreto de cliente**.

> A partir de ONTAP 9.10.1, puede obtener más información sobre el coste de utilizar la nube haciendo clic en **más información sobre el costo de usar la nube**.

3. Haga clic en **conectar y activar Cloud Backup Service**.
4. En la página **Activar Cloud Backup Service**, proporcione los siguientes detalles, en función del proveedor que haya seleccionado.

Para este proveedor de cloud…	Introduzca los siguientes datos…
Azure	• ID de suscripción de Azure • Región • Nombre del grupo de recursos (existente o nuevo)
AWS	• ID de cuenta de AWS • Clave de acceso • Clave secreta • Región
Google Cloud Project (GCP)	• Nombre del proyecto de Google Cloud • Clave de acceso a Google Cloud • Clave secreta de Google Cloud • Región
StorageGRID (ONTAP 9.10.1 y versiones posteriores y solo para la implementación on-premises de BlueXP)	• Servidor • Clave de acceso de SG • Clave secreta de SG

5. Seleccione una **Política de protección**:
   - **Política existente**: Elija una política existente.
   - **Nueva directiva**: Especifique un nombre y configure un programa de transferencia.

> A partir de ONTAP 9.10.1, es posible especificar si desea habilitar el archivado con Azure o AWS.

> Si habilita el archivado para un volumen con Azure o AWS, no podrá deshabilitar el archivado.

Si habilita el archivado para Azure o AWS, especifique lo siguiente:

- El número de días después de los cuales se archiva el volumen.
- La cantidad de backups que se retendrán en el archivo. Especifique “0” (cero) para archivar hasta la última copia de seguridad.
- Para AWS, seleccione la clase de almacenamiento de archivado.

6. Seleccione los volúmenes de los que desea realizar el backup.
7. Seleccione **Guardar**.

Edite la política de protección usada para Cloud Backup

Puede cambiar la política de protección que se usa con Cloud Backup.

Pasos

1. En el Administrador del sistema, haga clic en **Protección > Descripción general** y, a continuación, desplácese a la sección **Cloud Backup Service**.
2. Haga clic en ⋮, Luego **Editar**.
3. Seleccione una **Política de protección**:
   - **Política existente**: Elija una política existente.
   - **Nueva directiva**: Especifique un nombre y configure un programa de transferencia.

> A partir de ONTAP 9.10.1, es posible especificar si desea habilitar el archivado con Azure o AWS.

> Si habilita el archivado para un volumen con Azure o AWS, no podrá deshabilitar el archivado.

Si habilita el archivado para Azure o AWS, especifique lo siguiente:

- El número de días después de los cuales se archiva el volumen.
- La cantidad de backups que se retendrán en el archivo. Especifique “0” (cero) para archivar hasta la última copia de seguridad.
- Para AWS, seleccione la clase de almacenamiento de archivado.

4. Seleccione **Guardar**.

Proteja nuevos volúmenes o LUN en el cloud

Cuando se crea un volumen o LUN nuevo, puede establecer una relación de protección de SnapMirror que permita realizar backups en el cloud del volumen o LUN.

Antes de empezar

- Debe tener una licencia de SnapMirror.
- Deben configurarse las LIF de interconexión de clústeres.
- NTP debe configurarse.
- El clúster debe ejecutar ONTAP 9.9.1.

Acerca de esta tarea

No puede proteger volúmenes o LUN nuevos en el cloud para las siguientes configuraciones de clúster:

- El clúster no puede estar en un entorno de MetroCluster.
- No se admite SVM-DR.
- No se pueden realizar backups de FlexGroups con Cloud Backup.

Pasos

1. Al aprovisionar un volumen o LUN, en la página **Protección** del Administrador del sistema, seleccione la casilla de verificación con la etiqueta **Activar SnapMirror (local o remoto)**.
2. Seleccione el tipo de política Cloud Backup.
3. Si la copia de seguridad en la nube no está activada, seleccione **Activar Cloud Backup Service**.

Proteja los volúmenes o LUN existentes en el cloud

Puede establecer una relación de protección de SnapMirror para volúmenes y LUN existentes.

Pasos

1. Seleccione un volumen o LUN existente y haga clic en **proteger**.
2. En la página **Protect Volumes**, especifique **copia de seguridad utilizando Cloud Backup Service** para la directiva de protección.
3. Haga clic en **proteger**.
4. En la página **Protección**, seleccione la casilla de verificación **Activar SnapMirror (local o remoto)**.
5. Seleccione **Activar Cloud Backup Service**.

Restaurar datos de archivos de copia de seguridad

Puede realizar operaciones de administración de copias de seguridad, como restaurar datos, actualizar relaciones y eliminar relaciones, sólo cuando utilice la interfaz BlueXP. Consulte "Restaurar datos a partir de archivos de copia de seguridad" si quiere más información.

Relaciones entre iguales de clústeres y SVM con la CLI

Información general sobre relaciones entre iguales de clústeres y SVM con la CLI

Puede crear una relación entre iguales de clústeres de origen y de destino, y entre máquinas virtuales de almacenamiento (SVM) de origen y de destino. Debe crear relaciones entre iguales entre estas entidades antes de poder replicar copias de Snapshot con SnapMirror.

ONTAP 9.3 ofrece mejoras que simplifican la forma de configurar relaciones entre iguales entre clústeres y SVM. Los procedimientos de paridad de clústeres y SVM están disponibles para todas las versiones de

ONTAP 9. Debe utilizar el procedimiento adecuado para su versión de ONTAP.

Los procedimientos se realizan mediante la interfaz de línea de comandos (CLI), no con System Manager ni con una herramienta de secuencias de comandos automatizadas.

Prepare la relación entre iguales de clústeres y SVM

Conceptos básicos de peering

Debe crear *peer Relationships* entre los clústeres de origen y de destino, y entre las SVM de origen y de destino antes de poder replicar copias de Snapshot con SnapMirror. Una relación de paridad define las conexiones de red que permiten que clústeres y SVM intercambien datos de forma segura.

Los clústeres y las SVM en relaciones entre iguales se comunican a través de la red de interconexión de clústeres mediante las interfaces lógicas de interconexión de clústeres (LIF)._ una LIF de interconexión de clústeres es una LIF compatible con el servicio de interfaz de red «núcleo entre clústeres» y normalmente se crea mediante la política de servicio de interfaz de red de «interconexión de clústeres predeterminada». Debe crear LIF de interconexión de clústeres en cada nodo en los clústeres que se van a establecer una relación entre iguales.

Las LIF de interconexión de clústeres utilizan las rutas que pertenecen a la SVM del sistema a la que se han asignado. ONTAP crea automáticamente una SVM del sistema para las comunicaciones a nivel de clúster dentro de un espacio IP.

Se admiten topologías en cascada y distribución ramificada. En una topología en cascada, solo necesita crear redes de interconexión de clústeres entre los clústeres principal y secundario, y entre los clústeres secundario y terciario. No es necesario crear una red de interconexión de clústeres entre el clúster principal y el terciario.

> Es posible (pero no aconsejable) que un administrador elimine el servicio interclúster-core de la directiva de servicio de interconexión de clústeres predeterminada. Si esto sucede, las LIF creadas con «interconexión de clústeres predeterminada» no serán realmente LIF de interconexión de clústeres. Para confirmar que la política de servicio de interconexión de clústeres predeterminada contiene el servicio principal entre clústeres, utilice el siguiente comando:
>
> ```
> network interface service-policy show -policy default-intercluster
> ```

Requisitos previos para la relación de clústeres entre iguales

Antes de configurar cluster peering, debe confirmar que la conectividad, el puerto, la dirección IP, subred, firewall, y se cumplen los requisitos de nomenclatura de los clústeres.

> A partir de ONTAP 9,6, el cifrado de pares de clústeres proporciona compatibilidad de cifrado TLS 1,2 AES-256 GCM para la replicación de datos de forma predeterminada. Los cifrados de seguridad predeterminados («PSK-AES256-GCM-SHA384») son necesarios para que el emparejamiento de clústeres funcione incluso si el cifrado está desactivado.
>
> A partir de ONTAP 9.11.1, los cifrados de seguridad DHE-PSK están disponibles por defecto.

Requisitos de conectividad

Todas las LIF de interconexión de clústeres del clúster local deben poder comunicarse con todas las LIF de interconexión de clústeres del clúster remoto.

Aunque no es necesario, generalmente es más fácil configurar las direcciones IP que se usan para las LIF de interconexión de clústeres de la misma subred. Las direcciones IP pueden residir en la misma subred que las LIF de datos, o en una subred diferente. La subred que se utiliza en cada clúster debe cumplir los siguientes requisitos:

- La subred debe pertenecer al dominio de retransmisión que contenga los puertos que se utilizan para la comunicación entre clústeres.
- La subred debe tener suficientes direcciones IP disponibles para asignar a una LIF de interconexión de clústeres por nodo.

  Por ejemplo, en un clúster de cuatro nodos, la subred que se usa para la comunicación entre clústeres debe tener cuatro direcciones IP disponibles.

Cada nodo debe tener una LIF de interconexión de clústeres con una dirección IP en la red de interconexión de clústeres.

Las LIF entre clústeres pueden tener una dirección IPv4 o IPv6.

> ONTAP le permite migrar sus redes entre iguales de IPv4 a IPv6 si, de manera opcional, permite que ambos protocolos estén presentes simultáneamente en las LIF de interconexión de clústeres. En las versiones anteriores, todas las relaciones de interconexión de clústeres de todo un clúster eran IPv4 o IPv6. Esto significaba que el cambio de protocolos era un evento que podía provocar interrupciones.

Requisitos de puertos

Se pueden usar puertos dedicados para la comunicación entre clústeres o para compartir puertos que usa la red de datos. Los puertos deben cumplir con los siguientes requisitos:

- Todos los puertos que se utilizan para comunicarse con un clúster remoto determinado deben estar en el mismo espacio IP.

  Se pueden utilizar varios espacios IP para establecer la misma relación entre iguales con varios clústeres. La conectividad de malla completa en par sólo se requiere dentro de un espacio IP.

- El dominio de retransmisión que se usa para la comunicación entre clústeres debe incluir al menos dos puertos por nodo para que la comunicación entre clústeres pueda conmutar por error de un puerto a otro.

  Los puertos que se añaden a un dominio de retransmisión pueden ser puertos de red físicos, VLAN o grupos de interfaces (ifgrps).

- Todos los puertos deben estar cableadas.
- Todos los puertos deben estar en buen estado.
- La configuración de MTU de los puertos debe ser coherente.

Requisitos del firewall

> A partir de ONTAP 9.10.1, las políticas de firewall están obsoletas y sustituidas por completo por políticas de servicios LIF. Para obtener más información, consulte "Configurar políticas de firewall para LIF".

Los firewalls y la política de firewall de interconexión de clústeres deben permitir los siguientes protocolos:

- Tráfico ICMP bidireccional
- Tráfico TCP iniciado bidireccional hacia las direcciones IP de todas las LIF de interconexión de clústeres a través de los puertos 11104 y 11105
- HTTPS bidireccional entre las LIF de interconexión de clústeres

  Aunque HTTPS no es necesario cuando se configura una relación de clústeres entre iguales con la CLI, se requiere HTTPS más adelante si se utiliza System Manager para configurar la protección de datos.

El valor predeterminado `intercluster` La directiva de firewall permite el acceso a través del protocolo HTTPS y desde todas las direcciones IP (0.0.0.0/0). Puede modificar o reemplazar la política si es necesario.

Requisitos del clúster

Los clústeres deben cumplir los siguientes requisitos:

- No puede haber un clúster en una relación de paridad con más de 255 clústeres.

Utilice puertos compartidos o dedicados

Se pueden usar puertos dedicados para la comunicación entre clústeres o para compartir puertos que usa la red de datos. Para decidir si se comparten puertos, debe tener en cuenta el ancho de banda de la red, el intervalo de replicación y la disponibilidad del puerto.

> Es posible compartir puertos en un clúster con una relación entre iguales mientras se usan puertos dedicados en el otro.

Ancho de banda de red

Si tiene una red de alta velocidad, como 10 GbE, es posible que tenga suficiente ancho de banda LAN local para realizar la replicación con los mismos puertos de 10 GbE que se utilizan para el acceso a datos.

Incluso entonces, debería comparar su ancho de banda WAN disponible con su ancho de banda LAN. Si el ancho de banda WAN disponible es significativamente inferior a 10 GbE, es posible que deba utilizar puertos dedicados.

> La única excepción a esta regla podría ser cuando todos los nodos del clúster replican los datos, en cuyo caso la utilización de ancho de banda suele extenderse por todos los nodos.

Si no utiliza puertos dedicados, el tamaño máximo de unidad de transmisión (MTU) de la red de replicación debe ser, por lo general, el mismo tamaño de MTU de la red de datos.

El intervalo de replicación

Si la replicación se realiza en horas de menor actividad, debería poder utilizar puertos de datos para la

replicación incluso sin conexión LAN de 10 GbE.

Si la replicación se realiza durante el horario laboral normal, debe tener en cuenta la cantidad de datos que se replicarán y si se requiere tanto ancho de banda como para provocar la contención con protocolos de datos. Si el uso de la red por protocolos de datos (SMB, NFS e iSCSI) supera el 50%, debe usar puertos dedicados para la comunicación entre clústeres con el fin de no degradar el rendimiento en caso de producirse una conmutación por error de nodo.

Disponibilidad de puertos

Si determina que el tráfico de replicación interfiere con el tráfico de datos, puede migrar las LIF de interconexión de clústeres a cualquier otro puerto compartido compatible con la interconexión de clústeres en el mismo nodo.

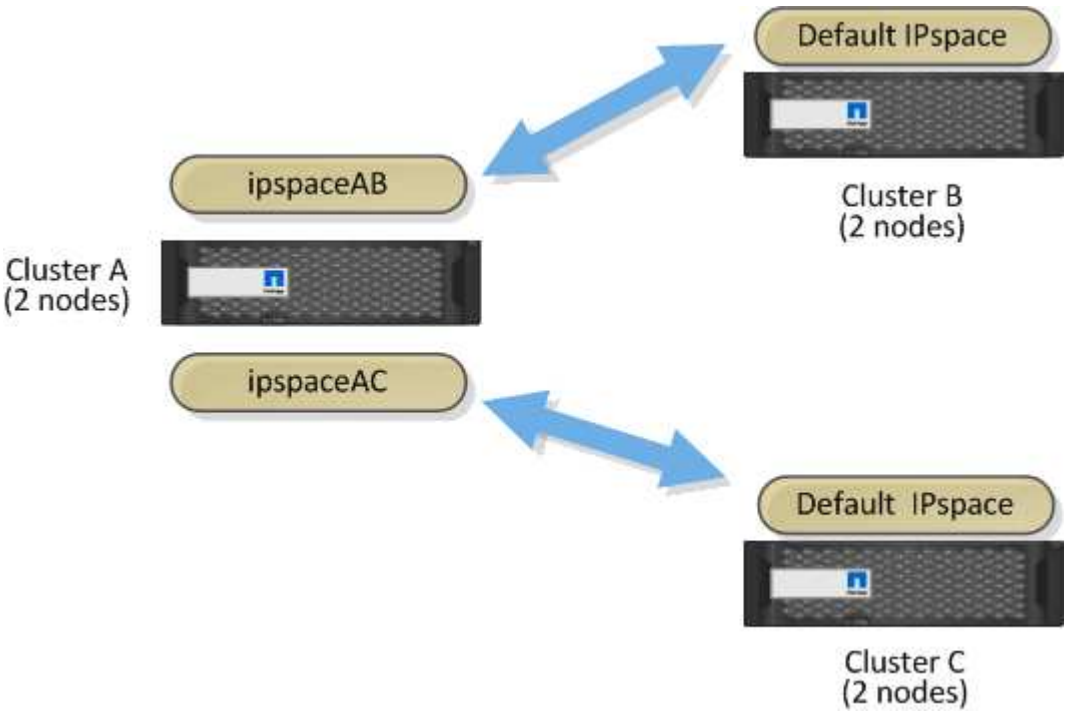
También puede dedicar puertos VLAN para la replicación. El ancho de banda del puerto se comparte entre todas las VLAN y el puerto base.

Utilice espacios IP personalizados para aislar el tráfico de replicación

Puede utilizar espacios IP personalizados para separar las interacciones que tiene un clúster con sus iguales. Esta configuración, denominada conectividad entre clústeres designada_, permite a los proveedores de servicios aislar el tráfico de replicación en entornos multi-tenant.

Suponga, por ejemplo, que desea que el tráfico de replicación entre el clúster A y el clúster B esté separado del tráfico de replicación entre el clúster A y el clúster C. Para ello, puede crear dos espacios IP en el clúster A.

Un espacio IP contiene las LIF entre clústeres que utiliza para comunicarse con el clúster B. La otra contiene las LIF de interconexión de clústeres que utiliza para comunicarse con el clúster C, como se muestra en la siguiente ilustración.



Para obtener información sobre la configuración personalizada del espacio IP, consulte *Network Management*

Guide.

Configure las LIF de interconexión de clústeres

Configure las LIF de interconexión de clústeres en puertos de datos compartidos

Las LIF de interconexión de clústeres se pueden configurar en los puertos compartidos con la red de datos. De este modo, se reduce el número de puertos necesarios para interconectar redes.

Pasos

1. Enumere los puertos del clúster:

   ```
   network port show
   ```

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el siguiente ejemplo se muestran los puertos de red en `cluster01`:

   ```
   cluster01::> network port show
                                                                     Speed
   (Mbps)
   Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
   ------ --------- ------------ ---------------- ----- -------
   ------------
   cluster01-01
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
   cluster01-02
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
   ```

2. Cree LIF de interconexión de clústeres en una SVM de administrador (espacio IP predeterminado) o una SVM de sistema (espacio IP personalizado):

Opción	Descripción
En ONTAP 9.6 y posterior:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service -policy default-intercluster -home -node` *`node`* `-home-port port -address` *`port_IP`* `-netmask` *`netmask`*

Opción	Descripción
En ONTAP 9.5 y anteriores:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home -port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo se crean LIF de interconexión de clústeres `cluster01_icl01` y.. `cluster01_icl02`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Compruebe que se han creado las LIF de interconexión de clústeres:

Opción	Descripción
En ONTAP 9.6 y posterior:	`network interface show -service-policy default-intercluster`
En ONTAP 9.5 y anteriores:	`network interface show -role intercluster`

Para obtener una sintaxis de comando completa, consulte la página man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Compruebe que las LIF de interconexión de clústeres son redundantes:

Opción	Descripción
En ONTAP 9.6 y posterior:	`network interface show –service-policy default-intercluster -failover`
En ONTAP 9.5 y anteriores:	`network interface show -role intercluster -failover`

Para obtener una sintaxis de comando completa, consulte la página man.

El siguiente ejemplo muestra las LIF de interconexión de clústeres `cluster01_icl01` y.. `cluster01_icl02` en la `e0c` el puerto se conmuta al nodo de respaldo `e0d` puerto.

```
cluster01::> network interface show -service-policy default-intercluster
–failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

Configure las LIF de interconexión de clústeres en puertos dedicados

Puede configurar LIF de interconexión de clústeres en puertos dedicados. Al hacerlo, normalmente aumenta el ancho de banda disponible para el tráfico de replicación.

Pasos

1. Enumere los puertos del clúster:

   ```
   network port show
   ```

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el siguiente ejemplo se muestran los puertos de red en `cluster01`:

   ```
   cluster01::> network port show
                                                                     Speed
   (Mbps)
   Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
   ------ --------- ------------ ---------------- ----- -------
   ------------
   cluster01-01
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
          e0e       Default      Default          up     1500   auto/1000
          e0f       Default      Default          up     1500   auto/1000
   cluster01-02
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
          e0e       Default      Default          up     1500   auto/1000
          e0f       Default      Default          up     1500   auto/1000
   ```

2. Determine qué puertos están disponibles para dedicar a la comunicación entre clústeres:

   ```
   network interface show -fields home-port,curr-port
   ```

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el siguiente ejemplo se muestran los puertos `e0e` y.. `e0f` No se han asignado LIF:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. Cree un grupo de recuperación tras fallos para los puertos dedicados:

   `network interface failover-groups create -vserver` *`system_SVM`* `-failover-group` *`failover_group`* `-targets` *`physical _or_logical_ports`*

   En el siguiente ejemplo se asignan puertos `e0e` y.. `e0f` al grupo de recuperación tras fallos `intercluster01` En la SVM del sistema `cluster01`:

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Compruebe que el grupo de recuperación tras fallos se ha creado:

   `network interface failover-groups show`

   Para obtener una sintaxis de comando completa, consulte la página man.

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. Cree LIF de interconexión de clústeres en la SVM del sistema y asígnelas al grupo de recuperación tras fallos.

Opción	Descripción
En ONTAP 9.6 y posterior:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service -policy default-intercluster -home -node` *`node`* `-home- port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`* `-failover -group` *`failover_group`*
En ONTAP 9.5 y anteriores:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home -port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`* `-failover-group` *`failover_group`*

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo se crean LIF de interconexión de clústeres `cluster01_icl01` y.. `cluster01_icl02` en el grupo de recuperación tras fallos `intercluster01`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Compruebe que se han creado las LIF de interconexión de clústeres:

Opción	Descripción
En ONTAP 9.6 y posterior:	`network interface show -service-policy default-intercluster`
En ONTAP 9.5 y anteriores:	`network interface show -role intercluster`

Para obtener una sintaxis de comando completa, consulte la página man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

7. Compruebe que las LIF de interconexión de clústeres son redundantes:

Opción	Descripción
En ONTAP 9.6 y posterior:	`network interface show -service-policy default-intercluster -failover`
En ONTAP 9.5 y anteriores:	`network interface show -role intercluster -failover`

Para obtener una sintaxis de comando completa, consulte la página man.

El siguiente ejemplo muestra las LIF de interconexión de clústeres `cluster01_icl01` y.. `cluster01_icl02` En la SVM`e0e` el puerto se conmuta al nodo de respaldo `e0f` puerto.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Configure las LIF de interconexión de clústeres en espacios IP personalizados

Puede configurar LIF de interconexión de clústeres en espacios IP personalizados. Al hacerlo, puede aislar el tráfico de replicación en entornos multi-tenant.

Cuando crea un espacio IP personalizado, el sistema crea una máquina virtual de almacenamiento (SVM) del sistema para que actúe como contenedor de los objetos del sistema en ese espacio IP. Puede usar la nueva SVM como contenedor de cualquier LIF entre clústeres del nuevo espacio IP. La nueva SVM tiene el mismo nombre que el espacio IP personalizado.

Pasos

1. Enumere los puertos del clúster:

   `network port show`

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el siguiente ejemplo se muestran los puertos de red en `cluster01`:

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

2. Cree espacios IP personalizados en el clúster:

   `network ipspace create -ipspace` *`ipspace`*

   En el siguiente ejemplo se crea el espacio IP personalizado `ipspace-IC1`:

   ```
   cluster01::> network ipspace create -ipspace ipspace-IC1
   ```

3. Determine qué puertos están disponibles para dedicar a la comunicación entre clústeres:

   `network interface show -fields home-port,curr-port`

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el siguiente ejemplo se muestran los puertos `e0e` y.. `e0f` No se han asignado LIF:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01_clus1   e0a       e0a
Cluster cluster01_clus2   e0b       e0b
Cluster cluster02_clus1   e0a       e0a
Cluster cluster02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

4. Elimine los puertos disponibles del dominio de difusión predeterminado:

   `network port broadcast-domain remove-ports -broadcast-domain Default -ports ports`

   Un puerto no puede estar en más de un dominio de retransmisión a la vez. Para obtener una sintaxis de comando completa, consulte la página man.

   En el ejemplo siguiente se quitan puertos `e0e` y.. `e0f` desde el dominio de difusión predeterminado:

```
cluster01::> network port broadcast-domain remove-ports -broadcast
-domain Default -ports
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

5. Compruebe que los puertos se han eliminado del dominio de retransmisión predeterminado:

   `network port show`

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el siguiente ejemplo se muestran los puertos `e0e` y.. `e0f` se han eliminado del dominio de difusión predeterminado:

```
cluster01::> network port show
                                                          Speed (Mbps)
Node   Port    IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ ------- --------- --------------- ----- ------- ------------
cluster01-01
       e0a     Cluster    Cluster          up    9000  auto/1000
       e0b     Cluster    Cluster          up    9000  auto/1000
       e0c     Default    Default          up    1500  auto/1000
       e0d     Default    Default          up    1500  auto/1000
       e0e     Default    -                up    1500  auto/1000
       e0f     Default    -                up    1500  auto/1000
       e0g     Default    Default          up    1500  auto/1000
cluster01-02
       e0a     Cluster    Cluster          up    9000  auto/1000
       e0b     Cluster    Cluster          up    9000  auto/1000
       e0c     Default    Default          up    1500  auto/1000
       e0d     Default    Default          up    1500  auto/1000
       e0e     Default    -                up    1500  auto/1000
       e0f     Default    -                up    1500  auto/1000
       e0g     Default    Default          up    1500  auto/1000
```

6. Cree un dominio de retransmisión en el espacio IP personalizado:

   `network port broadcast-domain create -ipspace` *`ipspace`* `-broadcast-domain` *`broadcast_domain`* `-mtu` *`MTU`* `-ports` *`ports`*

   En el siguiente ejemplo se crea el dominio de retransmisión `ipspace-IC1-bd` En el espacio IP `ipspace-IC1`:

```
cluster01::> network port broadcast-domain create -ipspace ipspace-IC1
-broadcast-domain
ipspace-IC1-bd -mtu 1500 -ports cluster01-01:e0e,cluster01-01:e0f,
cluster01-02:e0e,cluster01-02:e0f
```

7. Compruebe que se ha creado el dominio de retransmisión:

   `network port broadcast-domain show`

   Para obtener una sintaxis de comando completa, consulte la página man.

```
cluster01::> network port broadcast-domain show
IPspace Broadcast                                         Update
Name    Domain Name    MTU  Port List                     Status Details
------- ----------- ------  ------------------------------ --------------
Cluster Cluster       9000
                            cluster01-01:e0a              complete
                            cluster01-01:e0b              complete
                            cluster01-02:e0a              complete
                            cluster01-02:e0b              complete
Default Default       1500
                            cluster01-01:e0c              complete
                            cluster01-01:e0d              complete
                            cluster01-01:e0f              complete
                            cluster01-01:e0g              complete
                            cluster01-02:e0c              complete
                            cluster01-02:e0d              complete
                            cluster01-02:e0f              complete
                            cluster01-02:e0g              complete
ipspace-IC1
        ipspace-IC1-bd
                      1500
                            cluster01-01:e0e              complete
                            cluster01-01:e0f              complete
                            cluster01-02:e0e              complete
                            cluster01-02:e0f              complete
```

8. Cree LIF de interconexión de clústeres en la SVM del sistema y asígnelas al dominio de retransmisión:

Opción	Descripción
En ONTAP 9.6 y posterior:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service -policy default-intercluster -home -node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*
En ONTAP 9.5 y anteriores:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home -port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

La LIF se crea en el dominio de retransmisión al que está asignado el puerto inicial. El dominio de difusión tiene un grupo de conmutación por error predeterminado con el mismo nombre que el dominio de difusión. Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo se crean LIF de interconexión de clústeres `cluster01_icl01` y.. `cluster01_icl02` en el dominio de retransmisión `ipspace-IC1-bd`:

```
cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0
```

9. Compruebe que se han creado las LIF de interconexión de clústeres:

Opción	Descripción
En ONTAP 9.6 y posterior:	`network interface show -service-policy default-intercluster`
En ONTAP 9.5 y anteriores:	`network interface show -role intercluster`

Para obtener una sintaxis de comando completa, consulte la página man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
ipspace-IC1
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

10. Compruebe que las LIF de interconexión de clústeres son redundantes:

Opción	Descripción
En ONTAP 9.6 y posterior:	`network interface show -service-policy default-intercluster -failover`
En ONTAP 9.5 y anteriores:	`network interface show -role intercluster -failover`

Para obtener una sintaxis de comando completa, consulte la página man.

El siguiente ejemplo muestra las LIF de interconexión de clústeres `cluster01_icl01` y.. `cluster01_icl02` En la SVM `e0e` conmutación por error de puerto al puerto'e0f'port:

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
ipspace-IC1
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Configure las relaciones de paridad

Cree una relación de paridad entre clústeres

Puede utilizar el `cluster peer create` comando para crear una relación entre iguales entre un clúster local y remoto. Una vez creada la relación de paridad, puede ejecutarse `cluster peer create` en el clúster remoto para autenticarse en el clúster local.

Antes de empezar

- Debe haber creado LIF de interconexión de clústeres en todos los nodos de los clústeres que se están interponiendo.
- Los clústeres deben ejecutar ONTAP 9.3 o una versión posterior. (Si los clústeres ejecutan ONTAP 9.2 o una versión anterior, consulte los procedimientos en "este documento archivado".)

Pasos

Lleve a cabo esta tarea mediante System Manager de ONTAP o la interfaz de línea de comandos de ONTAP.

System Manager

1. En el clúster local, haga clic en **Clúster > Configuración**.
2. En la sección **Intercluster Settings**, haga clic en **Add Network Interfaces** y agregue interfaces de red de interconexión de clústeres para el clúster.

   Repita este paso en el clúster remoto.

3. En el clúster remoto, haga clic en **Clúster > Configuración**.
4. Haga clic en ⋮ En la sección **Peones del clúster** y seleccione **Generar contraseña**.
5. Seleccione la versión del clúster de ONTAP remoto.
6. Copie la clave de acceso generada.
7. En el clúster local, en **Cluster peers**, haga clic en ⋮ Y seleccione **Peer cluster**.
8. En la ventana **Peer cluster**, pega la frase de acceso y haz clic en **Iniciar interconexión de clústeres**.

CLI

1. En el clúster de destino, cree una relación entre iguales con el clúster de origen:

   ```
   cluster peer create -generate-passphrase -offer-expiration
   <MM/DD/YYYY HH:MM:SS>|1...7days|1...168hours -peer-addrs
   <peer_LIF_IPs > -initial-allowed-vserver-peers <svm_name>|* -ipspace
   <ipspace>
   ```

   Si especifica ambas `-generate-passphrase` y.. `-peer-addrs`, Sólo el clúster cuyas LIF de interconexión de clústeres se especifican en `-peer-addrs` puede utilizar la contraseña generada.

   Puede ignorar la `-ipspace` Si no está utilizando un espacio IP personalizado. Para obtener una sintaxis de comando completa, consulte la página man.

   Si va a crear la relación de paridad en ONTAP 9.6 o una versión posterior y no desea que se cifren las comunicaciones entre clústeres, debe utilizar el `-encryption-protocol-proposed none` opción para deshabilitar el cifrado.

   En el siguiente ejemplo, se crea una relación de paridad entre clústeres con un clúster remoto no especificado y se preautoriza relaciones entre iguales con SVM `vs1` y.. `vs2` en el clúster local:

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

                     Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
                Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

En el siguiente ejemplo se crea una relación entre iguales de clústeres con el clúster remoto en las direcciones IP de LIF entre clústeres 192.140.112.103 y 192.140.112.104, y se autoriza previamente una relación entre iguales con cualquier SVM del clúster local:

```
cluster02::> cluster peer create -generate-passphrase -peer-addrs
192.140.112.103,192.140.112.104 -offer-expiration 2days -initial
-allowed-vserver-peers *

                     Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
                Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101,192.140.112.102
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

En el siguiente ejemplo, se crea una relación de paridad entre clústeres con un clúster remoto no especificado y se preautoriza relaciones entre iguales con SVM`vs1` y.. `vs2` en el clúster local:

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

                     Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
                Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

2. En el clúster de origen, autentique el clúster de origen al clúster de destino:

```
cluster peer create -peer-addrs <peer_LIF_IPs> -ipspace <ipspace>
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo se autentica el clúster local en el clúster remoto en las direcciones IP de LIF entre clústeres 192.140.112.101 y 192.140.112.102:

```
cluster01::> cluster peer create -peer-addrs
192.140.112.101,192.140.112.102

Notice: Use a generated passphrase or choose a passphrase of 8 or
more characters.
        To ensure the authenticity of the peering relationship, use
a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

Introduzca la frase de acceso para la relación entre iguales cuando se le solicite.

3. Compruebe que se ha creado la relación de paridad entre clústeres:

```
cluster peer show -instance
```

```
cluster01::> cluster peer show -instance

                              Peer Cluster Name: cluster02
                   Remote Intercluster Addresses: 192.140.112.101,
192.140.112.102
              Availability of the Remote Cluster: Available
                            Remote Cluster Name: cluster2
                            Active IP Addresses: 192.140.112.101,
192.140.112.102
                          Cluster Serial Number: 1-80-123456
                  Address Family of Relationship: ipv4
            Authentication Status Administrative: no-authentication
               Authentication Status Operational: absent
                                Last Update Time: 02/05 21:05:41
                    IPspace for the Relationship: Default
```

4. Compruebe la conectividad y el estado de los nodos en la relación de paridad:

```
cluster peer health show
```

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health
Avail…
---------- --------------------------- ---------  ---------------
--------
cluster01-01
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
```

Otras maneras de hacerlo en ONTAP

Para ejecutar estas tareas con…	Ver este contenido…
System Manager rediseñado (disponible con ONTAP 9.7 y versiones posteriores)	"Prepare el mirroring y el almacenamiento"
System Manager Classic (disponible con ONTAP 9.7 y versiones anteriores)	"Información general de preparación para la recuperación ante desastres de volúmenes"

Cree una relación entre iguales de SVM entre clústeres

Puede utilizar el `vserver peer create` Comando para crear una relación entre iguales entre SVM en clústeres locales y remotos.

Antes de empezar

- Los clústeres de origen y destino deben tener una relación entre iguales.
- Los clústeres deben ejecutar ONTAP 9.3. (Si los clústeres ejecutan ONTAP 9.2 o una versión anterior, consulte los procedimientos en "este documento archivado".)
- Debe tener relaciones entre iguales "preautorizadas" para las SVM en el clúster remoto.

  Para obtener más información, consulte "Creación de una relación de paridad entre clústeres".

Acerca de esta tarea

En ONTAP 9,2 y versiones anteriores, solo se puede autorizar una relación entre iguales para una SVM a la vez. Esto significa que debe ejecutar el `vserver peer accept` Comando cada vez que se autoriza una relación entre iguales de SVM pendiente.

A partir de ONTAP 9.3, puede "preautorizar" relaciones entre iguales para varias SMV mediante la lista de las SMV en el `-initial-allowed-vserver` opción cuando se crea una relación de paridad entre clústeres. Para obtener más información, consulte "Creación de una relación de paridad entre clústeres".

Pasos

1. En el clúster de destino de protección de datos, muestre las SVM que están autorizadas previamente para la paridad:

   `vserver peer permission show`

   ```
   cluster02::> vserver peer permission show
   Peer Cluster         Vserver               Applications
   -------------------  --------------------  --------------------
   cluster02            vs1,vs2               snapmirror
   ```

2. En el clúster de origen de protección de datos, cree una relación entre iguales con una SVM preautorizada en el clúster de destino de protección de datos:

   `vserver peer create -vserver` *`local_SVM`* `-peer-vserver` *`remote_SVM`*

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el siguiente ejemplo se crea una relación entre iguales entre la SVM local `pvs1` Y la SVM remota preautorizada `vs1`:

   ```
   cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
   ```

3. Compruebe las relaciones entre iguales de SVM:

   `vserver peer show`

```
cluster01::> vserver peer show
            Peer        Peer                            Peering
Remote
Vserver     Vserver     State        Peer Cluster      Applications
Vserver
----------- ----------- ------------ ----------------- --------------
---------
pvs1        vs1         peered       cluster02         snapmirror
vs1
```

Añada una relación entre iguales de SVM de interconexión de clústeres

Si crea una SVM después de configurar una relación de paridad de clústeres, deberá añadir una relación de paridad para la SVM manualmente. Puede utilizar el `vserver peer create` Comando para crear una relación entre iguales entre SVM. Una vez creada la relación de paridad, puede ejecutarse `vserver peer accept` en el clúster remoto para autorizar la relación de paridad.

Antes de empezar

Los clústeres de origen y destino deben tener una relación entre iguales.

Acerca de esta tarea

Puede crear relaciones entre iguales entre SVM en el mismo clúster para el backup de datos local. Para obtener más información, consulte `vserver peer create` página de manual.

Los administradores utilizan ocasionalmente el `vserver peer reject` Comando para rechazar una relación de paridad de SVM propuesta. Si la relación entre las SVM está en la `rejected` estado, debe eliminar la relación antes de poder crear una nueva. Para obtener más información, consulte `vserver peer delete` página de manual.

Pasos

1. En el clúster de origen de protección de datos, cree una relación entre iguales con una SVM en el clúster de destino de protección de datos:

   `vserver peer create -vserver` *`local_SVM`* `-peer-vserver` *`remote_SVM`* `-applications snapmirror|file-copy|lun-copy -peer-cluster` *`remote_cluster`*

   En el siguiente ejemplo se crea una relación entre iguales entre la SVM local`pvs1` Y la SVM remota`vs1`

   ```
   cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
   -applications snapmirror -peer-cluster cluster02
   ```

   Si las SVM locales y remotas tienen los mismos nombres, debe usar un *local name* para crear la relación entre iguales de SVM:

```
cluster01::> vserver peer create -vserver vs1 -peer-vserver
vs1 -applications snapmirror -peer-cluster cluster01
-local-name cluster1vs1LocallyUniqueName
```

2. En el clúster de origen de protección de datos, compruebe que se ha iniciado la relación de paridad:

   `vserver peer show-all`

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el siguiente ejemplo, se muestra la relación entre iguales entre SVM`pvs1` Y SVM`vs1` se ha iniciado:

```
cluster01::> vserver peer show-all
            Peer        Peer                        Peering
Vserver     Vserver     State      Peer Cluster   Applications
--------    --------    ---------  -------------  ------------
pvs1        vs1         initiated   Cluster02       snapmirror
```

3. En el clúster de destino de la protección de datos, muestre la relación entre iguales de SVM pendiente:

   `vserver peer show`

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el siguiente ejemplo, se enumeran las relaciones entre iguales pendientes para `cluster02`:

```
cluster02::> vserver peer show

                   Peer               Peer
Vserver            Vserver            State
-----------        -----------        ------------
vs1                pvs1               pending
```

4. En el clúster de destino de la protección de datos, autorice la relación entre iguales pendiente:

   `vserver peer accept -vserver` *`local_SVM`* `-peer-vserver` *`remote_SVM`*

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el siguiente ejemplo, se autoriza la relación entre iguales entre la SVM local `vs1` Y la SVM remota `pvs1`:

```
cluster02::> vserver peer accept -vserver vs1 -peer-vserver pvs1
```

5. Compruebe las relaciones entre iguales de SVM:

```
vserver peer show
```

```
cluster01::> vserver peer show
            Peer        Peer                            Peering
Remote
Vserver     Vserver     State        Peer Cluster      Applications
Vserver
----------- ----------- ------------ ----------------- --------------
---------
pvs1        vs1         peered       cluster02         snapmirror
vs1
```

Habilite el cifrado de paridad de clústeres en una relación de paridad existente

A partir de ONTAP 9.6, el cifrado de paridad de clústeres está habilitado de forma predeterminada en todas las relaciones de paridad de clústeres que haya creado recientemente. El cifrado de interconexión de clústeres utiliza una clave precompartida (PSK) y la capa de seguridad de transporte (TLS) para proteger las comunicaciones de interconexión entre clústeres. Esto añade una capa adicional de seguridad entre los clústeres con una relación entre iguales.

Acerca de esta tarea

Si va a actualizar clústeres con una relación entre iguales a ONTAP 9.6 o posterior y la relación de paridad se creó en ONTAP 9.5 o versiones anteriores, el cifrado de paridad de clústeres se debe habilitar manualmente después de la actualización. Ambos clústeres de la relación de paridad deben ejecutar ONTAP 9.6 o una versión posterior para habilitar el cifrado de paridad de clústeres.

Pasos

1. En el clúster de destino, habilite el cifrado para las comunicaciones con el clúster de origen:

   ```
   cluster peer modify source_cluster -auth-status-admin use-authentication
   -encryption-protocol-proposed tls-psk
   ```

2. Cuando se le solicite, introduzca una frase de contraseña.
3. En el clúster de origen de la protección de datos, habilite el cifrado para la comunicación con el clúster de destino de la protección de datos:

   ```
   cluster peer modify data_protection_destination_cluster -auth-status-admin
   use-authentication -encryption-protocol-proposed tls-psk
   ```

4. Cuando se le solicite, escriba la misma clave de acceso introducida en el clúster de destino.

Quite el cifrado de paridad de clústeres de una relación de paridad existente

De forma predeterminada, el cifrado de paridad de clústeres está habilitado en todas las relaciones entre iguales creadas en ONTAP 9.6 o posterior. Si no desea utilizar el cifrado para las comunicaciones entre clústeres entre iguales, puede deshabilitarlo.

Pasos

1. En el clúster de destino, modifique las comunicaciones con el clúster de origen para interrumpir el uso del cifrado de interconexión de clústeres :
   - Para eliminar el cifrado, pero mantener la autenticación, introduzca:

     ```
     cluster peer modify _source_cluster_ -auth-status-admin use-
     authentication -encryption-protocol-proposed none
     ```

   - Para eliminar el cifrado y la autenticación, introduzca:

     ```
     cluster peer modify _source_cluster_ -auth-status no-authentication
     ```

2. Cuando se le solicite, introduzca una frase de contraseña.
3. En el clúster de origen, deshabilite el cifrado para la comunicación con el clúster de destino:
   - Para eliminar el cifrado, pero mantener la autenticación, introduzca:

     ```
     cluster peer modify _destination_cluster_ -auth-status-admin use-
     authentication -encryption-protocol-proposed none
     ```

   - Para eliminar el cifrado y la autenticación, introduzca:

     ```
     cluster peer modify _destination_cluster_ -auth-status no-
     authentication
     ```

4. Cuando se le solicite, escriba la misma clave de acceso introducida en el clúster de destino.

Gestione copias Snapshot locales

Información general sobre la gestión de copias Snapshot locales

Una *Snapshot copy* es una imagen puntual de solo lectura de un volumen. La imagen consume un espacio de almacenamiento mínimo y tiene una sobrecarga del rendimiento mínima, ya que solo registra los cambios realizados en los archivos desde la última copia Snapshot.

Puede usar una copia Snapshot para restaurar el contenido completo de un volumen o para recuperar archivos o LUN individuales. Las copias Snapshot se almacenan en el directorio `.snapshot` en el volumen.

En ONTAP 9.3 y versiones anteriores, un volumen puede contener hasta 255 copias snapshot. A partir de la versión 9.4 de ONTAP, un volumen de FlexVol puede contener hasta 1023 copias snapshot.

A partir de ONTAP 9.8, los volúmenes FlexGroup pueden contener 1023 copias snapshot. Para obtener más información, consulte "Protección de volúmenes de FlexGroup mediante copias de Snapshot".

Configuración de políticas de Snapshot personalizadas

Información general de configuración de políticas de Snapshot personalizadas

Una *política de Snapshot* define el modo en que el sistema crea copias Snapshot. La política especifica cuándo crear copias Snapshot, cuántas copias se retendrán y cómo nombrarlas. Por ejemplo, un sistema puede crear una copia Snapshot todos los días a las 12:10, conservar las dos copias más recientes y nombrar las copias "día a día.`timestamp`."

La política predeterminada de un volumen crea automáticamente copias de Snapshot en la siguiente programación, con las copias de Snapshot más antiguas eliminadas para hacer espacio para las copias más nuevas:

- Un máximo de seis copias Snapshot cada hora tardan cinco minutos.
- Un máximo de dos copias Snapshot diarias que se tomaban de lunes a sábado a las 10 minutos después de la medianoche.
- Un máximo de dos copias snapshot semanales cada domingo a las 15 minutos después de la medianoche.

A menos que especifique una política de Snapshot cuando crea un volumen, el volumen hereda la política de Snapshot asociada con su máquina virtual de almacenamiento (SVM).

Cuándo configurar una política de Snapshot personalizada

Si la política de Snapshot predeterminada no es adecuada para un volumen, puede configurar una política personalizada que modifique la frecuencia, la retención y el nombre de las copias de Snapshot. La programación estará dictada principalmente por la tasa de cambio del sistema de archivos activo.

Puede ser recomendable realizar el backup de un sistema de archivos muy utilizado, como una base de datos, cada hora, mientras que el backup de archivos de uso poco frecuente una vez al día. Incluso en el caso de una base de datos, suele ejecutar un backup completo una o dos veces al día, mientras realiza el backup de los registros de transacciones cada hora.

Otros factores son la importancia de los archivos para la organización, el SLA, el RPO y el RTO. En general, sólo debe conservar tantas copias snapshot como sea necesario.

Crear una programación de trabajo de Snapshot

Una política de Snapshot requiere al menos una programación de trabajo de copia de Snapshot. Puede utilizar el `job schedule cron create` para crear una programación de trabajo.

Acerca de esta tarea

De forma predeterminada, ONTAP forma los nombres de las copias Snapshot anexando una Marca de tiempo

al nombre de la programación del trabajo.

Si especifica valores para el día del mes y el día de la semana, los valores se consideran independientes. Por ejemplo, una programación cron con la especificación del día `Friday` y el día de la especificación del mes `13` Funciona todos los viernes y el día 13 de cada mes, no sólo cada viernes 13.

Paso

1. Crear un programa de trabajo:

   `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

   Para `-month`, `-dayofweek`, y. `-hour`, puede especificar `all` para ejecutar el trabajo cada mes, día de la semana y hora, respectivamente.

   A partir de ONTAP 9.10.1, puede incluir Vserver para su programación de trabajo:

   `job schedule cron create -name job_name -vserver Vserver_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

   En el ejemplo siguiente se crea una programación de trabajo denominada `myweekly` Es decir, los sábados a las 3:00 horas:

   ```
   cluster1::> job schedule cron create -name myweekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

   En el siguiente ejemplo se crea una programación llamada `myweeklymulti` esto especifica varios días, horas y minutos:

   ```
   job schedule cron create -name myweeklymulti -dayofweek
   "Monday,Wednesday,Sunday" -hour 3,9,12 -minute 0,20,50
   ```

Cree una política de Snapshot

Una política de Snapshot especifica cuándo crear copias de Snapshot, cuántas copias se retendrán y cómo nombrarlas. Por ejemplo, un sistema puede crear una copia Snapshot todos los días a las 12:10, conservar las dos copias más recientes y nombrarlas "día tras día.*timestamp*.'" Una política de Snapshot puede contener hasta cinco programaciones de trabajo.

Acerca de esta tarea

De forma predeterminada, ONTAP forma los nombres de las copias Snapshot anexando una Marca de tiempo al nombre de programación de trabajo:

```
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
```

Si lo prefiere, puede sustituir un prefijo por el nombre del programa de trabajo.

La `snapmirror-label` Esta opción es para la replicación de SnapMirror. Para obtener más información, consulte "Definición de una regla para una política".

Paso

1. Cree una política de Snapshot:

   `volume snapshot policy create -vserver` *`SVM`* `-policy` *`policy_name`* `-enabled true|false -schedule1` *`schedule1_name`* `-count1` *`copies_to_retain`* `-prefix1` *`snapshot_prefix`* `-snapmirror-label1` *`snapshot_label`* … `-schedule5` *`schedule5_name`* `-count5` *`copies_to_retain`*`-prefix5` *`snapshot_prefix`* `-snapmirror-label5` *`snapshot_label`*

   En el ejemplo siguiente se crea una política de Snapshot llamada `snap_policy_daily` eso se ejecuta en un `daily` programación. La política tiene un máximo de cinco copias Snapshot, cada una con el nombre `daily.`*`timestamp`* Y la etiqueta de SnapMirror `daily`:

   ```
   cluster1::> volume snapshot policy create -vserver vs0 -policy
   snap_policy_daily -schedule1 daily -count1 5 -snapmirror-label1 daily
   ```

Gestionar copias Snapshot manualmente

Crear y eliminar copias Snapshot manualmente

Puede crear copias Snapshot manualmente cuando no se puede esperar a que se cree una copia Snapshot programada para eliminar copias Snapshot cuando ya no son necesarias.

Crear una copia Snapshot manualmente

Puede crear manualmente una copia Snapshot mediante System Manager o la interfaz de línea de comandos de ONTAP.

System Manager

Pasos

1. Vaya a **Almacenamiento > Volúmenes** y seleccione la pestaña **Copias de instantánea**.
2. Haga clic en + Add .
3. En la ventana **Agregar una copia snapshot**, acepte el nombre predeterminado de la copia snapshot o edítelo si lo desea.
4. **Opcional**: Añade una etiqueta de SnapMirror.
5. Haga clic en **Agregar**.

CLI

1. Cree una copia Snapshot:

```
volume snapshot create -vserver <SVM> -volume <volume> -snapshot
<snapshot_name>
```

Eliminar una copia Snapshot de forma manual

Puede eliminar manualmente una copia Snapshot mediante System Manager o la interfaz de línea de comandos de ONTAP.

System Manager

Pasos

1. Vaya a **Almacenamiento > Volúmenes** y seleccione la pestaña **Copias de instantánea**.
2. Busque la copia Snapshot que desee eliminar y haga clic en ⋮, Y seleccione **Eliminar**.
3. En la ventana **Eliminar copia de instantánea**, seleccione **Eliminar copia de instantánea**.
4. Haga clic en **Eliminar**.

CLI

1. Eliminar una copia Snapshot:

```
volume snapshot delete -vserver <SVM> -volume <volume> -snapshot
<snapshot_name>
```

Gestione la reserva de copias Snapshot

Gestione la descripción general de la reserva de copias Snapshot

El *Snapshot copy reserve* deja un porcentaje del espacio en disco para las copias Snapshot, del cinco por ciento de forma predeterminada. Debido a que las copias Snapshot utilizan espacio en el sistema de archivos activo cuando se agota la reserva de

copia Snapshot, puede aumentar la reserva de copia Snapshot según sea necesario. También puede realizar copias Snapshot de forma automática cuando la reserva esté llena.

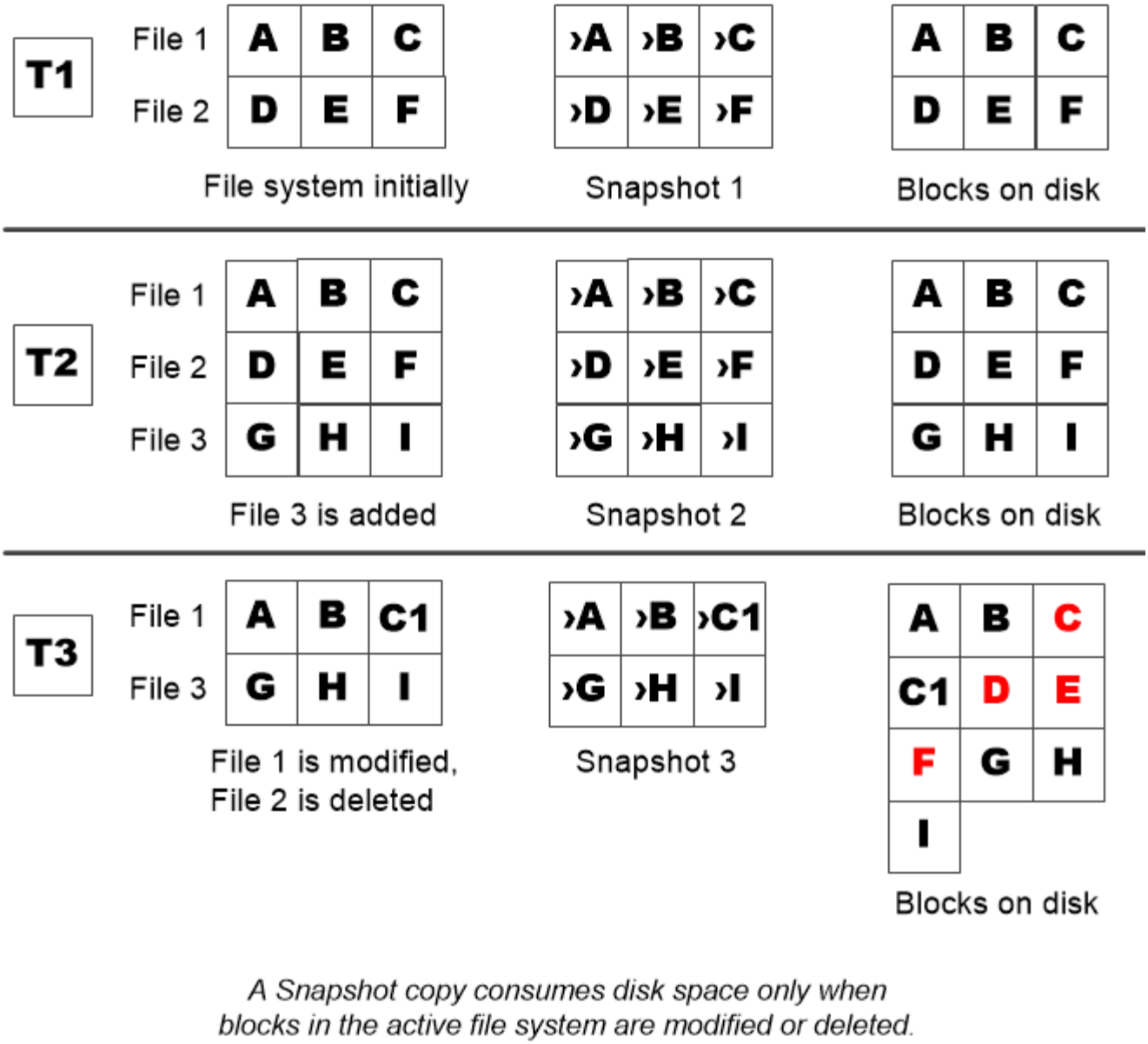
Cuándo aumentar la reserva para copias Snapshot

Para decidir si se debe aumentar la reserva Snapshot, es importante recordar que una copia Snapshot solo registra los cambios en los archivos desde que se realizó la última copia Snapshot. Consume espacio en disco solo si se modifican o eliminan bloques del sistema de archivos activo.

Esto significa que la tasa de cambio del sistema de archivos es el factor clave para determinar la cantidad de espacio en disco que utilizan las copias snapshot. No importa cuántas copias snapshot cree, no consumirán espacio en disco si el sistema de archivos activo no ha cambiado.

Por ejemplo, un volumen FlexVol que contenga registros de transacciones de base de datos puede tener una reserva de copia Snapshot de hasta el 20 % para justificar su mayor tasa de cambio. No solo querrá crear más copias Snapshot para capturar las actualizaciones más frecuentes de la base de datos, sino que también querrá tener una reserva de copia Snapshot mayor para gestionar el espacio en disco adicional que consumen las copias Snapshot.

Una copia Snapshot consta de punteros a bloques en lugar de copias de bloques. Puede pensar en un puntero como «reclamación» en un bloque: «Mantiene» ONTAP el bloque hasta que se elimine la copia snapshot.



A Snapshot copy consumes disk space only when blocks in the active file system are modified or deleted.

La eliminación de archivos protegidos puede reducir el espacio de archivos de lo esperado

Una copia snapshot señala a un bloque incluso después de eliminar el archivo que utilizó el bloque. Esto explica por qué una reserva de copia snapshot agotada puede dar lugar al resultado contrario-intuitivo en el que la eliminación de todo un sistema de archivos da como resultado menos espacio disponible que el sistema de archivos ocupado.

Observe el siguiente ejemplo. Antes de eliminar cualquier archivo, el `df` el resultado del comando es el siguiente:

```
Filesystem           kbytes  used    avail  capacity
/vol/vol0/           3000000 3000000 0       100%
/vol/vol0/.snapshot 1000000 500000  500000   50%
```

Tras eliminar todo el sistema de archivos y realizar una copia snapshot del volumen, la `df` el comando genera

la siguiente salida:

```
Filesystem          kbytes  used    avail  capacity
/vol/vol0/          3000000 2500000 500000   83%
/vol/vol0/.snapshot 1000000 3500000 0       350%
```

Tal y como se muestra en el resultado, ahora los 3 GB completos que utilizaba el sistema de archivos activo son utilizados por las copias snapshot, además de los 0.5 GB utilizados antes de la eliminación.

Como el espacio en disco utilizado por las copias snapshot supera ahora la reserva de copia snapshot, el desbordamiento de 2.5 GB de «píldoras» en el espacio reservado para los archivos activos, dejándole con 0.5 GB de espacio libre para los archivos en los que razonablemente se podrían haber esperado 3 GB.

Supervisar el consumo de discos de la copia snapshot

Puede supervisar el consumo de discos de copias Snapshot mediante la `df` comando. El comando muestra la cantidad de espacio libre en el sistema de archivos activo y la reserva de copias de Snapshot.

Paso

1. Mostrar consumo de disco de copia Snapshot: `df`

   El siguiente ejemplo muestra el consumo de discos de copia Snapshot:

   ```
   cluster1::> df
   Filesystem          kbytes  used    avail  capacity
   /vol/vol0/          3000000 3000000 0       100%
   /vol/vol0/.snapshot 1000000 500000  500000   50%
   ```

Compruebe la reserva de copias Snapshot disponibles en un volumen

Puede comprobar la cantidad de reserva de copias Snapshot disponible en un volumen mediante el `snapshot-reserve-available` con el `volume show` comando.

Paso

1. Compruebe la reserva de copia Snapshot disponible en un volumen:

   `vol show -vserver` *`SVM`* `-volume` *`volume`* `-fields snapshot-reserve-available`

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el ejemplo siguiente se muestra la reserva disponible de copias Snapshot para `vol1`:

```
cluster1::> vol show -vserver vs0 -volume vol1 -fields snapshot-reserve-
available

vserver volume snapshot-reserve-available
------- ------ -------------------------
vs0     vol1   4.84GB
```

Modificar la reserva de copias Snapshot

Se recomienda configurar una reserva de copia de Snapshot más grande para evitar que las copias de Snapshot utilicen el espacio reservado para el sistema de archivos activo. Puede reducir la reserva de copias Snapshot cuando ya no necesite tanto espacio para las copias Snapshot.

Paso

1. Modifique la reserva de copias Snapshot:

   `volume modify -vserver` *`SVM`* `-volume` *`volume`* `-percent-snapshot-space` *`snap_reserve`*

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el ejemplo siguiente se establece la reserva de copias Snapshot para `vol1` al 10 por ciento:

   ```
   cluster1::> volume modify -vserver vs0 -volume vol1 -percent-snapshot
   -space 10
   ```

Eliminación automática de copias snapshot

Puede utilizar el `volume snapshot autodelete modify` Comando para activar la eliminación automática de copias Snapshot cuando se supera la reserva Snapshot. De manera predeterminada, las copias de Snapshot más antiguas se eliminan primero.

Acerca de esta tarea

Los clones de LUN y archivos se eliminan cuando no hay más copias snapshot que se pueden eliminar.

Paso

1. Eliminación automática de copias Snapshot:

   `volume snapshot autodelete modify -vserver` *`SVM`* `-volume` *`volume`* `-enabled true|false -trigger volume|snap_reserve`

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el ejemplo siguiente se eliminan automáticamente las copias Snapshot para `vol1` Cuando la reserva de la copia Snapshot se haya agotado:

```
cluster1::> volume snapshot autodelete modify -vserver vs0 -volume vol1
-enabled true -trigger snap_reserve
```

Restaurar archivos desde copias snapshot

Restaurar un archivo de una copia Snapshot en un cliente NFS o SMB

Un usuario en un cliente NFS o SMB puede restaurar un archivo directamente desde una copia Snapshot sin la intervención de un administrador del sistema de almacenamiento.

Cada directorio del sistema de archivos contiene un subdirectorio llamado `.snapshot` Accesible para los usuarios de NFS y SMB. La `.snapshot` Este subdirectorio contiene subdirectorios que corresponden a las copias snapshot del volumen:

```
$ ls .snapshot
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
```

Cada subdirectorio contiene los archivos a los que hace referencia la copia snapshot. Si los usuarios eliminan o sobrescriben accidentalmente un archivo, pueden restaurarlo al directorio primario de lectura y escritura copiando el archivo desde el subdirectorio Snapshot al directorio de lectura y escritura:

```
$ ls my.txt
ls: my.txt: No such file or directory
$ ls .snapshot
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
$ ls .snapshot/hourly.2017-05-15_1306/my.txt
my.txt
$ cp .snapshot/hourly.2017-05-15_1306/my.txt .
$ ls my.txt
my.txt
```

Habilitar y deshabilitar el acceso de clientes NFS y SMB al directorio de copia Snapshot

Para determinar si el directorio de copia Snapshot es visible para los clientes NFS y SMB para restaurar un archivo o LUN de una copia Snapshot, puede habilitar y deshabilitar el acceso al directorio de la copia Snapshot con el `-snapdir-access` opción de `volume modify` comando.

Pasos

1. Compruebe el estado de acceso al directorio de Snapshot:

   `volume show -vserver SVM_name -volume vol_name -fields snapdir-access`

   Ejemplo:

   ```
   clus1::> volume show -vserver vs0 -volume vol1 -fields snapdir-access
   vserver volume snapdir-access
   ------- ------ --------------
   vs0     vol1   false
   ```

2. Habilite o deshabilite el acceso al directorio de copia Snapshot:

   `volume modify -vserver SVM_name -volume vol_name -snapdir-access true|false`

   En el ejemplo siguiente se habilita el acceso al directorio de copia Snapshot en vol1:

   ```
   clus1::> volume modify -vserver vs0 -volume vol1 -snapdir-access true
   Volume modify successful on volume vol1 of Vserver vs0.
   ```

Restaure un solo archivo de una copia Snapshot

Puede utilizar el `volume snapshot restore-file` Comando para restaurar un solo archivo o LUN desde una copia Snapshot. Es posible restaurar el archivo a otra ubicación en el volumen primario de lectura y escritura si no desea reemplazar un archivo existente.

Acerca de esta tarea

Si va a restaurar una LUN existente, se crea un clon de LUN y se realiza un backup en forma de copia Snapshot. Durante la operación de restauración, puede leer la LUN y escribir en ella.

Los archivos con flujos se restauran de forma predeterminada.

Pasos

1. Enumere las copias Snapshot en un volumen:

   `volume snapshot show -vserver SVM -volume volume`

   Para obtener una sintaxis de comando completa, consulte la página man.

   El ejemplo siguiente muestra las copias Snapshot en `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1  vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Restaurar un archivo desde una copia Snapshot:

   `volume snapshot restore-file -vserver` *`SVM`* `-volume` *`volume`* `-snapshot` *`snapshot`* `-path` *`file_path`* `-restore-path` *`destination_path`*

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el siguiente ejemplo se restaura el archivo `myfile.txt`:

```
cluster1::> volume snapshot restore-file -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010 -path /myfile.txt
```

Restaurar parte de un archivo desde una copia snapshot

Puede utilizar el `volume snapshot partial-restore-file` Comando para restaurar un rango de datos desde una copia Snapshot a una LUN o un archivo de contenedor NFS o SMB, suponiendo que se conozca el desplazamiento de bytes de inicio de los datos y el número de bytes. Este comando puede usarse para restaurar una de las bases de datos en un host que almacena varias bases de datos en el mismo LUN.

A partir de ONTAP 9.12.1, hay una restauración parcial disponible para los volúmenes en una relación de SM-BC.

Pasos

1. Enumere las copias Snapshot en un volumen:

   `volume snapshot show -vserver` *`SVM`* `-volume` *`volume`*

   Para obtener una sintaxis de comando completa, consulte la página man.

   El ejemplo siguiente muestra las copias Snapshot en `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1  vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Restaurar parte de un archivo desde una copia Snapshot:

   `volume snapshot partial-restore-file -vserver` *`SVM`* `-volume` *`volume`* `-snapshot` *`snapshot`* `-path` *`file_path`* `-start-byte` *`starting_byte`* `-byte-count` *`byte_count`*

   El desplazamiento de bytes de inicio y el número de bytes deben ser múltiplos de 4,096.

   En el ejemplo siguiente se restauran los primeros 4,096 bytes del archivo `myfile.txt`:

```
cluster1::> volume snapshot partial-restore-file -vserver vs0 -volume
vol1 -snapshot daily.2013-01-25_0010 -path /myfile.txt -start-byte 0
-byte-count 4096
```

Restaure el contenido de un volumen de una copia Snapshot

Puede utilizar el `volume snapshot restore` Comando para restaurar el contenido de un volumen desde una copia Snapshot.

Acerca de esta tarea

Si el volumen tiene relaciones de SnapMirror, replique manualmente todas las copias de reflejo del volumen inmediatamente después de restaurar desde una copia de Snapshot. Si no lo hace, puede provocar copias reflejadas inutilizables que se deban eliminar y volver a crear.

1. Enumere las copias Snapshot en un volumen:

   `volume snapshot show -vserver` *`SVM`* `-volume` *`volume`*

   El ejemplo siguiente muestra las copias Snapshot en `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1  vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Restaure el contenido de un volumen de una copia Snapshot:

   `volume snapshot restore -vserver` *`SVM`* `-volume` *`volume`* `-snapshot` *`snapshot`*

   En el ejemplo siguiente se restaura el contenido de `vol1`:

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1 -snapshot
daily.2013-01-25_0010
```

Replicación de volúmenes de SnapMirror

Conceptos básicos de la recuperación ante desastres de SnapMirror asíncrono

SnapMirror es la tecnología de recuperación ante desastres diseñada para la conmutación al nodo de respaldo del almacenamiento principal al secundario en un sitio geográficamente remoto. Como su nombre indica, SnapMirror crea una réplica, o *mirror,* de sus datos de trabajo en el almacenamiento secundario desde el cual puede continuar proporcionando datos en caso de catástrofe en el sitio principal.

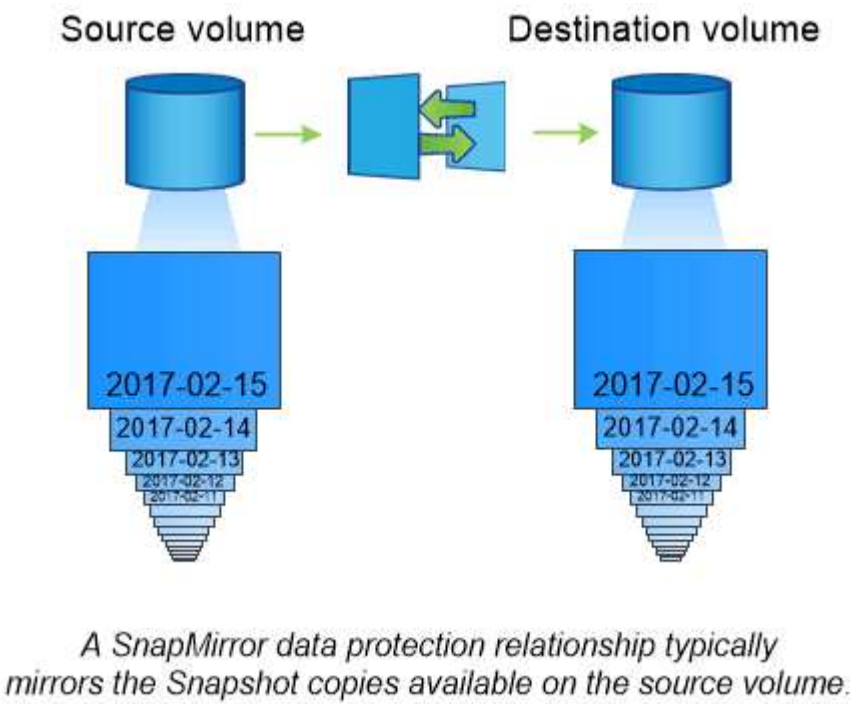
Si el sitio primario sigue disponible para servir datos, sólo tiene que transferir cualquier dato que necesite y no facilitar el servicio a los clientes del espejo. Como se indica en el caso de uso de conmutación por error, las controladoras del sistema secundario deben ser equivalentes o casi equivalentes a las controladoras del sistema primario para servir datos de forma eficiente desde el almacenamiento reflejado.

Relaciones de protección de datos

Los datos se reflejan en el nivel de volumen. La relación entre el volumen de origen del almacenamiento primario y el volumen de destino del almacenamiento secundario se denomina «relación de protección de datos»._ los clústeres en los que residen los volúmenes y las SVM que sirven datos de los volúmenes deben tener una relación entre iguales._ Una relación entre iguales permite que los clústeres y las SVM se intercambien datos con seguridad.

"Relaciones entre iguales de clústeres y SVM"

La siguiente figura muestra las relaciones de protección de datos de SnapMirror.



Ámbito de las relaciones de protección de datos

Puede crear una relación de protección de datos directamente entre los volúmenes o entre las SVM que poseen los volúmenes. En una relación de protección de datos _SVM, se replica toda la configuración de SVM o parte de ella, desde las exportaciones NFS y los recursos compartidos de SMB a RBAC, así como los datos de los volúmenes que posee la SVM.

También puede utilizar SnapMirror para aplicaciones especiales de protección de datos:

- Una copia *mirror* de uso compartido de la carga del volumen raíz de la SVM garantiza que los datos permanecen accesibles en caso de interrupción del servicio o conmutación por error de un nodo.
- Una relación de protección de datos entre *SnapLock Volumes* permite replicar los archivos WORM en el almacenamiento secundario.

  "Archivado y cumplimiento de normativas con tecnología SnapLock"

- A partir de ONTAP 9.13.1, se puede utilizar SnapMirror asíncrono para proteger grupos de consistencia. A partir de ONTAP 9.14.1, se puede utilizar SnapMirror asíncrono para replicar copias Snapshot granulares de volúmenes en el clúster de destino mediante la relación del grupo de coherencia. Para obtener más información, consulte Configurar la protección asíncrona de SnapMirror.

Cómo se inicializan las relaciones de protección de datos de SnapMirror

La primera vez que se invoca SnapMirror, se realiza una transferencia *baseline* del volumen de origen al volumen de destino. La directiva *SnapMirror* de la relación define el contenido de la línea base y las actualizaciones.

Transferencia completa con la política de SnapMirror predeterminada `MirrorAllSnapshots` implica los siguientes pasos:

- Haga una copia Snapshot del volumen de origen.
- Transfiera la copia Snapshot y todos los bloques de datos que hace referencia al volumen de destino.
- Transferir las copias snapshot restantes y menos recientes del volumen de origen al volumen de destino para su uso en caso de que el espejo «activo» esté dañado.

Cómo se actualizan las relaciones de protección de datos de SnapMirror

Las actualizaciones son asíncronas, según la programación configurada. La retención refleja la política de Snapshot en el origen.

En cada actualización bajo `MirrorAllSnapshots` Política, SnapMirror crea una copia Snapshot del volumen de origen y transfiere esa copia Snapshot y todas las copias Snapshot que se hayan realizado desde la última actualización. En el siguiente resultado de la `snapmirror policy show` comando para `MirrorAllSnapshots` política, tenga en cuenta lo siguiente:

- `Create Snapshot` es «'verdadero'», lo que lo indica `MirrorAllSnapshots` Crea una copia Snapshot cuando SnapMirror actualiza la relación.
- `MirrorAllSnapshots` Dispone de las reglas «m_creado» y «'all_source_snapshots», lo cual indica que tanto la copia snapshot creada por SnapMirror como cualquier copia snapshot realizada desde la última actualización se transfieren cuando SnapMirror actualiza la relación.

```
cluster_dst::> snapmirror policy show -policy MirrorAllSnapshots -instance

                     Vserver: vs0
      SnapMirror Policy Name: MirrorAllSnapshots
      SnapMirror Policy Type: async-mirror
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: true
                     Comment: Asynchronous SnapMirror policy for mirroring
all snapshots
                              and the latest active file system.
       Total Number of Rules: 2
                  Total Keep: 2
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
                              all_source_snapshots    1  false       0 -
-
```

Política de MirrorLatest

Preconfigurados `MirrorLatest` la política funciona exactamente de la misma manera que `MirrorAllSnapshots`, Excepto que sólo la copia snapshot creada por SnapMirror se transfiere al inicializar y actualizar.

```
                        Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                               ----------------     ----  -------- ----
-------- ------
                               sm_created              1  false       0 -
-
```

Conceptos básicos de la recuperación ante desastres de SnapMirror Synchronous

A partir de ONTAP 9.5, la tecnología SnapMirror síncrono (SM-S) es compatible con todas las plataformas FAS y AFF que tengan al menos 16 GB de memoria y en todas las plataformas ONTAP Select. La tecnología SnapMirror Synchronous es una función con licencia por nodo que proporciona replicación de datos síncrona a nivel de volumen.

Esta funcionalidad aborda las normativas regulatorias y nacionales para la replicación síncrona en sectores financieros, sanitarios y otros regulados, en los que no es necesaria una pérdida de datos nula.

Operaciones síncronas de SnapMirror permitidas

El límite del número de operaciones de replicación síncrona de SnapMirror por par de alta disponibilidad depende del modelo de controladora.

En la siguiente tabla, se enumera el número de operaciones de SnapMirror Synchronous que se permiten por par de alta disponibilidad en función del tipo de plataforma y la versión ONTAP.

Plataforma	Versiones anteriores a ONTAP 9.9.1	ONTAP 9.9.1	ONTAP 9.10.1	ONTAP 9.11.1 a ONTAP 9.14.1
AFF	80	160	200	400
ASA	80	160	200	400
FAS	40	80	80	80
ONTAP Select	20	40	40	40

Funciones admitidas

La siguiente tabla indica las funciones compatibles con SnapMirror Synchronous y las versiones de ONTAP que admiten.

Función	Se admite la primera versión	Información adicional
Antivirus en el volumen primario de la relación de SnapMirror síncrono	ONTAP 9,6	
Replicación de copia Snapshot creada por la aplicación	ONTAP 9,7	Si una copia Snapshot se etiqueta con la etiqueta correspondiente en el momento de la `snapshot create` Funcionamiento, mediante la interfaz de línea de comandos o la API de ONTAP, SnapMirror Synchronous replica las copias Snapshot, tanto las creadas por el usuario como las creadas con scripts externos, tras desactivar las aplicaciones. Las copias Snapshot programadas creadas con una política de Snapshot no se replican. Para obtener más información sobre la replicación de copias Snapshot creadas por la aplicación, consulte el artículo de la base de conocimientos: "Cómo replicar las copias Snapshot de aplicación creadas con SnapMirror Synchronous".
Clonar eliminación automática	ONTAP 9,6	
Los agregados de FabricPool con política de organización en niveles de Ninguna, Snapshot o Automática son compatibles con el origen y el destino de SnapMirror síncrono.	ONTAP 9,5	El volumen de destino de un agregado de FabricPool no se puede establecer en la política de organización en niveles All.
FC	ONTAP 9,5	En todas las redes para las que la latencia no supere los 10ms ms
FC-NVMe	ONTAP 9,7	
Clones de archivo	ONTAP 9,7	
FPolicy en el volumen primario de la relación de SnapMirror síncrono	ONTAP 9,6	
Cuotas duras y flexibles en el volumen principal de la relación síncrona de SnapMirror	ONTAP 9,6	Las reglas de cuota no se replican en el destino; por lo tanto, la base de datos de cuotas no se replica en el destino.
Relaciones síncronas dentro del clúster	ONTAP 9.14.1	La alta disponibilidad se proporciona cuando los volúmenes de origen y de destino se encuentran en diferentes pares de alta disponibilidad. Si se desactiva todo el clúster, no será posible el acceso a los volúmenes hasta que se recupere el clúster. Las relaciones síncronas de SnapMirror dentro del clúster contribuirán al límite general de datos simultáneos Relaciones por pareja de alta disponibilidad.
ISCSI	ONTAP 9,5	
Clones LUN y clones de espacio de nombres NVMe	ONTAP 9,7	

Clones LUN respaldados por copias Snapshot creadas por la aplicación	ONTAP 9,7	
Acceso de protocolo mixto (NFS v3 y SMB)	ONTAP 9,6	
Restauración de NDMP/NDMP	ONTAP 9.13.1	El clúster de origen y de destino deben ejecutar ONTAP 9.13.1 o versiones posteriores para usar NDMP con SnapMirror síncrono. Para obtener más información, consulte Transferencia de datos mediante la copia ndmp.
Operaciones síncronas de SnapMirror (NDO) sin interrupciones en plataformas AFF/ASA, solo.	ONTAP 9.12.1	La compatibilidad con operaciones no disruptivas le permite realizar muchas tareas de mantenimiento comunes sin necesidad de programar un tiempo de inactividad. Las operaciones admitidas incluyen la toma de control y el retorno al nodo primario, y el movimiento de volúmenes, siempre y cuando haya un solo nodo superviviente entre cada uno de los dos clústeres.
NFS v4,2	ONTAP 9.10.1	
NFS v4,3	ONTAP 9,5	
NFS v4,0	ONTAP 9,6	
NFS v4,1	ONTAP 9,6	
NVMe/TCP	9.10.1	
Eliminación de una limitación elevada de la frecuencia de funcionamiento de metadatos	ONTAP 9,6	
Seguridad para datos confidenciales en tránsito con cifrado TLS 1.2	ONTAP 9,6	
Restauración parcial de archivos y archivos individuales	ONTAP 9.13.1	
SMB 2,0 o posterior	ONTAP 9,6	
Cascada de reflejo-reflejo síncrono de SnapMirror	ONTAP 9,6	La relación del volumen de destino de la relación de SnapMirror síncrono debe ser una relación de SnapMirror asíncrono.

Recuperación ante desastres de SVM	ONTAP 9,6	* Un origen de SnapMirror Synchronous también puede ser un origen de recuperación ante desastres de SVM, por ejemplo, una configuración ramificada con SnapMirror Synchronous como un tramo y recuperación ante desastres de SVM como el otro. * Un origen de SnapMirror Synchronous no puede ser un destino de recuperación ante desastres de SVM porque SnapMirror Synchronous no admite la configuración en cascada de un origen de protección de datos. Debe liberar la relación síncrona antes de ejecutar un cambio de sincronización de recuperación ante desastres de SVM en el clúster de destino. * Un destino de SnapMirror síncrono no puede ser un origen de recuperación ante desastres de SVM porque la recuperación ante desastres de SVM no admite la replicación de volúmenes de DP. Una resincronización flip del origen síncrono provocaría la recuperación ante desastres de SVM excepto el volumen DP en el clúster de destino.
Restauración basada en cinta al volumen de origen	ONTAP 9.13.1	
Paridad de marca de hora entre los volúmenes de origen y destino para NAS	ONTAP 9,6	Si se actualizó de ONTAP 9,5 a ONTAP 9,6, la marca de tiempo se replica solo para todos los archivos nuevos y modificados en el volumen de origen. La Marca de hora de los archivos existentes en el volumen de origen no está sincronizada.

Funciones no admitidas

Las siguientes funciones no se admiten con las relaciones de SnapMirror síncrono:

- Grupos de consistencia
- Sistemas DPO optimizados para DP
- Volúmenes de FlexGroup
- Volúmenes de FlexCache
- Limitación global
- En una configuración de dispersión, solo una relación puede ser una relación de SnapMirror síncrono; todas las demás relaciones del volumen de origen deben ser relaciones de SnapMirror asíncronas.
- Movimiento de LUN
- Configuraciones de MetroCluster
- Acceso SAN y NVMe mixto
  El mismo volumen o SVM no admiten espacios de nombres LUN y NVMe.
- SnapCenter
- Volúmenes de SnapLock

- Copias Snapshot a prueba de manipulaciones
- Backup a cinta o restauración con volcado y SMTape en el volumen de destino
- Piso de rendimiento (QoS mín.) para volúmenes de origen
- SnapRestore de volumen
- VVol

Modos de funcionamiento

SnapMirror Synchronous tiene dos modos de funcionamiento basados en el tipo de política de SnapMirror utilizada:

- **Modo de sincronización**
  En el modo de sincronización, las operaciones de I/O de la aplicación se envían en paralelo al primario y el secundario
  sistemas de almacenamiento. Si la escritura en el almacenamiento secundario no se realiza por ningún motivo, se permite que la aplicación continúe escribiendo en el almacenamiento principal. Una vez corregida la condición de error, la tecnología SnapMirror Synchronous vuelve a sincronizar automáticamente con el almacenamiento secundario y reanuda la replicación del almacenamiento principal al almacenamiento secundario en modo síncrono.
  En el modo síncrono, RPO=0 y RTO son muy bajos hasta que se produce un fallo de replicación secundaria en el momento en el que el objetivo de punto de recuperación y el objetivo de tiempo de recuperación se vuelven indeterminados, pero igual que el tiempo para reparar el problema que provocó un error en la replicación secundaria y para finalizar la resincronización.
- **Modo StrictSync**
  SnapMirror Synchronous puede funcionar opcionalmente en el modo StrictSync. Si la escritura en el almacenamiento secundario no se completa por ningún motivo, las operaciones de I/o de la aplicación fallan y, por lo tanto, se garantiza que el almacenamiento primario y secundario sean idénticos. Las operaciones de I/o de la aplicación en el principal se reanudan solo una vez que la relación de SnapMirror se devuelve a la `InSync` estado. Si falla el almacenamiento primario, se pueden reanudar las operaciones de I/o de la aplicación en el almacenamiento secundario después de la conmutación por error, sin pérdida de datos.
  En el modo StrictSync, el objetivo de punto de recuperación es siempre cero y el objetivo de tiempo de recuperación es muy bajo.

Estado de la relación

El estado de una relación de SnapMirror Synchronous siempre está en la `InSync` estado durante el funcionamiento normal. Si por algún motivo la transferencia de SnapMirror falla, el destino no está sincronizado con el origen y puede ir a la `OutofSync` estado.

Para las relaciones de SnapMirror Synchronous, el sistema comprueba automáticamente el estado de la relación `InSync` o. `OutofSync`) a un intervalo fijo. Si el estado de la relación es `OutofSync`, ONTAP activa automáticamente el proceso de resincronización automática para devolver la relación al `InSync` estado. La resincronización automática se activa solo si la transferencia falla debido a alguna operación, como la conmutación por error no planificada del almacenamiento en el origen o en el destino, o una interrupción del servicio de red. Operaciones iniciadas por el usuario como, por ejemplo `snapmirror quiesce` y.. `snapmirror break` no active la resincronización automática.

Si el estado de la relación es `OutofSync` Para una relación de SnapMirror Synchronous en el modo StrictSync, se detienen todas las operaciones de I/o del volumen primario. La `OutofSync` el estado de la relación SnapMirror Synchronous en el modo Sync no genera interrupciones en el volumen primario, y se

permiten las operaciones de I/o en el volumen primario.

Información relacionada

"Informe técnico de NetApp 4733: Prácticas recomendadas y configuración de SnapMirror síncrono"

Acerca de las cargas de trabajo compatibles con las políticas de StrictSync y Sync

Las políticas de StrictSync y Sync admiten todas las aplicaciones basadas en LUN con los protocolos FC, iSCSI y FC-NVMe, así como los protocolos NFSv3 y NFSv4 para aplicaciones empresariales como bases de datos, VMware, Quota, SMB, etc. A partir de ONTAP 9.6, SnapMirror Synchronous se puede utilizar para servicios de archivos empresariales como los de automatización de diseño electrónico (EDA), directorios iniciales y cargas de trabajo de creación de software.

En ONTAP 9.5, para una política de sincronización, debe tener en cuenta algunos aspectos importantes a la vez que selecciona las cargas de trabajo NFSv3 o NFSv4. No se tiene en cuenta la cantidad de datos que realizan las operaciones de lectura o escritura por parte de las cargas de trabajo, ya que la política de sincronización puede gestionar cargas de trabajo de lectura o escritura elevadas. En ONTAP 9.5, las cargas de trabajo que tienen una creación de archivos, una creación de directorios, cambios de permisos de archivos o cambios de permisos de directorio pueden no ser adecuadas (estas se denominan cargas de trabajo con metadatos elevados). Un ejemplo típico de una carga de trabajo con metadatos altos es una carga de trabajo de DevOps en la que se crean varios archivos de prueba, se ejecuta la automatización y se eliminan los archivos. Otro ejemplo es la carga de trabajo de compilación paralela que genera varios archivos temporales durante la compilación. El impacto de una tasa alta de la actividad de metadatos de escritura es que puede provocar que la sincronización entre los reflejos se rompa temporalmente, lo que bloquea la I/o de lectura y escritura del cliente.

A partir de ONTAP 9.6, se eliminan estas limitaciones y se puede utilizar SnapMirror Synchronous para las cargas de trabajo de servicios de archivos empresariales que incluyen entornos de varios usuarios, como directorios iniciales y cargas de trabajo de compilación de software.

Información relacionada

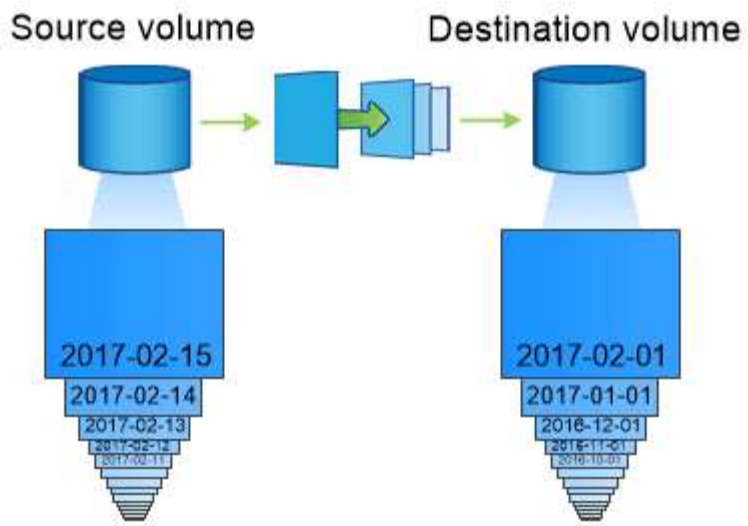
"Configuración síncrona de SnapMirror y prácticas recomendadas"

Archivado de vault con tecnología SnapMirror

Las políticas de almacén de SnapMirror sustituyen a la tecnología SnapVault en ONTAP 9.3 y versiones posteriores. Se utiliza una política de almacén de SnapMirror para la replicación de copias Snapshot de disco a disco para el cumplimiento de normativas y otros fines relacionados con la gobernanza. A diferencia de la relación de SnapMirror, en la que el destino normalmente solo contiene las copias Snapshot que actualmente se encuentran en el volumen de origen, un destino de almacén normalmente conserva las copias Snapshot puntuales creadas durante un período mucho más largo.

Es posible que desee conservar copias Snapshot mensuales de sus datos en un plazo de 20 años, por ejemplo, para cumplir con las normativas de contabilidad gubernamental de su empresa. Como no hay necesidad de servir datos desde un almacenamiento de almacén, puede utilizar discos más lentos y menos costosos en el sistema de destino.

La siguiente figura muestra las relaciones de protección de datos de SnapMirror Vault.



A SnapVault data protection relationship typically retains point-in-time Snapshot copies created over a longer period than the Snapshot copies on the source volume.

Cómo se inicializan las relaciones de protección de datos del almacén

La política de SnapMirror para la relación define el contenido de la línea de base y cualquier actualización.

Una transferencia de línea de base en la política de almacén predeterminada `XDPDefault` Realiza una copia Snapshot del volumen de origen, luego transfiere esa copia y los bloques de datos que hace referencia al volumen de destino. A diferencia de las relaciones de SnapMirror, un backup de almacén no incluye copias Snapshot anteriores en la base.

Cómo se actualizan las relaciones de protección de datos de almacén

Las actualizaciones son asíncronas, según la programación configurada. Las reglas que defina en la política para la relación identifican qué nuevas copias Snapshot deben incluir en las actualizaciones y cuántas copias deben retener. Las etiquetas definidas en la política ("mensual", por ejemplo) deben coincidir con una o más etiquetas definidas en la política de Snapshot en la fuente. De lo contrario, la replicación falla.

En cada actualización bajo `XDPDefault` Política, SnapMirror transfiere copias Snapshot que se han realizado desde la última actualización, siempre que tengan las etiquetas que coincidan con las etiquetas definidas en las reglas de la política. En el siguiente resultado de la `snapmirror policy show` comando para `XDPDefault` política, tenga en cuenta lo siguiente:

- `Create Snapshot` es «falso», lo que lo indica `XDPDefault` No crea una copia Snapshot cuando SnapMirror actualiza la relación.
- `XDPDefault` Dispone de reglas «diaria» y «semanal», que indican que todas las copias Snapshot con etiquetas coincidentes del origen se transfieren cuando SnapMirror actualiza la relación.

```
cluster_dst::> snapmirror policy show -policy XDPDefault -instance

                     Vserver: vs0
      SnapMirror Policy Name: XDPDefault
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Default policy for XDP relationships with
daily and weekly
                              rules.
       Total Number of Rules: 2
                  Total Keep: 59
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              daily                   7  false       0 -
-
                              weekly                 52  false       0 -
-
```

Conceptos básicos de la replicación unificada de SnapMirror

SnapMirror *Unified replication* permite configurar la recuperación ante desastres y el archivado en el mismo volumen de destino. Cuando la replicación unificada es apropiada, ofrece ventajas en la reducción de la cantidad de almacenamiento secundario que se necesita, lo que limita el número de transferencias básicas y reduce el tráfico de red.

Cómo se inicializan las relaciones de protección de datos unificadas

Al igual que sucede con SnapMirror, la protección de datos unificada realiza una transferencia de referencia la primera vez que se invoca. La política de SnapMirror para la relación define el contenido de la línea de base y cualquier actualización.

Una transferencia completa con la política de protección de datos unificada predeterminada `MirrorAndVault` Realiza una copia Snapshot del volumen de origen, luego transfiere esa copia y los bloques de datos que hace referencia al volumen de destino. Al igual que el archivado de almacenes, la protección de datos unificada no incluye copias Snapshot anteriores en la referencia.

Cómo se actualizan las relaciones de protección de datos unificadas

En cada actualización bajo `MirrorAndVault` Política, SnapMirror crea una copia Snapshot del volumen de origen y transfiere esa copia Snapshot y todas las copias Snapshot que se hayan realizado desde la última actualización, siempre que tengan las etiquetas que coincidan con los definidos en las reglas de la política de Snapshot. En el siguiente resultado de la `snapmirror policy show` comando para `MirrorAndVault` política, tenga en cuenta lo siguiente:

- `Create Snapshot` es «'verdadero'», lo que lo indica `MirrorAndVault` Crea una copia Snapshot cuando SnapMirror actualiza la relación.
- `MirrorAndVault` Dispone de las reglas «m_creado», «diario» y «semanal», que indican que tanto la copia snapshot creada por SnapMirror como las copias Snapshot con etiquetas coincidentes en el origen se transfieren cuando SnapMirror actualiza la relación.

```
cluster_dst::> snapmirror policy show -policy MirrorAndVault -instance

                     Vserver: vs0
      SnapMirror Policy Name: MirrorAndVault
      SnapMirror Policy Type: mirror-vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: true
                     Comment: A unified Synchronous SnapMirror and
SnapVault policy for
                              mirroring the latest file system and daily
and weekly snapshots.
       Total Number of Rules: 3
                  Total Keep: 59
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
                              daily                   7  false       0 -
-
                              weekly                 52  false       0 -
-
```

Política Unified7year

Preconfigurados `Unified7year` la política funciona exactamente de la misma manera que `MirrorAndVault`, Excepto que una cuarta regla transfiere copias snapshot mensuales y las conserva

durante siete años.

```
                        Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                               ----------------     ----  -------- ----
-------- ------
                               sm_created              1  false       0 -
-
                               daily                   7  false       0 -
-
                               weekly                 52  false       0 -
-
                               monthly                84  false       0 -
-
```

Proporcionar protección frente a una posible corrupción de datos

La replicación unificada limita el contenido de la transferencia básica a la copia de Snapshot creada por SnapMirror en el momento de la inicialización. En cada actualización, SnapMirror crea otra copia Snapshot del origen y transfiere esa copia Snapshot y todas las copias Snapshot nuevas que tengan las etiquetas que coincidan con los definidos en las reglas de la política de Snapshot.

Puede protegerse contra la posibilidad de que una copia Snapshot actualizada esté dañada al crear una copia de la última copia Snapshot transferida en el destino. Esta «copia local» se conserva independientemente de las reglas de retención del origen, de modo que, aunque la copia Snapshot transferida mediante SnapMirror ya no esté disponible en el origen, dicha copia estará disponible en el destino.

Cuándo utilizar la replicación de datos unificada

Debe sopesar las ventajas que supone mantener una copia completa frente a las ventajas que ofrece la replicación unificada para reducir la cantidad de almacenamiento secundario, limitar el número de transferencias básicas y reducir el tráfico de red.

El factor clave para determinar la idoneidad de la replicación unificada es la tasa de cambio del sistema de archivos activo. Un reflejo tradicional puede ser más adecuado para un volumen que contiene copias Snapshot cada hora de los registros de transacciones de las bases de datos, por ejemplo.

XDP sustituye a DP como la opción predeterminada de SnapMirror

A partir de ONTAP 9.3, el modo de protección de datos ampliada (XDP) de SnapMirror sustituye al modo de protección de datos (DP) de SnapMirror como valor predeterminado.

Antes de actualizar a ONTAP 9.12.1, debe convertir las relaciones de tipo DP existentes a XDP antes de poder actualizar a ONTAP 9.12.1 y versiones posteriores. Para obtener más información, consulte "Convierta una relación de tipo DP existente a XDP".

Hasta ONTAP 9.3, SnapMirror invocado en modo DP y SnapMirror invocado en modo XDP utilizaba distintos motores de replicación, con distintos enfoques respecto a la dependencia de versión:

- SnapMirror que se invoca en el modo DP utilizaba un motor de replicación *version-dependent* en el que la versión de ONTAP debía ser la misma en el almacenamiento primario y secundario:

```
cluster_dst::>  snapmirror create -type DP -source-path ... -destination
-path ...
```

- SnapMirror, al que se invocó en el modo XDP, utilizó un motor de replicación de *version-flexible* que admitía diferentes versiones de ONTAP en el almacenamiento primario y secundario:

```
cluster_dst::>  snapmirror create -type XDP -source-path ...
-destination-path ...
```

Las importantes ventajas de SnapMirror, que ofrece una versión flexible, superan la ligera ventaja del rendimiento de la replicación obtenido con el modo basado en la versión. Por este motivo, a partir de ONTAP 9.3, se ha creado el modo XDP como nuevo valor predeterminado, y cualquier invocación del modo DP en la línea de comandos o en scripts nuevos o existentes se convierte automáticamente al modo XDP.

Las relaciones existentes no se ven afectadas. Si una relación ya es del tipo DP, seguirá siendo del tipo DP. A partir de ONTAP 9.5, MirrorAndVault es la nueva política predeterminada cuando no se especifica ningún modo de protección de datos o cuando se especifica el modo XDP como tipo de relación. La siguiente tabla muestra el comportamiento que puede esperar.

Si especifica…	El tipo es…	La política predeterminada (si no se especifica una política) es…
PROTECCIÓN DE DATOS	XDP	MirrorAllSnapshots (recuperación ante desastres de SnapMirror)
Nada	XDP	MirrorAndVault (replicación unificada)
XDP	XDP	MirrorAndVault (replicación unificada)

Como se muestra en la tabla, las directivas predeterminadas asignadas a XDP en circunstancias diferentes garantizan que la conversión mantenga la equivalencia funcional de los tipos antiguos. Por supuesto, puede utilizar diferentes políticas según sea necesario, incluidas las políticas para la replicación unificada:

Si especifica…	Y la política es…	El resultado es…
PROTECCIÓN DE DATOS	MirrorAllSnapshots	Recuperación ante desastres de SnapMirror
XDPDefault	SnapVault	Reflejo de AndVault
Replicación unificada	XDP	MirrorAllSnapshots

Recuperación ante desastres de SnapMirror	XDPDefault	SnapVault

Las únicas excepciones a la conversión son las siguientes:

- Las relaciones de protección de datos de SVM siguen siendo las predeterminadas para el modo DP en ONTAP 9.3 y versiones anteriores.

  A partir de ONTAP 9.4, las relaciones de protección de datos de la SVM se establecen en el modo XDP de manera predeterminada.

- Las relaciones de protección de datos con uso compartido de carga de volumen raíz continúan hasta los valores predeterminados en el modo DP.
- Las relaciones de protección de datos de SnapLock continúan en el modo DP de ONTAP 9.4 y versiones anteriores.

  A partir de ONTAP 9.5, las relaciones de protección de datos de SnapLock se establecen en el modo XDP de manera predeterminada.

- Las invocaciones explícitas de DP siguen en el modo DP de forma predeterminada si establece la siguiente opción para todo el clúster:

  ```
  options replication.create_data_protection_rels.enable on
  ```

  Esta opción se ignora si no invoca explícitamente DP.

Cuando un volumen de destino aumenta automáticamente

Durante una transferencia de mirroring para la protección de datos, el volumen de destino aumenta automáticamente su tamaño si se ha incrementado el volumen de origen, siempre y cuando haya espacio disponible en el agregado que contiene el volumen.

Este comportamiento se produce independientemente de cualquier configuración de crecimiento automático en el destino. No es posible limitar el crecimiento del volumen ni evitar que ONTAP lo haga.

De manera predeterminada, los volúmenes de protección de datos se establecen en `grow_shrink` el modo autosize, que permite que el volumen crezca o se reduzca en respuesta a la cantidad de espacio usado. El tamaño máximo automático de los volúmenes de protección de datos es igual al tamaño máximo de FlexVol y depende de la plataforma. Por ejemplo:

- FAS6220, volumen DP predeterminado máx.-autosize = 70 TB
- FAS8200, volumen DP predeterminado máx.-autosize = 100 TB

Para obtener más información, consulte "Hardware Universe de NetApp".

Puestas en marcha de protección de datos en cascada y distribución ramificada

Puede utilizar una implementación de *fan-out* para ampliar la protección de datos a

varios sistemas secundarios. Puede utilizar una implementación *Cascade* para ampliar la protección de datos a sistemas terciarios.

Tanto las puestas en marcha en cascada como de distribución ramificada admiten cualquier combinación de recuperación ante desastres de SnapMirror, SnapVault o replicación unificada. Sin embargo, las relaciones de SnapMirror síncrono (compatibles a partir de ONTAP 9.5) solo admiten puestas en marcha en cascada con una o más relaciones de SnapMirror asíncronas y no admiten puestas en marcha en cascada. Solo una relación en la configuración de dispersión puede ser una relación de SnapMirror síncrono, todas las demás relaciones del volumen de origen deben ser relaciones de SnapMirror asíncronas. Continuidad del negocio de SnapMirror (Se admite a partir de ONTAP 9.8) también admite configuraciones de dispersión.

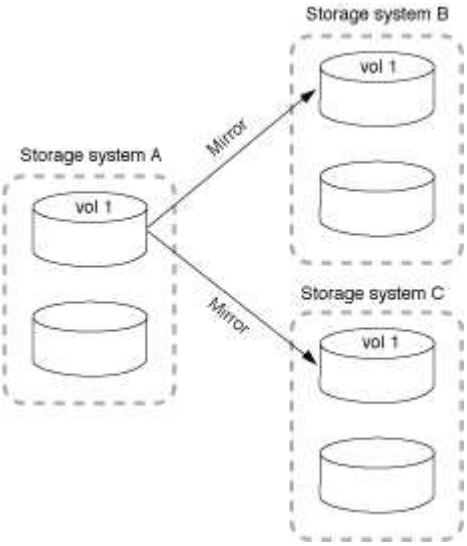
> Puede utilizar una implementación *fan-in* para crear relaciones de protección de datos entre varios sistemas principales y un único sistema secundario. Cada relación debe usar un volumen diferente en el sistema secundario.

> Debe saber que los volúmenes que forman parte de una configuración ramificada o en cascada pueden tardar más en
> resincronizar. No es poco frecuente ver los informes de relaciones de SnapMirror
> el estado de preparación para un período de tiempo extendido.

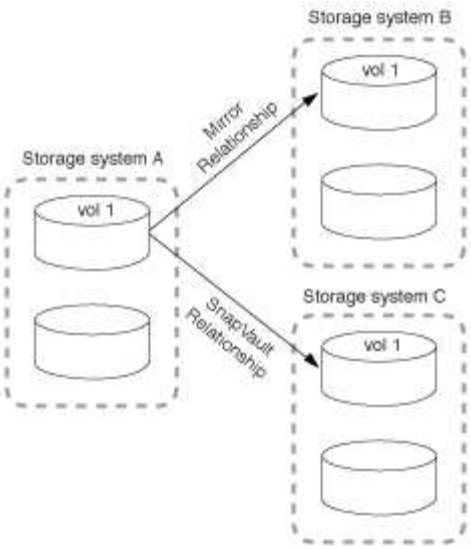
Cómo funcionan las implementaciones de dispersión

SnapMirror admite la puesta en marcha de «varios duplicados_ y de «mirror-vault» con «fan-out».

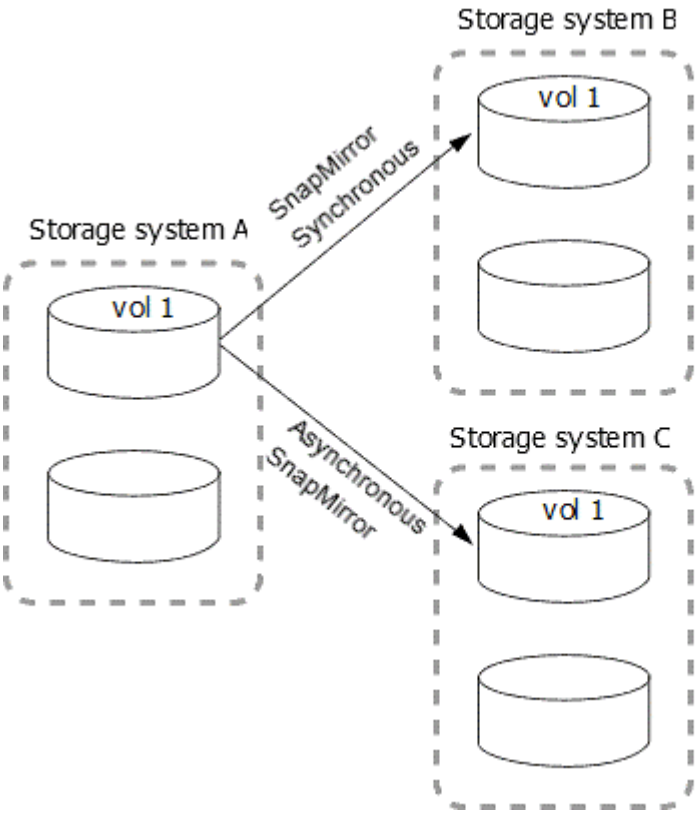
Una puesta en marcha de «fan-out» de varios reflejos consiste en un volumen de origen que tiene una relación de reflejo con varios volúmenes secundarios.



Una implementación de «fan-out» de reflejo-almacén consta de un volumen de origen que tiene una relación de mirroring con un volumen secundario y una relación de SnapVault con otro volumen secundario.



A partir de ONTAP 9.5, puede tener implementaciones de dispersión con relaciones de SnapMirror síncrono; sin embargo, solo una relación de la configuración de dispersión puede ser una relación de SnapMirror síncrono, todas las demás relaciones del volumen de origen deben ser relaciones de SnapMirror asíncronas.

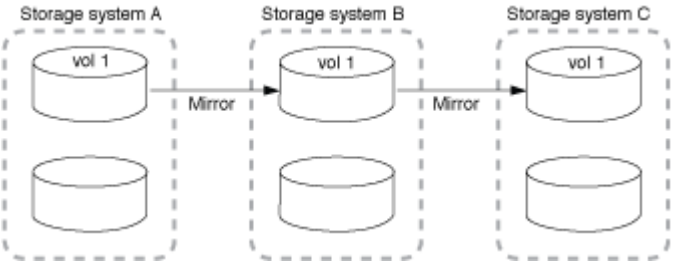


Cómo funcionan las implementaciones en cascada

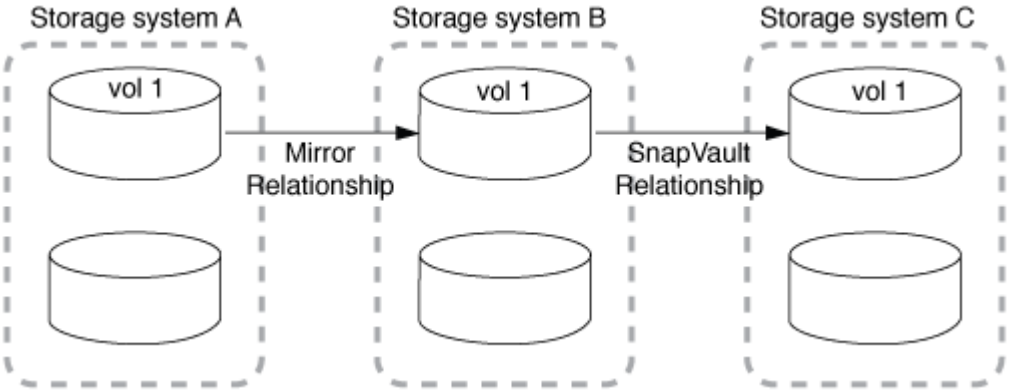
SnapMirror admite puestas en marcha en cascada de *mirror-mirror*, *mirror-vault*, *vault-mirror* y *vault-vault*.

Una puesta en marcha en cascada de reflejos consiste en una cadena de relaciones en las que un volumen de origen se refleja en un volumen secundario, mientras que el volumen secundario se duplica en un volumen terciario. Si el volumen secundario deja de estar disponible, puede sincronizar la relación entre los volúmenes primario y terciario sin necesidad de realizar una nueva transferencia de base de referencia.

A partir de ONTAP 9.6, se admiten las relaciones SnapMirror síncrono en una puesta en marcha en cascada de reflejos. Solo los volúmenes primario y secundario pueden estar en una relación de SnapMirror Synchronous. La relación entre los volúmenes secundarios y los volúmenes terciarios debe ser asíncrona.



Una puesta en marcha en cascada de copias-vault consta de una cadena de relaciones en las que un volumen de origen se refleja en un volumen secundario y el volumen secundario se realiza en un volumen terciario.



También se admiten operaciones de mirroring de vault y, a partir de ONTAP 9.2, puestas en marcha en cascada de vault-vault:

- Una puesta en marcha en cascada de reflejos de almacén consta de una cadena de relaciones en las que se realiza un volumen de origen en un volumen secundario, mientras que el volumen secundario se duplica en un volumen terciario.
- (A partir de ONTAP 9.2) una puesta en marcha en cascada de vault consta de una cadena de relaciones en las que se realiza una copia vault de un volumen de origen a un volumen secundario y a la que se realiza la copia del volumen secundario en un volumen terciario.

Lecturas adicionales

- Reanude la protección en una configuración de salida de ventilador con SM-BC

Licencias de SnapMirror

Información general sobre la licencia de SnapMirror

A partir de ONTAP 9.3, se ha simplificado la licencia para la replicación entre instancias de ONTAP. En las versiones ONTAP 9, la licencia de SnapMirror admite tanto relaciones de almacén como de mirroring. Puede usar una licencia de SnapMirror para admitir la replicación de ONTAP tanto en casos prácticos de backup como de recuperación ante desastres.

Antes de la versión 9,3 de ONTAP, era necesaria una licencia independiente de SnapVault para configurar las

relaciones *vault* entre las instancias de ONTAP, donde la instancia de DP podía retener una mayor cantidad de copias de Snapshot para admitir casos de uso de backup con tiempos de retención más largos, y se necesitaba una licencia de SnapMirror para configurar las relaciones *mirror* entre las instancias de ONTAP, en las que cada instancia de ONTAP mantendría el mismo número de copias de Snapshot (es decir, una imagen *mirror*) para admitir casos de uso de recuperación ante desastres para hacer posible la recuperación tras fallos de clústeres. Las licencias de SnapMirror y SnapVault siguen usándose y son compatibles con las versiones de ONTAP 8.x y 9.x.

Aunque las licencias de SnapVault siguen funcionando y son compatibles con las versiones ONTAP 8.x y 9.x, la licencia de SnapMirror puede usarse en lugar de una licencia de SnapVault y puede usarse para configuraciones de mirroring y almacén.

Para la replicación asíncrona de ONTAP, a partir de ONTAP 9.3, se usa un único motor de replicación unificado para configurar las políticas de modo de protección de datos ampliado (XDP), donde la licencia de SnapMirror se puede configurar para una política de mirroring, una normativa de almacén o una política de mirroring-almacén. Se requiere una licencia de SnapMirror en los clústeres de origen y destino. Una licencia de SnapVault no es necesaria si ya se ha instalado una licencia de SnapMirror. La licencia perpetua asíncrona de SnapMirror se incluye en la suite de software ONTAP One que está instalada en los nuevos sistemas AFF y FAS.

Los límites de configuración de protección de datos se determinan por varios factores, como la versión de ONTAP, la plataforma de hardware y las licencias instaladas. Para obtener más información, consulte "Hardware Universe".

Licencia de SnapMirror Synchronous

A partir de ONTAP 9.5, se admiten las relaciones de SnapMirror síncrono. Requiere las siguientes licencias para crear una relación de SnapMirror síncrono:

- Se requiere la licencia de SnapMirror Synchronous en el clúster de origen y en el de destino.

  La licencia de SnapMirror Synchronous forma parte de la "Suite de licencia ONTAP ONE".

  Si su sistema fue adquirido antes del 2019 de junio con un paquete Premium o Flash, puede descargar una clave maestra de NetApp para obtener la licencia de SnapMirror Synchronous necesaria en el sitio de soporte de NetApp: "Claves de licencia principal".

- Se requiere la licencia de SnapMirror en los clústeres de origen y destino.

Licencia de SnapMirror Cloud

A partir de ONTAP 9.8, la licencia Cloud de SnapMirror proporciona la replicación asíncrona de copias Snapshot de instancias de ONTAP a extremos de almacenamiento de objetos. Los destinos de replicación se pueden configurar usando almacenes de objetos locales, así como servicios de almacenamiento de objetos en cloud público compatibles con S3 y S3. Los sistemas ONTAP admiten relaciones de cloud de SnapMirror para destinos de almacenamiento de objetos preconfigurados.

SnapMirror Cloud no está disponible como licencia independiente. Solo se necesita una licencia por clúster ONTAP. Además de una licencia de SnapMirror Cloud, también se necesita la licencia asíncrona de SnapMirror.

Requiere las siguientes licencias para crear una relación de cloud de SnapMirror:

- Tanto una licencia de SnapMirror como una licencia de SnapMirror Cloud para replicar directamente en el extremo del almacén de objetos.

- Cuando se configura un flujo de trabajo de replicación de varias políticas (por ejemplo, disco a disco y al cloud), se requiere una licencia de SnapMirror en todas las instancias de ONTAP, mientras que la licencia de SnapMirror Cloud solo se requiere para el clúster de origen que se replica directamente en el extremo de almacenamiento de objetos.

A partir de ONTAP 9,9.1, puede hacerlo "Utilice System Manager para la replicación de SnapMirror Cloud".

En la página web de NetApp se publica una lista de aplicaciones de terceros autorizadas de SnapMirror Cloud.

Licencia optimizada de Data Protection

Las licencias de protección de datos optimizada (DPO) ya no se venden y DPO no es compatible con las plataformas actuales; sin embargo, si tiene una licencia DPO instalada en una plataforma compatible, NetApp sigue ofreciendo soporte hasta el fin de la disponibilidad de dicha plataforma.

DPO no se incluye con el paquete de licencia ONTAP One y no se puede actualizar al paquete de licencia ONTAP One si la licencia DPO está instalada en un sistema.

Para obtener más información sobre las plataformas compatibles, consulte "Hardware Universe".

Instalar las licencias de SnapMirror Cloud

Las relaciones de SnapMirror Cloud se pueden orquestar con aplicaciones de backup de terceros cualificadas previamente. A partir de ONTAP 9,9.1, también puede usar System Manager para orquestar la replicación de SnapMirror Cloud. Tanto las licencias de capacidad de SnapMirror como de SnapMirror Cloud son necesarias al utilizar System Manager para orquestar backups de almacenamiento de objetos de ONTAP en las instalaciones. También deberás solicitar e instalar la licencia de SnapMirror Cloud API.

Acerca de esta tarea

Las licencias de SnapMirror Cloud y SnapMirror S3 son licencias de clúster, no licencias de nodos, por lo que se suministran *no* con el paquete de licencia ONTAP One. Estas licencias están incluidas en el paquete de compatibilidad ONTAP One aparte. Si desea habilitar SnapMirror Cloud, debe solicitar este paquete.

Además, la orquestación de System Manager de backups de SnapMirror Cloud en el almacenamiento de objetos requiere una clave de la API de SnapMirror Cloud. Esta licencia de API es una licencia para todo el clúster de instancia única, lo que significa que no es necesario instalarla en todos los nodos del clúster.

Pasos

Necesita solicitar y descargar el paquete de compatibilidad de ONTAP One y la licencia de API de SnapMirror Cloud y, posteriormente, instalarlos mediante System Manager.

1. Localice y registre el UUID de clúster del clúster para el que desea obtener licencia.

   El UUID de clúster se requiere cuando envía la solicitud para solicitar el bundle de compatibilidad ONTAP One para el clúster.

2. Póngase en contacto con su equipo de ventas de NetApp y solicite el paquete de compatibilidad de ONTAP One.
3. Solicite la licencia de la API de SnapMirror Cloud siguiendo las instrucciones que se proporcionan en el sitio de soporte de NetApp.

"Solicite la clave de licencia de SnapMirror Cloud API"

4. Cuando haya recibido y descargado los archivos de licencia, use System Manager para cargar al clúster la NLF de compatibilidad con cloud de ONTAP y la NLF de la API de cloud de SnapMirror:
   a. Haga clic en **clúster > Configuración**.
   b. En la ventana **Configuración**, haz clic en **Licencias**.
   c. En la ventana **Licencias**, haga clic en + Add .
   d. En el cuadro de diálogo **Agregar licencia**, haga clic en **examinar** para seleccionar el NLF que descargó y, a continuación, haga clic en **Agregar** para cargar el archivo en el clúster.

Información relacionada

"Realice backups de datos en el cloud con SnapMirror"

"Búsqueda de licencias de software de NetApp"

Los sistemas DPO ofrecen mejoras

A partir de ONTAP 9.6, el número máximo de volúmenes FlexVol admitidos aumenta cuando se instala la licencia DP_Optimized (DPO). A partir de la versión 9,4 de ONTAP, los sistemas con licencia DPO admiten el respaldo de SnapMirror, la deduplicación en segundo plano entre volúmenes, el uso de bloques Snapshot como donantes y la compactación.

A partir de ONTAP 9.6, se ha incrementado el número máximo admitido de volúmenes FlexVol en sistemas secundarios o de protección de datos, lo que permite escalar hasta 2,500 volúmenes FlexVol por nodo o hasta 5,000 en modo de conmutación por error. El aumento de los volúmenes de FlexVol se habilita con el "Licencia DP_Optimized (DPO)". A. "Licencia de SnapMirror" también se requiere en los nodos de origen y destino.

A partir de ONTAP 9.4, se realizan las siguientes mejoras en las funciones de los sistemas DPO:

- Backoff de SnapMirror: En sistemas DPO, el tráfico de replicación tiene la misma prioridad que se da a las cargas de trabajo del cliente.

  La funcionalidad de backup de SnapMirror está deshabilitada de forma predeterminada en los sistemas DPO.

- Deduplicación en segundo plano de volumen y deduplicación en segundo plano entre volúmenes: Se habilitan la deduplicación en segundo plano de volúmenes y la deduplicación en segundo plano entre volúmenes en sistemas DPO.

  Puede ejecutar el `storage aggregate efficiency cross-volume-dedupe start -aggregate` *`aggregate_name`* `-scan-old-data true` comando para deduplicar los datos existentes. La práctica recomendada es ejecutar el comando durante las horas de menor actividad para reducir el impacto en el rendimiento.

- Mayor ahorro usando los bloques Snapshot como donantes: Los bloques de datos que no están disponibles en el sistema de archivos activo, pero están atrapados en las copias Snapshot se utilizan como donantes para la deduplicación de volúmenes.

  Los datos nuevos pueden deduplicarse con los datos que estaban atrapados en las copias Snapshot, compartiendo de forma efectiva también los bloques Snapshot. El aumento del espacio de los donantes permite obtener más ahorro, especialmente cuando el volumen tiene un gran número de copias snapshot.

- Compactación: La compactación de datos está habilitada de forma predeterminada en los volúmenes DPO.

Gestione la replicación de volúmenes de SnapMirror

Flujo de trabajo de replicación de SnapMirror

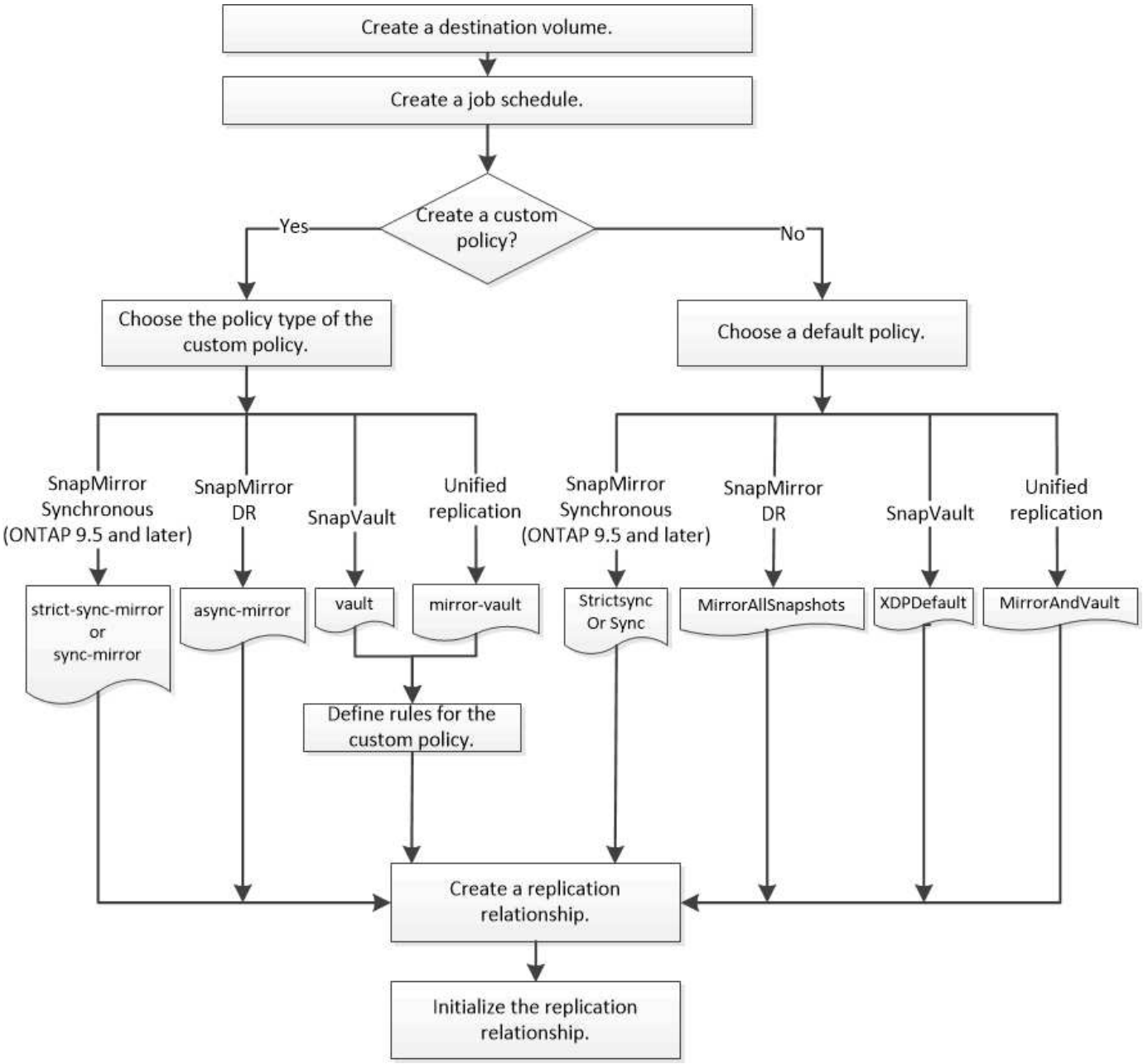
SnapMirror ofrece tres tipos de relación de protección de datos: Recuperación ante desastres de SnapMirror, archivado (anteriormente conocido como SnapVault) y replicación unificada. Puede seguir el mismo flujo de trabajo básico para configurar cada tipo de relación.

A partir de la disponibilidad general de ONTAP 9.9.1, SnapMirror Business Continuity (SM-BC) proporciona un objetivo de tiempo de recuperación cero (RTO cero) o recuperación tras fallos de aplicaciones transparente (TAF) para permitir la conmutación automática al nodo de respaldo de aplicaciones vitales para el negocio en entornos SAN. SM-BC se admite en una configuración de dos clústeres AFF o dos clústeres de Cabina SAN all-flash (ASA).

"Documentación de NetApp: Continuidad empresarial de SnapMirror"

Para cada tipo de relación de protección de datos de SnapMirror, el flujo de trabajo es el mismo: Crear un volumen de destino, crear una programación de trabajos, especificar una política, crear e inicializar la relación.

A partir de ONTAP 9.3, puede utilizar la `snapmirror protect` comando para configurar una relación de protección de datos en un solo paso. Incluso si usted utiliza `snapmirror protect`, debe comprender cada paso del flujo de trabajo.



Configurar una relación de replicación en un paso

A partir de ONTAP 9.3, puede utilizar la `snapmirror protect` comando para configurar una relación de protección de datos en un solo paso. Especifique una lista de volúmenes que se van a replicar, una SVM en el clúster de destino, una programación de trabajos y una política de SnapMirror. `snapmirror protect` hace el resto.

Lo que necesitará

- Las SVM y los clústeres de origen y destino deben tener una relación entre iguales.

  "Relaciones entre iguales de clústeres y SVM"

- El idioma del volumen de destino debe ser el mismo que el del volumen de origen.

Acerca de esta tarea

La `snapmirror protect` El comando elige un agregado asociado con la SVM especificada. Si no hay ningún agregado asociado con la SVM, elige de todos los agregados del clúster. La elección del agregado se basa en la cantidad de espacio libre y el número de volúmenes del agregado.

La `snapmirror protect` a continuación, el comando realiza los siguientes pasos:

- Crea un volumen de destino con un tipo adecuado y la cantidad de espacio reservado para cada volumen de la lista de volúmenes que se van a replicar.
- Configura una relación de replicación adecuada para la directiva que usted especifique.
- Inicializa la relación.

El nombre del volumen de destino tiene el formato *`source_volume_name_dst`*. En caso de un conflicto con un nombre existente, el comando añade un número al nombre del volumen. Puede especificar un prefijo o sufijo en las opciones del comando. El sufijo sustituye al suministrado por el sistema `dst` sufijo.

En ONTAP 9.3 y versiones anteriores, los volúmenes de destino pueden contener hasta 251 copias Snapshot. A partir de la versión 9.4 de ONTAP, un volumen de destino puede contener hasta 1019 copias snapshot.

> La inicialización puede requerir mucho tiempo. `snapmirror protect` no espera a que se complete la inicialización antes de que termine el trabajo. Por esta razón, debe utilizar la `snapmirror show` en lugar de la `job show` comando para determinar cuándo se ha completado la inicialización.

A partir de ONTAP 9.5, las relaciones de SnapMirror síncrono se pueden crear mediante el `snapmirror protect` comando.

Paso

1. Cree e inicialice una relación de replicación en un paso:

   Antes de ejecutar este comando, debe sustituir las variables entre paréntesis angulares por los valores requeridos.

   ```
   snapmirror protect -path-list <SVM:volume> -destination-vserver
   <destination_SVM> -policy <policy> -schedule <schedule> -auto-initialize
   <true|false> -destination-volume-prefix <prefix> -destination-volume
   -suffix <suffix>
   ```

   > Se debe ejecutar este comando desde la SVM de destino o el clúster de destino. La `-auto -initialize` la opción predeterminada es «'true'».

   En el siguiente ejemplo se crea e inicializa una relación de recuperación ante desastres de SnapMirror con los valores predeterminados `MirrorAllSnapshots` política:

   ```
   cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
   -destination-vserver svm_backup -policy MirrorAllSnapshots -schedule
   replication_daily
   ```

> Puede utilizar una directiva personalizada si lo prefiere. Para obtener más información, consulte "Creación de una política de replicación personalizada".

En el siguiente ejemplo se crea e inicializa una relación SnapVault con el valor predeterminado `XDPDefault` política:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy XDPDefault -schedule
replication_daily
```

En el ejemplo siguiente se crea e inicializa una relación de replicación unificada con el valor predeterminado `MirrorAndVault` política:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy MirrorAndVault
```

En el siguiente ejemplo se crea e inicializa una relación de SnapMirror síncrono con el valor predeterminado `Sync` política:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_sync -policy Sync
```

> Para las políticas de SnapVault y de replicación unificada, puede que sea útil definir una programación para crear una copia de la última copia de Snapshot transferida en el destino. Para obtener más información, consulte "Definir una programación para crear una copia local en el destino".

Después de terminar

Utilice la `snapmirror show` Comando para verificar que la relación de SnapMirror se ha creado. Para obtener una sintaxis de comando completa, consulte la página man.

Configure una relación de replicación paso a paso

Crear un volumen de destino

Puede utilizar el `volume create` comando en el destino para crear un volumen de destino. El volumen de destino debe tener el mismo tamaño o más que el volumen de origen.

Paso

1. Cree un volumen de destino:

   `volume create -vserver` *`SVM`* `-volume volume -aggregate` *`aggregate`* `-type DP -size` *`size`*

Para obtener una sintaxis de comando completa, consulte la página man.

En el ejemplo siguiente se crea un volumen de destino de 2 GB denominado `volA_dst`:

```
cluster_dst::> volume create -vserver SVM_backup -volume volA_dst
-aggregate node01_aggr -type DP -size 2GB
```

Cree una programación de trabajo de replicación

Puede utilizar el `job schedule cron create` comando para crear una programación de trabajo de replicación. La programación de tareas determina el momento en que SnapMirror actualiza automáticamente la relación de protección de datos a la que se asigna la programación.

Acerca de esta tarea

Debe asignar una programación de tareas cuando crea una relación de protección de datos. Si no asigna una programación de trabajo, debe actualizar la relación manualmente.

Paso

1. Crear un programa de trabajo:

   `job schedule cron create -name` *`job_name`* `-month` *`month`* `-dayofweek` *`day_of_week`* `-day` *`day_of_month`* `-hour` *`hour`* `-minute` *`minute`*

   Para `-month`, `-dayofweek`, y. `-hour`, puede especificar `all` para ejecutar el trabajo cada mes, día de la semana y hora, respectivamente.

   A partir de ONTAP 9.10.1, puede incluir Vserver para su programación de trabajo:

   `job schedule cron create -name` *`job_name`* `-vserver` *`Vserver_name`* `-month` *`month`* `-dayofweek` *`day_of_week`* `-day` *`day_of_month`* `-hour` *`hour`* `-minute` *`minute`*

   > La programación mínima admitida (RPO) para volúmenes FlexVol en una relación de SnapMirror para volúmenes es de 5 minutos. La programación mínima admitida (RPO) para volúmenes FlexGroup en una relación de SnapMirror para volúmenes es de 30 minutos.

   En el ejemplo siguiente se crea una programación de trabajo denominada `my_weekly` Es decir, los sábados a las 3:00 horas:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

Personalizar una política de replicación

Cree una política de replicación personalizada

Puede crear una directiva de replicación personalizada si la directiva predeterminada

para una relación no es adecuada. Puede que desee comprimir datos en una transferencia de red, por ejemplo, o modificar el número de intentos que realiza SnapMirror para transferir copias Snapshot.

Puede usar una directiva predeterminada o personalizada al crear una relación de replicación. Para un archivo personalizado (anteriormente SnapVault) o una política de replicación unificada, debe definir una o más *rules* que determinen qué copias Snapshot se transfieren durante la inicialización y la actualización. También es posible que desee definir una programación para crear copias Snapshot locales en el destino.

El *policy type* de la directiva de replicación determina el tipo de relación que admite. En la siguiente tabla se muestran los tipos de directivas disponibles.

Tipo de política	Tipo de relación
reflejo asíncrono	Recuperación ante desastres de SnapMirror
almacén	SnapVault
mirror-vault	Replicación unificada
estricto-síncrono-mirror	SnapMirror Synchronous en el modo StrictSync (compatible empezando con ONTAP 9.5)
reflejo síncrono	SnapMirror Synchronous en el modo Sync (admitido empezando por ONTAP 9.5)

Al crear una directiva de replicación personalizada, es una buena idea modelar la directiva después de una directiva predeterminada.

Paso

1. Cree una política de replicación personalizada:

   ```
   snapmirror policy create -vserver SVM -policy policy -type async-
   mirror|vault|mirror-vault|strict-sync-mirror|sync-mirror -comment comment
   -tries transfer_tries -transfer-priority low|normal -is-network-compression
   -enabled true|false
   ```

   Para obtener una sintaxis de comando completa, consulte la página man.

   A partir de ONTAP 9.5, puede especificar la programación para crear una programación de copia Snapshot común para relaciones de SnapMirror síncrono mediante la `-common-snapshot-schedule` parámetro. De forma predeterminada, la programación común de copias de Snapshot para relaciones de SnapMirror síncrono es una hora. Puede especificar un valor de 30 minutos a dos horas para la programación de la copia de Snapshot para las relaciones de SnapMirror Synchronous.

   En el ejemplo siguiente se crea una política de replicación personalizada para la recuperación ante desastres de SnapMirror que permite la compresión de red para las transferencias de datos:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
DR_compressed -type async-mirror -comment “DR with network compression
enabled” -is-network-compression-enabled true
```

En el ejemplo siguiente se crea una política de replicación personalizada para SnapVault:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_snapvault -type vault
```

En el ejemplo siguiente se crea una política de replicación personalizada para la replicación unificada:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy my_unified
-type mirror-vault
```

En el ejemplo siguiente se crea una política de replicación personalizada para la relación de SnapMirror Synchronous en el modo StrictSync:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_strictsync -type strict-sync-mirror -common-snapshot-schedule
my_sync_schedule
```

Después de terminar

En el caso de los tipos de políticas «'vault» y «mercado», deberá definir las reglas que determinen las copias snapshot que se transfieren durante la inicialización y actualización.

Utilice la `snapmirror policy show` Comando para comprobar que la política de SnapMirror se ha creado. Para obtener una sintaxis de comando completa, consulte la página man.

Defina una regla para una política

En el caso de las directivas personalizadas con el tipo de política «'vault» o «márror-vault», debe definir al menos una regla que determine qué copias snapshot se transfieren durante la inicialización y la actualización. También puede definir reglas para las políticas predeterminadas con el tipo de política «'vault» o «'mirror-vault».

Acerca de esta tarea

Todas las normas que tengan el tipo de política «'vault» o « márror-vault» deberán tener una regla que especifique qué copias snapshot replicar. La regla «'bimensual'», por ejemplo, indica que sólo deben replicarse las copias snapshot asignadas a la etiqueta «'bimensual'» de SnapMirror. Debe especificar la etiqueta de SnapMirror al configurar la política de Snapshot en el origen.

Cada tipo de política está asociado a una o más reglas definidas por el sistema. Estas reglas se asignan automáticamente a una directiva cuando se especifica su tipo de directiva. La siguiente tabla muestra las reglas definidas por el sistema.

Regla definida por el sistema	Se utiliza en tipos de políticas	Resultado
sm_creado	Reflejo asíncrono, reflejo-almacén, sincronización, StrictSync	Una copia Snapshot creada por SnapMirror se transfiere tras la inicialización y la actualización.
all_source_snapshots	reflejo asíncrono	Las nuevas copias snapshot del origen se transfieren tras la inicialización y actualización.
todos los días	almacén, reflejo-almacén	Las nuevas copias snapshot del origen con la etiqueta de SnapMirror «día» se transfieren durante la inicialización y actualización.
semanal	almacén, reflejo-almacén	Al inicializar y actualizar, se transfieren las nuevas copias snapshot del origen con la etiqueta de SnapMirror «'Weekly».
mensual	mirror-vault	Las nuevas copias snapshot en el origen con la etiqueta de SnapMirror «mensual» se transfieren durante la inicialización y actualización.
coherente con la aplicación	Sync, StrictSync	Las copias Snapshot con la etiqueta de SnapMirror «'app_coherente» en el origen se replican de forma síncrona en el destino. Compatible a partir de ONTAP 9.7.

Excepto para el tipo de política «'duplicación asíncrona'», puede especificar reglas adicionales según sea necesario, para directivas predeterminadas o personalizadas. Por ejemplo:

- Para el valor predeterminado `MirrorAndVault` Política puede crear una regla llamada «bimensual» para hacer coincidir las copias Snapshot de la fuente con la etiqueta «bimensual» de SnapMirror.
- En el caso de una política personalizada con el tipo de política «mercado de productos vault», puede crear una regla llamada «bisemanal» para hacer coincidir las copias Snapshot del origen con la etiqueta de SnapMirror «bisemanales».

Paso

1. Definir una regla para una directiva:

   `snapmirror policy add-rule -vserver` *`SVM`* `-policy` *`policy_for_rule`* `-snapmirror -label` *`snapmirror-label`* `-keep` *`retention_count`*

   Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo, se añade una regla con la etiqueta de SnapMirror `bi-monthly` al valor predeterminado `MirrorAndVault` política:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
MirrorAndVault -snapmirror-label bi-monthly -keep 6
```

En el siguiente ejemplo, se añade una regla con la etiqueta de SnapMirror `bi-weekly` al personalizado `my_snapvault` política:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
my_snapvault -snapmirror-label bi-weekly -keep 26
```

En el siguiente ejemplo, se añade una regla con la etiqueta de SnapMirror `app_consistent` al personalizado `Sync` política:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy Sync
-snapmirror-label app_consistent -keep 1
```

Luego, puede replicar las copias Snapshot del clúster de origen que coincidan con esta etiqueta de SnapMirror:

```
cluster_src::> snapshot create -vserver vs1 -volume vol1 -snapshot
snapshot1 -snapmirror-label app_consistent
```

Defina una programación para crear una copia local en el destino

Para las relaciones de SnapVault y de replicación unificada, puede protegerse contra la posibilidad de que una copia Snapshot actualizada se dañe al crear una copia de la última copia Snapshot transferida en el destino. Esta «copia local» se conserva independientemente de las reglas de retención del origen, de modo que, aunque la copia Snapshot transferida mediante SnapMirror ya no esté disponible en el origen, dicha copia estará disponible en el destino.

Acerca de esta tarea

Se especifica la programación para crear una copia local en el `-schedule` opción de `snapmirror policy add-rule` comando.

Paso

1. Definir una programación para crear una copia local en el destino:

   `snapmirror policy add-rule -vserver` *`SVM`* `-policy` *`policy_for_rule`* `-snapmirror -label` *`snapmirror-label`* `-schedule` *`schedule`*

   Para obtener una sintaxis de comando completa, consulte la página man. Para ver un ejemplo de cómo

crear una programación de trabajos, consulte "Crear una programación de trabajo de replicación".

En el ejemplo siguiente se añade una programación para crear una copia local en los valores predeterminados `MirrorAndVault` política:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
MirrorAndVault -snapmirror-label my_monthly -schedule my_monthly
```

En el siguiente ejemplo, se agrega una programación para crear una copia local en el personalizado `my_unified` política:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
my_unified -snapmirror-label my_monthly -schedule my_monthly
```

Cree una relación de replicación

La relación entre el volumen de origen del almacenamiento principal y el volumen de destino del almacenamiento secundario se denomina *relación de protección de datos.* puede usar la `snapmirror create` Comando para crear relaciones de protección de datos de recuperación ante desastres, SnapVault o replicación unificada de SnapMirror.

Lo que necesitará

- Las SVM y los clústeres de origen y destino deben tener una relación entre iguales.

  "Relaciones entre iguales de clústeres y SVM"

- El idioma del volumen de destino debe ser el mismo que el del volumen de origen.

Acerca de esta tarea

Hasta ONTAP 9.3, SnapMirror invocado en modo DP y SnapMirror invocado en modo XDP utilizaba distintos motores de replicación, con distintos enfoques respecto a la dependencia de versión:

- SnapMirror que se invoca en el modo DP utilizaba un motor de replicación *version-dependent* en el que la versión de ONTAP debía ser la misma en el almacenamiento primario y secundario:

  ```
  cluster_dst::>  snapmirror create -type DP -source-path ... -destination
  -path ...
  ```

- SnapMirror, al que se invocó en el modo XDP, utilizó un motor de replicación de *version-flexible* que admitía diferentes versiones de ONTAP en el almacenamiento primario y secundario:

  ```
  cluster_dst::>  snapmirror create -type XDP -source-path ...
  -destination-path ...
  ```

Las importantes ventajas de SnapMirror, que ofrece una versión flexible, superan la ligera ventaja del

rendimiento de la replicación obtenido con el modo basado en la versión. Por este motivo, a partir de ONTAP 9.3, se ha creado el modo XDP como nuevo valor predeterminado, y cualquier invocación del modo DP en la línea de comandos o en scripts nuevos o existentes se convierte automáticamente al modo XDP.

Las relaciones existentes no se ven afectadas. Si una relación ya es del tipo DP, seguirá siendo del tipo DP. La siguiente tabla muestra el comportamiento que puede esperar.

Si especifica…	El tipo es…	La política predeterminada (si no se especifica una política) es…
PROTECCIÓN DE DATOS	XDP	MirrorAllSnapshots (recuperación ante desastres de SnapMirror)
Nada	XDP	MirrorAllSnapshots (recuperación ante desastres de SnapMirror)
XDP	XDP	XDPDefault (SnapVault)

Consulte también los ejemplos del procedimiento siguiente.

Las únicas excepciones a la conversión son las siguientes:

- Las relaciones de protección de datos de SVM siguen siendo las predeterminadas en el modo DP.

  Especifique XDP explícitamente para obtener el modo XDP con el valor predeterminado `MirrorAllSnapshots` política.

- Las relaciones de protección de datos con uso compartido de carga siguen siendo las predeterminadas en el modo DP.
- Las relaciones de protección de datos de SnapLock siguen siendo las predeterminadas en el modo DP.
- Las invocaciones explícitas de DP siguen en el modo DP de forma predeterminada si establece la siguiente opción para todo el clúster:

  ```
  options replication.create_data_protection_rels.enable on
  ```

  Esta opción se ignora si no invoca explícitamente DP.

En ONTAP 9.3 y versiones anteriores, los volúmenes de destino pueden contener hasta 251 copias Snapshot. A partir de la versión 9.4 de ONTAP, un volumen de destino puede contener hasta 1019 copias snapshot.

A partir de ONTAP 9.5, se admiten las relaciones de SnapMirror síncrono.

Paso

1. En el clúster de destino, cree una relación de replicación:

   Antes de ejecutar este comando, debe sustituir las variables entre paréntesis angulares por los valores requeridos.

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume> -type <DP|XDP> -schedule <schedule> -policy <policy>
```

Para obtener una sintaxis de comando completa, consulte la página man.

> La `schedule` No aplica el parámetro cuando se crean relaciones de SnapMirror síncrono.

En el siguiente ejemplo se crea una relación de recuperación ante desastres de SnapMirror con los valores predeterminados `MirrorLatest` política:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
MirrorLatest
```

En el siguiente ejemplo se crea una relación de SnapVault con los valores predeterminados `XDPDefault` política:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
XDPDefault
```

En el ejemplo siguiente se crea una relación de replicación unificada con la opción predeterminada `MirrorAndVault` política:

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination-path
svm_backup:volA_dst -type XDP -schedule my_daily -policy MirrorAndVault
```

En el siguiente ejemplo se crea una relación de replicación unificada mediante el método personalizado `my_unified` política:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
my_unified
```

En el siguiente ejemplo se crea una relación de SnapMirror Synchronous con el valor predeterminado `Sync` política:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy Sync
```

En el siguiente ejemplo se crea una relación de SnapMirror Synchronous con el valor predeterminado

`StrictSync` política:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy StrictSync
```

En el siguiente ejemplo se crea una relación de recuperación ante desastres de SnapMirror. Con el tipo de DP convertido automáticamente a XDP y sin ninguna directiva especificada, la política predeterminada es la `MirrorAllSnapshots` política:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type DP -schedule my_daily
```

En el siguiente ejemplo se crea una relación de recuperación ante desastres de SnapMirror. Si no se especifica ningún tipo o política, la directiva se establece de forma predeterminada en `MirrorAllSnapshots` política:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -schedule my_daily
```

En el siguiente ejemplo se crea una relación de recuperación ante desastres de SnapMirror. Sin ninguna directiva especificada, la directiva se establece de forma predeterminada en `XDPDefault` política:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily
```

En el siguiente ejemplo se crea una relación de SnapMirror Synchronous con la política predefinida `SnapCenterSync`:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy SnapCenterSync
```

> La política predefinida `SnapCenterSync` es de tipo `Sync`. Esta normativa replica cualquier copia snapshot que se cree con el `snapmirror-label` de "coherente con la aplicación".

Después de terminar

Utilice la `snapmirror show` Comando para verificar que la relación de SnapMirror se ha creado. Para obtener una sintaxis de comando completa, consulte la página man.

Información relacionada

- "Crear y eliminar volúmenes de prueba de conmutación al nodo de respaldo de SnapMirror".

Otras maneras de hacerlo en ONTAP

Para ejecutar estas tareas con…	Ver este contenido…
System Manager rediseñado (disponible con ONTAP 9.7 y versiones posteriores)	"Configure los reflejos y almacenes"
System Manager Classic (disponible con ONTAP 9.7 y versiones anteriores)	"Información general sobre backup de volúmenes mediante SnapVault"

Inicializar una relación de replicación

Para todos los tipos de relaciones, la inicialización realiza una *transferencia_de base*: Realiza una copia Snapshot del volumen de origen y, a continuación, transfiere esa copia y todos los bloques de datos a los que hace referencia al volumen de destino. De lo contrario, el contenido de la transferencia depende de la política.

Lo que necesitará

Las SVM y los clústeres de origen y destino deben tener una relación entre iguales.

"Relaciones entre iguales de clústeres y SVM"

Acerca de esta tarea

La inicialización puede requerir mucho tiempo. Puede ser conveniente ejecutar la transferencia básica en horas de menor actividad.

A partir de ONTAP 9.5, se admiten las relaciones de SnapMirror síncrono.

Paso

1. Inicializar una relación de replicación:

   ```
   snapmirror initialize -source-path SVM:volume|cluster://SVM/volume, …
   -destination-path SVM:volume|cluster://SVM/volume, …
   ```

   Para obtener una sintaxis de comando completa, consulte la página man.

   > Se debe ejecutar este comando desde la SVM de destino o el clúster de destino.

   En el siguiente ejemplo, se inicializa la relación entre el volumen de origen `volA` encendido `svm1` y el volumen de destino `volA_dst` encendido `svm_backup`:

   ```
   cluster_dst::> snapmirror initialize -source-path svm1:volA -destination
   -path svm_backup:volA_dst
   ```

Ejemplo: Configure una cascada de vault-vault

Un ejemplo mostrará en términos concretos cómo puede configurar las relaciones de replicación paso a paso. Puede utilizar la puesta en marcha en cascada de vault configurada en el ejemplo para conservar más de 251 copias snapshot con el nombre

«my semanal».

Lo que necesitará

- Las SVM y los clústeres de origen y destino deben tener una relación entre iguales.
- Debe ejecutar ONTAP 9,2 o una versión posterior. Las cascadas de vault-vault no son compatibles con versiones anteriores de ONTAP.

Acerca de esta tarea

En el ejemplo se dan por hechos los siguientes elementos:

- Se han configurado copias Snapshot en el clúster de origen con las etiquetas de SnapMirror «mi día a día», «mi semana a semana» y «mi mes».
- Ha configurado volúmenes de destino denominados «'Vola'» en los clústeres de destino secundario y terciario.
- Ha configurado programas de trabajos de replicación denominados «my_snapvault» en los clústeres de destino secundario y terciario.

El ejemplo muestra cómo crear relaciones de replicación basadas en dos políticas personalizadas:

- La política de «sinapvault_secondary» conserva 7 copias snapshot diarias, 52 semanales y 180 mensuales en el clúster de destino secundario.
- La «política de almacén_terciario» conserva 250 copias Snapshot semanales en el clúster de destino terciario.

Pasos

1. En el clúster secundario de destino, cree la política «napvault_secondary»:

   ```
   cluster_secondary::> snapmirror policy create -policy snapvault_secondary
   -type vault -comment “Policy on secondary for vault to vault cascade” -vserver
   svm_secondary
   ```

2. En el grupo secundario de destino, definir la regla «mi día a día» de la política:

   ```
   cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
   -snapmirror-label my-daily -keep 7 -vserver svm_secondary
   ```

3. En el grupo secundario de destino, definir la regla «mi semana» para la política:

   ```
   cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
   -snapmirror-label my-weekly -keep 52 -vserver svm_secondary
   ```

4. En el grupo secundario de destino, definir la regla «mi mes» de la política:

   ```
   cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
   -snapmirror-label my-monthly -keep 180 -vserver svm_secondary
   ```

5. En el clúster de destino secundario, compruebe la política:

   ```
   cluster_secondary::> snapmirror policy show snapvault_secondary -instance
   ```

```
                    Vserver: svm_secondary
      SnapMirror Policy Name: snapvault_secondary
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
            Create Snapshot: false
                    Comment: Policy on secondary for vault to vault
cascade
       Total Number of Rules: 3
                  Total Keep: 239
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              my-daily                7  false       0 -
-
                              my-weekly              52  false       0 -
-
                              my-monthly            180  false       0 -
-
```

6. En el clúster de destino secundario, cree la relación con el clúster de origen:

   ```
   cluster_secondary::> snapmirror create -source-path svm_primary:volA
   -destination-path svm_secondary:volA -type XDP -schedule my_snapvault -policy
   snapvault_secondary
   ```

7. En el clúster de destino secundario, inicialice la relación con el clúster de origen:

   ```
   cluster_secondary::> snapmirror initialize -source-path svm_primary:volA
   -destination-path svm_secondary:volA
   ```

8. En el clúster de destino terciario, cree la política «napvault_terciario»:

   ```
   cluster_tertiary::> snapmirror policy create -policy snapvault_tertiary -type
   vault -comment “Policy on tertiary for vault to vault cascade” -vserver
   svm_tertiary
   ```

9. En el grupo de destino terciario, defina la regla «mi semana» para la política:

   ```
   cluster_tertiary::> snapmirror policy add-rule -policy snapvault_tertiary
   -snapmirror-label my-weekly -keep 250 -vserver svm_tertiary
   ```

10. En el clúster de destino terciario, compruebe la política:

```
cluster_tertiary::> snapmirror policy show snapvault_tertiary -instance
```

```
                     Vserver: svm_tertiary
      SnapMirror Policy Name: snapvault_tertiary
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Policy on tertiary for vault to vault
cascade
       Total Number of Rules: 1
                  Total Keep: 250
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              my-weekly             250  false       0 -
-
```

11. En el clúster de destino terciario, cree la relación con el clúster secundario:

```
cluster_tertiary::> snapmirror create -source-path svm_secondary:volA
-destination-path svm_tertiary:volA -type XDP -schedule my_snapvault -policy
snapvault_tertiary
```

12. En el clúster de destino terciario, inicialice la relación con el clúster secundario:

```
cluster_tertiary::> snapmirror initialize -source-path svm_secondary:volA
-destination-path svm_tertiary:volA
```

Convierta una relación de tipo DP existente a XDP

Si actualiza a ONTAP 9.12.1 o una versión posterior, debe convertir las relaciones de tipo DP a XDP antes de realizar la actualización. ONTAP 9.12.1 y las versiones posteriores no admiten relaciones de tipo DP. Puede convertir fácilmente una relación de tipo de DP existente a XDP para poder aprovechar las ventajas de la flexibilidad de versión de SnapMirror.

Acerca de esta tarea

- SnapMirror no convierte automáticamente las relaciones de tipo DP existentes a XDP. Para convertir la relación, debe romper y eliminar la relación existente, crear una nueva relación XDP y volver a sincronizar la relación. Para obtener información previa, consulte "XDP sustituye a DP como la opción predeterminada de SnapMirror".

- Al planificar la conversión, tenga en cuenta que la preparación en segundo plano y la fase de almacenamiento de datos de una relación de SnapMirror para XDP pueden llevar mucho tiempo. No es poco frecuente ver la relación de SnapMirror que informa sobre el estado "preparación" para un periodo de tiempo prolongado.

> Después de convertir un tipo de relación de SnapMirror de DP a XDP, las configuraciones relacionadas con el espacio, como la configuración automática de tamaño y la garantía de espacio, ya no se replican en el destino.

Pasos

1. En el clúster de destino, compruebe que la relación SnapMirror sea del tipo DP, que el estado de mirroring sea en SnapMirror, que el estado de la relación sea inactivo y que la relación esté en buen estado:

```
snapmirror show -destination-path <SVM:volume>
```

En el siguiente ejemplo, se muestra el resultado de `snapmirror show` comando:

```
cluster_dst::>snapmirror show -destination-path svm_backup:volA_dst

Source Path: svm1:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```

> Puede que le resulte útil conservar una copia del `snapmirror show` salida de comando para realizar un seguimiento de la configuración de relaciones existente.

2. En los volúmenes de origen y destino, asegúrese de que ambos volúmenes tengan una copia Snapshot común:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

En el siguiente ejemplo se muestra el `volume snapshot show` salida de los volúmenes de origen y destino:

```
cluster_src:> volume snapshot show -vserver vsm1 -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm1 volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.


cluster_dest:> volume snapshot show -vserver svm_backup -volume volA_dst
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
```

3. Para garantizar que las actualizaciones programadas no se ejecuten durante la conversión, desactive la relación de tipo DP existente:

```
snapmirror quiesce -source-path <SVM:volume> -destination-path
<SVM:volume>
```

Para obtener una sintaxis completa del comando, consulte "página de manual".

> Se debe ejecutar este comando desde la SVM de destino o el clúster de destino.

En el siguiente ejemplo, se pausa la relación entre el volumen de origen `volA` encendido `svm1` y el volumen de destino `volA_dst` encendido `svm_backup`:

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

4. Rompa la relación de tipo de DP existente:

```
snapmirror break -destination-path <SVM:volume>
```

Para obtener una sintaxis completa del comando, consulte "página de manual".

> Se debe ejecutar este comando desde la SVM de destino o el clúster de destino.

En el siguiente ejemplo, se rompe la relación entre el volumen de origen `volA` encendido `svm1` y el volumen de destino `volA_dst` encendido `svm_backup`:

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

5. Si la eliminación automática de las copias Snapshot está habilitada en el volumen de destino, desactívelo:

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_
-enabled false
```

En el ejemplo siguiente se deshabilita la eliminación automática de copias Snapshot en el volumen de destino `volA_dst`:

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup
-volume volA_dst -enabled false
```

6. Elimine la relación de tipo de DP existente:

```
snapmirror delete -destination-path <SVM:volume>
```

Para obtener una sintaxis completa del comando, consulte "página de manual".

> Se debe ejecutar este comando desde la SVM de destino o el clúster de destino.

En el siguiente ejemplo, se elimina la relación entre el volumen de origen `volA` encendido `svm1` y el volumen de destino `volA_dst` encendido `svm_backup`:

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

7. Libere la relación de recuperación ante desastres de la SVM de origen en el origen:

```
snapmirror release -destination-path <SVM:volume> -relationship-info
-only true
```

En el ejemplo siguiente se libera la relación de recuperación de desastres de SVM:

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst
-relationship-info-only true
```

8. Puede utilizar la salida que ha retenido de `snapmirror show` Comando para crear la nueva relación de tipo XDP:

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume>  -type XDP -schedule <schedule> -policy <policy>
```

La nueva relación debe usar el mismo volumen de origen y destino. Para obtener una sintaxis de comando completa, consulte la página man.

> Se debe ejecutar este comando desde la SVM de destino o el clúster de destino.

En el siguiente ejemplo se crea una relación de recuperación de desastres de SnapMirror entre el volumen de origen `volA` encendido `svm1` y el volumen de destino `volA_dst` encendido `svm_backup` con el valor predeterminado `MirrorAllSnapshots` política:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst
-type XDP -schedule my_daily -policy MirrorAllSnapshots
```

9. Resincronización de los volúmenes de origen y destino:

```
snapmirror resync -source-path <SVM:volume> -destination-path
<SVM:volume>
```

Para mejorar el tiempo de resincronización, puede utilizar el `-quick-resync` opcional, pero debe tener en cuenta que se pueden perder ahorros en eficiencia del almacenamiento. Para obtener una sintaxis completa del comando, consulte la página man: "Comando SnapMirror resync".

> Se debe ejecutar este comando desde la SVM de destino o el clúster de destino. Aunque la resincronización no requiere una transferencia básica, puede requerir mucho tiempo. Puede que desee ejecutar la resincronización en horas de menor actividad.

En el siguiente ejemplo, vuelva a establecer la relación entre el volumen de origen `volA` encendido `svm1` y el volumen de destino `volA_dst` encendido `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

10. Si ha deshabilitado la eliminación automática de copias Snapshot, vuelva a habilitarla:

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>
-enabled true
```

Después de terminar

1. Utilice la `snapmirror show` Comando para verificar que la relación de SnapMirror se ha creado.
2. Una vez que el volumen de destino de SnapMirror XDP comienza a actualizar las copias snapshot tal como se define en la política de SnapMirror, utilice el resultado de `snapmirror list-destinations` Comando del clúster de origen para mostrar la nueva relación de XDP de SnapMirror.

Convierta el tipo de una relación de SnapMirror

A partir de ONTAP 9.5, SnapMirror Synchronous es compatible. Puede convertir una relación de SnapMirror asíncrona en una relación de SnapMirror síncrono o viceversa sin realizar una transferencia de referencia.

Acerca de esta tarea

No se puede convertir una relación de SnapMirror asíncrona en una relación de SnapMirror síncrono o viceversa cambiando la política de SnapMirror

Pasos

- **Convertir una relación asíncrona de SnapMirror en una relación de SnapMirror síncrono**

  a. En el clúster de destino, elimine la relación asíncrona de SnapMirror:

  `snapmirror delete -destination-path` *`SVM:volume`*

  ```
  cluster2::>snapmirror delete -destination-path vs1_dr:vol1
  ```

  b. A partir del clúster de origen, libere la relación SnapMirror sin eliminar las copias Snapshot comunes:

snapmirror release -relationship-info-only true -destination-path *dest_SVM:dest_volume*

```
cluster1::>snapmirror release -relationship-info-only true
-destination-path vs1_dr:vol1
```

c. En el clúster de destino, cree una relación de SnapMirror Synchronous:

snapmirror create -source-path *src_SVM:src_volume* -destination-path *dest_SVM:dest_volume* -policy sync-mirror

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
vs1_dr:vol1 -policy sync
```

d. Resincronice la relación de SnapMirror síncrono:

snapmirror resync -destination-path *dest_SVM:dest_volume*

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

- **Convertir una relación de SnapMirror Synchronous en una relación asíncrona de SnapMirror**

a. En el clúster de destino, desactive la relación de SnapMirror síncrono existente:

snapmirror quiesce -destination-path dest_SVM:dest_volume

```
cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
```

b. En el clúster de destino, elimine la relación asíncrona de SnapMirror:

snapmirror delete -destination-path *SVM:volume*

```
cluster2::>snapmirror delete -destination-path vs1_dr:vol1
```

c. A partir del clúster de origen, libere la relación SnapMirror sin eliminar las copias Snapshot comunes:

snapmirror release -relationship-info-only true -destination-path *dest_SVM:dest_volume*

```
cluster1::>snapmirror release -relationship-info-only true
-destination-path vs1_dr:vol1
```

d. A partir del clúster de destino, cree una relación de SnapMirror asíncrona:

   `snapmirror create -source-path src_SVM:src_volume -destination-path dest_SVM:dest_volume -policy MirrorAllSnapshots`

   ```
   cluster2::>snapmirror create -source-path vs1:vol1 -destination-path vs1_dr:vol1 -policy sync
   ```

e. Resincronice la relación de SnapMirror síncrono:

   `snapmirror resync -destination-path dest_SVM:dest_volume`

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

Convertir el modo de una relación de SnapMirror Synchronous

A partir de ONTAP 9.5, se admiten las relaciones de SnapMirror síncrono. Puede convertir el modo de una relación de SnapMirror Synchronous de StrictSync a Sync o viceversa.

Acerca de esta tarea

No se puede modificar la política de una relación de SnapMirror Synchronous para convertir su modo.

Pasos

1. En el clúster de destino, desactive la relación de SnapMirror síncrono existente:

   `snapmirror quiesce -destination-path dest_SVM:dest_volume`

   ```
   cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
   ```

2. En el clúster de destino, elimine la relación de SnapMirror Synchronous existente:

   `snapmirror delete -destination-path dest_SVM:dest_volume`

   ```
   cluster2::> snapmirror delete -destination-path vs1_dr:vol1
   ```

3. A partir del clúster de origen, libere la relación SnapMirror sin eliminar las copias Snapshot comunes:

   `snapmirror release -relationship-info-only true -destination-path dest_SVM:dest_volume`

   ```
   cluster1::> snapmirror release -relationship-info-only true -destination -path vs1_dr:vol1
   ```

4. Desde el clúster de destino, cree una relación SnapMirror Synchronous especificando el modo en que desea convertir la relación SnapMirror Synchronous:

   ```
   snapmirror create -source-path vs1:vol1 -destination-path dest_SVM:dest_volume
   -policy Sync|StrictSync
   ```

   ```
   cluster2::> snapmirror create -source-path vs1:vol1 -destination-path
   vs1_dr:vol1 -policy Sync
   ```

5. En el clúster de destino, resincronice la relación SnapMirror:

   ```
   snapmirror resync -destination-path dest_SVM:dest_volume
   ```

   ```
   cluster2::> snapmirror resync -destination-path vs1_dr:vol1
   ```

Crear y eliminar volúmenes de prueba de conmutación al nodo de respaldo de SnapMirror

A partir de ONTAP 9.14.1, puede usar System Manager para crear un clon de volumen a fin de probar la conmutación por error y la recuperación ante desastres de SnapMirror sin interrumpir la relación de SnapMirror activa. Cuando termine la prueba, puede limpiar los datos asociados y eliminar el volumen de prueba.

Crear un volumen de prueba de conmutación por error de SnapMirror

Acerca de esta tarea

- Puede llevar a cabo pruebas de conmutación al nodo de respaldo en relaciones de SnapMirror síncronas y asíncronas.
- Se crea un clon de volumen para realizar la prueba de recuperación ante desastres.
- El volumen clonado se crea en la misma máquina virtual de almacenamiento que el destino de SnapMirror.
- Se pueden usar las relaciones de SnapMirror de FlexVol y FlexGroup.
- Si ya existe un clon de prueba para la relación seleccionada, no puede crear otro clon para esa relación.
- No se admiten las relaciones de almacén de SnapLock.

Antes de empezar

- Debe ser un administrador de clústeres.
- La licencia de SnapMirror debe instalarse en los clústeres de origen y de destino.

Pasos

1. En el clúster de destino, seleccione **Protección > Relaciones**.
2. Seleccione ⋮ Junto al origen de la relación y elija **Test Failover**.
3. En la ventana **Test Failover**, selecciona **Test Failover**.
4. Seleccione **Almacenamiento > Volúmenes** y compruebe que el volumen de conmutación por error de prueba aparece en la lista.

5. Selecciona **Almacenamiento > Compartir**.
6. Haga clic en + Add Y elige **Share**.
7. En la ventana **Agregar recurso compartido**, escriba un nombre para el recurso compartido en el campo **Compartir nombre**.
8. En el campo **Carpeta**, seleccione **Examinar**, seleccione el volumen de clonación de prueba y **Guardar**.
9. En la parte inferior de la ventana **Agregar Compartir**, selecciona **Guardar**.
10. Abra el recurso compartido en el cliente y verifique que el volumen de prueba tenga capacidades de lectura y escritura.

Limpie los datos de conmutación por error y elimine el volumen de prueba

Después de completar las pruebas de conmutación al nodo de respaldo, puede borrar todos los datos asociados al volumen de prueba y eliminarlos.

Pasos

1. En el clúster de destino, seleccione **Protección > Relaciones**.
2. Seleccione ⋮ Junto a la fuente de la relación y elija **Limpiar prueba de failover**.
3. En la ventana **Limpiar prueba de failover**, selecciona **Limpiar**.
4. Seleccione **Almacenamiento > Volúmenes** y compruebe que se ha eliminado el volumen de prueba.

Proporcione datos desde un volumen de destino de recuperación ante desastres de SnapMirror

Haga que el volumen de destino sea modificable

Debe hacer que el volumen de destino sea editable, para poder proporcionar datos del volumen a los clientes. Puede utilizar el `snapmirror quiesce` comando para detener las transferencias programadas al destino, el `snapmirror abort` comando para detener las transferencias continuas y el `snapmirror break` comando para hacer que el destino sea editable.

Acerca de esta tarea

Debe realizar esta tarea desde la SVM de destino o el clúster de destino.

Pasos

1. Detenga las transferencias programadas al destino:

   ```
   snapmirror quiesce -source-path SVM:volume|cluster://SVM/volume, …
   -destination-path SVM:volume|cluster://SVM/volume, …
   ```

   Para obtener una sintaxis de comando completa, consulte la página man.

   El siguiente ejemplo detiene las transferencias programadas entre el volumen de origen `volA` encendido `svm1` y el volumen de destino `volA_dst` encendido `svm_backup`:

```
cluster_dst::> snapmirror quiesce -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

2. Detenga las transferencias continuas al destino:

   `snapmirror abort -source-path` *`SVM:volume|cluster://SVM/volume, …`* `-destination -path` *`SVM:volume|cluster://SVM/volume, …`*

   Para obtener una sintaxis de comando completa, consulte la página man.

   > Este paso no es necesario para relaciones de SnapMirror síncrono (se admite a partir de ONTAP 9.5).

   El siguiente ejemplo detiene las transferencias continuas entre el volumen de origen `volA` encendido `svm1` y el volumen de destino `volA_dst` encendido `svm_backup`:

```
cluster_dst::> snapmirror abort -source-path svm1:volA -destination-path
svm_backup:volA_dst
```

3. Rompa la relación de recuperación ante desastres de SnapMirror:

   `snapmirror break -source-path` *`SVM:volume|cluster://SVM/volume, …`* `-destination -path` *`SVM:volume|cluster://SVM/volume, …`*

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el siguiente ejemplo, se rompe la relación entre el volumen de origen `volA` encendido `svm1` y el volumen de destino `volA_dst` encendido `svm_backup`:

```
cluster_dst::> snapmirror break -source-path svm1:volA -destination-path
svm_backup:volA_dst
```

Otras maneras de hacerlo en ONTAP

Para ejecutar estas tareas con…	Ver este contenido…
System Manager rediseñado (disponible con ONTAP 9.7 y versiones posteriores)	"Sirva datos desde un destino de SnapMirror"
System Manager Classic (disponible con ONTAP 9.7 y versiones anteriores)	"Información general sobre la recuperación ante desastres de volúmenes"

Configure el volumen de destino para acceder a los datos

Tras hacer que el volumen de destino sea editable, debe configurar el volumen para el acceso a los datos. Los clientes NAS, el subsistema NVMe y hosts SAN pueden acceder a los datos desde el volumen de destino hasta que se reactive el volumen de origen.

Entorno NAS:

1. Monte el volumen NAS en el espacio de nombres mediante la misma ruta de unión en la que se montó el volumen de origen en la SVM de origen.
2. Aplique las ACL adecuadas para los recursos compartidos de SMB en el volumen de destino.
3. Asigne las políticas de exportación de NFS al volumen de destino.
4. Aplique las reglas de cuota al volumen de destino.
5. Redirija a los clientes al volumen de destino.
6. Vuelva a montar los recursos compartidos de NFS y SMB en los clientes.

ENTORNO SAN:

1. Asigne las LUN del volumen al iGroup correspondiente.
2. Para iSCSI, cree sesiones iSCSI desde los iniciadores de host SAN hasta las LIF DE SAN.
3. En el cliente SAN, realice una nueva exploración del almacenamiento para detectar las LUN conectadas.

Para obtener más información sobre el entorno NVMe, consulte "Administración de SAN".

Vuelva a activar el volumen de origen original

Puede restablecer la relación de protección de datos original entre los volúmenes de origen y destino cuando ya no necesite servir datos desde el destino.

Acerca de esta tarea

- En el siguiente procedimiento se asume que la línea base del volumen de origen original está intacta. Si la base de referencia no está intacta, debe crear e inicializar la relación entre el volumen desde el que se sirven datos y el volumen de origen original antes de realizar el procedimiento.
- La preparación en segundo plano y la fase de almacenamiento de datos de una relación de SnapMirror para XDP pueden llevar mucho tiempo. No es poco frecuente ver la relación de SnapMirror que informa sobre el estado "preparación" para un periodo de tiempo prolongado.

Pasos

1. Invierta la relación de protección de datos original:

   ```
   snapmirror resync -source-path SVM:volume -destination-path SVM:volume
   ```

   Para obtener una sintaxis de comando completa, consulte la página man.

   > Se debe ejecutar este comando desde la SVM de origen original o desde el clúster de origen original. Aunque la resincronización no requiere una transferencia básica, puede requerir mucho tiempo. Puede que desee ejecutar la resincronización en horas de menor actividad. El comando genera errores si no existe una copia Snapshot común en el origen y el destino. Uso `snapmirror initialize` para volver a inicializar la relación.

   En el siguiente ejemplo, se revierte la relación entre el volumen de origen original, `volA` encendido `svm1`, y el volumen desde el que se proporcionan datos, `volA_dst` encendido `svm_backup`:

```
cluster_src::> snapmirror resync -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

2. Una vez que esté listo para restablecer el acceso a los datos en el origen original, detenga el acceso al volumen de destino original. Una manera de hacerlo es detener la SVM de destino original:

   `vserver stop -vserver SVM`

   Para obtener una sintaxis de comando completa, consulte la página man.

   > Debe ejecutar este comando desde la SVM de destino original o desde el clúster de destino original. Este comando detiene el acceso del usuario a la SVM original completa de destino. Puede que desee detener el acceso al volumen de destino original mediante otros métodos.

   En el ejemplo siguiente se detiene la SVM de destino original:

```
cluster_dst::> vserver stop svm_backup
```

3. Actualice la relación de inversión:

   `snapmirror update -source-path SVM:volume -destination-path SVM:volume`

   Para obtener una sintaxis de comando completa, consulte la página man.

   > Se debe ejecutar este comando desde la SVM de origen original o desde el clúster de origen original.

   En el siguiente ejemplo, se actualiza la relación entre el volumen desde el que se proporcionan datos, `volA_dst` encendido `svm_backup`, y el volumen de origen original, `volA` encendido `svm1`:

```
cluster_src::> snapmirror update -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

4. Desde la SVM de origen original o el clúster de origen original, detenga las transferencias programadas para la relación inversa:

   `snapmirror quiesce -source-path SVM:volume -destination-path SVM:volume`

   Para obtener una sintaxis de comando completa, consulte la página man.

   > Se debe ejecutar este comando desde la SVM de origen original o desde el clúster de origen original.

   En el ejemplo siguiente se detienen las transferencias programadas entre el volumen de destino original, `volA_dst` encendido `svm_backup`, y el volumen de origen original, `volA` encendido `svm1`:

```
cluster_src::> snapmirror quiesce -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

5. Cuando la actualización final se completa y la relación indica "Quiesced" para el estado de la relación, ejecute el siguiente comando desde la SVM de origen original o el clúster de origen original para romper la relación inversa:

   `snapmirror break -source-path SVM:volume -destination-path SVM:volume`

   Para obtener una sintaxis de comando completa, consulte la página man.

   > Se debe ejecutar este comando desde la SVM de origen original o desde el clúster de origen.

   En el siguiente ejemplo, se rompe la relación entre el volumen de destino original, `volA_dst` encendido `svm_backup`, y el volumen de origen original, `volA` encendido `svm1`:

```
cluster_scr::> snapmirror break -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

6. En la SVM de origen original o en el clúster de origen original, elimine la relación de protección de datos inversa:

   `snapmirror delete -source-path SVM:volume -destination-path SVM:volume`

   Para obtener una sintaxis de comando completa, consulte la página man.

   > Se debe ejecutar este comando desde la SVM de origen original o desde el clúster de origen original.

   En el siguiente ejemplo, se elimina la relación inversa entre el volumen de origen original, `volA` encendido `svm1`, y el volumen desde el que se proporcionan datos, `volA_dst` encendido `svm_backup`:

```
cluster_src::> snapmirror delete -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

7. Libere la relación inversa de la SVM de destino original o el clúster de destino original.

   `snapmirror release -source-path SVM:volume -destination-path SVM:volume`

   > Debe ejecutar este comando desde la SVM de destino original o desde el clúster de destino original.

   En el ejemplo siguiente se libera la relación inversa entre el volumen de destino original, `volA_dst` encendido `svm_backup`, y el volumen de origen original, `volA` encendido `svm1`:

```
cluster_dst::> snapmirror release -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

8. Restablezca la relación de protección de datos original desde el destino original:

   `snapmirror resync -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el siguiente ejemplo, se restablece la relación entre el volumen de origen original, `volA` encendido `svm1`, y el volumen de destino original, `volA_dst` encendido `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

9. Si es necesario, inicie la SVM de destino original:

   `vserver start -vserver` *`SVM`*

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el ejemplo siguiente se inicia la SVM de destino original:

```
cluster_dst::> vserver start svm_backup
```

Después de terminar

Utilice la `snapmirror show` Comando para verificar que la relación de SnapMirror se ha creado. Para obtener una sintaxis de comando completa, consulte la página man.

Restaurar los archivos de un volumen de destino de SnapMirror

Restaure un solo espacio de nombres de archivos, LUN o NVMe desde un destino de SnapMirror

Puede restaurar un solo archivo, LUN, un conjunto de archivos o LUN a partir de una copia Snapshot o un espacio de nombres NVMe desde un volumen de destino de SnapMirror. A partir de ONTAP 9.7, también es posible restaurar espacios de nombres NVMe desde un destino de SnapMirror síncrono. Es posible restaurar archivos en el volumen de origen original o en otro volumen.

Lo que necesitará

Para restaurar un archivo o una LUN a partir de un destino de SnapMirror síncrono (compatible a partir de ONTAP 9.5), primero debe eliminar y liberar la relación.

Acerca de esta tarea

El volumen al que va a restaurar archivos o LUN (el volumen de destino) debe ser un volumen de lectura y escritura:

- SnapMirror realiza una *restauración incremental* si los volúmenes de origen y destino tienen una copia Snapshot común (como suele ocurrir cuando se restaura al volumen de origen original).
- De lo contrario, SnapMirror realiza una *restauración_base*, en la que la copia Snapshot especificada y todos los bloques de datos a los que hace referencia se transfieren al volumen de destino.

Pasos

1. Enumere las copias Snapshot en el volumen de destino:

   `volume snapshot show -vserver SVM -volume volume`

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el ejemplo siguiente se muestran las copias Snapshot en el `vserverB:secondary1` destino:

```
cluster_dst::> volume snapshot show -vserver vserverB -volume secondary1

Vserver     Volume      Snapshot                State    Size  Total%
Used%
-------     ------      ---------- ----------- ------   -----  ------
-----
vserverB    secondary1  hourly.2013-01-25_0005  valid   224KB     0%
0%
                        daily.2013-01-25_0010   valid   92KB      0%
0%
                        hourly.2013-01-25_0105  valid   228KB     0%
0%
                        hourly.2013-01-25_0205  valid   236KB     0%
0%
                        hourly.2013-01-25_0305  valid   244KB     0%
0%
                        hourly.2013-01-25_0405  valid   244KB     0%
0%
                        hourly.2013-01-25_0505  valid   244KB     0%
0%

7 entries were displayed.
```

2. Restaure un solo archivo o LUN, o un conjunto de archivos o LUN a partir de una copia Snapshot en un volumen de destino de SnapMirror:

   `snapmirror restore -source-path SVM:volume|cluster://SVM/volume, … -destination-path SVM:volume|cluster://SVM/volume, … -source-snapshot snapshot -file-list source_file_path,@destination_file_path`

   Para obtener una sintaxis de comando completa, consulte la página man.

   > Se debe ejecutar este comando desde la SVM de destino o el clúster de destino.

El siguiente comando restaura los archivos `file1` y.. `file2` Desde la copia Snapshot `daily.2013-01-25_0010` en el volumen de destino original `secondary1`, en la misma ubicación del sistema de archivos activo del volumen de origen original `primary1`:

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list /dir1/file1,/dir2/file2

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

El siguiente comando restaura los archivos `file1` y.. `file2` Desde la copia Snapshot `daily.2013-01-25_0010` en el volumen de destino original `secondary1`, a una ubicación diferente en el sistema de archivos activo del volumen de origen original `primary1`.

La ruta del archivo de destino comienza con el símbolo @ seguido por la ruta del archivo desde la raíz del volumen de origen original. En este ejemplo: `file1` se restaura a. `/dir1/file1.new` y file2 se restaura a. `/dir2.new/file2` encendido `primary1`:

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,@/dir2.new/file2

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

El siguiente comando restaura los archivos `file1` y.. `file3` Desde la copia Snapshot `daily.2013-01-25_0010` en el volumen de destino original `secondary1`, a distintas ubicaciones del sistema de archivos activo del volumen de origen original `primary1`, y restauraciones `file2` de `snap1` a la misma ubicación en el sistema de archivos activo de `primary1`.

En este ejemplo, el archivo `file1` se restaura a. `/dir1/file1.new` y.. `file3` se restaura a. `/dir3.new/file3`:

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,/dir3/file3,@/dir3.new/file3

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

Restaure el contenido de un volumen a partir de un destino de SnapMirror

Puede restaurar el contenido de un volumen completo desde una copia Snapshot en un volumen de destino de SnapMirror. Es posible restaurar el contenido del volumen en el volumen de origen original o en otro volumen.

Acerca de esta tarea

El volumen de destino de la operación de restauración debe ser uno de los siguientes:

- Un volumen de lectura y escritura, en cuyo caso SnapMirror realiza una *incremental restore*, siempre y cuando los volúmenes de origen y destino tengan una copia Snapshot común (como suele ser el caso en el momento de restaurar el volumen de origen original).

  > Error del comando si no hay una copia Snapshot común. No es posible restaurar el contenido de un volumen en un volumen vacío de lectura/escritura.

- Un volumen de protección de datos vacío, en cuyo caso SnapMirror ejecuta una *restauración básica*, en la que la copia Snapshot especificada y todos los bloques de datos a los que hace referencia se transfieren al volumen de origen.

La restauración del contenido de un volumen es una operación disruptiva. No debe ejecutarse el tráfico de SMB en el volumen primario de SnapVault cuando se ejecuta una operación de restauración.

Si el volumen de destino de la operación de restauración tiene la compresión habilitada y el volumen de origen no tiene la compresión habilitada, se debe deshabilitar la compresión en el volumen de destino. Es necesario volver a habilitar la compresión una vez que se completa la operación de restauración.

Las reglas de cuota definidas para el volumen de destino se desactivan antes de ejecutar la restauración. Puede utilizar el `volume quota modify` comando para reactivar las reglas de cuota una vez completada la operación de restauración.

Pasos

1. Enumere las copias Snapshot en el volumen de destino:

   ```
   volume snapshot show -vserver <SVM> -volume <volume>
   ```

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el ejemplo siguiente se muestran las copias Snapshot en el `vserverB:secondary1` destino:

```
cluster_dst::> volume snapshot show -vserver vserverB -volume secondary1

Vserver     Volume      Snapshot                State    Size  Total%
Used%
-------     ------      ---------- ----------- ------   -----  ------
-----
vserverB    secondary1  hourly.2013-01-25_0005  valid   224KB     0%
0%
                        daily.2013-01-25_0010   valid   92KB      0%
0%
                        hourly.2013-01-25_0105  valid   228KB     0%
0%
                        hourly.2013-01-25_0205  valid   236KB     0%
0%
                        hourly.2013-01-25_0305  valid   244KB     0%
0%
                        hourly.2013-01-25_0405  valid   244KB     0%
0%
                        hourly.2013-01-25_0505  valid   244KB     0%
0%

7 entries were displayed.
```

2. Restaure el contenido de un volumen de una copia Snapshot en un volumen de destino de SnapMirror:

   ```
   snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>
   -destination-path <SVM:volume>|<cluster://SVM/volume> -source-snapshot
   <snapshot>
   ```

   Para obtener una sintaxis de comando completa, consulte la página man.

   > Se debe ejecutar este comando desde la SVM de origen original o desde el clúster de origen original.

   El siguiente comando restaura el contenido del volumen de origen original `primary1` Desde la copia Snapshot `daily.2013-01-25_0010` en el volumen de destino original `secondary1`:

```
cluster_src::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010

Warning: All data newer than Snapshot copy daily.2013-01-25_0010 on
volume vserverA:primary1 will be deleted.

Do you want to continue? {y|n}: y

[Job 34] Job is queued: snapmirror restore from source
vserverB:secondary1 for the snapshot daily.2013-01-25_0010.
```

3. Vuelva a montar el volumen restaurado y reinicie todas las aplicaciones que utilizan el volumen.

Otras maneras de hacerlo en ONTAP

Para ejecutar estas tareas con…	Ver este contenido…
System Manager rediseñado (disponible con ONTAP 9.7 y versiones posteriores)	"Restaurar un volumen de una copia de Snapshot anterior"
System Manager Classic (disponible con ONTAP 9.7 y versiones anteriores)	"Información general sobre la restauración de volúmenes mediante SnapVault"

Actualice manualmente una relación de replicación

Es posible que deba actualizar una relación de replicación manualmente si falla una actualización debido a que se trasladó el volumen de origen.

Acerca de esta tarea

SnapMirror cancela todas las transferencias desde un volumen de origen movido hasta que se actualice la relación de replicación de forma manual.

A partir de ONTAP 9.5, se admiten las relaciones de SnapMirror síncrono. Si bien los volúmenes de origen y destino están sincronizados en todo momento en estas relaciones, la vista del clúster secundario se sincroniza con el primario solo por hora. Si desea ver los datos de un momento específico en el destino, debe realizar una actualización manual ejecutando el `snapmirror update` comando.

Paso

1. Actualice manualmente una relación de replicación:

   `snapmirror update -source-path` *`SVM:volume|cluster://SVM/volume`*`, … -destination -path` *`SVM:volume|cluster://SVM/volume`*`, …`

   Para obtener una sintaxis de comando completa, consulte la página man.

   > Se debe ejecutar este comando desde la SVM de destino o el clúster de destino. El comando genera errores si no existe una copia Snapshot común en el origen y el destino. Uso `snapmirror initialize` para volver a inicializar la relación.

En el ejemplo siguiente se actualiza la relación entre el volumen de origen `volA` encendido `svm1` y el volumen de destino `volA_dst` encendido `svm_backup`:

```
cluster_src::> snapmirror update -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Resincronice una relación de replicación

Es necesario volver a sincronizar una relación de replicación después de hacer que un volumen de destino sea modificable, después de un error en la actualización porque no existe una copia Snapshot común en los volúmenes de origen y destino o si desea cambiar la política de replicación de la relación.

Acerca de esta tarea

- Aunque la resincronización no requiere una transferencia básica, puede requerir mucho tiempo. Puede que desee ejecutar la resincronización en horas de menor actividad.
- Los volúmenes que forman parte de una configuración en cascada o de dispersión pueden tardar más en resincronizar. No es poco frecuente ver la relación de SnapMirror que informa sobre el estado "preparación" para un periodo de tiempo prolongado.

Paso

1. Resincronización de los volúmenes de origen y destino:

   `snapmirror resync -source-path` *`SVM:volume|cluster://SVM/volume`*`, … -destination -path` *`SVM:volume|cluster://SVM/volume`*`, … -type DP|XDP -policy` *`policy`*

   Para obtener una sintaxis de comando completa, consulte la página man.

   > Se debe ejecutar este comando desde la SVM de destino o el clúster de destino.

   En el siguiente ejemplo, vuelva a establecer la relación entre el volumen de origen `volA` encendido `svm1` y el volumen de destino `volA_dst` encendido `svm_backup`:

   ```
   cluster_dst::> snapmirror resync -source-path svm1:volA -destination
   -path svm_backup:volA_dst
   ```

Elimine una relación de replicación de volúmenes

Puede utilizar el `snapmirror delete` y.. `snapmirror release` comandos para eliminar una relación de replicación de volumen. A continuación, puede eliminar manualmente los volúmenes de destino innecesarios.

Acerca de esta tarea

La `snapmirror release` Comando elimina todas las copias Snapshot creadas con SnapMirror del origen. Puede utilizar el `-relationship-info-only` Opción a conservar las copias Snapshot.

Pasos

1. Desactive la relación de replicación:

   `snapmirror quiesce -destination-path` *`SVM:volume|cluster://SVM/volume`*

   ```
   cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
   ```

2. (Opcional) rompa la relación de replicación si requiere que el volumen de destino sea un volumen de lectura/escritura. Puede omitir este paso si planea eliminar el volumen de destino o si no necesita que el volumen sea de lectura/escritura:

   `snapmirror break -source-path SVM:volume|cluster://SVM/volume, … -destination -path SVM:volume|cluster://SVM/volume, …`

   ```
   cluster_dst::> snapmirror break -source-path svm1:volA -destination-path
   svm_backup:volA_dst
   ```

3. Elimine la relación de replicación:

   `snapmirror delete -source-path` *`SVM:volume|cluster://SVM/volume`*`, … -destination -path` *`SVM:volume|cluster://SVM/volume`*`, …`

   Para obtener una sintaxis de comando completa, consulte la página man.

   > Debe ejecutar este comando desde el clúster de destino o la SVM de destino.

   En el siguiente ejemplo, se elimina la relación entre el volumen de origen `volA` encendido `svm1` y el volumen de destino `volA_dst` encendido `svm_backup`:

   ```
   cluster_dst::> snapmirror delete -source-path svm1:volA -destination
   -path svm_backup:volA_dst
   ```

4. Libere la información de relaciones de replicación desde la SVM de origen:

   `snapmirror release -source-path` *`SVM:volume|cluster://SVM/volume`*`, … -destination-path` *`SVM:volume|cluster://SVM/volume`*`, …`

   Para obtener una sintaxis de comando completa, consulte la página man.

   > Se debe ejecutar este comando desde el clúster de origen o la SVM de origen.

   En el siguiente ejemplo, se libera información para la relación de replicación especificada desde la SVM de origen `svm1`:

```
cluster_src::> snapmirror release -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Gestión de la eficiencia del almacenamiento

SnapMirror mantiene la eficiencia del almacenamiento en los volúmenes de origen y destino, con una excepción, cuando se habilita la compresión de datos de postprocesamiento en el destino. En este caso, se pierde toda la eficiencia del almacenamiento en el destino. Para corregir este problema, hay que deshabilitar la compresión de postprocesamiento en el destino, actualizar la relación manualmente y volver a habilitar la eficiencia del almacenamiento.

Lo que necesitará

- Las SVM y los clústeres de origen y destino deben tener una relación entre iguales.

  "Relaciones entre iguales de clústeres y SVM"

- Debe deshabilitar la compresión de postprocesamiento en el destino.

Acerca de esta tarea

Puede utilizar el `volume efficiency show` comando para determinar si la eficiencia está habilitada en un volumen. Para obtener más información, consulte las páginas de manual.

Puede comprobar si SnapMirror mantiene la eficiencia del almacenamiento consultando los registros de auditoría de SnapMirror y buscando la descripción de la transferencia. Si aparece la descripción de la transferencia `transfer_desc=Logical Transfer`, SnapMirror no mantiene la eficiencia del almacenamiento. Si aparece la descripción de la transferencia `transfer_desc=Logical Transfer with Storage Efficiency`, SnapMirror mantiene la eficiencia del almacenamiento. Por ejemplo:

```
Fri May 22 02:13:02 CDT 2020 ScheduledUpdate[May 22 02:12:00]:cc0fbc29-
b665-11e5-a626-00a09860c273 Operation-Uuid=39fbcf48-550a-4282-a906-
df35632c73a1 Group=none Operation-Cookie=0 action=End source=<sourcepath>
destination=<destpath> status=Success bytes_transferred=117080571
network_compression_ratio=1.0:1 transfer_desc=Logical Transfer - Optimized
Directory Mode
```

Transferencia lógica con almacenamiento

A partir de ONTAP 9.3, ya no se requiere la actualización manual para volver a habilitar la eficiencia del almacenamiento. Si SnapMirror detecta que la compresión de postprocesamiento se ha deshabilitado, vuelve a habilitar automáticamente la eficiencia del almacenamiento en la siguiente actualización programada. Tanto el origen como el destino deben ejecutar ONTAP 9.3.

A partir de ONTAP 9.3, los sistemas AFF gestionan las configuraciones de eficiencia del almacenamiento de forma diferente a las de los sistemas FAS después de crear su escritura en un volumen de destino:

- Después de hacer que un volumen de destino pueda ser modificable mediante el `snapmirror break` la

política de almacenamiento en caché del volumen se establece automáticamente en "'auto'" (valor predeterminado).

> Este comportamiento se aplica solo a volúmenes FlexVol, y no se aplica a volúmenes FlexGroup.

- En la resincronización, la política de almacenamiento en caché se establece automáticamente en «'none» y la deduplicación y la compresión en línea se deshabilitan automáticamente, independientemente de la configuración original. Debe modificar los ajustes manualmente según sea necesario.

> Las actualizaciones manuales con eficiencia del almacenamiento, que pueden ser laboriosas. Se recomienda ejecutar la operación en horas de menor actividad.

Paso

1. Actualice una relación de replicación y vuelva a habilitar la eficiencia del almacenamiento:

   `snapmirror update -source-path` *`SVM:volume|cluster://SVM/volume`*`, … -destination -path` *`SVM:volume|cluster://SVM/volume`*`, … -enable-storage-efficiency true`

   Para obtener una sintaxis de comando completa, consulte la página man.

   > Se debe ejecutar este comando desde la SVM de destino o el clúster de destino. El comando genera errores si no existe una copia Snapshot común en el origen y el destino. Uso `snapmirror initialize` para volver a inicializar la relación.

   En el ejemplo siguiente se actualiza la relación entre el volumen de origen `volA` encendido `svm1` y el volumen de destino `volA_dst` encendido `svm_backup`y reactivación de la eficacia de almacenamiento:

   ```
   cluster_dst::> snapmirror update -source-path svm1:volA -destination
   -path svm_backup:volA_dst -enable-storage-efficiency true
   ```

Use la limitación global de SnapMirror

La limitación de red global está disponible para todas las transferencias de SnapMirror y SnapVault a nivel de nodo.

Acerca de esta tarea

La limitación global de SnapMirror restringe el ancho de banda utilizado por transferencias entrantes o salientes de SnapMirror y SnapVault. La restricción se aplica en todo el clúster en todos los nodos del clúster.

Por ejemplo, si el acelerador saliente está establecido en 100 Mbps, cada nodo del clúster tendrá el ancho de banda saliente establecido en 100 Mbps. Si la regulación global está deshabilitada, se desactiva en todos los nodos.

Aunque las velocidades de transferencia de datos a menudo se expresan en bits por segundo (bps), los valores del acelerador deben introducirse en kilobytes por segundo (kbps).

> En las versiones ONTAP 9.9.1 y anteriores, el acelerador no tiene ningún efecto activado `volume move` transferencias o transferencias de reflejos con uso compartido de la carga. A partir de ONTAP 9.10.0, es posible especificar una opción para acelerar las operaciones de movimiento de volúmenes. Para obtener más información, consulte "Cómo acelerar el movimiento del volumen en ONTAP 9.10 y versiones posteriores."

La limitación global funciona con la función acelerador por relación para transferencias de SnapMirror y SnapVault. El acelerador por relación se aplica hasta que el ancho de banda combinado de las transferencias por relación supere el valor de la aceleración global, después de lo cual se aplica la aceleración global. Un valor de acelerador `0` implica que la limitación global está desactivada.

> La regulación global de SnapMirror no tiene ningún efecto en las relaciones de SnapMirror síncrono cuando están en sincronización. Sin embargo, el acelerador hace efecto en las relaciones de SnapMirror síncrono cuando realizan una fase de transferencia asíncrona, como una operación de inicialización o después de un evento de no sincronización. Por este motivo, no se recomienda habilitar la regulación global con relaciones de SnapMirror síncrono.

Pasos

1. Habilitar la limitación global:

   `options -option-name replication.throttle.enable on|off`

   El siguiente ejemplo muestra cómo habilitar la regulación global de SnapMirror `cluster_dst`:

   ```
   cluster_dst::> options -option-name replication.throttle.enable on
   ```

2. Especifique el ancho de banda total máximo utilizado por las transferencias entrantes en el clúster de destino:

   `options -option-name replication.throttle.incoming.max_kbs` *KBps*

   El ancho de banda mínimo recomendado del acelerador es de 4 kbps y el máximo es de 2 TB/s. El valor predeterminado de esta opción es `unlimited`, lo que significa que no hay límite en el ancho de banda total utilizado.

   El siguiente ejemplo muestra cómo establecer el ancho de banda total máximo utilizado por las transferencias entrantes en 100 Mbps:

   ```
   cluster_dst::> options -option-name
   replication.throttle.incoming.max_kbs 12500
   ```

   > 100 Mbps = 12500 kbps

3. Especifique el ancho de banda total máximo que utilizan las transferencias salientes en el clúster de origen:

   `options -option-name replication.throttle.outgoing.max_kbs` *KBps*

   El ancho de banda mínimo recomendado del acelerador es de 4 kbps y el máximo es de 2 TB/s. El valor

predeterminado de esta opción es `unlimited`, lo que significa que no hay límite en el ancho de banda total utilizado. Los valores de los parámetros están en kbps.

En el siguiente ejemplo se muestra cómo establecer el ancho de banda total máximo utilizado por las transferencias salientes en 100 Mbps:

```
cluster_src::> options -option-name
replication.throttle.outgoing.max_kbs 12500
```

Gestione la replicación de SVM de SnapMirror

Acerca de la replicación de SVM de SnapMirror

Puede usar SnapMirror para crear una relación de protección de datos entre SVM. En este tipo de relación de protección de datos, se replica toda o parte de la configuración de la SVM, desde las exportaciones NFS y los recursos compartidos de SMB hasta el RBAC, así como los datos en los volúmenes que posee la SVM.

Tipos de relaciones admitidos

Solo los SVM que proporcionan servicios de datos pueden replicarse. Se admiten los siguientes tipos de relaciones de protección de datos:

- *SnapMirror DR,* en el que el destino normalmente solo contiene las copias Snapshot que están actualmente en el origen.

  A partir de ONTAP 9.9.1, este comportamiento cambia cuando se utiliza la directiva mirror-vault. A partir de ONTAP 9.9.1, puede crear diferentes políticas de Snapshot en el origen y el destino; las copias Snapshot en el destino no se sobrescriben con las copias Snapshot en el origen:

  - No se sobrescriben del origen al destino durante las operaciones programadas normales, las actualizaciones y la resincronización
  - No se eliminan durante las operaciones de interrupción.
  - No se eliminan durante las operaciones de resincronización.
    Cuando configura una relación de desastre de SVM con la política de reflejo-almacén con ONTAP 9.9.1 y versiones posteriores, la política se comporta de la siguiente manera:
  - Las políticas de copia de Snapshot definidas por el usuario en el origen no se copian en el destino.
  - Las políticas de copia de Snapshot definidas por el sistema no se copian en el destino.
  - La asociación de volumen con políticas de Snapshot definidas por el usuario y el sistema no se copia en el destino.

    SVM.
- A partir de ONTAP 9.2, se *replicación unificada de SnapMirror,* en el que el destino está configurado para recuperación ante desastres y retención a largo plazo.

Aquí puede encontrar información detallada sobre estos tipos de relaciones: "Replicación de volúmenes de SnapMirror".

El *policy type* de la directiva de replicación determina el tipo de relación que admite. La siguiente tabla muestra los tipos de políticas disponibles.

Tipo de política	Tipo de relación
reflejo asíncrono	Recuperación ante desastres de SnapMirror
mirror-vault	Replicación unificada

XDP sustituye a DP como la replicación SVM predeterminada en ONTAP 9.4

A partir de ONTAP 9.4, las relaciones de protección de datos de la SVM se establecen en el modo XDP de manera predeterminada. Las relaciones de protección de datos de SVM siguen siendo las predeterminadas para el modo DP en ONTAP 9.3 y versiones anteriores.

Las relaciones existentes no se ven afectadas por el nuevo valor predeterminado. Si una relación ya es del tipo DP, seguirá siendo del tipo DP. La siguiente tabla muestra el comportamiento que puede esperar.

Si especifica…	El tipo es…	La política predeterminada (si no se especifica una política) es…
PROTECCIÓN DE DATOS	XDP	MirrorAllSnapshots (recuperación ante desastres de SnapMirror)
Nada	XDP	MirrorAllSnapshots (recuperación ante desastres de SnapMirror)
XDP	XDP	MirrorAndVault (replicación unificada)

Puede encontrar más información sobre los cambios en el valor predeterminado aquí: "XDP sustituye a DP como la opción predeterminada de SnapMirror".

> La independencia de la versión no se admite para la replicación de SVM. En una configuración de recuperación ante desastres de SVM, la máquina virtual de almacenamiento de destino debe estar en un clúster que ejecute la misma versión de ONTAP que el clúster de SVM de origen para admitir operaciones de conmutación al nodo de respaldo y conmutación de conmutación por error.

"Versiones de ONTAP compatibles para relaciones de SnapMirror"

Cómo se replican las configuraciones de SVM

El contenido de una relación de replicación de SVM se determina por la interacción de los siguientes campos:

- La `-identity-preserve true` opción de `snapmirror create` El comando replica toda la configuración de SVM.

  La `-identity-preserve false` La opción replica solamente los volúmenes y las configuraciones de autenticación y autorización de la SVM, así como los ajustes del protocolo y del servicio de nombres indicados en "Configuraciones replicadas en las relaciones de recuperación ante desastres de máquina

virtual de almacenamiento".

- La `-discard-configs network` opción de `snapmirror policy create` El comando excluye las LIF y la configuración de red relacionada desde la replicación de SVM, para su uso en casos en los que las SVM de origen y destino se encuentran en subredes distintas.
- La `-vserver-dr-protection unprotected` opción de `volume modify` El comando excluye el volumen especificado de la replicación de SVM.

De lo contrario, la replicación de SVM es casi idéntica a la replicación de volúmenes. Puede utilizar prácticamente el mismo flujo de trabajo para la replicación de SVM que el que utiliza para la replicación de volúmenes.

Detalles de soporte

La siguiente tabla muestra detalles de soporte para la replicación de SVM de SnapMirror.

Recurso o característica	Detalles de soporte
Tipos de implementación	• Origen único en destino único • A partir de ONTAP 9.4, punto de salida. Solo puede fan-out a dos destinos. De forma predeterminada, solo se permite una relación de conservación de identidad real por SVM de origen.
Tipos de relación	• Recuperación ante desastres con SnapMirror • A partir de ONTAP 9.2, la replicación unificada de SnapMirror
Alcance de replicación	Solo interconexión de clústeres. No puede replicar SVM en el mismo clúster.
Protección autónoma de ransomware	• Compatible a partir de ONTAP 9.12.1. Para obtener más información, consulte "Protección autónoma de ransomware"
Compatibilidad asíncrona de grupos de coherencia	A partir de ONTAP 9.14.1, se admiten un máximo de 32 relaciones de recuperación ante desastres de SVM cuando hay grupos de coherencia. Consulte "Proteja un grupo de consistencia" y.. "Límites del grupo de consistencia" si quiere más información.
FabricPool	A partir de ONTAP 9.6, la replicación de SVM de SnapMirror es compatible con FabricPool.

MetroCluster	A partir de ONTAP 9.11.1, ambos lados de una relación de recuperación ante desastres de SVM dentro de una configuración de MetroCluster pueden actuar como origen para configuraciones de recuperación ante desastres adicionales de SVM. A partir de ONTAP 9.5, la replicación de SVM de SnapMirror es compatible con las configuraciones de MetroCluster. • En versiones anteriores a ONTAP 9,10.X, una configuración de MetroCluster no puede ser el destino de una relación de recuperación ante desastres de SVM. • En ONTAP 9.10.1 y versiones posteriores, una configuración de MetroCluster puede ser el destino de una relación de recuperación de desastres de SVM únicamente con fines de migración y debe cumplir con todos los requisitos necesarios descritos en "TR-4966: Migración de una SVM a una solución de MetroCluster". • Solo una SVM activa en una configuración de MetroCluster puede ser el origen de una relación de recuperación ante desastres de SVM. Un origen puede ser una SVM sincronizada en origen antes de realizar una conmutación de sitios o una SVM sincronizada en destino después de efectuar una conmutación de sitios. • Cuando una configuración de MetroCluster presenta un estado estable, la SVM sincronizada en destino de MetroCluster no puede ser el origen de una relación de recuperación ante desastres de SVM, ya que los volúmenes no están en línea. • Cuando la SVM sincronizada en origen es el origen de una relación de recuperación ante desastres de SVM, la información sobre la relación de recuperación ante desastres de SVM de origen se replica en el partner de MetroCluster. • Durante los procesos de conmutación de sitios y conmutación de estado, se podría producir un error en la replicación al destino de recuperación ante desastres de SVM. Sin embargo, una vez que finalice el proceso de conmutación de sitios o conmutación de estado, se realizarán las siguientes actualizaciones programadas para la recuperación ante desastres de la máquina virtual de almacenamiento.

Grupo de consistencia	Compatible a partir de ONTAP 9.14.1. Para obtener más información, consulte Proteja un grupo de consistencia.
ONTAP S3	No compatible con la recuperación ante desastres de SVM.
SnapMirror síncrono	No compatible con la recuperación ante desastres de SVM.
Independencia de versiones	No admitido.
Cifrado de volúmenes	• Los volúmenes cifrados en el origen se cifran en el destino. • Los servidores incorporados de Key Manager o KMIP deben configurarse en el destino. • En el destino se generan nuevas claves de cifrado. • Si el destino no contiene un nodo compatible con el cifrado de volúmenes ., la replicación se realiza correctamente, pero los volúmenes de destino no están cifrados.

Configuraciones replicadas en las relaciones de recuperación ante desastres de máquina virtual de almacenamiento

La siguiente tabla muestra la interacción del `snapmirror create -identity-preserve` y la `snapmirror policy create -discard-configs network` opción:

Configuración replicada		**`-identity-preserve true`**		**`-identity-preserve false`**
		Política sin `-discard-configs network` set	**Política con `-discard-configs network` set**	
Red	LIF NAS	Sí	No	No
Configuración de Kerberos para LIF	Sí	No	No	LIF SAN
No	No	No	Directivas de firewall	Sí
Sí	No	Normativas de servicio	Sí	Sí
No	Rutas	Sí	No	No

Dominio de retransmisión	No	No	No	Subred
No	No	No	Espacio IP	No
No	No	SMB	Servidor SMB	Sí
Sí	No	Grupos locales y usuario local	Sí	Sí
Sí	Privilegio	Sí	Sí	Sí
Copia oculta	Sí	Sí	Sí	BranchCache
Sí	Sí	Sí	Opciones del servidor	Sí
Sí	Sí	Seguridad del servidor	Sí	Sí
No	Directorio inicial, compartir	Sí	Sí	Sí
Enlace simbólico	Sí	Sí	Sí	Política de Fpolicy, política de FSecurity y NTFS de FSecurity
Sí	Sí	Sí	Asignación de nombres y asignación de grupos	Sí
Sí	Sí	Información de auditoría	Sí	Sí
Sí	NFS	Políticas de exportación	Sí	Sí
No	Reglas de la política de exportación	Sí	Sí	No
Servidor NFS	Sí	Sí	No	RBAC

Certificados de seguridad	Sí	Sí	No	Inicio de sesión de usuario, clave pública, función y configuración de funciones
Sí	Sí	Sí	SSL	Sí
Sí	No	Servicios de nombres	Hosts DNS y DNS	Sí
Sí	No	Usuario UNIX y grupo UNIX	Sí	Sí
Sí	Kerberos Reino y bloques de claves Kerberos	Sí	Sí	No
Cliente LDAP y LDAP	Sí	Sí	No	Grupo de red
Sí	Sí	No	NIS	Sí
Sí	No	Acceso Web y Web	Sí	Sí
No	Volumen	Objeto	Sí	Sí
Sí	Copias Snapshot, políticas de Snapshot y políticas de eliminación automática	Sí	Sí	Sí
Política de eficiencia	Sí	Sí	Sí	Regla de política de cuotas y de política de cuotas
Sí	Sí	Sí	Cola de recuperación	Sí
Sí	Sí	Volumen raíz	Espacio de nombres	Sí
Sí	Sí	Datos de usuarios	No	No
No	Qtrees	No	No	No

Cuotas	No	No	No	Calidad de servicio en el nivel de los archivos
No	No	No	Atributos: estado del volumen raíz, garantía de espacio, tamaño, tamaño automático y número total de archivos	No
No	No	Calidad de servicio del almacenamiento	Grupo de políticas de calidad de servicio	Sí
Sí	Sí	Fibre Channel (FC)	No	No
No	ISCSI	No	No	No
LUN	Objeto	Sí	Sí	Sí
grupos de iniciadores	No	No	No	conjuntos de puertos
No	No	No	Números de serie	No
No	No	SNMP	usuarios v3	Sí

Límites de almacenamiento para recuperación ante desastres de SVM

En la siguiente tabla se muestra el número máximo recomendado de volúmenes y relaciones de recuperación ante desastres de SVM admitidas por objeto de almacenamiento. Debe ser consciente de que los límites dependen a menudo de la plataforma. Consulte la "Hardware Universe" para conocer los límites de su configuración específica.

Objeto de almacenamiento	Límite
SVM	300 volúmenes flexibles
Pareja de HA	1,000 volúmenes flexibles
Clúster	128 Relaciones de desastre de SVM

Replicar las configuraciones de SVM

Flujo de trabajo de replicación SVM de SnapMirror

La replicación SVM de SnapMirror implica la creación de la SVM de destino, la creación de una programación de trabajos de replicación y la creación e inicialización de una relación de SnapMirror.

Debe determinar qué flujo de trabajo de replicación se adapta mejor a sus necesidades:

- "Replique toda una configuración de SVM"
- "Excluya las LIF y la configuración de red relacionada desde la replicación de SVM"
- "Exlude red, servicio de nombres y otros ajustes de la configuración de la máquina virtual de almacenamiento"

Criterios para colocar volúmenes en las SVM de destino

Al replicar volúmenes de la SVM de origen a la SVM de destino, es importante conocer los criterios para la selección de agregados.

Los agregados se seleccionan según los siguientes criterios:

- Los volúmenes siempre se colocan en agregados que no son raíz.
- Los agregados no raíz se seleccionan en función del espacio libre disponible y de la cantidad de volúmenes que ya se encuentran alojados en el agregado.

  Los agregados con más espacio libre y menos volúmenes tienen prioridad. Se selecciona el agregado con la prioridad más alta.

- Los volúmenes de origen en agregados de FabricPool se colocan en agregados de FabricPool en el destino con la misma política de organización en niveles.
- Si un volumen de la SVM de origen se encuentra en un agregado de Flash Pool, el volumen se coloca en un agregado de Flash Pool en la SVM de destino, si existe un agregado de este tipo y tiene suficiente espacio libre.
- Si la `-space-guarantee` la opción del volumen que se replica se establece en `volume`, sólo se tienen en cuenta los agregados con un espacio libre superior al tamaño del volumen.
- El tamaño del volumen crece automáticamente en la SVM de destino durante la replicación, según el tamaño del volumen de origen.

  Si desea reservar de antemano el tamaño en la SVM de destino, debe cambiar el tamaño del volumen. El tamaño del volumen no se reduce automáticamente en la SVM de destino según la SVM de origen.

Si desea mover un volumen de un agregado a otro, puede usar el `volume move` En la SVM de destino.

Replique toda una configuración de SVM

Puede utilizar el `-identity-preserve true` opción de `snapmirror create` Para replicar una configuración de SVM completa.

Antes de empezar

Las SVM y los clústeres de origen y destino deben tener una relación entre iguales.
Para obtener más información, consulte "Cree una relación de paridad entre clústeres" y.. "Cree una relación

de interconexión de clústeres entre iguales de SVM".

Para obtener una sintaxis de comando completa, consulte la página man.

Acerca de esta tarea

Este flujo de trabajo supone que ya está usando una directiva predeterminada o una directiva de replicación personalizada.

A partir de ONTAP 9.9.1, cuando se utiliza la política de mirroring-almacén, puede crear diferentes políticas de Snapshot en la SVM de origen y de destino; las copias de Snapshot en el destino no se sobrescriben con las copias Snapshot en el origen. Para obtener más información, consulte "Replicación de SVM de SnapMirror".

Pasos

1. Cree una SVM de destino:

   `vserver create -vserver SVM_name -subtype dp-destination`

   El nombre de SVM debe ser único en los clústeres de origen y destino.

   En el ejemplo siguiente se crea una SVM de destino llamada `svm_backup`:

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
   ```

2. En el clúster de destino, cree una relación entre iguales de SVM mediante el `vserver peer create` comando.

   Para obtener más información, consulte "Cree una relación de interconexión de clústeres entre iguales de SVM".

3. Crear una programación de trabajo de replicación:

   `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

   Para `-month`, `-dayofweek`, y. `-hour`, puede especificar `all` para ejecutar el trabajo cada mes, día de la semana y hora, respectivamente.

   > La programación mínima admitida (RPO) para volúmenes FlexVol en una relación de SnapMirror de SVM es de 15 minutos. La programación mínima admitida (RPO) para volúmenes FlexGroup en una relación de SnapMirror de SVM es de 30 minutos.

   En el ejemplo siguiente se crea una programación de trabajo denominada `my_weekly` Es decir, los sábados a las 3:00 horas:

   ```
   cluster_dst::> job schedule cron create -name my_weekly -dayofweek
   saturday -hour 3 -minute 0
   ```

4. A partir de la SVM de destino o el clúster de destino, cree una relación de replicación:

   `snapmirror create -source-path SVM_name: -destination-path SVM_name: -type`

`DP|XDP -schedule schedule -policy policy -identity-preserve true`

> Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones.

En el siguiente ejemplo se crea una relación de recuperación ante desastres de SnapMirror con los valores predeterminados `MirrorAllSnapshots` política:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAllSnapshots
-identity-preserve true
```

En el ejemplo siguiente se crea una relación de replicación unificada con la opción predeterminada `MirrorAndVault` política:

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAndVault
-identity-preserve true
```

Suponiendo que ha creado una directiva personalizada con el tipo de directiva `async-mirror`, En el siguiente ejemplo se crea una relación de recuperación ante desastres de SnapMirror:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_mirrored -identity
-preserve true
```

Suponiendo que ha creado una directiva personalizada con el tipo de directiva `mirror-vault`, en el ejemplo siguiente se crea una relación de replicación unificada:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_unified -identity
-preserve true
```

5. Detenga la SVM de destino:

   `vserver stop`

   `SVM name`

   En el ejemplo siguiente se detiene una SVM de destino denominada dvs1:

   ```
   cluster_dst::> vserver stop -vserver dvs1
   ```

6. En la SVM de destino o en el clúster de destino, inicialice la relación de replicación de SVM: +

   `snapmirror initialize -source-path SVM_name: -destination-path SVM_name:`

   En el siguiente ejemplo se inicializa la relación entre la SVM de origen, `svm1`Y la SVM de destino, `svm_backup`:

   ```
   cluster_dst::> snapmirror initialize -source-path svm1: -destination
   -path svm_backup:
   ```

Excluya las LIF y la configuración de red relacionada desde la replicación de SVM

Si las SVM de origen y destino están en subredes diferentes, puede utilizar `-discard -configs network` opción de `snapmirror policy create` Comando para excluir LIF y configuración de red relacionada desde la replicación de SVM.

Lo que necesitará

Las SVM y los clústeres de origen y destino deben tener una relación entre iguales.

Para obtener más información, consulte "Cree una relación de paridad entre clústeres" y.. "Cree una relación de interconexión de clústeres entre iguales de SVM".

Acerca de esta tarea

La `-identity-preserve` opción de `snapmirror create` el comando debe estar establecido en `true` Al crear la relación de replicación de SVM.

Para obtener una sintaxis de comando completa, consulte la página man.

Pasos

1. Cree una SVM de destino:

   `vserver create -vserver SVM -subtype dp-destination`

   El nombre de SVM debe ser único en los clústeres de origen y destino.

   En el ejemplo siguiente se crea una SVM de destino llamada `svm_backup`:

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
   ```

2. En el clúster de destino, cree una relación entre iguales de SVM mediante el `vserver peer create` comando.

   Para obtener más información, consulte "Cree una relación de interconexión de clústeres entre iguales de SVM".

3. Crear un programa de trabajo:

   `job schedule cron create -name job_name -month month -dayofweek day_of_week`

`-day day_of_month -hour hour -minute minute`

Para `-month`, `-dayofweek`, y. `-hour`, puede especificar `all` para ejecutar el trabajo cada mes, día de la semana y hora, respectivamente.

> La programación mínima admitida (RPO) para volúmenes FlexVol en una relación de SnapMirror de SVM es de 15 minutos. La programación mínima admitida (RPO) para volúmenes FlexGroup en una relación de SnapMirror de SVM es de 30 minutos.

En el ejemplo siguiente se crea una programación de trabajo denominada `my_weekly` Es decir, los sábados a las 3:00 horas:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

4. Cree una política de replicación personalizada:

   `snapmirror policy create -vserver SVM -policy policy -type async-mirror|vault|mirror-vault -comment comment -tries transfer_tries -transfer -priority low|normal -is-network-compression-enabled true|false -discard -configs network`

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el ejemplo siguiente se crea una normativa de replicación personalizada para recuperación ante desastres de SnapMirror que excluye las LIF:

   ```
   cluster_dst::> snapmirror policy create -vserver svm1 -policy
   DR_exclude_LIFs -type async-mirror -discard-configs network
   ```

   En el ejemplo siguiente se crea una directiva de replicación personalizada para la replicación unificada que excluye las LIF:

   ```
   cluster_dst::> snapmirror policy create -vserver svm1 -policy
   unified_exclude_LIFs -type mirror-vault -discard-configs network
   ```

5. A partir de la SVM de destino o el clúster de destino, ejecute el siguiente comando para crear una relación de replicación:

   `snapmirror create -source-path SVM: -destination-path SVM: -type DP|XDP -schedule schedule -policy policy -identity-preserve true|false`

   > Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea los ejemplos a continuación.

   En el ejemplo siguiente se crea una relación de recuperación ante desastres de SnapMirror que excluye las LIF:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy DR_exclude_LIFs
-identity-preserve true
```

En el ejemplo siguiente se crea una relación de replicación unificada de SnapMirror que excluye las LIF:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy unified_exclude_LIFs
-identity-preserve true
```

6. Detenga la SVM de destino:

   `vserver stop`

   `SVM name`

   En el ejemplo siguiente se detiene una SVM de destino denominada dvs1:

   ```
   cluster_dst::> vserver stop -vserver dvs1
   ```

7. En la SVM de destino o el clúster de destino, inicialice una relación de replicación:

   `snapmirror initialize -source-path` *`SVM`*`: -destination-path` *`SVM`*`:`

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el siguiente ejemplo se inicializa la relación entre el origen, `svm1` y el destino, `svm_backup`:

   ```
   cluster_dst::> snapmirror initialize -source-path svm1: -destination
   -path svm_backup:
   ```

Después de terminar

Es necesario configurar la red y los protocolos en la SVM de destino para acceder a los datos en caso de que se produzca un desastre.

Excluya la red, el servicio de nombres y otras configuraciones de la replicación de SVM

Puede utilizar el `-identity-preserve false` opción de `snapmirror create` Comando para replicar solo los volúmenes y las configuraciones de seguridad de una SVM. También se conservan algunos ajustes de protocolo y servicio de nombres.

Acerca de esta tarea

Para obtener una lista de los ajustes de protocolo y servicio de nombres conservados, consulte "Configuraciones replicadas en relaciones de recuperación ante desastres de SVM".

Para obtener una sintaxis de comando completa, consulte la página man.

Antes de empezar

Las SVM y los clústeres de origen y destino deben tener una relación entre iguales.

Para obtener más información, consulte "Cree una relación de paridad entre clústeres" y.. "Cree una relación de interconexión de clústeres entre iguales de SVM".

Pasos

1. Cree una SVM de destino:

   `vserver create -vserver SVM -subtype dp-destination`

   El nombre de SVM debe ser único en los clústeres de origen y destino.

   En el ejemplo siguiente se crea una SVM de destino llamada `svm_backup`:

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
   ```

2. En el clúster de destino, cree una relación entre iguales de SVM mediante el `vserver peer create` comando.

   Para obtener más información, consulte "Cree una relación de interconexión de clústeres entre iguales de SVM".

3. Crear una programación de trabajo de replicación:

   `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

   Para `-month`, `-dayofweek`, y. `-hour`, puede especificar `all` para ejecutar el trabajo cada mes, día de la semana y hora, respectivamente.

   > La programación mínima admitida (RPO) para volúmenes FlexVol en una relación de SnapMirror de SVM es de 15 minutos. La programación mínima admitida (RPO) para volúmenes FlexGroup en una relación de SnapMirror de SVM es de 30 minutos.

   En el ejemplo siguiente se crea una programación de trabajo denominada `my_weekly` Es decir, los sábados a las 3:00 horas:

   ```
   cluster_dst::> job schedule cron create -name my_weekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

4. Cree una relación de replicación que excluya la red, el servicio de nombres y otras opciones de configuración:

   `snapmirror create -source-path SVM: -destination-path SVM: -type DP|XDP -schedule schedule -policy policy -identity-preserve false`

> Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea los ejemplos a continuación. Se debe ejecutar este comando desde la SVM de destino o el clúster de destino.

En el siguiente ejemplo se crea una relación de recuperación ante desastres de SnapMirror con los valores predeterminados `MirrorAllSnapshots` política. La relación excluye la red, el servicio de nombres y otras opciones de configuración de la replicación de SVM:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAllSnapshots
-identity-preserve false
```

En el ejemplo siguiente se crea una relación de replicación unificada con la opción predeterminada `MirrorAndVault` política. La relación excluye la red, el servicio de nombres y otras opciones de configuración:

```
cluster_dst:> snapmirror create svm1: -destination-path svm_backup:
-type XDP -schedule my_daily -policy MirrorAndVault -identity-preserve
false
```

Suponiendo que ha creado una directiva personalizada con el tipo de directiva `async-mirror`, En el siguiente ejemplo se crea una relación de recuperación ante desastres de SnapMirror. La relación excluye la red, el servicio de nombres y otras opciones de configuración de la replicación de SVM:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_mirrored -identity
-preserve false
```

Suponiendo que ha creado una directiva personalizada con el tipo de directiva `mirror-vault`, en el ejemplo siguiente se crea una relación de replicación unificada. La relación excluye la red, el servicio de nombres y otras opciones de configuración de la replicación de SVM:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_unified -identity
-preserve false
```

5. Detenga la SVM de destino:

   `vserver stop`

   `SVM name`

   En el ejemplo siguiente se detiene una SVM de destino denominada dvs1:

```
destination_cluster::> vserver stop -vserver dvs1
```

6. Si utiliza SMB, también debe configurar un servidor SMB.

   Consulte "Solo SMB: Crear un servidor SMB".

7. En la SVM de destino o el clúster de destino, inicialice la relación de replicación de SVM:

   `snapmirror initialize -source-path SVM_name: -destination-path SVM_name:`

Después de terminar

Es necesario configurar la red y los protocolos en la SVM de destino para acceder a los datos en caso de que se produzca un desastre.

Especifique los agregados que se utilizarán para las relaciones de recuperación ante desastres de SVM

Después de crear una SVM de recuperación ante desastres, puede usar la `aggr-list` opción con `vserver modify` Comando para limitar qué agregados se usan para alojar los volúmenes de destino de recuperación ante desastres de SVM.

Paso

1. Cree una SVM de destino:

   `vserver create -vserver SVM -subtype dp-destination`

2. Modifique la lista de agregados de la SVM para recuperación ante desastres a fin de limitar los agregados que se usan para alojar el volumen de la SVM para recuperación ante desastres:

   `cluster_dest::> vserver modify -vserver SVM -aggr-list <comma-separated-list>`

SMB Only: Cree un servidor SMB

Si la SVM de origen tiene una configuración de SMB y se optó por establecer `identity-preserve` para `false`, Debe crear un servidor SMB para la SVM de destino. En algunas configuraciones SMB, como los recursos compartidos durante la inicialización de la relación de SnapMirror, es necesario el servidor SMB.

Pasos

1. Inicie la SVM de destino con el `vserver start` comando.

```
destination_cluster::> vserver start -vserver dvs1
[Job 30] Job succeeded: DONE
```

2. Compruebe que la SVM de destino está en la `running` el estado y el subtipo es `dp-destination` mediante el uso de `vserver show` comando.

```
destination_cluster::> vserver show
                                   Admin      Operational Root
Vserver  Type    Subtype           State      State       Volume
Aggregate
-------- ------- ----------       ---------- ----------- ----------
----------
dvs1     data    dp-destination    running    running       -         -
```

3. Cree una LIF mediante el `network interface create` comando.

```
destination_cluster::>network interface create -vserver dvs1 -lif NAS1
-role data -data-protocol cifs -home-node destination_cluster-01 -home
-port a0a-101  -address 192.0.2.128 -netmask 255.255.255.128
```

4. Cree una ruta mediante `network route create` comando.

```
destination_cluster::>network route create -vserver dvs1 -destination
0.0.0.0/0
-gateway 192.0.2.1
```

"Gestión de redes"

5. Configure DNS mediante la `vserver services dns create` comando.

```
destination_cluster::>vserver services dns create -domains
mydomain.example.com -vserver
dvs1 -name-servers 192.0.2.128 -state enabled
```

6. Agregue el controlador de dominio preferido mediante `vserver cifs domain preferred-dc add` comando.

```
destination_cluster::>vserver cifs domain preferred-dc add -vserver dvs1
-preferred-dc
192.0.2.128 -domain mydomain.example.com
```

7. Cree el servidor SMB mediante el `vserver cifs create` comando.

```
destination_cluster::>vserver cifs create -vserver dvs1 -domain
mydomain.example.com
-cifs-server CIFS1
```

8. Detenga la SVM de destino con el `vserver stop` comando.

```
destination_cluster::> vserver stop -vserver dvs1
[Job 46] Job succeeded: DONE
```

Excluya volúmenes de la replicación de SVM

De forma predeterminada, se replican todos los volúmenes de datos RW de la SVM de origen. Si no desea proteger todos los volúmenes de la SVM de origen, puede usar la `-vserver-dr-protection unprotected` opción de `volume modify` Comando para excluir volúmenes de la replicación de SVM.

Pasos

1. Excluya un volumen de la replicación SVM:

   `volume modify -vserver` *`SVM`* `-volume` *`volume`* `-vserver-dr-protection unprotected`

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el siguiente ejemplo, se excluye el volumen `volA_src` A partir de la replicación de SVM:

   ```
   cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
   -protection unprotected
   ```

   Si más adelante desea incluir un volumen en la replicación de SVM que originalmente excluyó, ejecute el siguiente comando:

   `volume modify -vserver` *`SVM`* `-volume` *`volume`* `-vserver-dr-protection protected`

   En el siguiente ejemplo, se incluye el volumen `volA_src` En la replicación de SVM:

   ```
   cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
   -protection protected
   ```

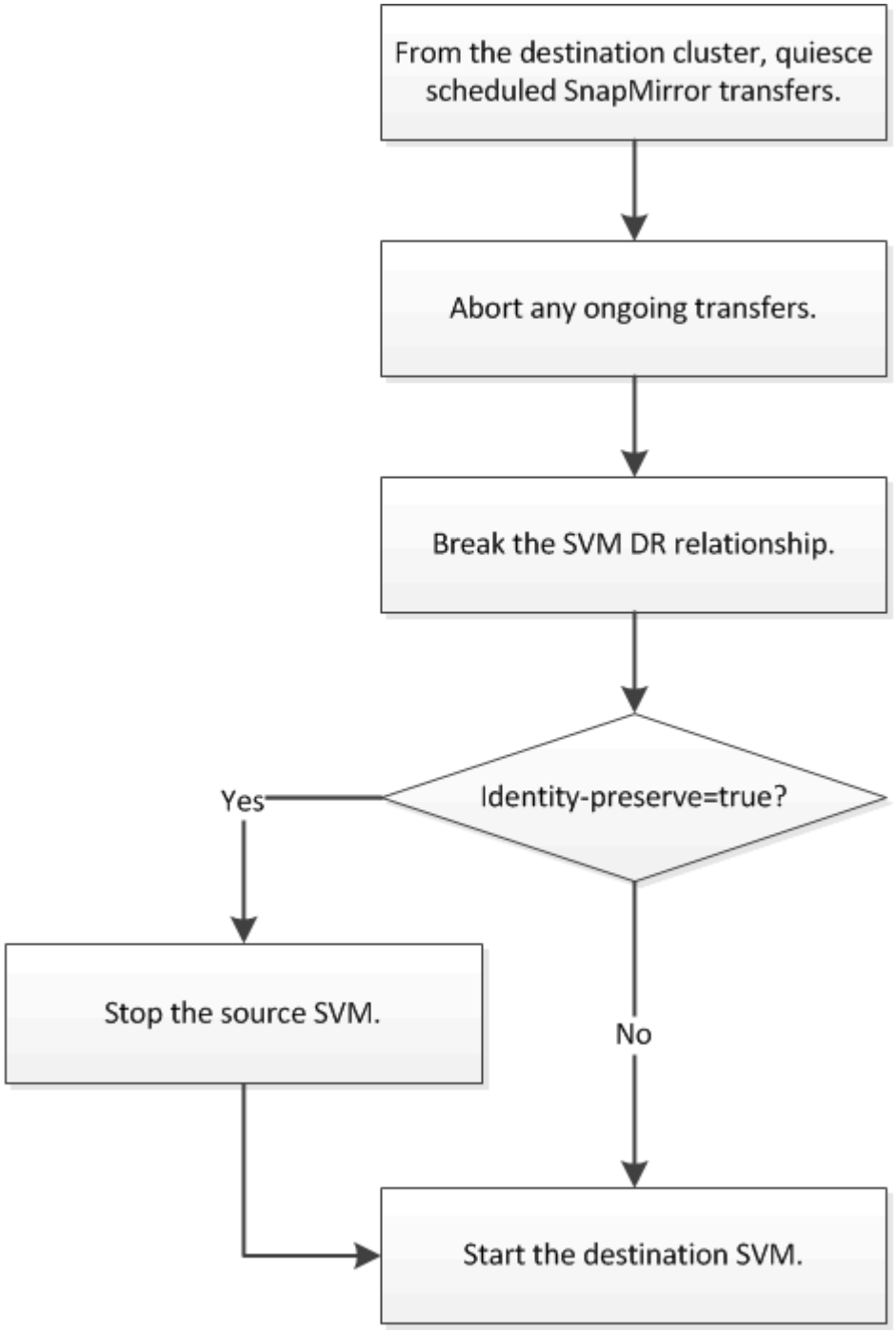
2. Cree e inicialice la relación de replicación de SVM como se describe en "Replicar una configuración de SVM completa".

Proporcione datos desde un destino de recuperación ante desastres de SVM

Flujo de trabajo de recuperación ante desastres de SVM

Para la recuperación ante desastres y proporcionar datos desde la SVM de destino, debe activar la SVM de destino. La activación de la SVM de destino implica la detención de transferencias programadas de SnapMirror, la anulación de las transferencias continuas de SnapMirror, la ruptura de la relación de replicación, la detención de la SVM de origen

y la inicio de la SVM de destino.



Haga que se puedan escribir los volúmenes de destino de SVM

Debe hacer que los volúmenes de destino de SVM sean editables antes de proporcionar datos a los clientes. El procedimiento es en gran medida idéntico al procedimiento de replicación de volúmenes, con una excepción. Si ha configurado `-identity-preserve true` Cuando se creó la relación de replicación de SVM, debe detener la SVM de origen antes de activar la SVM de destino.

Acerca de esta tarea

Para obtener una sintaxis de comando completa, consulte la página man.

> En una situación de recuperación ante desastres, no puede realizar una actualización de SnapMirror del SVM de origen a la SVM de destino de recuperación ante desastres porque no podrá acceder a la SVM de origen y a sus datos, así como porque las actualizaciones desde la última resincronización pueden estar dañadas o estar dañadas.

Pasos

1. Desde la SVM de destino o el clúster de destino, detenga las transferencias programadas hacia el destino:

   `snapmirror quiesce -source-path` *`SVM`*`: -destination-path` *`SVM`*`:`

   > Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea el ejemplo siguiente.

   En el siguiente ejemplo, se detienen las transferencias programadas entre la SVM de origen `svm1` Y la SVM de destino `svm_backup`:

   ```
   cluster_dst::> snapmirror quiesce -source-path svm1: -destination-path
   svm_backup:
   ```

2. Desde la SVM de destino o el clúster de destino, detenga las transferencias continuas al destino:

   `snapmirror abort -source-path` *`SVM`*`: -destination-path` *`SVM`*`:`

   > Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea el ejemplo siguiente.

   En el siguiente ejemplo, se detienen las transferencias continuas entre la SVM de origen `svm1` Y la SVM de destino `svm_backup`:

   ```
   cluster_dst::> snapmirror abort -source-path svm1: -destination-path
   svm_backup:
   ```

3. Desde la SVM de destino o el clúster de destino, rompa la relación de replicación:

   `snapmirror break -source-path` *`SVM`*`: -destination-path` *`SVM`*`:`

   > Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea el ejemplo siguiente.

   En el siguiente ejemplo, se rompe la relación entre la SVM de origen `svm1` Y la SVM de destino `svm_backup`:

   ```
   cluster_dst::> snapmirror break -source-path svm1: -destination-path
   svm_backup:
   ```

4. Si ha configurado `-identity-preserve true` Cuando creó la relación de replicación de SVM, detenga la SVM de origen:

   `vserver stop -vserver` *SVM*

   En el ejemplo siguiente se detiene la SVM de origen `svm1`:

   ```
   cluster_src::> vserver stop svm1
   ```

5. Inicie la SVM de destino:

   `vserver start -vserver` *SVM*

   En el ejemplo siguiente se inicia la SVM de destino `svm_backup`:

   ```
   cluster_dst::> vserver start svm_backup
   ```

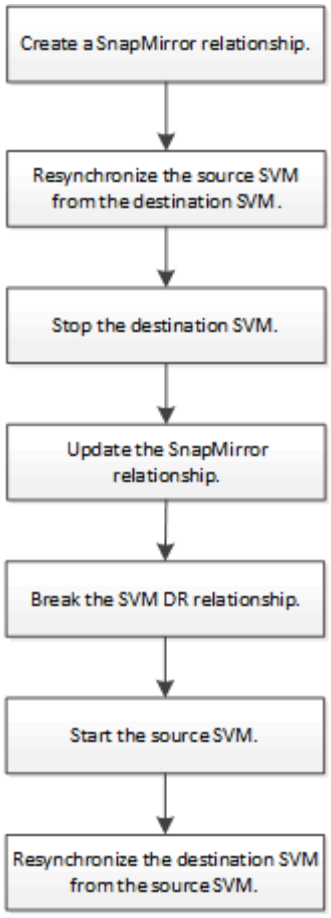
Después de terminar

Configure los volúmenes de destino de SVM para acceder a los datos, como se describe en "Configurar el volumen de destino para acceder a los datos".

Reactivar la SVM de origen

Flujo de trabajo de reactivación de SVM de origen

Si la SVM de origen existe después de un desastre, puede reactivarlo y protegerlo; para ello, vuelva a crear la relación de recuperación ante desastres de SVM.



Reactivar la SVM de origen original

Puede restablecer la relación original de protección de datos entre la SVM de origen y la de destino cuando ya no necesite servir datos desde el destino. El procedimiento es en gran medida idéntico al procedimiento de replicación de volúmenes, con una excepción. Debe detener la SVM de destino antes de volver a activar la SVM de origen.

Antes de empezar

Si ha aumentado el tamaño del volumen de destino mientras se sirven los datos, antes de reactivar el volumen de origen, debería aumentar manualmente el tamaño máximo automático en el volumen de origen original para garantizar que pueda crecer lo suficiente.

"Cuando un volumen de destino aumenta automáticamente"

Acerca de esta tarea

A partir de ONTAP 9.11.1, puede reducir el tiempo de resincronización durante un ensayo de recuperación ante desastres mediante el `-quick-resync true` opción de `snapmirror resync` Comando mientras se realiza una resincronización inversa de una relación de recuperación ante desastres de SVM. Una resincronización rápida puede reducir el tiempo que lleva volver a la producción evitando las operaciones de reconstrucción y restauración del almacén de datos.

> Una resincronización rápida no conserva la eficiencia del almacenamiento de los volúmenes de destino. Al habilitar una resincronización rápida, puede aumentar el espacio de volumen utilizado por los volúmenes de destino.

En este procedimiento se asume que la línea base del volumen de origen original está intacta. Si la base de referencia no está intacta, debe crear e inicializar la relación entre el volumen desde el que se sirven datos y el volumen de origen original antes de realizar el procedimiento.

Para obtener una sintaxis completa del comando en los comandos, consulte la página man.

Pasos

1. A partir de la SVM de origen original o del clúster de origen original, cree una relación de recuperación ante desastres de SVM inversa con la misma configuración, política y conservación de identidad que la relación de recuperación ante desastres de SVM original:

   `snapmirror create -source-path SVM: -destination-path SVM:`

   > Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea el ejemplo siguiente.

   En el siguiente ejemplo se crea una relación entre la SVM desde la cual se proporcionan datos, `svm_backup`Y la SVM de origen original, `svm1`:

   ```
   cluster_src::> snapmirror create -source-path svm_backup: -destination
   -path svm1:
   ```

2. Desde la SVM de origen original o el clúster de origen original, ejecute el siguiente comando para invertir la relación de protección de datos:

   `snapmirror resync -source-path *SVM*: -destination-path *SVM*:`

   > Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea el ejemplo siguiente.

   Aunque la resincronización no requiere una transferencia básica, puede requerir mucho tiempo. Puede que desee ejecutar la resincronización en horas de menor actividad.

   > El comando genera errores si no existe una copia Snapshot común en el origen y el destino. Uso `snapmirror initialize` para reiniciar la relación.

   En el siguiente ejemplo se revierte la relación entre la SVM de origen original, `svm1`, Y la SVM desde la que se proporcionan datos, `svm_backup`:

   ```
   cluster_src::> snapmirror resync -source-path svm_backup: -destination
   -path svm1:
   ```

   Ejemplo con la opción -Quick-resync:

   ```
   cluster_src::> snapmirror resync -source-path svm_backup: -destination
   -path svm1: -quick-resync true
   ```

3. Cuando esté listo para restablecer el acceso a los datos a la SVM de origen original, detenga la SVM de destino original para desconectar los clientes que actualmente estén conectados a la SVM de destino original.

   `vserver stop -vserver SVM`

   En el ejemplo siguiente se detiene la SVM de destino original, que actualmente proporciona datos:

   ```
   cluster_dst::> vserver stop svm_backup
   ```

4. Compruebe que la SVM de destino original esté en estado detenido con el `vserver show` comando.

   ```
   cluster_dst::> vserver show
                                    Admin      Operational Root
   Vserver        Type    Subtype    State      State       Volume
   Aggregate
   --------       ------- ---------- ---------- ----------- ----------
   ----------
   svm_backup     data    default    stopped    stopped     rv
   aggr1
   ```

5. A partir de la SVM de origen original o del clúster de origen original, ejecute el siguiente comando para realizar la actualización final de la relación inversa para transferir todos los cambios de la SVM de destino original a la SVM de origen original:

   `snapmirror update -source-path SVM: -destination-path SVM:`

   > Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea el ejemplo siguiente.

   En el ejemplo siguiente se actualiza la relación entre la SVM de destino original a partir de la cual se proporcionan datos,`svm_backup`Y la SVM de origen original, `svm1`:

   ```
   cluster_src::> snapmirror update -source-path svm_backup: -destination
   -path svm1:
   ```

6. Desde la SVM de origen original o el clúster de origen original, ejecute el siguiente comando para detener las transferencias programadas para la relación inversa:

   `snapmirror quiesce -source-path SVM: -destination-path SVM:`

   > Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea el ejemplo siguiente.

   En el ejemplo siguiente se detienen las transferencias programadas entre la SVM desde la que se proporcionan datos: `svm_backup`Y la SVM original, `svm1`:

```
cluster_src::> snapmirror quiesce -source-path svm_backup: -destination
-path svm1:
```

7. Cuando la actualización final se completa y la relación indica "Quiesced" para el estado de la relación, ejecute el siguiente comando desde la SVM de origen original o el clúster de origen original para romper la relación inversa:

   `snapmirror break -source-path SVM: -destination-path SVM:`

   > Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea el ejemplo siguiente.

   En el siguiente ejemplo, se rompe la relación entre la SVM de destino original, en la que se estaban sirviendo datos. `svm_backup`Y la SVM de origen original, `svm1`:

```
cluster_src::> snapmirror break -source-path svm_backup: -destination
-path svm1:
```

8. Si la SVM de origen se había detenido anteriormente, desde el clúster de origen original, inicie la SVM de origen original:

   `vserver start -vserver SVM`

   En el ejemplo siguiente se inicia la SVM de origen original:

```
cluster_src::> vserver start svm1
```

9. A partir de la SVM de destino original o del clúster de destino original, restablezca la relación de protección de datos original:

   `snapmirror resync -source-path SVM: -destination-path SVM:`

   > Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea el ejemplo siguiente.

   En el siguiente ejemplo, se vuelve a establecer la relación entre la SVM de origen original, `svm1`Y la SVM de destino original, `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

10. Desde la SVM de origen original o el clúster de origen original, ejecute el siguiente comando para eliminar la relación de protección de datos inversa:

    `snapmirror delete -source-path SVM: -destination-path SVM:`

> Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea el ejemplo siguiente.

En el siguiente ejemplo, se elimina la relación inversa entre la SVM de destino original, `svm_backup`Y la SVM de origen original, `svm1`:

```
cluster_src::> snapmirror delete -source-path svm_backup: -destination
-path svm1:
```

11. Desde la SVM de destino original o el clúster de destino original, libere la relación de protección de datos inversa:

    `snapmirror release -source-path SVM: -destination-path SVM:`

    > Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea el ejemplo siguiente.

    En el siguiente ejemplo, se libera la relación inversa entre la SVM de destino original, svm_backup y la SVM de origen original, `svm1`

    ```
    cluster_dst::> snapmirror release -source-path svm_backup: -destination
    -path svm1:
    ```

Después de terminar

Utilice la `snapmirror show` Comando para verificar que la relación de SnapMirror se ha creado. Para obtener una sintaxis de comando completa, consulte la página man.

Reactivar la SVM de origen original (solo volúmenes de FlexGroup)

Puede restablecer la relación original de protección de datos entre la SVM de origen y la de destino cuando ya no necesite servir datos desde el destino. Para reactivar la SVM de origen original cuando usa volúmenes de FlexGroup, debe realizar algunos pasos adicionales, como la eliminación de la relación de recuperación ante desastres de SVM original y la liberación de la relación original antes de revertir la relación. También debe liberar la relación inversa y volver a crear la relación original antes de detener las transferencias programadas.

Pasos

1. De la SVM de destino original o del clúster de destino original, elimine la relación de recuperación ante desastres de SVM original:

   `snapmirror delete -source-path SVM: -destination-path SVM:`

   > Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea el ejemplo siguiente.

En el siguiente ejemplo, se elimina la relación original entre la SVM de origen, svm1 y la SVM de destino original, `svm_backup`:

```
cluster_dst::> snapmirror delete -source-path svm1: -destination-path
svm_backup:
```

2. A partir de la SVM de origen original o del clúster de origen original, libere la relación original mientras mantiene las copias Snapshot intactas:

   `snapmirror release -source-path SVM: -destination-path SVM: -relationship-info -only true`

   > Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea el ejemplo siguiente.

   En el siguiente ejemplo, se libera la relación original entre la SVM de origen, svm1 y la SVM de destino original, `svm_backup`.

```
cluster_src::> snapmirror release -source-path svm1: -destination-path
svm_backup: -relationship-info-only true
```

3. A partir de la SVM de origen original o del clúster de origen original, cree una relación de recuperación ante desastres de SVM inversa con la misma configuración, política y conservación de identidad que la relación de recuperación ante desastres de SVM original:

   `snapmirror create -source-path SVM: -destination-path SVM:`

   > Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea el ejemplo siguiente.

   En el siguiente ejemplo se crea una relación entre la SVM desde la cual se proporcionan datos, `svm_backup`Y la SVM de origen original, `svm1:

```
cluster_src::> snapmirror create -source-path svm_backup: -destination
-path svm1:
```

4. Desde la SVM de origen original o el clúster de origen original, ejecute el siguiente comando para invertir la relación de protección de datos:

   `snapmirror resync -source-path *SVM*: -destination-path *SVM*:`

   > Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea el ejemplo siguiente.

   Aunque la resincronización no requiere una transferencia básica, puede requerir mucho tiempo. Puede que desee ejecutar la resincronización en horas de menor actividad.

> El comando genera errores si no existe una copia Snapshot común en el origen y el destino. Uso `snapmirror initialize` para reiniciar la relación.

En el siguiente ejemplo se revierte la relación entre la SVM de origen original, `svm1`, Y la SVM desde la que se proporcionan datos, `svm_backup`:

```
cluster_src::> snapmirror resync -source-path svm_backup: -destination
-path svm1:
```

5. Cuando esté listo para restablecer el acceso a los datos a la SVM de origen original, detenga la SVM de destino original para desconectar los clientes que actualmente estén conectados a la SVM de destino original.

   `vserver stop -vserver SVM`

   En el ejemplo siguiente se detiene la SVM de destino original, que actualmente proporciona datos:

```
cluster_dst::> vserver stop svm_backup
```

6. Compruebe que la SVM de destino original esté en estado detenido con el `vserver show` comando.

```
cluster_dst::> vserver show
                                  Admin      Operational Root
Vserver        Type    Subtype    State      State       Volume
Aggregate
--------       ------- ---------- ---------- ----------- ----------
----------
svm_backup     data    default    stopped    stopped     rv
aggr1
```

7. A partir de la SVM de origen original o del clúster de origen original, ejecute el siguiente comando para realizar la actualización final de la relación inversa para transferir todos los cambios de la SVM de destino original a la SVM de origen original:

   `snapmirror update -source-path SVM: -destination-path SVM:`

   > Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea el ejemplo siguiente.

   En el ejemplo siguiente se actualiza la relación entre la SVM de destino original a partir de la cual se proporcionan datos,`svm_backup`Y la SVM de origen original, `svm1:

```
cluster_src::> snapmirror update -source-path svm_backup: -destination
-path svm1:
```

8. Desde la SVM de origen original o el clúster de origen original, ejecute el siguiente comando para detener las transferencias programadas para la relación inversa:

   `snapmirror quiesce -source-path SVM: -destination-path SVM:`

   > Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea el ejemplo siguiente.

   En el ejemplo siguiente se detienen las transferencias programadas entre la SVM desde la que se proporcionan datos: `svm_backup`Y la SVM original, `svm1:`

   ```
   cluster_src::> snapmirror quiesce -source-path svm_backup: -destination
   -path svm1:
   ```

9. Cuando la actualización final se completa y la relación indica "Quiesced" para el estado de la relación, ejecute el siguiente comando desde la SVM de origen original o el clúster de origen original para romper la relación inversa:

   `snapmirror break -source-path SVM: -destination-path SVM:`

   > Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea el ejemplo siguiente.

   En el siguiente ejemplo, se rompe la relación entre la SVM de destino original, en la que se estaban sirviendo datos. `svm_backup`Y la SVM de origen original, `svm1:`

   ```
   cluster_src::> snapmirror break -source-path svm_backup: -destination
   -path svm1:
   ```

10. Si la SVM de origen se había detenido anteriormente, desde el clúster de origen original, inicie la SVM de origen original:

    `vserver start -vserver SVM`

    En el ejemplo siguiente se inicia la SVM de origen original:

    ```
    cluster_src::> vserver start svm1
    ```

11. En la SVM de origen original o en el clúster de origen, elimine la relación de recuperación ante desastres de SVM inversa:

    `snapmirror delete -source-path SVM: -destination-path SVM:`

    > Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea el ejemplo siguiente.

En el siguiente ejemplo, se elimina la relación inversa entre la SVM de destino original, svm_backup y la SVM de origen original, `svm1`:

```
cluster_src::> snapmirror delete -source-path svm_backup: -destination
-path svm1:
```

12. Desde la SVM de destino original o el clúster de destino original, libere la relación inversa mientras mantiene las copias Snapshot intactas:

    `snapmirror release -source-path SVM: -destination-path SVM: -relationship-info -only true`

    > Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea el ejemplo siguiente.

    En el siguiente ejemplo, se libera la relación inversa entre la SVM de destino original, svm_backup y la SVM de origen original, svm1:

    ```
    cluster_dst::> snapmirror release -source-path svm_backup: -destination
    -path svm1: -relationship-info-only true
    ```

13. Desde la SVM de destino original o el clúster de destino original, vuelva a crear la relación original. Utilice la misma configuración, política y conservación de identidad que la relación de recuperación ante desastres original de la SVM:

    `snapmirror create -source-path SVM: -destination-path SVM:`

    > Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea el ejemplo siguiente.

    En el siguiente ejemplo, se crea una relación entre la SVM de origen original, `svm1`Y la SVM de destino original, `svm_backup`:

    ```
    cluster_dst::> snapmirror create -source-path svm1: -destination-path
    svm_backup:
    ```

14. A partir de la SVM de destino original o del clúster de destino original, restablezca la relación de protección de datos original:

    `snapmirror resync -source-path *SVM*: -destination-path *SVM*:`

    > Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea el ejemplo siguiente.

    En el siguiente ejemplo, se vuelve a establecer la relación entre la SVM de origen original, `svm1`Y la SVM de destino original, `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

Convertir relaciones de replicación de volúmenes en una relación de replicación de SVM

Puede convertir relaciones de replicación entre volúmenes en una relación de replicación entre las máquinas virtuales de almacenamiento (SVM) a las que pertenecen los volúmenes, siempre que se replique cada volumen del origen (excepto el volumen raíz), y cada volumen del origen (incluido el volumen raíz) tiene el mismo nombre que el volumen en el destino.

Acerca de esta tarea

Utilice la `volume rename` Comando cuando la relación de SnapMirror está inactiva para cambiar el nombre de los volúmenes de destino si es necesario.

Pasos

1. Desde la SVM de destino o el clúster de destino, ejecute el siguiente comando para volver a sincronizar los volúmenes de origen y destino:

   `snapmirror resync -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`* `-type DP|XDP -policy` *`policy`*

   Para obtener una sintaxis de comando completa, consulte la página man.

   > Aunque la resincronización no requiere una transferencia básica, puede requerir mucho tiempo. Puede que desee ejecutar la resincronización en horas de menor actividad.

   En el siguiente ejemplo, vuelva a establecer la relación entre el volumen de origen `volA` encendido `svm1` y el volumen de destino `volA` encendido `svm_backup`:

   ```
   cluster_dst::> snapmirror resync -source-path svm1:volA -destination
   -path svm_backup:volA
   ```

2. Cree una relación de replicación de SVM entre las SVM de origen y de destino, como se describe en "Replicando configuraciones de SVM".

   Debe utilizar el `-identity-preserve true` opción de `snapmirror create` comando al crear la relación de replicación.

3. Detenga la SVM de destino:

   `vserver stop -vserver` *`SVM`*

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el ejemplo siguiente se detiene la SVM de destino `svm_backup`:

```
cluster_dst::> vserver stop svm_backup
```

4. Desde la SVM de destino o el clúster de destino, ejecute el siguiente comando para volver a sincronizar las SVM de origen y destino:

   `snapmirror resync -source-path SVM: -destination-path SVM: -type DP|XDP -policy policy`

   Para obtener una sintaxis de comando completa, consulte la página man.

   > Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea el ejemplo siguiente.
   >
   > Aunque la resincronización no requiere una transferencia básica, puede requerir mucho tiempo. Puede que desee ejecutar la resincronización en horas de menor actividad.

   En el siguiente ejemplo, vuelva a establecer la relación entre la SVM de origen `svm1` Y la SVM de destino `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

Eliminar una relación de replicación de SVM

Puede utilizar el `snapmirror delete` y.. `snapmirror release` Comandos para eliminar una relación de replicación de SVM. A continuación, puede eliminar manualmente los volúmenes de destino innecesarios.

Acerca de esta tarea

La `snapmirror release` Comando elimina todas las copias Snapshot creadas con SnapMirror del origen. Puede utilizar el `-relationship-info-only` Opción a conservar las copias Snapshot.

Para obtener una sintaxis completa del comando en los comandos, consulte la página man.

Pasos

1. Ejecute el siguiente comando desde la SVM de destino o el clúster de destino para romper la relación de replicación:

   `snapmirror break -source-path SVM: -destination-path SVM:`

   > Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea el ejemplo siguiente.

   En el siguiente ejemplo, se rompe la relación entre la SVM de origen `svm1` Y la SVM de destino `svm_backup`:

```
cluster_dst::> snapmirror break -source-path svm1: -destination-path
svm_backup:
```

2. Ejecute el siguiente comando desde la SVM de destino o el clúster de destino para eliminar la relación de replicación:

   `snapmirror delete -source-path SVM: -destination-path SVM:`

   > Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea el ejemplo siguiente.

   En el siguiente ejemplo, se elimina la relación entre la SVM de origen `svm1` Y la SVM de destino `svm_backup`:

```
cluster_dst::> snapmirror delete -source-path svm1: -destination-path
svm_backup:
```

3. Ejecute el siguiente comando desde la SVM de origen o el clúster de origen para liberar la información de relaciones de replicación desde la SVM de origen:

   `snapmirror release -source-path SVM: -destination-path SVM:`

   > Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea el ejemplo siguiente.

   En el siguiente ejemplo, se libera información para la relación de replicación especificada desde la SVM de origen `svm1`:

```
cluster_src::> snapmirror release -source-path svm1: -destination-path
svm_backup:
```

Gestionar la replicación de volúmenes raíz de SnapMirror

Información general sobre la replicación de volúmenes raíz de Manage SnapMirror

Cada SVM de un entorno NAS cuenta con un espacio de nombres único. El volumen SVM *root,* que contiene sistema operativo e información relacionada, es el punto de entrada de la jerarquía del espacio de nombres. Para garantizar que los clientes puedan acceder a los datos en caso de interrupción del servicio o conmutación al nodo de respaldo, debería crear una copia de mirroring con uso compartido de la carga del volumen raíz de la SVM.

El principal objetivo de los reflejos de uso compartido de carga para los volúmenes raíz de SVM ya no es para el uso compartido de carga; en su lugar, su finalidad es la recuperación ante desastres.

- Si el volumen raíz no está disponible temporalmente, el reflejo de uso compartido de carga proporciona acceso de solo lectura a los datos del volumen raíz.
- Si el volumen raíz no está disponible permanentemente, se puede promocionar uno de los volúmenes compartidos de carga para proporcionar acceso de escritura a los datos del volumen raíz.

Crear e inicializar relaciones de mirroring de uso compartido de carga

Debe crear un reflejo de uso compartido de carga (LSM) para cada volumen raíz de SVM que sirva datos NAS en el clúster. En el caso de los clústeres formados por dos o más pares de alta disponibilidad, debe considerar los reflejos de uso compartido de carga de los volúmenes raíz de SVM para garantizar que los clientes sigan accesible el espacio de nombres en caso de que esto siga siendo
Los dos nodos de una pareja de alta disponibilidad fallan. Los reflejos de uso compartido de carga no son adecuados para clústeres que constan de una única pareja de alta disponibilidad.

Acerca de esta tarea

Si crea un LSM en el mismo nodo y el nodo no está disponible, tendrá un único punto de error y no tendrá una segunda copia para garantizar que los datos sigan siendo accesibles para los clientes. Pero cuando crea el LSM en un nodo distinto al que contiene el volumen raíz o en un par de alta disponibilidad diferente, todavía se puede acceder a los datos en caso de una interrupción del servicio.

Por ejemplo, en un clúster de cuatro nodos con volumen raíz en tres nodos:

- Para el volumen raíz en el nodo 1 de alta disponibilidad, cree el LSM en el nodo 1 de alta disponibilidad 2 o el nodo 2 de alta disponibilidad.
- Para el volumen raíz en el nodo de alta disponibilidad 1 2, cree el LSM en el nodo de alta disponibilidad 2 1 o el nodo de alta disponibilidad 2.
- Para el volumen raíz en el nodo 1 de alta disponibilidad 2, cree el LSM en el nodo 1 de alta disponibilidad o el nodo 2 de alta disponibilidad 1.

Pasos

1. Crear un volumen de destino para el LSM:

   Antes de ejecutar este comando, debe sustituir las variables entre paréntesis angulares por los valores requeridos.

   ```
   volume create -vserver <SVM> -volume <volume> -aggregate <aggregate>
   -type DP -size <size>
   ```

   El tamaño del volumen de destino debe ser igual o mayor que el del volumen raíz.

   Se recomienda nombrar el volumen raíz y el volumen de destino con sufijos, como `_root` y.. `_m1`.

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el siguiente ejemplo, se crea un volumen de reflejos de uso compartido de carga para el volumen raíz `svm1_root` pulg `cluster_src`:

```
cluster_src:> volume create -vserver svm1 -volume svm1_m1 -aggregate
aggr_1 -size 1gb -state online -type DP
```

2. "Cree un programa de trabajo de replicaciones".
3. Crear una relación de mirroring de uso compartido de carga entre el volumen raíz de SVM y el volumen de destino para LSM:

   Antes de ejecutar este comando, debe sustituir las variables entre paréntesis angulares por los valores requeridos.

   ```
   snapmirror create -source-path <SVM:volume> -destination-path
   <SVM:volume> -type LS -schedule <schedule>
   ```

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el siguiente ejemplo, se crea una relación de reflejo de uso compartido de la carga entre el volumen raíz `svm1_root` y el volumen reflejado de uso compartido de la carga `svm1_m1`:

   ```
   cluster_src::> snapmirror create -source-path svm1:svm1_root
   -destination-path svm1:svm1_m1 -type LS -schedule hourly
   ```

   El atributo type del reflejo de carga compartida cambia de `DP` para `LS`.

4. Inicialice el reflejo de uso compartido de carga:

   Antes de ejecutar este comando, debe sustituir las variables entre paréntesis angulares por los valores requeridos.

   ```
   snapmirror initialize-ls-set -source-path <SVM:volume>
   ```

   La inicialización puede requerir mucho tiempo. Puede ser conveniente ejecutar la transferencia básica en horas de menor actividad.

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el ejemplo siguiente se inicializa el reflejo de uso compartido de carga para el volumen raíz `svm1_root`:

   ```
   cluster_src::> snapmirror initialize-ls-set -source-path svm1:svm1_root
   ```

Actualizar una relación de reflejo de carga compartida

Las relaciones de mirroring (LSM) de uso compartido de carga se actualizan

automáticamente para los volúmenes raíz de SVM después de montar o desmontar un volumen en la SVM, y durante esta `volume create` operaciones que incluyen la "opción de la ruta de unión". Puede actualizar manualmente una relación LSM si desea actualizarla antes de la siguiente actualización programada.

Las relaciones de reflejos de uso compartido de carga se actualizan automáticamente en las siguientes circunstancias:

- Ha llegado el momento de realizar una actualización programada
- Se realiza una operación de montaje o desmontaje en un volumen del volumen raíz de la SVM
- A. `volume create` se emite el comando que incluye la `juntion-path` opción

Paso

1. Actualice manualmente una relación de reflejo de carga compartida:

   Antes de ejecutar este comando, debe sustituir las variables entre paréntesis angulares por los valores requeridos.

   ```
   snapmirror update-ls-set -source-path <SVM:volume>
   ```

   En el siguiente ejemplo se actualiza la relación de reflejo de uso compartido de carga para el volumen raíz `svm1_root`:

   ```
   cluster_src::> snapmirror update-ls-set -source-path svm1:svm1_root
   ```

Promover un espejo de uso compartido de la carga

Si un volumen raíz no está disponible de forma permanente, se puede promocionar el volumen de reflejos de uso compartido de carga (LSM) para proporcionar acceso de escritura a los datos del volumen raíz.

Lo que necesitará

Para esta tarea, debe utilizar comandos de nivel de privilegio avanzado.

Pasos

1. Cambie al nivel de privilegio avanzado:

   ```
   set -privilege advanced
   ```

2. Ascender un volumen LSM:

   Antes de ejecutar este comando, debe sustituir las variables entre paréntesis angulares por los valores requeridos.

```
snapmirror promote -destination-path <SVM:volume>
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo, se promociona el volumen `svm1_m2` Como nuevo volumen raíz de la SVM:

```
cluster_src::*> snapmirror promote -destination-path svm1:svm1_m2

Warning: Promote will delete the offline read-write volume
         cluster_src://svm1/svm1_root and replace it with
         cluster_src://svm1/svm1_m2. Because the volume is offline,
         it is not possible to determine whether this promote will
         affect other relationships associated with this source.
Do you want to continue? {y|n}: y
```

Introduzca `y`. ONTAP convierte al volumen LSM en un volumen de lectura/escritura y elimina el volumen raíz original, si es accesible.

> Es posible que el volumen raíz promocionado no tenga todos los datos que estaban en el volumen raíz original, si no se realizó la última actualización recientemente.

3. Volver al nivel de privilegio de administrador:

```
set -privilege admin
```

4. Cambie el nombre del volumen promocionado según la convención de nomenclatura que utilizó para el volumen raíz:

   Antes de ejecutar este comando, debe sustituir las variables entre paréntesis angulares por los valores requeridos.

```
volume rename -vserver <SVM> -volume <volume> -newname <new_name>
```

   En el ejemplo siguiente se cambia el nombre del volumen promocionado `svm1_m2` con el nombre `svm1_root`:

```
cluster_src::> volume rename -vserver svm11 -volume svm1_m2 -newname
svm1_root
```

5. Proteja el volumen raíz cambiado de nombre, tal como se describe en el paso 3 hasta el paso 4 en "Creación e inicialización de relaciones de mirroring de uso compartido de carga".

Detalles técnicos de SnapMirror

Utilizar coincidencia de patrón de nombre de ruta de acceso

Puede utilizar la coincidencia de patrones para especificar las rutas de origen y destino en `snapmirror` comandos.

```
`snapmirror` los comandos utilizan nombres de ruta completos con el
siguiente formato: `vserver:volume`. No se puede introducir el nombre de
la SVM para abreviar el nombre de la ruta de acceso. Si lo hace, el
`snapmirror` El comando asume el contexto de SVM local del usuario.
```

Suponiendo que la SVM se denomine «'vserver1'» y que el volumen se llama «'vol1'», el nombre de ruta completo es `vserver1:vol1`.

Puede utilizar el asterisco (*) en las rutas de acceso como comodín para seleccionar nombres de ruta de acceso coincidentes y completos. En la siguiente tabla, se proporcionan ejemplos del uso del comodín para seleccionar un rango de volúmenes.

`*`	Coincide con todas las rutas.
`vs*`	Coincide con todas las SVM y los volúmenes con nombres de SVM que comienzan con `vs`.
`:*src`	Coincide con todas las SVM con los nombres de los volúmenes que contienen `src` texto.
`:vol`	Coincide con todas las SVM con nombres de volúmenes que comienzan con `vol`.

```
vs1::> snapmirror show -destination-path *:*dest*

Progress
Source              Destination  Mirror        Relationship  Total
Last
Path          Type  Path         State         Status        Progress
Healthy Updated
------------- ---- ------------ ------------- -------------- ----------
------- --------
vs1:sm_src2
              DP   vs2:sm_dest1
                                Snapmirrored  Idle           -
true    -
```

Use consultas ampliadas para actuar en muchas relaciones de SnapMirror

Puede utilizar *extended queries* para realizar operaciones de SnapMirror en varias relaciones de SnapMirror a la vez. Por ejemplo, es posible que tenga varias relaciones SnapMirror no inicializarse que desea inicializar con un comando.

Acerca de esta tarea

Puede aplicar consultas ampliadas a las siguientes operaciones de SnapMirror:

- Inicializando relaciones no iniciadas
- Reanude relaciones en modo inactivo
- Resincronizando relaciones rotas
- Actualizando relaciones de inactividad
- Anulación de transferencias de datos de relaciones

Paso

1. Realice una operación de SnapMirror en varias relaciones:

   snapmirror command {-state state } *

   El siguiente comando inicializa las relaciones de SnapMirror que se encuentran en un `Uninitialized` provincia:

   ```
   vs1::> snapmirror initialize {-state Uninitialized} *
   ```

Garantice una copia Snapshot común en una instalación de mirror-vault

Puede utilizar el `snapmirror snapshot-owner create` Comando para conservar una copia Snapshot etiquetada en el secundario en una implementación de reflejo-almacén. Al hacerlo se garantiza que exista una copia snapshot común para la actualización de la relación de almacén.

Acerca de esta tarea

Si utiliza una combinación de ventilador-almacén de reflejos o puesta en marcha en cascada, debe tener en cuenta que fallarán las actualizaciones si no existe una copia snapshot común en los volúmenes de origen y destino.

Esto no supone ningún problema en la relación de mirroring en una puesta en marcha en cascada o en distribución ramificada-vault, ya que SnapMirror siempre crea una copia snapshot del volumen de origen antes de realizar la actualización.

Puede ser un problema en la relación de almacén, sin embargo, ya que SnapMirror no crea una copia Snapshot del volumen de origen al actualizar una relación de almacén. Debe utilizar el `snapmirror snapshot-owner create` Para garantizar que hay al menos una copia Snapshot común en el origen y el destino de la relación del almacén.

Pasos

1. En el volumen de origen, asigne un propietario a la copia Snapshot etiquetada que desea conservar:

   `snapmirror snapshot-owner create -vserver SVM -volume volume -snapshot snapshot -owner owner`

   El ejemplo siguiente asigna `ApplicationA` como propietario del `snap1` Copia Snapshot:

   ```
   clust1::> snapmirror snapshot-owner create -vserver vs1 -volume vol1
   -snapshot snap1 -owner ApplicationA
   ```

2. Actualice la relación de reflejo, como se describe en "Actualizar manualmente una relación de replicación".

   También puede esperar a la actualización programada de la relación de reflejo.

3. Transfiera la copia Snapshot etiquetada como al destino de almacén:

   `snapmirror update -source-path SVM:volume|cluster://SVM/volume, … -destination -path SVM:volume|cluster://SVM/volume, … -source-snapshot snapshot`

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el siguiente ejemplo se transfiere el `snap1` Copia Snapshot

   ```
   clust1::> snapmirror update -vserver vs1 -volume vol1
   -source-snapshot snap1
   ```

   La copia snapshot etiquetada se conservará cuando se actualice la relación de almacén.

4. En el volumen de origen, quite el propietario de la copia Snapshot etiquetada:

   `snapmirror snapshot-owner delete -vserver SVM -volume volume -snapshot snapshot -owner owner`

   Los ejemplos siguientes eliminan `ApplicationA` como propietario del `snap1` Copia Snapshot:

   ```
   clust1::> snapmirror snapshot-owner delete -vserver vs1 -volume vol1
   -snapshot snap1 -owner ApplicationA
   ```

Versiones de ONTAP compatibles para relaciones de SnapMirror

Los volúmenes de origen y destino deben ejecutar versiones de ONTAP compatibles antes de crear una relación de protección de datos de SnapMirror. Antes de actualizar ONTAP, debe comprobar que la versión actual de ONTAP sea compatible con la versión de ONTAP de destino para las relaciones de SnapMirror.

Relaciones de replicación unificadas

En lo que respecta a las relaciones de SnapMirror del tipo «'XDP», utilizando las versiones locales o de Cloud Volumes ONTAP:

> A partir de ONTAP 9,9.0:
>
> - Las versiones ONTAP 9.x,0 son versiones de solo cloud y son compatibles con los sistemas Cloud Volumes ONTAP. El asterisco (*) después de la versión indica una versión de sólo nube.
> - Las versiones ONTAP 9.x,1 son versiones generales y son compatibles tanto con los sistemas locales como con los sistemas Cloud Volumes ONTAP.

> La interoperabilidad es bidireccional.

Interoperabilidad para ONTAP versión 9,3 y posterior

Versión ONTAP…	Interactúa con estas versiones anteriores de ONTAP…																	
	9.14.1	9.14.0*	9.13.1	9.13.0*	9.12.1	9.12.0*	9.11.1	9.11.0*	9.10.1	9.10.0*	9.9.1	9.9.0*	9,8	9,7	9,6	9,5	9,4	9,3
9.14.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No	No	No	No	No
9.14.0*	**Sí**	**Sí**	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	No	No	No	No
9.13.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No	No	No	No
9.13.0*	**Sí**	No	**Sí**	**Sí**	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	No	No	No	No
9.12.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No	No	No
9.12.0*	**Sí**	No	**Sí**	No	**Sí**	**Sí**	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	**Sí**	No	No	No	No
9.11.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No	No
9.11.0*	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	**Sí**	**Sí**	No	**Sí**	No	**Sí**	**Sí**	**Sí**	No	No	No
9.10.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No
9.10.0*	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	**Sí**	**Sí**	No	**Sí**	**Sí**	**Sí**	**Sí**	No	No
9.9.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No

9.9.0*	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No
9,8	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	**Sí**
9,7	No	No	No	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	**Sí**
9,6	No	No	No	No	No	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	**Sí**
9,5	No	No	No	No	No	No	No	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**
9,4	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	**Sí**	**Sí**	**Sí**
9,3	No	No	No	No	No	No	No	No	No	No	No	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**

Relaciones de SnapMirror Synchronous

SnapMirror Synchronous no es compatible con las instancias de cloud de ONTAP.

Versión ONTAP …	Interactúa con estas versiones anteriores de ONTAP…									
	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9,8	9,7	9,6	9,5
9.14.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No	No
9.13.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No
9.12.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No
9.11.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No	No	No
9.10.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No	No
9.9.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No
9,8	**Sí**	**Sí**	**Sí**	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No
9,7	No	**Sí**	**Sí**	No	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**
9,6	No	No	No	No	No	No	**Sí**	**Sí**	**Sí**	**Sí**
9,5	No	No	No	No	No	No	No	**Sí**	**Sí**	**Sí**

Relaciones de recuperación ante desastres de SVM de SnapMirror

- Para los datos de recuperación ante desastres de SVM y la protección de SVM:

  La recuperación ante desastres de SVM solo se admite entre clústeres que ejecutan la misma versión de ONTAP. **La independencia de versiones no es compatible con la replicación de SVM**.

- Para la recuperación ante desastres de SVM para la migración de SVM:
  - La replicación es compatible en una sola dirección de una versión anterior de ONTAP en origen para que la misma versión de ONTAP o una posterior en el destino.
- La versión de ONTAP en el clúster de destino no debe tener más de dos versiones locales principales más nuevas o dos versiones de cloud principales más recientes, como se muestra en la tabla a continuación.
  - La replicación no es compatible con los casos de uso de protección de datos a largo plazo.

El asterisco (*) después de la versión indica una versión de sólo nube.

Para determinar la compatibilidad, busque la versión de origen en la columna de la tabla izquierda y, a continuación, busque la versión de destino en la fila superior (DR/Migración para versiones similares y Migración sólo para versiones más recientes).

Origen	Destino																	
	9,3	9,4	9,5	9,6	9,7	9,8	9.9.0*	9.9.1	9.10.0*	9.10.1	9.11.0*	9.11.1	9.12.0*	9.12.1	9.13.0*	9.13.1	9.14.0*	9.14.1
9,3	Recuperación antedesastres/Migración	Migración	Migración	Migración	Migración													
9,4		Recuperación antedesastres/Migración	Migración	Migración	Migración	Migración												
9,5			Recuperación antedesastres/Migración	Migración	Migración	Migración	Migración											

9,6				Recuperación antedesastres/Migración	Migración	Migración	Migración	Migración										
9,7					Recuperación antedesastres/Migración	Migración	Migración	Migración	Migración									
9,8						Recuperación antedesastres/Migración	Migración	Migración	Migración	Migración								
9.9.0*							Recuperación antedesastres/Migración	Migración	Migración	Migración	Migración							

9.9.1								Recuperación antedesastres/Migración	Migración	Migración	Migración	Migración						
9.10.0*									Recuperación antedesastres/Migración	Migración	Migración	Migración	Migración					
9.10.1										Recuperación antedesastres/Migración	Migración	Migración	Migración	Migración				
9.11.0*											Recuperación antedesastres/Migración	Migración	Migración	Migración	Migración			

9.11.1												Recuperación antedesastres/Migración	Migración	Migración	Migración	Migración		
9.12.0*													Recuperación antedesastres/Migración	Migración	Migración	Migración	Migración	
9.12.1														Recuperación antedesastres/Migración	Migración	Migración	Migración	Migración
9.13.0*															Recuperación antedesastres/Migración	Migración	Migración	Migración

9.13.1																Recuperación antedesastres/Migración	Migración	Migración
9.14.0*																	Recuperación antedesastres/Migración	Migración
9.14.1																		Recuperación antedesastres/Migración

Relaciones de recuperación ante desastres de SnapMirror

Para relaciones de SnapMirror del tipo «DP» y del tipo de política «duplicación asíncrona»:

> Los reflejos de tipo DP no se pueden inicializar comenzando con ONTAP 9.11.1 y están completamente obsoletos en ONTAP 9.12.1. Para obtener más información, consulte "Amortización de las relaciones de SnapMirror para la protección de datos".

> En la siguiente tabla, la columna de la izquierda indica la versión de ONTAP en el volumen de origen y la fila superior indica las versiones de ONTAP que se pueden tener en el volumen de destino.

Origen	Destino											
	9.11.1	9.10.1	9.9.1	9,8	9,7	9,6	9,5	9,4	9,3	9,2	9,1	9
9.11.1	Sí	No	No	No	No	No	No	No	No	No	No	No

9.10.1	Sí	Sí	No	No	No	No	No	No	No	No	No	No
9.9.1	Sí	Sí	Sí	No	No	No	No	No	No	No	No	No
9,8	No	Sí	Sí	Sí	No	No	No	No	No	No	No	No
9,7	No	No	Sí	Sí	Sí	No	No	No	No	No	No	No
9,6	No	No	No	Sí	Sí	Sí	No	No	No	No	No	No
9,5	No	No	No	No	Sí	Sí	Sí	No	No	No	No	No
9,4	No	No	No	No	No	Sí	Sí	Sí	No	No	No	No
9,3	No	No	No	No	No	No	Sí	Sí	Sí	No	No	No
9,2	No	No	No	No	No	No	No	Sí	Sí	Sí	No	No
9,1	No	No	No	No	No	No	No	No	Sí	Sí	Sí	No
9	No	No	No	No	No	No	No	No	No	Sí	Sí	Sí

La interoperabilidad no es bidireccional.

Limitaciones de SnapMirror

Debe conocer las limitaciones básicas de SnapMirror antes de crear una relación de protección de datos.

- Un volumen de destino solo puede tener un volumen de origen.

  Un volumen de origen puede tener varios volúmenes de destino. El volumen de destino puede ser el volumen de origen de cualquier tipo de relación de replicación de SnapMirror.

- Según el modelo de cabinas, se pueden distribuir de forma ramificada un máximo de ocho o dieciséis volúmenes de destino de un único volumen de origen. Consulte "Hardware Universe" para obtener detalles sobre su configuración específica.
- No puede restaurar archivos en el destino de una relación de recuperación ante desastres de SnapMirror.
- Los volúmenes de SnapVault de origen o destino no pueden tener 32 bits.
- El volumen de origen de una relación de SnapVault no debe ser un volumen FlexClone.

  La relación funcionará, pero no se conservará la eficiencia que ofrecen los volúmenes FlexClone.

Archivado y cumplimiento de normativas con tecnología SnapLock

Qué es SnapLock

SnapLock es una solución de cumplimiento de normativas de alto rendimiento para organizaciones que utilizan almacenamiento WORM para conservar archivos de forma no modificada a efectos de regulación y gobernanza.

SnapLock ayuda a evitar la eliminación, el cambio de nombre o el cambio de nombre de los datos para cumplir normativas como SEC 17a-4, HIPAA, FINRA, CFTC y RGPD. Gracias a SnapLock, puede crear volúmenes con fines especiales en los que los archivos se pueden almacenar y comprometidos a mantener su estado no borrable y no modificable durante un período de retención determinado o de forma indefinida. SnapLock permite llevar a cabo esta retención en el nivel de archivo mediante protocolos de archivos abiertos estándar como CIFS y NFS. Los protocolos de archivos abiertos compatibles con SnapLock son NFS (versiones 2, 3 y 4) y CIFS (SMB 1.0, 2.0 y 3.0).

Con SnapLock, se conservan archivos y copias Snapshot en almacenamiento WORM y se establecen períodos de retención para datos protegidos WORM. El almacenamiento WORM de SnapLock utiliza la tecnología Snapshot de NetApp y puede aprovechar la replicación de SnapMirror y los backups de SnapVault como tecnología base para ofrecer protección de recuperación de datos mediante backup.
Más información sobre el almacenamiento WORM: "Almacenamiento WORM conforme a la normativa con SnapLock de NetApp: TR-4526".

Puede usar una aplicación para comprometer archivos a WORM mediante NFS o CIFS, o utilizar la función de compromiso automático de SnapLock para comprometer archivos automáticamente a WORM. Puede utilizar un *WORM appable file* para conservar datos que se escriben de forma incremental, como la información de registro. Para obtener más información, consulte "Use el modo de adición de volúmenes para crear archivos WORM flexibles".

SnapLock admite métodos de protección de datos que deberían satisfacer la mayoría de los requisitos de cumplimiento de normativas:

- Puede usar SnapLock para SnapVault para proteger CON WORM las copias Snapshot en el almacenamiento secundario. Consulte "Copias Snapshot a WORM".
- Puede usar SnapMirror para replicar archivos WORM a otra ubicación geográfica a fin de realizar la recuperación ante desastres. Consulte "Refleje los archivos WORM".

SnapLock es una función basada en licencia de NetApp ONTAP. Una única licencia le da derecho a usar SnapLock en modo de cumplimiento estricto para satisfacer mandatos externos como la normativa SEC 17a-4 y un modo empresarial más flexible, con el fin de cumplir las normativas internas aplicables a la protección de activos digitales. Las licencias de SnapLock forman parte de la "ONTAP One" suite de software.

SnapLock es compatible con todos los sistemas AFF y FAS, así como con ONTAP Select. SnapLock no es una solución exclusivamente de software, es una solución integrada de hardware y software. Esta distinción es importante para las estrictas regulaciones DE WORM, como SEC 17a-4, que requieren una solución de hardware y software integrada. Para obtener más información, consulte "SEC interpretation: Almacenamiento electrónico de registros de intermediarios y concesionarios".

Puede hacer con SnapLock

Después de configurar SnapLock, es posible completar las siguientes tareas:

- "Los archivos cumplen CON WORM"
- "Conservar copias Snapshot a WORM para su almacenamiento secundario"
- "Refleje los archivos WORM para la recuperación ante desastres"
- "Conserve los archivos WORM durante su litigio gracias a su conservación legal"
- "Elimine los archivos WORM utilizando la función de eliminación privilegiada"
- "Defina el período de retención de archivos"
- "Mover un volumen de SnapLock"

- "Bloquee una copia Snapshot para obtener protección contra ataques de ransomware"
- "Revise el uso de SnapLock con el registro de auditoría"
- "Utilice las API de SnapLock"

Modos SnapLock Compliance y Enterprise

Los modos SnapLock Compliance y Enterprise difieren principalmente en el nivel en el que cada modo protege los archivos WORM:

Modo SnapLock	Nivel de protección	Archivo WORM eliminado durante la retención
Modo de cumplimiento	A nivel de archivo	No se puede eliminar
Modo empresarial	En el nivel de disco	El administrador de cumplimiento puede eliminar mediante un procedimiento auditado de “eliminación privilegiada”

Una vez transcurrido el período de retención, es responsable de eliminar los archivos que ya no se necesiten. Una vez que un archivo se ha comprometido con WORM, ya sea en modo Compliance o Enterprise, no se podrá modificar, ni siquiera después de que haya caducado el período de retención.

No se puede mover un archivo WORM durante el período de retención o después del mismo. Puede copiar un archivo WORM, pero la copia no conservará sus características WORM.

En la siguiente tabla se muestran las diferencias en las capacidades que admiten los modos SnapLock Compliance y Enterprise:

Capacidad	Cumplimiento de normativas SnapLock	Empresa SnapLock
Activar y eliminar archivos mediante la eliminación con privilegios	No	Sí
Reinicie los discos	No	Sí
Destrucción de agregados y volúmenes de SnapLock durante el período de retención	No	Sí, con la excepción del volumen de registro de auditoría de SnapLock
Cambie el nombre de los agregados o volúmenes	No	Sí
Utilice discos que no sean de NetApp	No	Sí (con "Virtualización FlexArray")

Use el volumen SnapLock para el registro de auditoría	Sí	Sí, a partir de ONTAP 9,5

Funciones compatibles y no compatibles con SnapLock

En la siguiente tabla se muestran las funciones compatibles con el modo de cumplimiento de normativas SnapLock, el modo SnapLock Enterprise o ambos:

Función	Compatible con SnapLock Compliance	Compatible con SnapLock Enterprise
Grupos de consistencia	No	No
Volúmenes cifrados	Sí, a partir de ONTAP 9,2. Más información acerca de Cifrado y SnapLock.	Sí, a partir de ONTAP 9,2. Más información acerca de Cifrado y SnapLock.
FabricPool en agregados de SnapLock	No	Sí, a partir de ONTAP 9.8. Más información acerca de FabricPool en agregados de SnapLock Enterprise.
Agregados de Flash Pool	Sí, a partir de ONTAP 9,1.	Sí, a partir de ONTAP 9,1.
FlexClone	Es posible clonar volúmenes de SnapLock, pero no es posible clonar archivos en un volumen de SnapLock.	Es posible clonar volúmenes de SnapLock, pero no es posible clonar archivos en un volumen de SnapLock.
Volúmenes de FlexGroup	Sí, a partir de ONTAP 9.11.1. Más información acerca de [flexgroup].	Sí, a partir de ONTAP 9.11.1. Más información acerca de [flexgroup].
LUN	No Más información acerca de Compatibilidad con LUN Con SnapLock.	No Más información acerca de Compatibilidad con LUN Con SnapLock.
Configuraciones de MetroCluster	Sí, a partir de ONTAP 9,3. Más información acerca de Soporte de MetroCluster.	Sí, a partir de ONTAP 9,3. Más información acerca de Soporte de MetroCluster.
Verificación multi-admin (MAV)	Sí, a partir de ONTAP 9.13.1. Más información acerca de Compatibilidad con MAV.	Sí, a partir de ONTAP 9.13.1. Más información acerca de Compatibilidad con MAV.
SAN	No	No
SnapRestore de archivo único	No	Sí

Continuidad del negocio de SnapMirror	No	No
SnapRestore	No	Sí
SMTape	No	No
SnapMirror síncrono	No	No
SSD	Sí, a partir de ONTAP 9,1.	Sí, a partir de ONTAP 9,1.
Funcionalidades de eficiencia del almacenamiento	Sí, a partir de ONTAP 9,9.1. Más información acerca de soporte de eficiencia del almacenamiento.	Sí, a partir de ONTAP 9,9.1. Más información acerca de soporte de eficiencia del almacenamiento.

FabricPool en agregados de SnapLock Enterprise

Las instancias de FabricPool son compatibles con los agregados empresariales de SnapLock, a partir de ONTAP 9.8. Sin embargo, su equipo de cuenta tiene que abrir una solicitud de variación de productos que documente que SnapLock ya no protege los datos de FabricPool organizados en niveles en un cloud público o privado porque un administrador de cloud puede eliminar dichos datos.

> Cualquier dato que FabricPool proporcione en niveles en un cloud público o privado ya no está protegido por SnapLock, ya que un administrador de cloud puede eliminar estos datos.

Volúmenes de FlexGroup

SnapLock admite volúmenes FlexGroup que comiencen con ONTAP 9.11.1; sin embargo, no se admiten las siguientes funciones:

- Conservación legal
- Retención basada en eventos
- SnapLock para SnapVault (compatible a partir de ONTAP 9.12.1)

También debe ser consciente de los siguientes comportamientos:

- El reloj de cumplimiento de volumen (VCC) de un volumen FlexGroup está determinado por el VCC del componente raíz. Todos los componentes que no son de raíz tendrán su VCC estrechamente sincronizado con la VCC raíz.
- Las propiedades de configuración de SnapLock se establecen únicamente en la FlexGroup en su conjunto. Los componentes individuales no pueden tener diferentes propiedades de configuración, como el tiempo de retención predeterminado y el período de compromiso automático.

Compatibilidad con LUN

Los LUN se admiten en volúmenes de SnapLock solo en casos en los que las copias de Snapshot creadas en un volumen distinto de SnapLock se transfieren a un volumen de SnapLock para la protección como parte de la relación de almacén de SnapLock. Los LUN no son compatibles con los volúmenes de SnapLock de lectura/escritura. Las copias Snapshot a prueba de manipulaciones son compatibles tanto con los volúmenes

de origen como con los volúmenes de destino de SnapMirror que contienen LUN.

Soporte de MetroCluster

La compatibilidad con SnapLock en configuraciones MetroCluster es diferente del modo de cumplimiento de normativas SnapLock al modo empresarial de SnapLock.

Cumplimiento de normativas SnapLock

- A partir de ONTAP 9.3, SnapLock Compliance se admite en los agregados de MetroCluster no reflejados.
- A partir de ONTAP 9.3, SnapLock Compliance se admite en agregados reflejados, pero solo si el agregado se utiliza para alojar los volúmenes de registros de auditoría de SnapLock.
- Las configuraciones de SnapLock específicas para SVM se pueden replicar en sitios principales y secundarios mediante MetroCluster.

Empresa SnapLock

- A partir de la versión 9 de ONTAP, se admiten los agregados de SnapLock Enterprise.
- A partir de ONTAP 9.3, se admiten los agregados de SnapLock Enterprise con eliminación privilegiada.
- Las configuraciones de SnapLock específicas para SVM se pueden replicar en ambos sitios mediante MetroCluster.

Configuraciones de MetroCluster y relojes de cumplimiento

Las configuraciones de MetroCluster utilizan dos mecanismos de reloj de conformidad, el reloj de cumplimiento de volumen (VCC) y el reloj de cumplimiento del sistema (SCC). El VCC y el SCC están disponibles para todas las configuraciones SnapLock. Cuando se crea un nuevo volumen en un nodo, su VCC se inicializa con el valor actual del SCC en ese nodo. Una vez creado el volumen, el VCC siempre se realiza un seguimiento del volumen y del tiempo de retención de archivos.

Cuando un volumen se replica en otro sitio, su VCC también se replica. Cuando se produce una conmutación de volumen, del sitio A al sitio B, por ejemplo, el VCC continúa siendo actualizado en el sitio B mientras que el SCC en el sitio A se detiene cuando el sitio A se desconecta.

Cuando el sitio A se vuelve a poner en línea y se realiza la vuelta de volumen, el reloj SCC del sitio se reinicia mientras el VCC del volumen continúa siendo actualizado. Como el VCC se actualiza continuamente, independientemente de las operaciones de conmutación de sitios y conmutación de estado, los tiempos de retención de archivos no dependen de los relojes SCC y no se amplían.

Compatibilidad con verificación multiadministrador (MAV)

A partir de la versión ONTAP 9.13.1, un administrador de clúster puede habilitar de forma explícita la verificación multiadministrador en un clúster para requerir la aprobación de quórum antes de ejecutar algunas operaciones de SnapLock. Cuando MAV está activado, las propiedades del volumen SnapLock como default-retention-time, minimum-retention-time, maximum-retention-time, volume-append-mode, autocommit-period y privileged-delete requerirán aprobación del quórum. Más información acerca de "MAV".

Eficiencia del almacenamiento

A partir de ONTAP 9.9.1, SnapLock admite funciones de eficiencia del almacenamiento, como la compactación de datos, la deduplicación entre volúmenes y la compresión adaptativa para volúmenes y agregados de SnapLock. Para obtener más información sobre la eficiencia del almacenamiento, consulte "Información general sobre la gestión de almacenamiento lógico con la CLI".

Cifrado

ONTAP ofrece tecnologías de cifrado basadas en software y hardware para garantizar que los datos en reposo no se puedan leer en caso de reasignación, devolución, pérdida o robo del medio de almacenamiento.

Exención de responsabilidad: NetApp no puede garantizar que los archivos WORM protegidos SnapLock en unidades o volúmenes de autocifrado se puedan recuperar si se pierde la clave de autenticación o si el número de intentos de autenticación con errores supera el límite especificado y hace que la unidad se bloquee de forma permanente. Usted es responsable de garantizar el cumplimiento de los fallos de autenticación.

> A partir de ONTAP 9.2, los volúmenes cifrados se admiten en agregados de SnapLock.

Transición de 7-Mode

Puede migrar volúmenes SnapLock de 7-Mode a ONTAP usando la función de transición basada en copias (CBT) de la herramienta de transición de 7-Mode. El modo SnapLock del volumen de destino, Compliance o Enterprise, debe coincidir con el modo SnapLock del volumen de origen. No se puede usar la transición sin copia (CFT) para migrar volúmenes de SnapLock.

Configure SnapLock

Configure SnapLock

Antes de utilizar SnapLock, tiene que configurar SnapLock realizando varias tareas, como "Instale la licencia de SnapLock" Para cada nodo que aloja un agregado con un volumen SnapLock, inicialice el "Reloj de cumplimiento", Crear un agregado de SnapLock para clusters que ejecuten versiones de ONTAP anteriores a ONTAP 9.10.1, "Cree y monte un volumen de SnapLock", y más.

Inicialice el reloj de cumplimiento

SnapLock utiliza *volume Compliance Clock* para garantizar la manipulación que puede alterar el período de retención de los archivos WORM. Primero, debe inicializar *system ComplianceClock* en cada nodo que aloje un agregado de SnapLock.

A partir de ONTAP 9.14.1, puede inicializar o reinicializar el reloj de cumplimiento de normativas del sistema cuando no hay volúmenes de SnapLock o ningún volumen con el bloqueo de copia de Snapshot habilitado. La capacidad de reinicializar permite a los administradores del sistema restablecer el reloj de cumplimiento del sistema en casos en los que podría haberse inicializado incorrectamente o corregir la desviación del reloj del sistema. En ONTAP 9.13.1 y versiones anteriores, una vez que se inicializa el reloj de cumplimiento de normativas en un nodo, no puede volver a inicializarlo.

Antes de empezar

Para reinicializar el reloj de conformidad:

- Todos los nodos del clúster deben tener el estado correcto.
- Todos los volúmenes deben estar en línea.
- No puede haber volúmenes presentes en la cola de recuperación.
- No hay volúmenes SnapLock presentes.
- No se puede presentar ningún volumen con bloqueo de copia de SnapVault habilitado.

Requisitos generales para inicializar el reloj de conformidad:

- Para realizar esta tarea, debe ser un administrador de clústeres.
- "La licencia de SnapLock debe instalarse en el nodo".

Acerca de esta tarea

La hora en el reloj de cumplimiento del sistema se hereda por el *volume Compliance Clock*, este último de los cuales controla el período de retención de los archivos WORM en el volumen. El reloj de cumplimiento de normativas del volumen se inicializa automáticamente cuando se crea un volumen de SnapLock nuevo.

> El ajuste inicial del reloj de cumplimiento del sistema se basa en el reloj del sistema de hardware actual. Por este motivo, debe verificar que la hora y la zona horaria del sistema sean correctas antes de inicializar el reloj de cumplimiento de normativas del sistema en cada nodo. Una vez que se inicializa el reloj de cumplimiento de normativas del sistema en un nodo, no se puede volver a inicializar cuando hay volúmenes de SnapLock o volúmenes con el bloqueo habilitado.

Pasos

Es posible usar la interfaz de línea de comandos de ONTAP para inicializar el reloj de cumplimiento de normativas o, a partir de ONTAP 9.12.1, puede utilizar System Manager para inicializar el reloj de cumplimiento de normativas.

System Manager

1. Vaya a **Cluster > Overview**.
2. En la sección **Nodes**, haga clic en **inicializar reloj de cumplimiento de SnapLock**.
3. Para mostrar la columna **Reloj de cumplimiento** y verificar que el Reloj de cumplimiento está inicializado, en la sección **Clúster > Descripción general > Nodos**, haga clic en **Mostrar/ocultar** y seleccione **Reloj de cumplimiento de SnapLock**.

CLI

1. Inicialice el reloj de cumplimiento del sistema:

   `snaplock compliance-clock initialize -node` *`node_name`*

   El siguiente comando inicializa el reloj de cumplimiento del sistema `node1`:

   ```
   cluster1::> snaplock compliance-clock initialize -node node1
   ```

2. Cuando se le solicite, confirme que el reloj del sistema es correcto y que desea inicializar el reloj de conformidad:

   ```
   Warning: You are about to initialize the secure ComplianceClock of
   the node "node1" to the current value of the node's system clock.
   This procedure can be performed only once on a given node, so you
   should ensure that the system time is set correctly before
   proceeding.

   The current node's system clock is: Mon Apr 25 06:04:10 GMT 2016

   Do you want to continue? (y|n): y
   ```

3. Repita este procedimiento para cada nodo que aloje un agregado de SnapLock.

Habilite la resincronización del reloj de cumplimiento de normativas para un sistema configurado por NTP

Puede habilitar la función de sincronización de hora de reloj de cumplimiento de normativas SnapLock cuando se configura un servidor NTP.

Lo que necesitará

- Esta función solo está disponible en el nivel de privilegios avanzado.
- Para realizar esta tarea, debe ser un administrador de clústeres.
- "La licencia de SnapLock debe instalarse en el nodo".
- Esta función sólo está disponible para plataformas Cloud Volumes ONTAP, ONTAP Select y VSIM.

Acerca de esta tarea

Cuando el daemon de reloj seguro de SnapLock detecta una desviación más allá del umbral, ONTAP utiliza la

hora del sistema para restablecer los relojes de cumplimiento del sistema y del volumen. Se establece un período de 24 horas como umbral de desviación. Esto significa que el reloj de cumplimiento del sistema se sincroniza con el reloj del sistema solo si la inclinación tiene más de un día de antigüedad.

El daemon de reloj seguro de SnapLock detecta una inclinación y cambia el reloj de cumplimiento a la hora del sistema. Cualquier intento de modificar la hora del sistema para forzar que el reloj de cumplimiento se sincronice con la hora del sistema falla, ya que el reloj de cumplimiento se sincroniza con la hora del sistema solo si la hora del sistema está sincronizada con la hora NTP.

Pasos

1. Habilite la función de sincronización de hora del reloj de cumplimiento de normativas de SnapLock cuando se configure un servidor NTP:

   `snaplock compliance-clock ntp`

   El siguiente comando habilita la función de sincronización de hora del reloj de cumplimiento de normativas del sistema:

   ```
   cluster1::*> snaplock compliance-clock ntp modify -is-sync-enabled true
   ```

2. Cuando se le solicite, confirme que los servidores NTP configurados son de confianza y que el canal de comunicación es seguro para habilitar la función:
3. Compruebe que la función está activada:

   `snaplock compliance-clock ntp show`

   El siguiente comando comprueba que la función de sincronización de hora del reloj de cumplimiento de normativas del sistema esté habilitada:

   ```
   cluster1::*> snaplock compliance-clock ntp show

   Enable clock sync to NTP system time: true
   ```

Cree un agregado de SnapLock

Se utiliza el volumen `-snaplock-type` Opción para especificar un tipo de volumen Compliance o Enterprise SnapLock. Para las versiones anteriores a ONTAP 9.10.1, se debe crear un agregado de SnapLock independiente. A partir de ONTAP 9.10.1, los volúmenes de SnapLock y otros de SnapLock pueden existir en el mismo agregado; por lo tanto, ya no es necesario crear un agregado de SnapLock separado si se utiliza ONTAP 9.10.1.

Antes de empezar

- Para realizar esta tarea, debe ser un administrador de clústeres.
- El SnapLock "se debe instalar la licencia" en el nodo. Esta licencia se incluye en "ONTAP One".
- "Se debe inicializar el reloj de cumplimiento de normativas del nodo".

- Si ha particionado los discos como «'root'», «dn1» y «atado2», deberá asegurarse de que los discos de repuesto están disponibles.

Consideraciones de renovación

Al actualizar a ONTAP 9.10.1, los agregados existentes de SnapLock y otros componentes de SnapLock se actualizan para admitir la existencia de volúmenes SnapLock y distintos de SnapLock; sin embargo, los atributos de volumen de SnapLock existentes no se actualizan automáticamente. Por ejemplo, los campos de compactación de datos, deduplicación entre volúmenes y deduplicación entre volúmenes en segundo plano siguen sin cambios. Los nuevos volúmenes SnapLock creados en agregados existentes tienen los mismos valores predeterminados que los volúmenes que no son de SnapLock, y los valores predeterminados de los nuevos volúmenes y agregados dependen de la plataforma.

Consideraciones sobre la reversión

Si necesita volver a una versión de ONTAP anterior a la 9.10.1, debe mover todos los volúmenes de SnapLock Compliance, SnapLock Enterprise y SnapLock a sus propios agregados de SnapLock.

Acerca de esta tarea

- No se pueden crear agregados de cumplimiento para las LUN de FlexArray, pero los agregados de SnapLock Compliance son compatibles con las LUN de FlexArray.
- No se pueden crear agregados de cumplimiento con la opción SyncMirror.
- Solo se pueden crear agregados de cumplimiento reflejado en una configuración de MetroCluster si el agregado se utiliza para alojar volúmenes de registro de auditoría de SnapLock.

> En una configuración MetroCluster, es compatible con SnapLock Enterprise con los agregados reflejados y no reflejados. SnapLock Compliance solo se admite en agregados no reflejados.

Pasos

1. Cree un agregado de SnapLock:

   ```
   storage aggregate create -aggregate <aggregate_name> -node <node_name>
   -diskcount <number_of_disks> -snaplock-type <compliance|enterprise>
   ```

   La página man del comando contiene una lista completa de opciones.

   El siguiente comando crea una SnapLock `Compliance` agregado con nombre `aggr1` con tres discos activados `node1`:

   ```
   cluster1::> storage aggregate create -aggregate aggr1 -node node1
   -diskcount 3 -snaplock-type compliance
   ```

Cree y monte volúmenes de SnapLock

Debe crear un volumen SnapLock para los archivos o las copias de Snapshot que desee confirmar al estado WORM. A partir de ONTAP 9.10.1, todos los volúmenes que cree, independientemente del tipo de agregado, se crearán de forma predeterminada como

volumen que no sea de SnapLock. Debe utilizar el `-snaplock-type` Opción para crear explícitamente un volumen de SnapLock especificando Compliance o Enterprise como el tipo de SnapLock. De forma predeterminada, el tipo de SnapLock se establece en `non-snaplock`.

Antes de empezar

- El agregado de SnapLock debe estar en línea.
- Usted debe "Compruebe que hay instalada una licencia de SnapLock". Si no hay una licencia de SnapLock instalada en el nodo, debe "instale" ti. Esta licencia se incluye con "ONTAP One". Antes de ONTAP One, la licencia de SnapLock se incluía en el paquete de seguridad y cumplimiento de normativas. El paquete de seguridad y cumplimiento ya no se ofrece, pero sigue siendo válido. Aunque actualmente no es obligatorio, los clientes existentes pueden optar por hacerlo "Actualice a ONTAP One".
- "Se debe inicializar el reloj de cumplimiento de normativas del nodo".

Acerca de esta tarea

Con los permisos de SnapLock adecuados, puede destruir un volumen empresarial o cambiar su nombre en cualquier momento. No se puede destruir un volumen de cumplimiento hasta que haya transcurrido el período de retención. Nunca se puede cambiar el nombre de un volumen de cumplimiento.

Es posible clonar volúmenes de SnapLock, pero no es posible clonar archivos en un volumen de SnapLock. El volumen clonado tendrá el mismo tipo de SnapLock que el volumen principal.

> Los LUN no son compatibles con los volúmenes de SnapLock. Los LUN se admiten en volúmenes de SnapLock solo en casos en los que las copias de Snapshot creadas en un volumen distinto de SnapLock se transfieren a un volumen de SnapLock para la protección como parte de la relación de almacén de SnapLock. Los LUN no son compatibles con los volúmenes de SnapLock de lectura/escritura. Las copias Snapshot a prueba de manipulaciones son compatibles tanto con los volúmenes de origen como con los volúmenes de destino de SnapMirror que contienen LUN.

Lleve a cabo esta tarea mediante System Manager de ONTAP o la interfaz de línea de comandos de ONTAP.

System Manager

A partir de ONTAP 9.12.1, se puede usar System Manager para crear un volumen de SnapLock.

Pasos

1. Vaya a **almacenamiento > volúmenes** y haga clic en **Agregar**.
2. En la ventana **Agregar volumen**, haga clic en **más opciones**.
3. Introduzca la nueva información del volumen, incluidos el nombre y el tamaño del volumen.
4. Seleccione **Activar SnapLock** y elija el tipo de SnapLock, ya sea Compliance o Enterprise.
5. En la sección **Archivos de registro automático**, seleccione **modificado** e introduzca la cantidad de tiempo que un archivo debe permanecer sin cambios antes de que se confirme automáticamente. El valor mínimo es de 5 minutos y el valor máximo es de 10 años.
6. En la sección **retención de datos**, seleccione el período de retención mínimo y máximo.
7. Seleccione el período de retención predeterminado.
8. Haga clic en **Guardar**.
9. Seleccione el nuevo volumen en la página **Volumes** para verificar la configuración de SnapLock.

CLI

1. Cree un volumen de SnapLock:

   ```
   volume create -vserver <SVM_name> -volume <volume_name> -aggregate
   <aggregate_name> -snaplock-type <compliance|enterprise>
   ```

   Para obtener una lista completa de las opciones, consulte la página de manual del comando. Las siguientes opciones no están disponibles para SnapLock Volumes: `-nvfail`, `-atime-update`, `-is-autobalance-eligible`, `-space-mgmt-try-first`, y. `vmalign`.

   El siguiente comando crea una SnapLock `Compliance` volumen denominado `vol1` encendido `aggr1` encendido `vs1`:

   ```
   cluster1::> volume create -vserver vs1 -volume vol1 -aggregate aggr1
   -snaplock-type compliance
   ```

Montar un volumen de SnapLock

Puede montar un volumen SnapLock en una ruta de unión en el espacio de nombres de la SVM para el acceso de clientes NAS.

Lo que necesitará

El volumen SnapLock debe estar en línea.

Acerca de esta tarea

- Los volúmenes de SnapLock solo se pueden montar en la raíz de la SVM.

- No se puede montar un volumen normal en un volumen de SnapLock.

Pasos

1. Montar un volumen de SnapLock:

   `volume mount -vserver` *`SVM_name`* `-volume` *`volume_name`* `-junction-path` *`path`*

   Para obtener una lista completa de las opciones, consulte la página de manual del comando.

   El siguiente comando monta un volumen SnapLock llamado `vol1` a la ruta de unión `/sales` en la `vs1` espacio de nombres:

   ```
   cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
   ```

Establezca el tiempo de retención

Se puede establecer el tiempo de retención de un archivo explícitamente o se puede usar el período de retención predeterminado para el volumen a fin de obtener el tiempo de retención. A menos que se establezca el tiempo de retención explícitamente, SnapLock utiliza el período de retención predeterminado para calcular el tiempo de retención. También es posible configurar la retención de archivos después de un evento.

Acerca del período de retención y del tiempo de retención

El *retention period* para un archivo WORM especifica la cantidad de tiempo que debe conservarse el archivo después de comprometerse al estado WORM. El *retention time* para un archivo WORM es el tiempo a partir del cual ya no es necesario retener el archivo. Un período de retención de 20 años para un archivo comprometido con EL estado WORM el 10 de noviembre a las 2020 6:00, por ejemplo, daría como resultado un período de retención de 10 de noviembre a las 2040 6:00 a.m.

> A partir de ONTAP 9.10.1, se puede establecer un tiempo de retención hasta el 26 de octubre de 3058 y un período de retención de hasta 100 años. Al ampliar las fechas de retención, las directivas más antiguas se convierten automáticamente. En ONTAP 9.9.1 y versiones anteriores, a menos que se establezca el período de retención predeterminado en infinito, el tiempo de retención máximo admitido es el 19 2071 de enero (GMT).

Consideraciones importantes sobre la replicación

Cuando se establece una relación de SnapMirror con un volumen de origen de SnapLock con una fecha de retención posterior al 19 de enero de 2071 (GMT), el clúster de destino debe ejecutar ONTAP 9.10.1 o una versión posterior, o se producirá un error en la transferencia de SnapMirror.

Consideraciones importantes sobre la reversión

ONTAP impide que se pueda revertir un clúster de ONTAP 9.10.1 a una versión de ONTAP anterior cuando hay archivos con un período de retención posterior a “19 de enero de 2071 8:44:07 AM”.

Descripción de los períodos de retención

Los volúmenes de empresa o de cumplimiento de normativas de SnapLock tienen cuatro períodos de retención:

- Período de retención mínimo (`min`), con un valor predeterminado de 0
- Período de retención máximo (`max`), con un valor por defecto de 30 años
- Período de retención predeterminado, con un valor predeterminado igual a. `min` Tanto para el modo de cumplimiento como para el modo de empresa a partir de ONTAP 9.10.1. En las versiones de ONTAP anteriores a ONTAP 9.10.1, el período de retención predeterminado depende del modo:
  - Para el modo de cumplimiento, el valor predeterminado es igual a `max`.
  - Para el modo Enterprise, el valor predeterminado es igual a. `min`.
- Período de retención no especificado.

  A partir de ONTAP 9.8, es posible establecer el período de retención en los archivos de un volumen en `unspecified`, para permitir que el archivo se conserve hasta que se establezca un tiempo de retención absoluto. Puede establecer un archivo con tiempo de retención absoluto en retención no especificada y volver a la retención absoluta siempre y cuando el nuevo tiempo de retención absoluto sea posterior al tiempo absoluto establecido anteriormente.

  A partir de ONTAP 9.12.1, archivos WORM con el período de retención establecido en `unspecified` Estén garantizados para que el período de retención se haya establecido en el período de retención mínimo configurado para el volumen de SnapLock. Al cambiar el período de retención de archivos de `unspecified` para un tiempo de retención absoluto, el nuevo tiempo de retención especificado debe ser superior al tiempo de retención mínimo establecido en el archivo.

Por lo tanto, si no establece el tiempo de retención explícitamente antes de confirmar un archivo de modo de cumplimiento en el estado WORM y no modifica los valores predeterminados, el archivo se conservará durante 30 años. Del mismo modo, si no establece el tiempo de retención explícitamente antes de comprometer un archivo de modo empresarial con el estado WORM, y no modifica los valores predeterminados, el archivo se conservará durante 0 años o, efectivamente, De nada.

Establecer el período de retención predeterminado

Puede utilizar el `volume snaplock modify` Comando para establecer el período de retención predeterminado para los archivos de un volumen de SnapLock.

Lo que necesitará

El volumen SnapLock debe estar en línea.

Acerca de esta tarea

En la siguiente tabla se muestran los posibles valores para la opción de período de retención predeterminado:

> El período de retención predeterminado debe ser mayor o igual que (>=) el período de retención mínimo y menor o igual que (<=) el período de retención máximo.

Valor	Unidad	Notas
0 - 65535	segundos	

Valor	Unidad	Notas
0 - 24	horas	
0 - 365	días	
0 - 12	meses	
0 - 100	años	A partir de ONTAP 9.10.1, Para versiones anteriores de ONTAP, el valor es 0 - 70.
capacidad	-	Usar el período de retención máximo.
espacio	-	Use el período de retención mínimo.
infinita	-	Conserve los archivos para siempre.
sin especificar	-	Conserve los archivos hasta que se defina un período de retención absoluto.

Los valores y los rangos para los períodos de retención máximo y mínimo son idénticos, excepto para `max` y.. `min`, que no son aplicables. Para obtener más información acerca de esta tarea, consulte "Establezca la visión general de la hora de retención".

Puede utilizar el `volume snaplock show` comando para ver la configuración del período de retención del volumen. Para obtener más información, consulte la página man del comando.

> Después de que un archivo se haya comprometido con el estado WORM, puede ampliar el período de retención, pero no acortar.

Pasos

1. Establezca el período de retención predeterminado para los archivos en un volumen de SnapLock:

   ```
   volume snaplock modify -vserver SVM_name -volume volume_name -default
   -retention-period default_retention_period -minimum-retention-period
   min_retention_period -maximum-retention-period max_retention_period
   ```

   Para obtener una lista completa de las opciones, consulte la página de manual del comando.

   > En los siguientes ejemplos se asume que los períodos de retención mínimo y máximo no se han modificado previamente.

   El siguiente comando establece el período de retención predeterminado para un volumen de Compliance o Enterprise en 20 días:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period 20days
```

El siguiente comando establece el período de retención predeterminado para un volumen de cumplimiento en 70 años:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -maximum
-retention-period 70years
```

El comando siguiente establece el período de retención predeterminado para un volumen de Enterprise en 10 años:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period max -maximum-retention-period 10years
```

Los siguientes comandos establecen el período de retención predeterminado para un volumen de empresa en 10 días:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -minimum
-retention-period 10days
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period min
```

El siguiente comando establece el período de retención predeterminado para un volumen de cumplimiento en infinito:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period infinite -maximum-retention-period infinite
```

Establezca explícitamente el tiempo de retención de un archivo

Puede establecer explícitamente el tiempo de retención de un archivo modificando su última hora de acceso. Puede usar cualquier comando o programa adecuado a través de NFS o CIFS para modificar la última hora de acceso.

Acerca de esta tarea

Después de haber comprometido un archivo con WORM, puede ampliar el tiempo de retención, pero no reducir este. El tiempo de retención se almacena en la `atime` para el archivo.

> No se puede establecer explícitamente el tiempo de retención de un archivo en `infinite`. Ese valor solo está disponible cuando se utiliza el período de retención predeterminado para calcular el tiempo de retención.

Pasos

1. Utilice un comando o programa adecuado para modificar la última hora de acceso para el archivo cuyo tiempo de retención desee establecer.

   En un shell de UNIX, utilice el comando siguiente para establecer una hora de retención de 21 de noviembre de 2020 6:00 a.m. en un archivo llamado `document.txt`:

   ```
   touch -a -t 202011210600 document.txt
   ```

   Puede utilizar cualquier comando o programa adecuado para modificar la última hora de acceso en Windows.

Establezca el período de retención de archivos después de un evento

A partir de ONTAP 9.3, puede definir cuánto tiempo se retiene un archivo después de que se produzca un evento mediante la función SnapLock *Event Based Retention (EBR)*.

Lo que necesitará

- Debe ser un administrador de SnapLock para realizar esta tarea.

  "Cree una cuenta de administrador de SnapLock"

- Debe haber iniciado sesión en una conexión segura (SSH, Console o ZAPI).

Acerca de esta tarea

La directiva *event retention* define el período de retención del archivo después de que se produzca el evento. La directiva se puede aplicar a un único archivo o a todos los archivos de un directorio.

- Si un archivo no es UN archivo WORM, se comprometerá con el estado WORM para el período de retención definido en la política.
- Si un archivo es UN archivo WORM o un archivo ampliable WORM, su período de retención se extenderá por el período de retención que se define en la política.

Puede usar un volumen de modo de cumplimiento o de modo empresarial.

Las políticas de EBR no se pueden aplicar a los archivos de una retención legal.

Para un uso avanzado, consulte "Almacenamiento WORM conforme a la normativa con SnapLock de NetApp".

usar EBR para ampliar el período de retención de archivos WORM ya existentes

EBR resulta muy práctico cuando se desea ampliar el período de retención de archivos WORM ya existentes. Por ejemplo, podría ser la política de su empresa retener los registros del empleado W-4 en forma no modificada durante tres años después de que el empleado cambie una elección de retención. Otra política de la empresa podría requerir que los registros W-4 se retengan durante cinco años después de que el empleado haya terminado.

En este caso, podría crear una política EBR con un período de retención de cinco años. Una vez que el empleado ha terminado (el "'evento'"), aplicaría la política de EBR al registro W-4 del empleado, lo que provocaría que se ampliara su período de retención. Esto suele ser más sencillo que ampliar el período de retención manualmente, especialmente cuando se trata de un gran número de archivos.

Pasos

1. Crear una política EBR:

   snaplock event-retention policy create -vserver *SVM_name* -name *policy_name* -retention-period *retention_period*

   El siguiente comando crea la política EBR `employee_exit` encendido `vs1` con un período de retención de diez años:

   ```
   cluster1::>snaplock event-retention policy create -vserver vs1 -name
   employee_exit -retention-period 10years
   ```

2. Aplicar una política EBR:

   snaplock event-retention apply -vserver *SVM_name* -name *policy_name* -volume *volume_name* -path *path_name*

   El siguiente comando aplica la política EBR `employee_exit` encendido `vs1` a todos los archivos del directorio `d1`:

   ```
   cluster1::>snaplock event-retention apply -vserver vs1 -name
   employee_exit -volume vol1 -path /d1
   ```

Cree un registro de auditoría

Si utiliza ONTAP 9.9.1 o una versión anterior, primero debe crear un agregado de SnapLock y, a continuación, debe crear un registro de auditoría protegido por SnapLock antes de ejecutar una eliminación con privilegios o mover volúmenes de SnapLock. El registro de auditoría registra la creación y eliminación de cuentas de administrador de SnapLock, las modificaciones realizadas en el volumen de registro, si la eliminación con privilegios está habilitada, las operaciones de eliminación con privilegios y las operaciones de movimiento de volúmenes SnapLock.

A partir de ONTAP 9.10.1, ya no se crea un agregado de SnapLock. Debe utilizar la opción -snaplock-type a. "Crear explícitamente un volumen SnapLock" Especificando Compliance o Enterprise como tipo SnapLock.

Antes de empezar

Si se utiliza ONTAP 9.9.1 o una versión anterior, debe ser un administrador de clústeres para crear un agregado de SnapLock.

Acerca de esta tarea

No se puede eliminar un registro de auditoría hasta que haya transcurrido el período de retención del archivo de registro. No es posible modificar un registro de auditoría incluso después de transcurrido el período de retención. Esto es así tanto para el modo de cumplimiento de normativas SnapLock como para el modo de empresa.

> En ONTAP 9.4 y versiones anteriores, no se puede usar un volumen de empresa SnapLock para el registro de auditoría. Se debe usar un volumen de cumplimiento de normativas de SnapLock. En ONTAP 9.5 y versiones posteriores, se puede usar un volumen de empresa SnapLock o un volumen de cumplimiento de SnapLock para el registro de auditoría. En todos los casos, el volumen de registro de auditoría debe montarse en la ruta de unión `/snaplock_audit_log`. Ningún otro volumen puede utilizar esta ruta de unión.

Los registros de auditoría de SnapLock se pueden encontrar en la `/snaplock_log` directorio en la raíz del volumen de registro de auditoría, en subdirectorios denominados `privdel_log` (operaciones de eliminación con privilegios) y. `system_log` (todo lo demás). Los nombres de archivos de registro de auditoría contienen la Marca de hora de la primera operación de registro, lo que facilita la búsqueda de registros en el momento aproximado en que se ejecutaron las operaciones.

- Puede utilizar el `snaplock log file show` comando para ver los archivos de registro en el volumen del registro de auditoría.
- Puede utilizar el `snaplock log file archive` para archivar el archivo de registro actual y crear uno nuevo, lo que resulta útil en los casos en los que se necesita registrar la información del registro de auditoría en un archivo independiente.

Para obtener más información, consulte las páginas de manual de los comandos.

> No se puede usar un volumen de protección de datos como volumen de registro de auditoría de SnapLock.

Pasos

1. Cree un agregado de SnapLock.

   Cree un agregado de SnapLock

2. En la SVM que desee configurar para el registro de auditoría, cree un volumen de SnapLock.

   Cree un volumen de SnapLock

3. Configure la SVM para el registro de auditoría:

   `snaplock log create -vserver` *`SVM_name`* `-volume` *`snaplock_volume_name`* `-max-log -size` *`size`* `-retention-period` *`default_retention_period`*

> El período de retención mínimo predeterminado para archivos de registro de auditoría es de seis meses. Si el período de retención de un archivo afectado es más largo que el período de retención del registro de auditoría, el período de retención del registro hereda el período de retención del archivo. Por lo tanto, si el período de retención de un archivo eliminado mediante eliminación privilegiada es de 10 meses y el período de retención del registro de auditoría de 8 meses, el período de retención del registro se extiende a 10 meses. Para obtener más información sobre el tiempo de retención y el período de retención predeterminado, consulte "Establezca el tiempo de retención".

Se configura el siguiente comando `SVM1` Para el registro de auditoría mediante el volumen SnapLock `logVol`. El registro de auditoría tiene un tamaño máximo de 20 GB y se conserva durante ocho meses.

```
SVM1::> snaplock log create -vserver SVM1 -volume logVol -max-log-size
20GB -retention-period 8months
```

4. En la SVM que haya configurado para el registro de auditoría, monte el volumen SnapLock en la ruta de unión `/snaplock_audit_log`.

   Montar un volumen de SnapLock

Comprobar la configuración de SnapLock

Puede utilizar el `volume file fingerprint start` y.. `volume file fingerprint dump` Comandos para ver información clave sobre archivos y volúmenes, incluido el tipo de archivo (normal, WORM o WORM, que puede adaptarse a ellas), la fecha de caducidad del volumen, etc.

Pasos

1. Generar una huella digital de archivo:

   `volume file fingerprint start -vserver` *`SVM_name`* `-file` *`file_path`*

   ```
   svm1::> volume file fingerprint start -vserver svm1 -file
   /vol/sle/vol/f1
   File fingerprint operation is queued. Run "volume file fingerprint show
   -session-id 16842791" to view the fingerprint session status.
   ```

   El comando genera un ID de sesión que puede usar como entrada en el `volume file fingerprint dump` comando.

   > Puede utilizar el `volume file fingerprint show` Comando con el ID de sesión para supervisar el progreso de la operación de huella digital. Asegúrese de que la operación haya finalizado antes de intentar mostrar la huella.

2. Mostrar la huella digital del archivo:

   `volume file fingerprint dump -session-id` *`session_ID`*

```
svm1::> volume file fingerprint dump -session-id 33619976
        Vserver:svm1
        Session-ID:33619976
        Volume:slc_vol
        Path:/vol/slc_vol/f1
        Data
Fingerprint:MOFJVevxNSJm3C/4Bn5oEEYH51CrudOzZYK4r5Cfy1g=Metadata

Fingerprint:8iMjqJXiNcqgXT5XuRhLiEwIrJEihDmwS0hrexnjgmc=Fingerprint
Algorithm:SHA256
        Fingerprint Scope:data-and-metadata
        Fingerprint Start Time:1460612586
        Formatted Fingerprint Start Time:Thu Apr 14 05:43:06 GMT 2016
        Fingerprint Version:3
        **SnapLock License:available**
        Vserver UUID:acf7ae64-00d6-11e6-a027-0050569c55ae
        Volume MSID:2152884007
        Volume DSID:1028
        Hostname:my_host
        Filer ID:5f18eda2-00b0-11e6-914e-6fb45e537b8d
        Volume Containing Aggregate:slc_aggr1
        Aggregate ID:c84634aa-c757-4b98-8f07-eefe32565f67
        **SnapLock System ComplianceClock:1460610635
        Formatted SnapLock System ComplianceClock:Thu Apr 14 05:10:35
GMT 2016
        Volume SnapLock Type:compliance
        Volume ComplianceClock:1460610635
        Formatted Volume ComplianceClock:Thu Apr 14 05:10:35 GMT 2016
        Volume Expiry Date:1465880998**
         Is Volume Expiry Date Wraparound:false
        Formatted Volume Expiry Date:Tue Jun 14 05:09:58 GMT 2016
        Filesystem ID:1028
        File ID:96
        File Type:worm
        File Size:1048576
        Creation Time:1460612515
        Formatted Creation Time:Thu Apr 14 05:41:55 GMT 2016
        Modification Time:1460612515
        Formatted Modification Time:Thu Apr 14 05:41:55 GMT 2016
        Changed Time:1460610598
        Is Changed Time Wraparound:false
        Formatted Changed Time:Thu Apr 14 05:09:58 GMT 2016
        Retention Time:1465880998
        Is Retention Time Wraparound:false
        Formatted Retention Time:Tue Jun 14 05:09:58 GMT 2016
```

```
        Access Time:-
        Formatted Access Time:-
        Owner ID:0
        Group ID:0
        Owner SID:-
        Fingerprint End Time:1460612586
        Formatted Fingerprint End Time:Thu Apr 14 05:43:06 GMT 2016
```

Gestione los archivos WORM

Gestione los archivos WORM

Puede gestionar archivos WORM de las siguientes formas:

- "Los archivos cumplen CON WORM"
- "Confirmar copias Snapshot a WORM en un destino de almacén"
- "Refleje los archivos WORM para la recuperación ante desastres"
- "Conserve los archivos WORM durante su proceso de litigio"
- "Eliminar los archivos WORM"

Los archivos cumplen CON WORM

Puede confirmar archivos a WORM (escritura única y lectura múltiple) o bien manualmente, o bien conserva los archivos automáticamente. También puede crear archivos flexibles WORM.

Confirmar los archivos a WORM manualmente

Los archivos se comprometen a WORM manualmente haciendo que el archivo sea de solo lectura. Puede utilizar cualquier comando o programa adecuado a través de NFS o CIFS para cambiar el atributo de lectura y escritura de un archivo a sólo lectura. Puede optar por confirmar los archivos manualmente si desea garantizar que una aplicación haya terminado de escribir en un archivo de modo que el archivo no se confirme prematuramente o si hay problemas de escalado para el analizador de compromiso automático debido a un gran número de volúmenes.

Lo que necesitará

- El archivo que desea confirmar debe residir en un volumen de SnapLock.
- El archivo debe ser editable.

Acerca de esta tarea

El tiempo de la instancia de ComplianceClock del volumen se escribe en `ctime` campo del archivo cuando se ejecuta el comando o el programa. La hora de la instancia de ComplianceClock determina cuándo se ha alcanzado el tiempo de retención del archivo.

Pasos

1. Utilice un comando o programa adecuado para cambiar el atributo de lectura y escritura de un archivo a sólo lectura.

En un shell UNIX, utilice el siguiente comando para crear un archivo denominado `document.txt` solo lectura:

```
chmod -w document.txt
```

En un shell de Windows, utilice el siguiente comando para crear un archivo denominado `document.txt` solo lectura:

```
attrib +r document.txt
```

Confirmar archivos a WORM automáticamente

La función de compromiso automático de SnapLock le permite confirmar los archivos automáticamente a WORM. La función de compromiso automático confirma un archivo en estado WORM en un volumen SnapLock si el archivo no cambió en el período de compromiso automático duración. La función de compromiso automático está deshabilitada de forma predeterminada.

Lo que necesitará

- Los archivos que desea confirmar automáticamente deben residir en un volumen de SnapLock.
- El volumen SnapLock debe estar en línea.
- El volumen SnapLock debe ser un volumen de lectura/escritura.

> La función SnapLock autocommit analiza todos los archivos del volumen y confirma un archivo si cumple con el requisito de compromiso automático. Es posible que haya un intervalo de tiempo entre cuando el archivo esté listo para la confirmación automática y cuando el escáner de confirmación automática de SnapLock lo confirme realmente. Sin embargo, el sistema de archivos sigue protegiendo el archivo de las modificaciones y eliminaciones en cuanto sea apto para la confirmación automática.

Acerca de esta tarea

El *autocommit Period* especifica la cantidad de tiempo que los archivos deben permanecer sin cambios antes de que se autocomprometan. Al cambiar un archivo antes de que haya transcurrido el período de compromiso automático, se reinicia el período de compromiso automático del archivo.

En la siguiente tabla se muestran los posibles valores para el período de compromiso automático:

Valor	Unidad	Notas
ninguno	-	El valor predeterminado.
5 - 5256000	minutos	-
1 - 87600	horas	-
1 - 3650	días	-

Valor	Unidad	Notas
1 - 120	meses	-
1 - 10	años	-

El valor mínimo es de 5 minutos y el valor máximo es de 10 años.

Pasos

1. Los archivos de confirmación automática en un volumen SnapLock a WORM:

   volume snaplock modify -vserver *SVM_name* -volume *volume_name* -autocommit -period *autocommit_period*

   Para obtener una lista completa de las opciones, consulte la página de manual del comando.

   El siguiente comando confirma automáticamente los archivos en el volumen `vol1` De SVM vs1, siempre y cuando los archivos permanezcan inalterados durante 5 horas:

   ```
   cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -autocommit
   -period 5hours
   ```

Crear un archivo ampliable WORM

Un archivo ampliable WORM conserva los datos escritos de forma incremental, como las entradas del registro. Puede utilizar cualquier comando o programa adecuado para crear un archivo que pueda adaptarse A WORM o la función SnapLock *volume append mode* para crear archivos WORM adaptados de forma predeterminada.

Utilice un comando o programa para crear un archivo que puede adaptarse A WORM

Puede utilizar cualquier comando o programa adecuado a través de NFS o CIFS para crear un archivo ampliable WORM. Un archivo ampliable WORM conserva los datos escritos de forma incremental, como las entradas del registro. Los datos se agregan al archivo en fragmentos de 256 KB. A medida que se escribe cada fragmento, el fragmento anterior se convierte en CON protección WORM. No se puede eliminar el archivo hasta que haya transcurrido el período de retención.

Lo que necesitará

El archivo ampliable WORM debe residir en un volumen SnapLock.

Acerca de esta tarea

Los datos no tienen que escribirse secuencialmente en el fragmento de 256 KB activo. Cuando se escriben datos en el byte n×256KB+1 del archivo, el segmento de 256 KB anterior se protege WORM.

Pasos

1. Utilice un comando o programa adecuado para crear un archivo de longitud cero con el tiempo de retención deseado.

   En un shell de UNIX, utilice el comando siguiente para establecer una hora de retención de 21 de

noviembre de 2020 6:00 a.m. en un archivo de longitud cero denominado `document.txt`:

```
touch -a -t 202011210600 document.txt
```

2. Utilice un comando o programa adecuado para cambiar el atributo de lectura y escritura del archivo a sólo lectura.

   En un shell UNIX, utilice el siguiente comando para crear un archivo denominado `document.txt` solo lectura:

```
chmod 444 document.txt
```

3. Utilice un comando o programa adecuado para cambiar el atributo de lectura y escritura del archivo a grabable.

   > Este paso no se considera un riesgo de cumplimiento de normativas porque no hay datos en el archivo.

   En un shell UNIX, utilice el siguiente comando para crear un archivo denominado `document.txt` modificable:

```
chmod 777 document.txt
```

4. Utilice un comando o programa adecuado para iniciar la escritura de datos en el archivo.

   En un shell UNIX, utilice el comando siguiente para escribir datos en `document.txt`:

```
echo test data >> document.txt
```

   > Vuelva a cambiar los permisos de archivo a sólo lectura cuando ya no necesite agregar datos al archivo.

Use el modo de adición de volúmenes para crear archivos WORM flexibles

A partir de ONTAP 9.3, se puede utilizar la función SnapLock *volume append mode* (VAM) para crear archivos WORM flexibles de forma predeterminada. Un archivo ampliable WORM conserva los datos escritos de forma incremental, como las entradas del registro. Los datos se agregan al archivo en fragmentos de 256 KB. A medida que se escribe cada fragmento, el fragmento anterior se convierte en CON protección WORM. No se puede eliminar el archivo hasta que haya transcurrido el período de retención.

Lo que necesitará

- El archivo ampliable WORM debe residir en un volumen SnapLock.
- El volumen SnapLock debe estar desmontado y vacío de las copias Snapshot y los archivos creados por el usuario.

Acerca de esta tarea

Los datos no tienen que escribirse secuencialmente en el fragmento de 256 KB activo. Cuando se escriben datos en el byte n×256KB+1 del archivo, el segmento de 256 KB anterior se protege WORM.

Si especifica un período de compromiso automático para el volumen, se comprometen a WORM los archivos flexibles que no se modifican durante un período superior al período de compromiso automático a WORM.

> No se admite el VAM en los volúmenes de registros de auditoría de SnapLock.

Pasos

1. Activar VAM:

   `volume snaplock modify -vserver` *`SVM_name`* `-volume` *`volume_name`* `-is-volume-append -mode-enabled true|false`

   Para obtener una lista completa de las opciones, consulte la página de manual del comando.

   El siguiente comando habilita VAM sobre el volumen `vol1` De SVM`vs1`:

   ```
   cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -is-volume
   -append-mode-enabled true
   ```

2. Utilice un comando o programa adecuado para crear archivos con permisos de escritura.

   De forma predeterminada, los archivos se pueden APPWORM.

Confirmar copias Snapshot a WORM en un destino de almacén

Puede usar SnapLock para SnapVault para proteger CON WORM las copias Snapshot en el almacenamiento secundario. Todas las tareas básicas de SnapLock se realizan en el destino del almacén. El volumen de destino es de solo lectura montado automáticamente, por lo que no es necesario confirmar explícitamente las copias Snapshot a WORM; por lo tanto, no se admiten la creación de copias Snapshot programadas en el volumen de destino mediante políticas de SnapMirror.

Antes de empezar

- El clúster de origen debe ejecutar ONTAP 8.2.2 o una versión posterior.
- Los agregados de origen y destino deben tener 64 bits.
- El volumen de origen no puede ser un volumen de SnapLock.
- Los volúmenes de origen y destino deben crearse en clústeres con una relación entre iguales con SVM.

  Para obtener más información, consulte "Conexión de clústeres entre iguales".

- Si se deshabilita el crecimiento automático de un volumen, el espacio libre en el volumen de destino debe ser al menos un cinco por ciento mayor que el espacio usado en el volumen de origen.

Acerca de esta tarea

El volumen de origen puede usar almacenamiento de NetApp o de terceros. Para el almacenamiento que no

sea de NetApp, debe usar la virtualización de FlexArray.

> No puede cambiar el nombre de una copia Snapshot que esté comprometida con el estado WORM.

Es posible clonar volúmenes de SnapLock, pero no es posible clonar archivos en un volumen de SnapLock.

> Los LUN no son compatibles con los volúmenes de SnapLock. Los LUN se admiten en volúmenes de SnapLock solo en casos en los que las copias de Snapshot creadas en un volumen distinto de SnapLock se transfieren a un volumen de SnapLock para la protección como parte de la relación de almacén de SnapLock. Los LUN no son compatibles con los volúmenes de SnapLock de lectura/escritura. Las copias Snapshot a prueba de manipulaciones son compatibles tanto con los volúmenes de origen como con los volúmenes de destino de SnapMirror que contienen LUN.

A partir de ONTAP 9.14.1, puede especificar períodos de retención para etiquetas de SnapMirror específicas en la política de SnapMirror de la relación de SnapMirror, de modo que las copias Snapshot replicadas del volumen de origen al de destino se conserven durante el período de retención especificado en la regla. Si no se especifica ningún período de retención, se utiliza el período de retención predeterminado del volumen de destino.

A partir de ONTAP 9.13.1, puede restaurar instantáneamente una copia Snapshot bloqueada en el volumen SnapLock de destino de una relación de almacén de SnapLock mediante la creación de un FlexClone con el `snaplock-type` Opción establecida en «non-snaplock» y especificando la copia Snapshot como la «parent-snapshot» al ejecutar la operación de creación de clones de volúmenes. Más información acerca de "Creación de un volumen FlexClone con un tipo de SnapLock".

Para las configuraciones de MetroCluster, debe tener en cuenta lo siguiente:

- Solo puede crear relaciones de SnapVault entre varias SVM sincronizada en origen, no entre una SVM sincronizada en origen y una SVM sincronizada en destino.
- Puede crear una relación de SnapVault entre un volumen en una SVM sincronizada en origen y una SVM que sirva datos.
- Puede crear una relación de SnapVault entre un volumen en una SVM que sirva datos y un volumen de DP en una SVM sincronizada en origen.

En la siguiente ilustración, se muestra el procedimiento para inicializar una relación de almacén de SnapLock:

Pasos

1. Identifique el clúster de destino.
2. En el clúster de destino, "Instale la licencia de SnapLock", "Inicialice el reloj de cumplimiento", Y, si está utilizando una versión de ONTAP anterior a 9.10.1, "Cree un agregado de SnapLock".
3. En el clúster de destino, cree un volumen de destino de SnapLock de tipo `DP` que tiene el mismo tamaño o mayor que el volumen de origen:

   ```
   volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name
   -snaplock-type compliance|enterprise -type DP -size size
   ```

> A partir de ONTAP 9.10.1, los volúmenes de SnapLock y otros de SnapLock pueden existir en el mismo agregado; por lo tanto, ya no es necesario crear un agregado de SnapLock separado si se utiliza ONTAP 9.10.1. La opción volume -snaplock-type se utiliza para especificar el tipo de volumen Compliance o Enterprise SnapLock. En las versiones de ONTAP anteriores a ONTAP 9.10.1, el modo SnapLock, Compliance o Enterprise, se hereda del agregado. No se admiten los volúmenes de destino con versión flexible. La configuración de idioma del volumen de destino debe coincidir con la configuración de idioma del volumen de origen.

El siguiente comando crea una SnapLock de 2 GB `Compliance` volumen denominado `dstvolB` pulg `SVM2` en el agregado `node01_aggr`:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

4. En el clúster de destino, establezca el período de retención predeterminado, tal como se describe en Establecer el período de retención predeterminado.

> Un volumen SnapLock que es un destino de almacén tiene asignado un período de retención predeterminado. El valor correspondiente a este período se establece inicialmente en un mínimo de 0 años para volúmenes de SnapLock Enterprise y un máximo de 30 años para volúmenes de SnapLock Compliance. Cada copia de Snapshot de NetApp se compromete con el primer período de retención predeterminado. El período de retención se puede ampliar más adelante, si fuera necesario. Para obtener más información, consulte Establecer información general sobre el tiempo de retención.

5. Cree una nueva relación de replicación Entre el origen que no es de SnapLock y el nuevo destino de SnapLock que creó en el paso 3.

   En este ejemplo, se crea una nueva relación de SnapMirror con el volumen de SnapLock de destino `dstvolB` utilizar una política de `XDPDefault` Para almacenar las copias snapshot etiquetadas como diaria y semanal en una programación horaria:

```
cluster2::> snapmirror create -source-path SVM1:srcvolA -destination
-path SVM2:dstvolB -vserver SVM2 -policy XDPDefault -schedule hourly
```

> Cree una política de replicación personalizada o a programación personalizada si los valores predeterminados disponibles no son adecuados.

6. En la SVM de destino, inicialice la relación de SnapVault creada en el paso 5:

   `snapmirror initialize -destination-path` *`destination_path`*

   El siguiente comando inicializa la relación entre el volumen de origen `srcvolA` encendido `SVM1` y el volumen de destino `dstvolB` encendido `SVM2`:

```
cluster2::> snapmirror initialize -destination-path SVM2:dstvolB
```

7. Después de inicializar y de estar inactiva la relación, utilice `snapshot show` Comando en el destino para comprobar el tiempo de caducidad de la SnapLock aplicado a las copias Snapshot replicadas.

   En este ejemplo, se enumeran las copias Snapshot en el volumen `dstvolB` Que tienen la etiqueta de SnapMirror y la fecha de caducidad de SnapLock:

   ```
   cluster2::> snapshot show -vserver SVM2 -volume dstvolB -fields
   snapmirror-label, snaplock-expiry-time
   ```

Información relacionada

"Relaciones entre iguales de clústeres y SVM"

"Backup de volúmenes mediante SnapVault"

Refleje los archivos WORM para la recuperación ante desastres

Puede usar SnapMirror para replicar archivos WORM a otra ubicación geográfica a efectos de recuperación ante desastres y otros fines. Tanto el volumen de origen como el de destino deben configurarse para SnapLock, y ambos volúmenes deben tener el mismo modo SnapLock, Compliance o Enterprise. Se replican todas las propiedades clave de la SnapLock del volumen y los archivos.

Requisitos previos

Los volúmenes de origen y destino deben crearse en clústeres con una relación entre iguales con SVM. Para obtener más información, consulte "Relaciones entre iguales de clústeres y SVM".

Acerca de esta tarea

- A partir de ONTAP 9.5, puede replicar archivos WORM con la relación de tipo XDP (protección de datos ampliada) de SnapMirror en lugar de la relación de tipo DP (protección de datos). El modo XDP es independiente de las versiones de ONTAP y es capaz de diferenciar los archivos almacenados en el mismo bloque, facilitando de este modo la resincronización de los volúmenes replicados de modo de cumplimiento. Para obtener información sobre cómo convertir una relación de tipo DP existente a una relación de tipo XDP, consulte "Protección de datos".
- Una operación de resincronización de tipo DP relación SnapMirror genera un error en un volumen de modo de cumplimiento si SnapLock determina que provocará la pérdida de datos. Si una operación de resincronización falla, puede utilizar el `volume clone create` comando para crear un clon del volumen de destino. A continuación, puede volver a sincronizar el volumen de origen con el clon.
- Una relación de SnapMirror del tipo XDP entre volúmenes compatibles con SnapLock admite una resincronización después de una interrupción aunque los datos del destino hayan divergido del origen posterior a la interrupción.

  En un resincronización, cuando se detecta una divergencia de datos entre el destino de origen más allá de la instantánea común, se corta una nueva instantánea en el destino para capturar esta divergencia. La nueva snapshot y la snapshot común están bloqueadas con un tiempo de retención de la siguiente manera:

  - La hora de caducidad del volumen del destino
  - Si el tiempo de caducidad del volumen es pasado o no se ha establecido, la copia de Snapshot se bloquea durante un período de 30 días

- Si el destino tiene retenciones legales, el período de caducidad real del volumen se oculta y aparece como "indefinido", sin embargo la instantánea se bloquea durante el período de caducidad real del volumen.

Si el volumen de destino tiene un período de caducidad posterior al origen, se conserva el período de caducidad del destino y no se sobrescribe con el período de caducidad del volumen de origen posterior a la resincronización.

Si el destino tiene retenciones legales en él que difieren de la fuente, no se permite una resincronización. El origen y el destino deben tener idénticas retenciones legales o todas las retenciones legales del destino deben liberarse antes de intentar realizar una resincronización.

Una copia Snapshot bloqueada en el volumen de destino creada para capturar los datos divergentes se puede copiar en el origen con la CLI ejecutando el `snapmirror update -s snapshot` comando. La instantánea una vez copiada seguirá bloqueada en la fuente.

- No se admiten las relaciones de protección de datos de SVM.
- No se admiten las relaciones de protección de datos con uso compartido de carga.

En la siguiente ilustración, se muestra el procedimiento para inicializar una relación de SnapMirror:

System Manager

A partir de ONTAP 9.12.1, puede usar System Manager para configurar la replicación de SnapMirror de archivos WORM.

Pasos

1. Vaya a **almacenamiento > volúmenes**.
2. Haga clic en **Mostrar/Ocultar** y seleccione **Tipo de SnapLock** para visualizar la columna en la ventana **volúmenes**.
3. Busque un volumen de SnapLock.
4. Haga clic en ⋮ Y seleccione **proteger**.
5. Elija el clúster de destino y la máquina virtual de almacenamiento de destino.
6. Haga clic en **más opciones**.
7. Seleccione **Mostrar políticas heredadas** y seleccione **DPDefault (Legacy)**.
8. En la sección **Detalles de la configuración de destino**, seleccione **Anular programa de transferencia** y seleccione **por hora**.
9. Haga clic en **Guardar**.
10. A la izquierda del nombre del volumen de origen, haga clic en la flecha para expandir los detalles del volumen y, en el lado derecho de la página, consulte los detalles de la protección remota de SnapMirror.
11. En el clúster remoto, vaya a **Relaciones de protección**.
12. Busque la relación y haga clic en el nombre del volumen de destino para ver los detalles de la relación.
13. Compruebe que el tipo de SnapLock del volumen de destino y otra información de SnapLock.

CLI

1. Identifique el clúster de destino.
2. En el clúster de destino, "Instale la licencia de SnapLock", "Inicialice el reloj de cumplimiento", Y, si está utilizando una versión de ONTAP anterior a 9.10.1, "Cree un agregado de SnapLock".
3. En el clúster de destino, cree un volumen de destino de SnapLock de tipo `DP` es el mismo tamaño que el volumen de origen o mayor:

   ```
   volume create -vserver SVM_name -volume volume_name -aggregate
   aggregate_name -snaplock-type compliance|enterprise -type DP -size size
   ```

   > A partir de ONTAP 9.10.1, los volúmenes de SnapLock y otros de SnapLock pueden existir en el mismo agregado; por lo tanto, ya no es necesario crear un agregado de SnapLock separado si se utiliza ONTAP 9.10.1. La opción volume -snaplock-type se utiliza para especificar el tipo de volumen Compliance o Enterprise SnapLock. En las versiones de ONTAP anteriores a ONTAP 9.10.1, el modo SnapLock (Compliance o Enterprise) se hereda del agregado. No se admiten los volúmenes de destino con versión flexible. La configuración de idioma del volumen de destino debe coincidir con la configuración de idioma del volumen de origen.

   El siguiente comando crea una SnapLock de 2 GB `Compliance` volumen denominado `dstvolB` pulg `SVM2` en el agregado `node01_aggr`:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

4. En la SVM de destino, cree una política de SnapMirror:

   snapmirror policy create -vserver *SVM_name* -policy *policy_name*

   El siguiente comando crea la política de toda la SVM `SVM1-mirror`:

   ```
   SVM2::> snapmirror policy create -vserver SVM2 -policy SVM1-mirror
   ```

5. En la SVM de destino, cree una programación de SnapMirror:

   job schedule cron create -name *schedule_name* -dayofweek *day_of_week* -hour *hour* -minute *minute*

   El siguiente comando crea una programación de SnapMirror con el nombre `weekendcron`:

   ```
   SVM2::> job schedule cron create -name weekendcron -dayofweek
   "Saturday, Sunday" -hour 3 -minute 0
   ```

6. En la SVM de destino, cree una relación de SnapMirror:

   snapmirror create -source-path *source_path* -destination-path *destination_path* -type XDP|DP -policy *policy_name* -schedule *schedule_name*

   El siguiente comando crea una relación de SnapMirror entre el volumen de origen `srcvolA` encendido `SVM1` y el volumen de destino `dstvolB` encendido `SVM2`, y asigna la directiva `SVM1-mirror` y el programa `weekendcron`:

   ```
   SVM2::> snapmirror create -source-path SVM1:srcvolA -destination
   -path SVM2:dstvolB -type XDP -policy SVM1-mirror -schedule
   weekendcron
   ```

   > El tipo XDP está disponible en ONTAP 9.5 y posterior. Debe usar el tipo de DP en ONTAP 9.4 y versiones anteriores.

7. En la SVM de destino, inicialice la relación de SnapMirror:

   snapmirror initialize -destination-path *destination_path*

   El proceso de inicialización realiza una *transferencia basal* al volumen de destino. SnapMirror realiza una copia Snapshot del volumen de origen y, a continuación, transfiere la copia y todos los bloques de datos que hace referencia al volumen de destino. También transfiere cualquier otra copia Snapshot del volumen de origen al volumen de destino.

El siguiente comando inicializa la relación entre el volumen de origen `srcvolA` encendido `SVM1` y el volumen de destino `dstvolB` encendido `SVM2`:

```
SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
```

Información relacionada

"Relaciones entre iguales de clústeres y SVM"

"Preparación para la recuperación ante desastres de volúmenes"

"Protección de datos"

Conserve los archivos WORM durante su litigio gracias a su conservación legal

A partir de ONTAP 9.3, puede conservar archivos WORM en modo de cumplimiento durante un litigio con la función *Legal Hold*.

Lo que necesitará

- Debe ser un administrador de SnapLock para realizar esta tarea.

  "Cree una cuenta de administrador de SnapLock"

- Debe haber iniciado sesión en una conexión segura (SSH, Console o ZAPI).

Acerca de esta tarea

Un archivo de retención legal se comporta como un archivo WORM con un período de retención indefinido. Es su responsabilidad especificar cuándo termina el período de retención legal.

El número de archivos que se pueden colocar en una conservación legal depende del espacio disponible en el volumen.

Pasos

1. Inicie una conservación legal:

   `snaplock legal-hold begin -litigation-name` *`litigation_name`* `-volume` *`volume_name`* `-path` *`path_name`*

   El siguiente comando inicia una retención legal para todos los archivos de `vol1`:

   ```
   cluster1::>snaplock legal-hold begin -litigation-name litigation1
   -volume vol1 -path /
   ```

2. Terminar una conservación legal:

   `snaplock legal-hold end -litigation-name` *`litigation_name`* `-volume` *`volume_name`* `-path` *`path_name`*

   El siguiente comando finaliza una retención legal para todos los archivos de `vol1`:

```
cluster1::>snaplock legal-hold end -litigation-name litigation1 -volume
vol1 -path /
```

Información general acerca de Delete WORM files

Puede eliminar archivos WORM en modo de empresa durante el período de retención mediante la función de eliminación con privilegios.
Antes de poder usar esta función, debe crear una cuenta de administrador de SnapLock y, a continuación, utilizar la cuenta, habilitar la función.

Cree una cuenta de administrador de SnapLock

Para realizar una eliminación con privilegios, debe tener privilegios de administrador de SnapLock. Estos privilegios se definen en el rol vsadmin-snaplock. Si todavía no ha asignado ese rol, puede solicitar al administrador de clúster que cree una cuenta de administrador de SVM con el rol de administrador de SnapLock.

Lo que necesitará

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Debe haber iniciado sesión en una conexión segura (SSH, Console o ZAPI).

Pasos

1. Cree una cuenta de administrador de SVM con el rol de administrador de SnapLock:

   security login create -vserver *SVM_name* -user-or-group-name *user_or_group_name* -application *application* -authmethod *authentication_method* -role *role* -comment *comment*

   El siguiente comando habilita la cuenta de administrador de SVM `SnapLockAdmin` con los predefinidos `vsadmin-snaplock` función a la que acceder `SVM1` con una contraseña:

   ```
   cluster1::> security login create -vserver SVM1 -user-or-group-name
   SnapLockAdmin -application ssh -authmethod password -role vsadmin-
   snaplock
   ```

Active la función de eliminación con privilegios

Debe habilitar explícitamente la función de eliminación con privilegios en el volumen de Enterprise que contiene los archivos WORM que desea eliminar.

Acerca de esta tarea

El valor de `-privileged-delete` la opción determina si la eliminación con privilegios está habilitada. Los valores posibles son `enabled`, `disabled`, y. `permanently-disabled`.

`permanently-disabled` es el estado del terminal. No se puede habilitar la eliminación con privilegios en el volumen después de establecer el estado en `permanently-disabled`.

Pasos

1. Habilitar la eliminación con privilegios para un volumen de SnapLock Enterprise:

   volume snaplock modify -vserver *SVM_name* -volume *volume_name* -privileged -delete disabled|enabled|permanently-disabled

   El siguiente comando habilita la función de eliminación con privilegios para el volumen de empresa `dataVol` encendido `SVM1`:

   ```
   SVM1::> volume snaplock modify -vserver SVM1 -volume dataVol -privileged
   -delete enabled
   ```

Elimine los archivos WORM de modo empresarial

Puede utilizar la función de eliminación con privilegios para eliminar archivos WORM en modo de empresa durante el período de retención.

Lo que necesitará

- Debe ser un administrador de SnapLock para realizar esta tarea.
- Debe haber creado un registro de auditoría de SnapLock y habilitado la función de eliminación privilegiada en el volumen empresarial.

Acerca de esta tarea

No puede utilizar una operación de eliminación privilegiada para eliminar un archivo WORM caducado. Puede utilizar el `volume file retention show` Comando para ver el tiempo de retención del archivo WORM que desea eliminar. Para obtener más información, consulte la página man del comando.

Paso

1. Eliminar un archivo WORM en un volumen empresarial:

   volume file privileged-delete -vserver *SVM_name* -file *file_path*

   El siguiente comando elimina el archivo `/vol/dataVol/f1` En la SVM`SVM1`:

   ```
   SVM1::> volume file privileged-delete -file /vol/dataVol/f1
   ```

Mover un volumen de SnapLock

A partir de ONTAP 9.8, puede mover un volumen SnapLock a un agregado de destino del mismo tipo, ya sea de empresa a empresa o de cumplimiento de normativas. Debe

tener asignado el rol de seguridad SnapLock para mover un volumen de SnapLock.

Cree una cuenta de administrador de seguridad de SnapLock

Debe tener privilegios de administrador de seguridad de SnapLock para realizar un movimiento de volúmenes de SnapLock. Este privilegio se le concede con el rol *SnapLock*, introducido en ONTAP 9.8. Si todavía no ha recibido ese rol, puede solicitar al administrador del clúster que cree un usuario de seguridad SnapLock con este rol de seguridad SnapLock.

Lo que necesitará

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Debe haber iniciado sesión en una conexión segura (SSH, Console o ZAPI).

Acerca de esta tarea

El rol SnapLock se asocia con la SVM de administrador, a diferencia del rol vsadmin-snaplock, que está asociada con la SVM de datos.

Paso

1. Cree una cuenta de administrador de SVM con el rol de administrador de SnapLock:

   security login create -vserver *SVM_name* -user-or-group-name *user_or_group_name* -application *application* -authmethod *authentication_method* -role *role* -comment *comment*

   El siguiente comando habilita la cuenta de administrador de SVM `SnapLockAdmin` con los predefinidos `snaplock` Rol para acceder a la SVM de administrador `cluster1` con una contraseña:

   ```
   cluster1::> security login create -vserver cluster1 -user-or-group-name
   SnapLockAdmin -application ssh -authmethod password -role snaplock
   ```

Mover un volumen de SnapLock

Puede utilizar el `volume move` Comando para mover un volumen de SnapLock a un agregado de destino.

Lo que necesitará

- Debe haber creado un registro de auditoría protegido en SnapLock antes de ejecutar el movimiento de volúmenes de SnapLock.

  "Cree un registro de auditoría".

- Si utiliza una versión de ONTAP anterior a ONTAP 9.10.1, el agregado de destino debe ser el mismo tipo de SnapLock que el volumen de SnapLock que desea mover: Compliance to Compliance o Enterprise to Enterprise. A partir de ONTAP 9.10.1, esta restricción se elimina y un agregado puede incluir volúmenes SnapLock de Compliance y Enterprise, así como volúmenes que no son de SnapLock.
- Debe haberse registrado como usuario con el rol de seguridad SnapLock.

Pasos

1. Con una conexión segura, inicie sesión en la LIF de gestión de clústeres de ONTAP:

   ssh snaplock_user@cluster_mgmt_ip

2. Mover un volumen de SnapLock:

   volume move start -vserver *SVM_name* -volume *SnapLock_volume_name* -destination -aggregate *destination_aggregate_name*

3. Compruebe el estado de la operación de movimiento de volúmenes:

   volume move show -volume *SnapLock_volume_name* -vserver *SVM_name* -fields volume,phase,vserver

Bloquee una copia Snapshot para obtener protección contra ataques de ransomware

A partir de ONTAP 9.12.1, puede bloquear una copia Snapshot en un volumen que no sea de SnapLock para proporcionar protección contra ataques de ransomware. El bloqueo de las copias Snapshot garantiza que no se puedan eliminar accidental o con malas intenciones.

La función de reloj de cumplimiento de normativas de SnapLock le permite bloquear las copias Snapshot durante un período determinado para que no se puedan eliminar hasta que llegue el momento de caducidad. Bloquear copias Snapshot las protege a prueba de manipulaciones e impedir las amenazas de ransomware. Puede usar copias Snapshot bloqueadas para recuperar los datos si un volumen se ve afectado por un ataque de ransomware.

A partir de ONTAP 9.14.1, el bloqueo de copias Snapshot admite copias Snapshot de retención a largo plazo en destinos de almacenes SnapLock y en volúmenes de destino que no sean de SnapMirror de SnapLock. El bloqueo de copia de Snapshot se habilita configurando el período de retención mediante las reglas de políticas de SnapMirror asociadas a un etiqueta de política existente. La regla anula el período de retención predeterminado establecido en el volumen. Si no existe un período de retención asociado con la etiqueta de SnapMirror, se utiliza el período de retención predeterminado del volumen.

Requisitos y consideraciones sobre copias Snapshot a prueba de manipulaciones

- Si utiliza la CLI de ONTAP, todos los nodos del clúster deben ejecutar ONTAP 9.12.1 o una versión posterior. Si utiliza System Manager, todos los nodos deben ejecutar ONTAP 9.13.1 o una versión posterior.
- "La licencia de SnapLock debe instalarse en el clúster". Esta licencia está incluida en "ONTAP One".
- "Es necesario inicializar el reloj de cumplimiento de normativas del clúster".
- Cuando se habilita el bloqueo de snapshots en un volumen, es posible actualizar los clústeres a una versión de ONTAP posterior a ONTAP 9.12.1; Sin embargo, no puede revertir a una versión anterior de ONTAP hasta que todas las copias snapshot bloqueadas hayan alcanzado su fecha de caducidad y se eliminen, y el bloqueo de la copia snapshot se ha deshabilitado.
- Cuando se bloquea una instantánea, el tiempo de caducidad del volumen se establece en el tiempo de caducidad de la copia snapshot. Si más de una copia Snapshot está bloqueada, el tiempo de caducidad del volumen refleja el mayor tiempo de caducidad de todas las copias Snapshot.
- El período de retención para las copias Snapshot bloqueadas tiene prioridad sobre el número de copias de Snapshot conservadas; esto significa que no se respeta el límite de conservación de recuento si no ha caducado el período de retención de copia de Snapshot para copias Snapshot bloqueadas.
- En una relación de SnapMirror, puede establecer un período de retención en una regla de política de reflejo-almacén y el período de retención se aplica a las copias Snapshot replicadas en el destino si el volumen de destino tiene la función de bloqueo de copias Snapshot habilitada. El período de retención

tiene prioridad sobre el recuento de retenciones; por ejemplo, las copias Snapshot que no hayan sobrepasado su vencimiento se retendrán aunque se supere el recuento de retenciones.

- Puede cambiar el nombre de una copia Snapshot en un volumen que no sea de SnapLock. Las operaciones de cambio de nombre de Snapshot en el volumen primario de una relación de SnapMirror se reflejan en el volumen secundario solo si la política es MirrorAllSnapshots. Para otros tipos de políticas, la copia Snapshot cuyo nombre se ha cambiado no se propaga durante las actualizaciones.
- Si utiliza la CLI de ONTAP, puede restaurar una copia Snapshot bloqueada con el `volume snapshot restore` Comando solo si la copia snapshot bloqueada es la más reciente. Si hay alguna copia Snapshot sin expirar más adelante que la que se va a restaurar, se produce un error en la operación de restauración de la copia de Snapshot.

Funciones compatibles con copias Snapshot a prueba de manipulaciones

- Volúmenes de FlexGroup

  Los volúmenes de FlexGroup admiten el bloqueo de copias Snapshot. El bloqueo de instantáneas solo se realiza en la copia snapshot que forma parte del componente raíz. Solo se permite eliminar el volumen FlexGroup si ha transcurrido el tiempo de caducidad del componente raíz.

- Conversión de FlexVol a FlexGroup

  Puede convertir un volumen FlexVol con copias snapshot bloqueadas en un volumen FlexGroup. Las copias snapshot permanecen bloqueadas después de la conversión.

- Clon de volumen y clon de archivo

  Es posible crear clones de volúmenes y clones de archivos a partir de una copia Snapshot bloqueada.

Funciones no admitidas

En la actualidad, las siguientes funciones no son compatibles con las copias Snapshot a prueba de manipulaciones:

- Cloud Volumes ONTAP
- Grupos de consistencia
- FabricPool
- Volúmenes de FlexCache
- SMTape
- Continuidad del negocio de SnapMirror (SM-BC)
- Reglas de política de SnapMirror mediante el `-schedule` parámetro
- SnapMirror síncrono
- Movilidad de datos de SVM (se usa para migrar o reubicar una SVM desde un clúster de origen a un clúster de destino)

Habilite el bloqueo de las copias snapshot al crear un volumen

A partir de ONTAP 9.12.1, se puede habilitar el bloqueo de copias snapshot cuando se crea un volumen nuevo o se modifica un volumen existente mediante el `-snapshot-locking-enabled` con la `volume create` y.. `volume modify` Comandos de la CLI. A partir de ONTAP 9.13.1, puede usar System Manager para habilitar el bloqueo de copias de SnapVault.

System Manager

1. Navegue hasta **Almacenamiento > Volúmenes** y seleccione **Agregar**.
2. En la ventana **Añadir volumen**, selecciona **Más opciones**.
3. Introduzca el nombre del volumen, el tamaño, la política de exportación y el nombre del recurso compartido.
4. Selecciona **Habilitar Bloqueo de instantáneas**. Esta selección no se muestra si la licencia de SnapLock no está instalada.
5. Si aún no está habilitado, selecciona **Inicializar reloj de cumplimiento de SnapLock**.
6. Guarde los cambios.
7. En la ventana **Volúmenes**, selecciona el volumen que actualizaste y selecciona **Resumen**.
8. Verifique que **SnapLock Bloqueo de copia instantánea** se muestre como **habilitado**.

CLI

1. Para crear un nuevo volumen y habilitar el bloqueo de copias Snapshot, introduzca el siguiente comando:

   ```
   volume create -vserver vserver_name -volume volume_name -snapshot-locking
   -enabled true
   ```

   El siguiente comando habilita el bloqueo de copias Snapshot en un nuevo volumen denominado vol1:

   ```
   > volume create -volume vol1 -aggregate aggr1 -size 100m -snapshot
   -locking-enabled true
   Warning: Snapshot copy locking is being enabled on volume “vol1” in
   Vserver “vs1”. It cannot be disabled until all locked Snapshot
   copies are past their expiry time. A volume with unexpired locked
   Snapshot copies cannot be deleted.
   Do you want to continue: {yes|no}: y
   [Job 32] Job succeeded: Successful
   ```

Habilite el bloqueo de copias snapshot en un volumen existente

A partir de ONTAP 9.12.1, puede habilitar el bloqueo de copia de snapshot en un volumen existente mediante la interfaz de línea de comandos de ONTAP. A partir de ONTAP 9.13.1, puede usar System Manager para habilitar el bloqueo de copias de Snapshot en un volumen existente.

System Manager

1. Vaya a **almacenamiento > volúmenes**.
2. Seleccione ⋮ Y elija **Editar > Volumen**.
3. En la ventana **Editar volumen**, localice la sección Configuración de copias snapshot (locales) y seleccione **Habilitar bloqueo de instantáneas**.

   Esta selección no se muestra si la licencia de SnapLock no está instalada.

4. Si aún no está habilitado, selecciona **Inicializar reloj de cumplimiento de SnapLock**.
5. Guarde los cambios.
6. En la ventana **Volúmenes**, selecciona el volumen que actualizaste y selecciona **Resumen**.
7. Verifique que **SnapLock Bloqueo de copia instantánea** se muestre como **habilitado**.

CLI

1. Para modificar un volumen existente para habilitar el bloqueo de copias Snapshot, introduzca el siguiente comando:

   ```
   volume modify -vserver vserver_name -volume volume_name -snapshot-locking
   -enabled true
   ```

Cree una política de copia de Snapshot bloqueada y aplique retención

A partir de ONTAP 9.12.1, puede crear políticas de copias de Snapshot para aplicar un período de retención de copias de Snapshot y aplicar la política a un volumen para bloquear las copias de Snapshot durante el período especificado. También puede bloquear una copia Snapshot mediante la configuración manual de un período de retención. A partir de ONTAP 9.13.1, puede usar System Manager para crear políticas de bloqueo de copias de Snapshot y aplicarlas a un volumen.

Cree una política de bloqueo de copias snapshot

System Manager

1. Vaya a **Storage > Storage VMs** y seleccione una VM de almacenamiento.
2. Selecciona **Ajustes**.
3. Localice **Políticas de instantánea** y seleccione →.
4. En la ventana **Add Snapshot Policy**, introduzca el nombre de la política.
5. Seleccione + Add .
6. Proporcione los detalles de la programación de la copia de Snapshot, incluido el nombre de la programación, el número máximo de copias de Snapshot que se deben conservar y el período de retención de SnapLock.
7. En la columna **SnapLock Retention Period**, introduzca el número de horas, días, meses o años que se van a conservar las copias snapshot. Por ejemplo, una política de copia de Snapshot con un período de retención de 5 días bloquea una copia de Snapshot por 5 días desde el momento en que se creó y no puede eliminarse durante ese período. Se admiten los siguientes rangos de períodos de retención:
   - Años: 0 - 100
   - Meses: 0 - 1200
   - Días: 0 - 36500
   - Horario: 0 - 24
8. Guarde los cambios.

CLI

1. Para crear una política de copias Snapshot, introduzca el siguiente comando:

   `volume snapshot policy create -policy policy_name -enabled true -schedule1 schedule1_name -count1 maximum_Snapshot_copies -retention-period1 _retention_period`

   El siguiente comando crea una política de bloqueo de copias de Snapshot:

   ```
   cluster1> volume snapshot policy create -policy policy_name -enabled
   true -schedule1 hourly -count1 24 -retention-period1 "1 days"
   ```

   No se reemplaza una copia Snapshot si se encuentra sujeta a una retención activa; es decir, el número de retención no se respetará si hay copias Snapshot bloqueadas que aún no han caducado.

Aplicar una política de bloqueo a un volumen

System Manager

1. Vaya a **almacenamiento > volúmenes**.
2. Seleccione ⋮ Y elija **Editar > Volumen**.
3. En la ventana **Editar volumen**, selecciona **Programar copias snapshot**.
4. Seleccione la política de copias de Snapshot bloqueadas de la lista.
5. Si el bloqueo de copias snapshot no está activado, selecciona **Activar bloqueo de instantáneas**.
6. Guarde los cambios.

CLI

1. Para aplicar una política de bloqueo de copias Snapshot a un volumen existente, introduzca el siguiente comando:

   ```
   volume modify -volume volume_name -vserver vserver_name -snapshot-policy
   policy_name
   ```

Aplicación del período de retención durante la creación manual de las copias de Snapshot

Es posible aplicar un período de retención de copia Snapshot cuando se crea manualmente una copia Snapshot. Debe habilitarse el bloqueo de copia de snapshot en el volumen; de lo contrario, se ignorará la configuración del período de retención.

System Manager

1. Navegue hasta **Almacenamiento > Volúmenes** y seleccione un volumen.
2. En la página de detalles del volumen, seleccione la pestaña **Copias de instantánea**.
3. Seleccione + Add .
4. Introduzca el nombre de la copia Snapshot y la hora de caducidad de SnapLock. Puede seleccionar el calendario para elegir la fecha y la hora de caducidad de la retención.
5. Guarde los cambios.
6. En la página **Volúmenes > Copias de instantáneas**, seleccione **Mostrar/Ocultar** y elija **Tiempo de caducidad de SnapLock** para mostrar la columna **Tiempo de caducidad de SnapLock** y verifique que el tiempo de retención esté establecido.

CLI

1. Para crear una copia Snapshot manualmente y aplicar un período de retención de bloqueo, introduzca el siguiente comando:

   `volume snapshot create -volume` *`volume_name`* `-snapshot` *`snapshot_copy_name`* `-snaplock-expiry-time` *`expiration_date_time`*

   El siguiente comando crea una nueva copia Snapshot y establece el período de retención:

   ```
   cluster1> volume snapshot create -vserver vs1 -volume vol1 -snapshot
   snap1 -snaplock-expiry-time "11/10/2022 09:00:00"
   ```

Aplique el período de retención a una copia Snapshot existente

System Manager

1. Navegue hasta **Almacenamiento > Volúmenes** y seleccione un volumen.
2. En la página de detalles del volumen, seleccione la pestaña **Copias de instantánea**.
3. Seleccione la copia Snapshot y seleccione ⋮, Y elija **Modificar tiempo de caducidad de SnapLock**. Puede seleccionar el calendario para elegir la fecha y la hora de caducidad de la retención.
4. Guarde los cambios.
5. En la página **Volúmenes > Copias de instantáneas**, seleccione **Mostrar/Ocultar** y elija **Tiempo de caducidad de SnapLock** para mostrar la columna **Tiempo de caducidad de SnapLock** y verifique que el tiempo de retención esté establecido.

CLI

1. Para aplicar manualmente un período de retención a una copia Snapshot existente, introduzca el siguiente comando:

   `volume snapshot modify-snaplock-expiry-time -volume` *`volume_name`* `-snapshot` *`snapshot_copy_name`* `-expiry-time` *`expiration_date_time`*

   En el siguiente ejemplo se aplica un período de retención a una copia Snapshot existente:

   ```
   cluster1> volume snapshot modify-snaplock-expiry-time -volume vol1
   -snapshot snap2 -expiry-time "11/10/2022 09:00:00"
   ```

Modifique una política existente para aplicar la retención a largo plazo

A partir de ONTAP 9.14.1, puede modificar una política de SnapMirror existente añadiendo una regla para establecer una retención a largo plazo de copias Snapshot. La regla se utiliza para anular el período de retención de volúmenes predeterminado en destinos de almacén de SnapLock y en volúmenes de destino que no son de SnapMirror de SnapLock.

1. Agregue una regla a una política de SnapMirror existente:

   ```
   snapmirror policy add-rule -vserver <SVM name> -policy <policy name>
   -snapmirror-label <label name> -keep <number of Snapshot copies> -retention
   -period [<integer> days|months|years]
   ```

   En el siguiente ejemplo se crea una regla que aplica un período de retención de 6 meses a la política existente denominada «lockvault»:

   ```
   snapmirror policy add-rule -vserver vs1 -policy lockvault -snapmirror
   -label test1 -keep 10 -retention-period "6 months"
   ```

API de SnapLock

Puede utilizar las API de Zephyr para integrar la funcionalidad de SnapLock en scripts o automatización de flujos de trabajo. Las API utilizan mensajería XML a través de HTTP,

HTTPS y DCE/RPC de Windows. Para obtener más información, consulte "Documentación de automatización de ONTAP".

archivo-huella-abortar

Anular una operación de huellas digitales de archivo.

volcado de huellas digitales de archivo

Mostrar información de huellas digitales del archivo.

file-fingerprint-get-iter

Muestra el estado de las operaciones de huella digital de archivos.

inicio de la huella digital de archivo

Genere una huella digital de archivo.

snaplock-archive-vserver-log

Archive el archivo de registro de auditoría activo.

snaplock-create-vserver-log

Cree una configuración de registro de auditoría para una SVM.

snaplock-delete-vserver-log

Eliminar una configuración de registro de auditoría para una SVM.

snaplock-file-privileged-delete

Ejecute una operación de eliminación privilegiada.

snaplock-get-file-retention

Obtenga el período de retención de un archivo.

snaplock-get-node-compliance-clock

Obtenga la fecha y la hora de la instancia de ComplianceClock del nodo.

snaplock-get-vserver-activo-log-files-iter

Mostrar el estado de los archivos de registro activos.

snaplock-get-vserver-log-iter

Muestre la configuración del registro de auditoría.

snaplock-modify-vserver-log

Modifique la configuración del registro de auditoría para una SVM.

retención de conjuntos de archivos de snaplock

Establezca el tiempo de retención de un archivo.

snaplock-set-node-compliance-clock

Establezca la fecha y la hora de la instancia de ComplianceClock del nodo.

snaplock-volume-set-privileged-delete

Establezca la opción Privileged-delete en un volumen SnapLock Enterprise.

volume-get-snaplock-attrs

Obtenga los atributos de un volumen de SnapLock.

volume-set-snaplock-attrs

Configure los atributos de un volumen SnapLock.

Grupos de consistencia

Información general sobre los grupos de consistencia

Un grupo de coherencia es una recogida de volúmenes que se gestionan como una sola unidad. En ONTAP, los grupos de coherencia proporcionan una gestión fácil y una garantía de protección para una carga de trabajo de la aplicación que abarca varios volúmenes.

Puede utilizar grupos de consistencia para simplificar la gestión del almacenamiento. Imagine que dispone de una base de datos importante que abarca veinte LUN. Puede administrar las LUN de forma individual o tratar las LUN como un conjunto de datos solitario, organizándolas en un único grupo de consistencia.

Los grupos de coherencia facilitan la gestión de cargas de trabajo de aplicaciones, proporcionando políticas de protección local y remota fáciles de configurar, y copias de Snapshot simultáneas consistentes con las aplicaciones y con los fallos de una colección de volúmenes en un momento específico. Las copias Snapshot de un grupo de coherencia permiten restaurar una carga de trabajo de la aplicación completa.

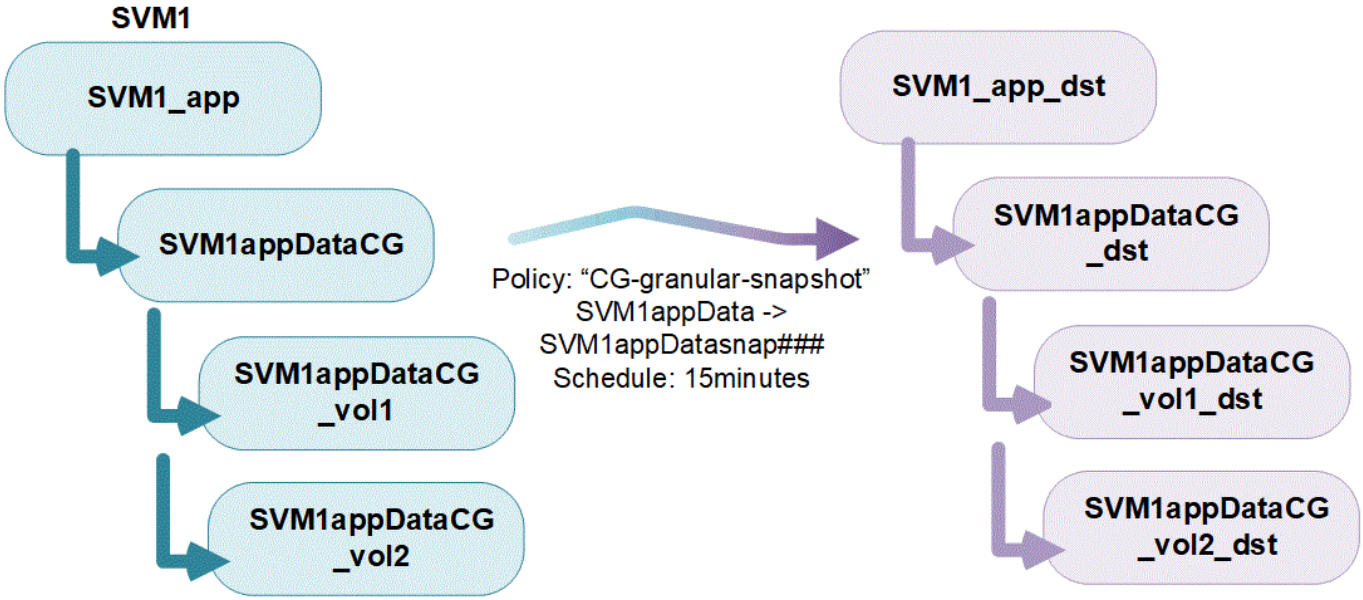
Obtenga más información sobre los grupos de consistencia

Los grupos de consistencia admiten cualquier volumen de FlexVol independientemente del protocolo (NAS, SAN o NVMe) y pueden gestionarse a través de la API REST de ONTAP o en System Manager, en el elemento de menú **almacenamiento > grupos de consistencia**. A partir de ONTAP 9.14.1, los grupos de consistencia se pueden administrar con la CLI de ONTAP.

Los grupos de consistencia pueden existir como entidades individuales (como una colección de volúmenes) o en una relación jerárquica, que consiste en otros grupos de consistencia. Los volúmenes individuales pueden tener su propia política de copias Snapshot granulares de volúmenes. Además, puede haber una política de Snapshot para todo el grupo de consistencia. El grupo de consistencia solo puede tener una relación de

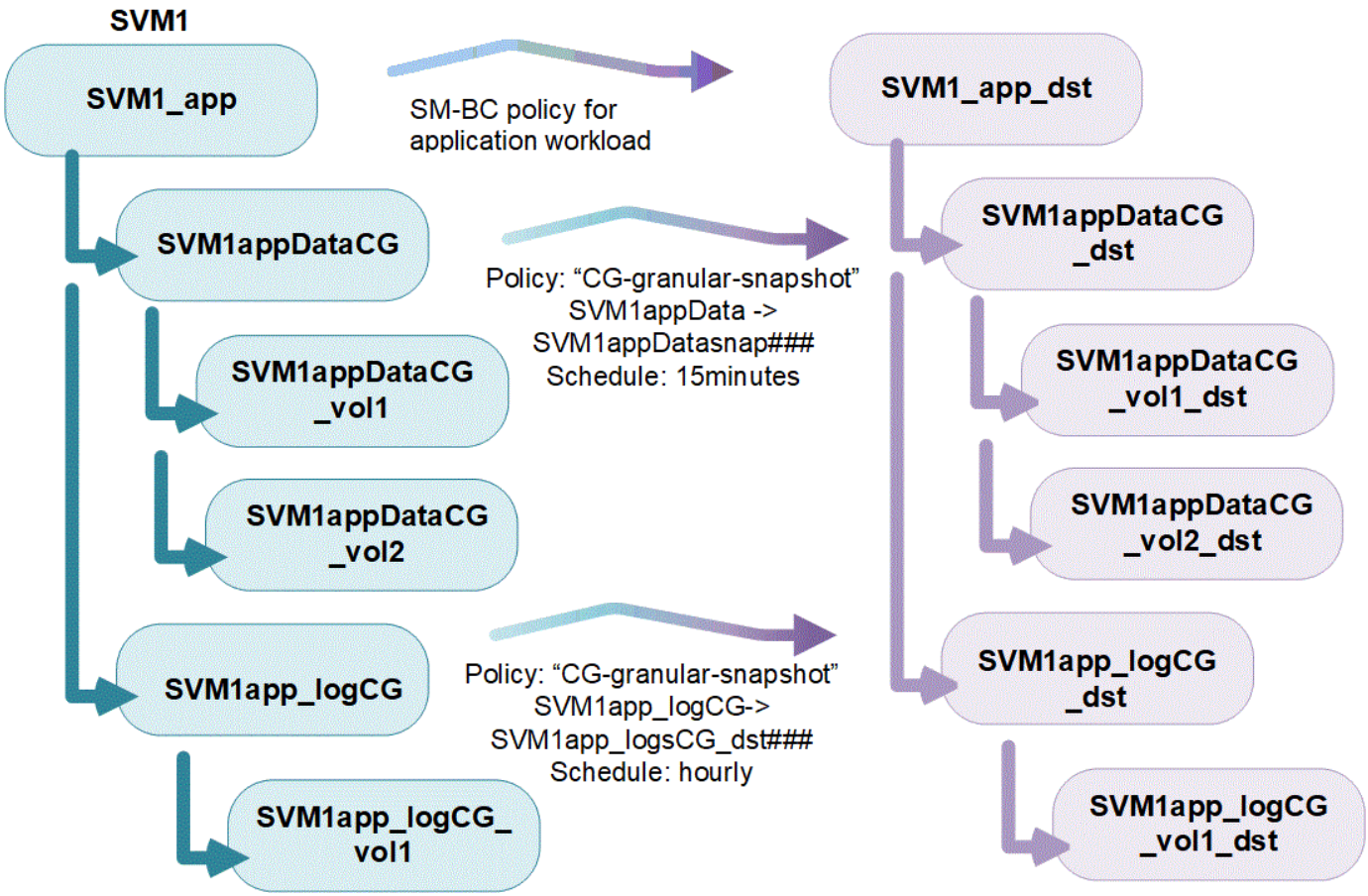
continuidad del negocio de SnapMirror (SM-BC) y una política de SM-BC compartida, que puede utilizarse para recuperar todo el grupo de consistencia.

En el siguiente diagrama se muestra cómo se puede utilizar un grupo de consistencia individual. Los datos de una aplicación alojada en `SVM1` abarca dos volúmenes: `vol1` y.. `vol2`. Una política de Snapshot en el grupo de consistencia captura copias Snapshot de los datos cada 15 minutos.



Las cargas de trabajo de aplicaciones más grandes pueden requerir varios grupos de coherencia. En estas situaciones, puede crear grupos de consistencia jerárquicos, donde un solo grupo de consistencia se convierte en componentes secundarios de un grupo de coherencia primario. El grupo de consistencia primario puede incluir hasta cinco grupos de consistencia secundarios. Al igual que en grupos de consistencia individuales, se puede aplicar una política de protección de SM-BC remota a toda la configuración de los grupos de consistencia (principal y secundario) para recuperar la carga de trabajo de la aplicación.

En el siguiente ejemplo, una aplicación se aloja en `SVM1`. El administrador ha creado un grupo de consistencia primario, `SVM1_app`, que incluye dos grupos de consistencia secundarios: `SVM1appDataCG` para los datos y. `SVM1app_logCG` para los registros. Cada grupo de consistencia secundario tiene su propia política de Snapshot. Copias Snapshot de los volúmenes en `SVM1appDataCG` se toman cada 15 minutos. Copias Snapshot de `SVM1app_logCG` se toman cada hora. El grupo de consistencia primario `SVM1_app` Tiene una política de SM-BC que replica los datos para garantizar un servicio continuado en caso de desastre.



A partir de ONTAP 9.12.1, admiten los grupos de consistencia clonado y modificar los miembros de la consistencia por agregar o quitar volúmenes Tanto en System Manager como en la API DE REST de ONTAP. A partir de ONTAP 9.12.1, la API de REST DE ONTAP también admite:

- Creación de grupos de coherencia con volúmenes NFS o SMB o espacios de nombres NVMe nuevos.
- Añadir volúmenes NFS o SMB o espacios de nombres NVMe nuevos o existentes a grupos de coherencia existentes.

Para obtener más información sobre la API de REST de ONTAP, consulte "Documentación de referencia de la API DE REST de ONTAP".

Supervisar grupos de consistencia

A partir de ONTAP 9.13.1, los grupos de consistencia ofrecen supervisión de capacidad y rendimiento en tiempo real e históricos, lo que proporciona información sobre el rendimiento de aplicaciones y grupos de coherencia individuales.

Los datos de supervisión se actualizan cada cinco minutos y se mantienen hasta un año. Puede realizar un seguimiento de las métricas para:

- Rendimiento: IOPS, latencia y rendimiento
- Capacidad: Tamaño, lógico utilizado, disponible

Puede ver los datos de supervisión en la pestaña **Información general** del menú del grupo de consistencia de System Manager o solicitándolos en la API DE REST. A partir de ONTAP 9.14.1, puede ver las métricas del grupo de consistencia con la CLI mediante el `consistency-group metrics show` comando.

En ONTAP 9.13.1, solo puede recuperar métricas históricas mediante la API de REST. A partir de ONTAP 9.14.1, las métricas históricas también están disponibles en System Manager.

Proteger los grupos de consistencia

Los grupos de consistencia ofrecen protección mediante:

- Políticas de Snapshot
- Continuidad del negocio de SnapMirror (SM-BC)
- [mcc] (A partir de ONTAP 9.11.1)
- SnapMirror asíncrono (A partir de ONTAP 9.13.1)
- "Recuperación ante desastres de SVM" (A partir de ONTAP 9.14.1)

La creación de un grupo de consistencia no habilita la protección automáticamente. Las políticas de protección local y remota se pueden establecer al crear o después de crear un grupo de coherencia.

Para configurar la protección en un grupo de consistencia, consulte "Proteja un grupo de consistencia".

Para poder utilizar la protección remota, debe cumplir los requisitos de Puestas en marcha de continuidad del negocio con SnapMirror.

No se pueden establecer relaciones de SM-BC en volúmenes montados para el acceso NAS.

Grupos de consistencia en configuraciones de MetroCluster

A partir de ONTAP 9.11.1, puede aprovisionar grupos de consistencia con nuevos volúmenes en un clúster dentro de una configuración de MetroCluster. Estos volúmenes se aprovisionan en agregados reflejados.

Después de que se hayan aprovisionado, puede mover los volúmenes asociados con grupos de coherencia entre los agregados reflejados y no reflejados. Por lo tanto, los volúmenes asociados con grupos de coherencia pueden ubicarse en agregados reflejados, agregados no reflejados o en ambos. Es posible modificar los agregados reflejados que contienen volúmenes asociados con grupos de coherencia para que no se reflejen. De igual manera, se pueden modificar los agregados no reflejados que contienen volúmenes asociados con grupos de coherencia para habilitar el mirroring.

Los volúmenes y las copias Snapshot asociados con grupos de consistencia ubicados en agregados reflejados se replican en el sitio remoto (sitio B). El contenido de los volúmenes del sitio B ofrece una garantía de escritura para el grupo de coherencia, lo que le permite recuperar desde el sitio B en caso de desastre. Puede acceder a copias de Snapshot de los grupos de consistencia mediante un grupo de consistencia con la API de REST y System Manager en los clústeres que ejecutan ONTAP 9.11.1 o una versión posterior. A partir de ONTAP 9.14.1, también puede acceder a las copias Snapshot con la CLI de ONTAP.

Si algunos o todos los volúmenes asociados con un grupo de consistencia se encuentran en agregados no reflejados a los que no se puede acceder actualmente, las operaciones GET o DELETE en el grupo de coherencia se comportan como si los volúmenes locales o los agregados de alojamiento están sin conexión.

Configuraciones del grupo de consistencia para la replicación

Si el sitio B ejecuta ONTAP 9.10.1 o una versión anterior, solo se replican los volúmenes asociados con los grupos de coherencia ubicados en agregados reflejados al sitio B. Las configuraciones del grupo de consistencia solo se replican en el sitio B, si ambos sitios ejecutan ONTAP 9.11.1 o una versión posterior. Una vez que el sitio B se actualiza a ONTAP 9.11.1, los datos de los grupos de consistencia del sitio A que tienen

todos los volúmenes asociados ubicados en agregados reflejados se replican en el sitio B.

> Se recomienda mantener al menos un 20% de espacio libre para agregados reflejados para lograr un rendimiento y una disponibilidad de almacenamiento óptimos. Aunque la recomendación es del 10% para agregados no duplicados, el sistema de archivos puede utilizar el 10% adicional del espacio para absorber cambios incrementales. Los cambios incrementales aumentan el aprovechamiento del espacio para agregados reflejados gracias a la arquitectura basada en Snapshot de copia en escritura de ONTAP. Si no se siguen estas mejores prácticas, puede tener un impacto negativo en el rendimiento.

Consideraciones de renovación

Los grupos de coherencia creados con SM-BC en ONTAP 9,8 y 9.9.1 se actualizarán automáticamente y se podrán gestionar en **Almacenamiento > Grupos de consistencia** en System Manager o la API REST DE ONTAP cuando se actualice a ONTAP 9.10.1 o una versión posterior. Para obtener más información sobre la actualización desde ONTAP 9,8 o 9,9.1, consulte "Consideraciones sobre la actualización y reversión de SM-BC".

Las copias de Snapshot de grupo de consistencia creadas en la API de REST pueden gestionarse a través de la interfaz del grupo de consistencia de System Manager y mediante extremos de la API de REST del grupo de consistencia. A partir de ONTAP 9.14.1, las copias Snapshot de grupo de consistencia también se pueden gestionar con la CLI de ONTAP.

> Copias Snapshot creadas con los comandos ONTAPI `cg-start` y.. `cg-commit` Se reconocen como las copias Snapshot de grupo de consistencia y, por lo tanto, no se pueden gestionar a través de la interfaz del grupo de consistencia de System Manager ni los extremos del grupo de consistencia en la API DE REST DE ONTAP. A partir de ONTAP 9.14.1, estas copias Snapshot se pueden reflejar en el volumen de destino si utiliza una política de SnapMirror asíncrono. Para obtener más información, consulte Configurar la protección asíncrona de SnapMirror.

Funciones compatibles por versión

	ONTAP 9.14.1	**ONTAP 9.13.1**	**ONTAP 9.12.1**	**ONTAP 9.11.1**	**ONTAP 9.10.1**
Grupos de consistencia jerárquicos	✓	✓	✓	✓	✓
Protección local con copias Snapshot	✓	✓	✓	✓	✓
Continuidad del negocio de SnapMirror	✓	✓	✓	✓	✓
Soporte de MetroCluster	✓	✓	✓	✓	
Confirmaciones bifásicas (solo API de REST)	✓	✓	✓	✓	
Etiquetas de aplicaciones y componentes	✓	✓	✓		
Clonar grupos de consistencia	✓	✓	✓		
Añadir y quitar volúmenes	✓	✓	✓		
Cree CG con los nuevos volúmenes NAS	✓	✓	Solo API DE REST		

	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
Crear CG con nuevos espacios de nombres NVMe	✓	✓	Solo API DE REST		
Mueva volúmenes entre grupos de coherencia secundarios	✓	✓			
Modificar la geometría del grupo de consistencia	✓	✓			
Supervisión	✓	✓			
SnapMirror asíncrono (solo grupos de consistencia individuales)	✓	✓			
Recuperación ante desastres de SVM (solo grupos de consistencia individuales)	✓				
Compatibilidad con CLI	✓				

Más información sobre los grupos de consistencia

Más información

- "Documentación de automatización de ONTAP"
- Continuidad del negocio de SnapMirror
- Conceptos básicos de la recuperación ante desastres de SnapMirror asíncrono
- "Documentación de MetroCluster"

Límites del grupo de consistencia

Al planificar y administrar los grupos de consistencia, tenga en cuenta los límites de objetos en el ámbito del clúster y del grupo de consistencia primario o secundario.

Límites impuestos

La siguiente tabla captura los límites de los grupos de coherencia. Se aplican límites separados para los grupos de coherencia que utilizan SnapMirror Business Continuity (SM-BC). Para obtener más información, consulte "Restricciones y limitaciones de SM-BC".

Límite	Ámbito	Mínimo	Máximo
Número de grupos de consistencia	Clúster	0	Igual que el número máximo de volúmenes en el clúster
Número de grupos de consistencia primarios	Clúster	0	Igual que el número máximo de volúmenes en el clúster
Número de grupos de consistencia individuales y primarios	Clúster	0	Igual que el número máximo de volúmenes en el clúster
Número de volúmenes en un grupo de consistencia	Grupo de consistencia único	1 tb de volumen	80 volúmenes
El número de volúmenes en el secundario de un grupo de consistencia primario	Grupo de consistencia primario	1 tb de volumen	80 volúmenes
El número de volúmenes en un grupo de coherencia secundario	Grupo de consistencia secundario	1 tb de volumen	80 volúmenes
Número de grupos de consistencia secundarios de un grupo de consistencia primario	Grupo de consistencia primario	1 grupo de consistencia	5 grupos de consistencia
Número de relaciones de recuperación ante desastres de SVM donde existe un grupo de consistencia (disponible a partir de ONTAP 9.14.1).	Clúster	0	32

Límites no aplicados

La programación mínima de copias Snapshot admitida para grupos de consistencia es de 30 minutos. Esta opción está basada en "Prueba para FlexGroups", Que comparten la misma infraestructura Snapshot que los grupos de consistencia.

Configure un único grupo de consistencia

Los grupos de consistencia se pueden crear con volúmenes existentes o con LUN o volúmenes nuevos (según la versión de ONTAP). Un volumen o LUN solo pueden asociarse a un grupo de coherencia a la vez.

Acerca de esta tarea

- No se admite la modificación de los volúmenes miembro de un grupo de coherencia después de su creación en ONTAP 9.10.1 a 9.11.1.

  A partir de ONTAP 9.12.1, es posible modificar los volúmenes miembro de un grupo de coherencia. Para obtener más información sobre este proceso, consulte Modificar un grupo de consistencia.

Cree un grupo de consistencia con nuevas LUN o volúmenes

En ONTAP 9.10.1 a 9.12.1, puede crear un grupo de consistencia utilizando nuevas LUN. A partir de ONTAP 9.13.1, System Manager también admite la creación de un grupo de consistencia con espacios de nombres NVMe nuevos o volúmenes NAS nuevos. (También es compatible con la API REST DE ONTAP a partir de ONTAP 9.12.1).

System Manager

Pasos

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione **+Agregar** y, a continuación, seleccione el protocolo para el objeto de almacenamiento.

   En ONTAP 9.10.1 a 9.12.1, la única opción para un nuevo objeto de almacenamiento es **utilizando nuevas LUN**. A partir de ONTAP 9.13.1, System Manager admite la creación de grupos de consistencia con espacios de nombres NVMe nuevos y volúmenes NAS nuevos.

3. Asigne un nombre al grupo de consistencia. Designe el número de volúmenes o LUN y la capacidad por volumen o LUN.
   a. **Tipo de aplicación**: Si está utilizando ONTAP 9.12.1 o posterior, seleccione un tipo de aplicación. Si no se selecciona ningún valor, se asignará al grupo de consistencia el tipo de **Other** de forma predeterminada. Obtenga más información sobre la coherencia de etiquetado en Etiquetas de aplicaciones y componentes. Si planea crear un grupo de consistencia con una política de protección remota, debe usar **Other**.
   b. Para **Nuevas LUN**: Seleccione el sistema operativo del host y el formato de LUN. Introduzca la información del iniciador del host.
   c. Para **Nuevos volúmenes NAS**: Elija la opción de exportación apropiada (NFS o SMB/CIFS) según la configuración NAS de su SVM.
   d. Para **Nuevos espacios de nombres NVMe**: Seleccione el sistema operativo del host y el subsistema NVMe.
4. Para configurar políticas de protección, agregar un grupo de consistencia secundario o permisos de acceso, seleccione **Más opciones**.
5. Seleccione **Guardar**.
6. Para confirmar que se ha creado el grupo de consistencia, vuelva al menú del grupo de consistencia principal, donde aparecerá una vez que se complete el trabajo. Si establece una política de protección, sabrá que se ha aplicado cuando ve un escudo verde bajo la directiva apropiada, remoto o local.

CLI

A partir de ONTAP 9.14.1, puede crear un grupo de consistencia nuevo con volúmenes nuevos mediante la CLI de ONTAP. Los parámetros específicos dependen de si los volúmenes son SAN, NVMe o NFS.

Crear un grupo de consistencia con volúmenes de NFS

1. Cree el grupo de consistencia:

   ```
   consistency-group create -vserver SVM_name -consistency-group consistency-
   group-name -volume volume-prefix -volume-count number -size size -export
   -policy policy_name
   ```

Crear un grupo de consistencia con volúmenes SAN

1. Cree el grupo de consistencia:

   ```
   consistency-group create -vserver SVM_name -consistency-group consistency-
   group-name -lun lun_name -size size -lun-count number -igroup igroup_name
   ```

Cree un grupo de consistencia con espacios de nombres NVMe

1. Cree el grupo de consistencia:

   ```
   consistency-group create -vserver SVM_name -consistency-group
   consistency_group_name -namespace namespace_name -volume-count number
   -namespace-count number -size size -subsystem subsystem_name
   ```

Después de terminar

1. Confirme que el grupo de consistencia se ha creado mediante el `consistency-group show` comando.

Cree un grupo de coherencia con volúmenes existentes

Es posible utilizar volúmenes existentes para crear un grupo de coherencia.

System Manager

Pasos

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione **+Agregar** y **utilizando volúmenes existentes**.
3. Asigne un nombre al grupo de consistencia y seleccione la máquina virtual de almacenamiento.
   a. **Tipo de aplicación**: Si está utilizando ONTAP 9.12.1 o posterior, seleccione un tipo de aplicación. Si no se selecciona ningún valor, se asignará al grupo de consistencia el tipo de **Other** de forma predeterminada. Obtenga más información sobre la coherencia de etiquetado en Etiquetas de aplicaciones y componentes. Si el grupo de consistencia tiene una relación SM-BC, debe utilizar **otros**.
4. Seleccione los volúmenes existentes que desea incluir. Solo se podrá seleccionar los volúmenes que todavía no sean parte de un grupo de coherencia.

   > Si crea un grupo de coherencia con volúmenes existentes, el grupo de coherencia es compatible con volúmenes FlexVol. Los volúmenes con relaciones de SnapMirror asíncrono o síncrono se pueden añadir a grupos de coherencia, pero no tienen en cuenta los grupos de consistencia. Los grupos de consistencia no admiten bloques S3 ni máquinas virtuales de almacenamiento con relaciones de SVMDR.

5. Seleccione **Guardar**.
6. Para confirmar que se ha creado el grupo de coherencia, vuelva al menú del grupo de consistencia principal, donde aparecerá una vez que se complete el trabajo de ONTAP. Si ha elegido una política de protección, confirme que se configuró correctamente al seleccionar un grupo de coherencia en el menú. Si establece una política de protección, sabrá que se ha aplicado cuando ve un escudo verde bajo la directiva apropiada, remoto o local.

CLI

A partir de ONTAP 9.14.1, puede crear un grupo de consistencia con volúmenes existentes mediante la CLI de ONTAP.

Pasos

1. Emita el `consistency-group create` comando. La `-volumes` parameter acepta una lista de nombres de volúmenes separados por comas.

   ```
   consistency-group create -vserver SVM_name -consistency-group consistency-group-name -volume volumes
   ```

2. Vea el grupo de consistencia mediante la `consistency-group show` comando.

Siguientes pasos

- Proteja un grupo de consistencia
- Modificar un grupo de consistencia
- Clonar un grupo de consistencia

Configurar un grupo de consistencia jerárquico

Los grupos de coherencia jerárquicos permiten gestionar cargas de trabajo grandes que

abarcan varios volúmenes, creando un grupo de coherencia primario que funciona como un paraguas para los grupos de coherencia secundarios.

Los grupos de consistencia jerárquicos tienen un primario que puede incluir hasta cinco grupos de consistencia individuales. Los grupos de coherencia jerárquicos pueden admitir diferentes políticas Snapshot locales en grupos de coherencia o volúmenes individuales. Si utiliza una política de protección remota, que se aplicará a todo el grupo de consistencia jerárquico (primario y secundario).

A partir de ONTAP 9.13.1, puede hacerlo modifique la geometría de sus grupos de consistencia y.. mueva volúmenes entre grupos de coherencia secundarios.

Para obtener información sobre los límites de objetos en los grupos de consistencia, consulte Límites de objetos para los grupos de consistencia.

Cree un grupo de consistencia jerárquico con nuevas LUN o volúmenes

Al crear un grupo de consistencia jerárquico, puede rellenarlo con nuevas LUN. A partir de ONTAP 9.13.1, también se pueden usar nuevos espacios de nombres NVMe y volúmenes NAS.

System Manager

Pasos

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione **+Agregar** y, a continuación, seleccione el protocolo para el objeto de almacenamiento.

   En ONTAP 9.10.1 a 9.12.1, la única opción para un nuevo objeto de almacenamiento es **utilizando nuevas LUN**. A partir de ONTAP 9.13.1, System Manager admite la creación de grupos de consistencia con espacios de nombres NVMe nuevos y volúmenes NAS nuevos.

3. Asigne un nombre al grupo de consistencia. Designe el número de volúmenes o LUN y la capacidad por volumen o LUN.
   a. **Tipo de aplicación**: Si está utilizando ONTAP 9.12.1 o posterior, seleccione un tipo de aplicación. Si no se selecciona ningún valor, se asignará al grupo de consistencia el tipo de **Other** de forma predeterminada. Obtenga más información sobre la coherencia de etiquetado en Etiquetas de aplicaciones y componentes. Si planea usar una política de protección remota, debe elegir **Otro**.
4. Seleccione el sistema operativo del host y el formato de LUN. Introduzca la información del iniciador del host.
   a. Para **Nuevas LUN**: Seleccione el sistema operativo del host y el formato de LUN. Introduzca la información del iniciador del host.
   b. Para **Nuevos volúmenes NAS**: Elija la opción de exportación apropiada (NFS o SMB/CIFS) según la configuración NAS de su SVM.
   c. Para **Nuevos espacios de nombres NVMe**: Seleccione el sistema operativo del host y el subsistema NVMe.
5. Para agregar un grupo de consistencia hijo, seleccione **Más opciones** y luego **+Agregar grupo de consistencia hijo**.
6. Seleccione el nivel de rendimiento, el número de LUN o volúmenes y la capacidad por LUN o volumen. Designe las configuraciones de exportación adecuadas o la información del sistema operativo en función del protocolo que esté utilizando.
7. Opcionalmente, seleccione una política de Snapshot local y establezca los permisos de acceso.
8. Repita desde un máximo de cinco grupos de consistencia secundarios.
9. Seleccione **Guardar**.
10. Para confirmar que se ha creado el grupo de coherencia, vuelva al menú del grupo de consistencia principal, donde aparecerá una vez que se complete el trabajo de ONTAP. Si establece una directiva de protección, mire bajo la directiva apropiada, remota o local, que debe mostrar un escudo verde con una Marca de verificación en ella.

CLI

A partir de ONTAP 9.14.1, puede crear un nuevo grupo de consistencia jerárquico mediante la CLI.

Paso

1. Cree el nuevo grupo de consistencia mediante el `consistency-group create` comando.

   La `volume-count` parameter configura la cantidad de volúmenes en cada grupo de coherencia secundario. Se puede crear un grupo de coherencia primario con un máximo de cinco grupos de consistencia secundarios.

```
consistency-group create -vserver SVM_name -consistency-group
consistency_group_name -parent-consistency-group
parent_consistency_group_name -cg-count number_of_child_consistency_groups
-volume volume_prefix -volume-count number -size size -export-policy
policy_name -storage-service extreme
```

Cree un grupo de coherencia jerárquico con volúmenes existentes

Se pueden organizar los volúmenes existentes en un grupo de coherencia jerárquico.

System Manager

Pasos

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione **+Agregar** y **utilizando volúmenes existentes**.
3. Seleccione la máquina virtual de almacenamiento.
4. Seleccione los volúmenes existentes que desea incluir. Solo se podrá seleccionar los volúmenes que todavía no sean parte de un grupo de coherencia.
5. Para agregar un grupo de consistencia hijo, seleccione **+Agregar grupo de consistencia hijo**. Cree los grupos de consistencia necesarios, que se nombrarán automáticamente.
   a. **Tipo de componente**: Si está utilizando ONTAP 9.12.1 o posterior, seleccione un tipo de componente de "datos", "registros" u "otro". Si no se selecciona ningún valor, se asignará al grupo de consistencia el tipo de **Other** de forma predeterminada. Obtenga más información sobre la coherencia de etiquetado en Etiquetas de aplicaciones y componentes. Si planea usar una política de protección remota, debe usar **Otro**.
6. Asigne volúmenes existentes a cada grupo de coherencia.
7. Opcionalmente, seleccione una política de Snapshot local.
8. Repita desde un máximo de cinco grupos de consistencia secundarios.
9. Seleccione **Guardar**.
10. Para confirmar que se ha creado el grupo de coherencia, vuelva al menú del grupo de consistencia principal, donde aparecerá una vez que se complete el trabajo de ONTAP. Si ha elegido una política de protección, confirme que se ha configurado correctamente seleccionando su grupo de consistencia en el menú; en el tipo de política correspondiente, verá un escudo verde con una Marca de verificación en el interior de la misma.

CLI

A partir de ONTAP 9.14.1, puede crear un grupo de consistencia jerárquico mediante la CLI.

Pasos

1. Aprovisione un nuevo grupo de coherencia primario y asigne volúmenes a un nuevo grupo de consistencia secundario:

   ```
   consistency-group create -vserver svm_name -consistency-group
   child_consistency_group_name -parent-consistency-group
   parent_consistency_group_name -volumes volume_names
   ```

2. Introduzca `y` para confirmar que desea crear un nuevo grupo de consistencia primario y secundario.

Siguientes pasos

- Modificar la geometría de un grupo de consistencia
- Modificar un grupo de consistencia
- Proteja un grupo de consistencia

Proteger los grupos de consistencia

Los grupos de coherencia ofrecen una protección local y remota de fácil gestión para

aplicaciones SAN, NAS y NVMe que abarcan varios volúmenes.

La creación de un grupo de consistencia no habilita la protección automáticamente. Las políticas de protección se pueden establecer en el momento de la creación o después de crear el grupo de consistencia. Puede proteger grupos de consistencia mediante:

- Copias Snapshot locales
- Continuidad del negocio de SnapMirror (SM-BC)
- MetroCluster (principios de 9.11.1)
- SnapMirror asíncrono (inicio de 9.13.1)
- Recuperación ante desastres asíncrona de SVM (comenzando 9.14.1)

Si utiliza grupos de consistencia anidados, puede establecer políticas de protección distintas para los grupos de coherencia primario y secundario.

A partir de ONTAP 9.11.1, se ofrecen los grupos de consistencia Creación de copias Snapshot de grupo de consistencia en dos fases. La operación Snapshot de dos fases ejecuta una comprobación previa para garantizar que la copia Snapshot se capture correctamente.

Se puede producir la recuperación de un grupo de consistencia completo, de un solo grupo de consistencia en una configuración jerárquica o de volúmenes individuales en el grupo de consistencia. Para lograr la recuperación, seleccione el grupo de consistencia del que desea recuperar, seleccione el tipo de copia Snapshot y, a continuación, identifique la copia Snapshot en la que se basa la restauración. Para obtener más información acerca de este proceso, consulte "Restaurar un volumen de una copia de Snapshot anterior".

Configurar una política de Snapshot local

Configurar una política de protección Snapshot local permite crear una política que abarque todos los volúmenes en un grupo de coherencia.

Acerca de esta tarea

La programación mínima de copias Snapshot admitida para grupos de consistencia es de 30 minutos. Esta opción está basada en "Prueba para FlexGroups", Que comparten la misma infraestructura Snapshot que los grupos de consistencia.

System Manager

Pasos

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de consistencia que ha creado en el menú del grupo de consistencia.
3. En la parte superior derecha de la página de descripción general del grupo de consistencia, seleccione **Editar**.
4. Marque la casilla junto a **programar copias Snapshot (local)**.
5. Seleccione una política de Snapshot. Para configurar una directiva nueva y personalizada, consulte "Cree una política de protección de datos personalizada".
6. Seleccione **Guardar**.
7. Volver al menú de descripción general del grupo de consistencia. En la columna izquierda bajo **copias Snapshot (local)**, el estado dirá protegido al lado .

CLI

A partir de ONTAP 9.14.1, puede modificar la política de protección de un grupo de consistencia con la CLI.

Paso

1. Ejecute el siguiente comando para establecer o modificar la política de protección:

   Si modifica la política de protección de una consistencia secundaria, debe identificar el grupo de consistencia primario mediante el `-parent-consistency-group` *`parent_consistency_group_name`* parámetro.

   ```
   consistency-group modify -vserver svm_name -consistency-group
   consistency_group_name -snapshot-policy policy_name
   ```

Cree una copia Snapshot bajo demanda

Si necesita crear una copia Snapshot del grupo de consistencia fuera de una política normalmente programada, puede crear una bajo demanda.

System Manager

Pasos

1. Vaya a **Almacenamiento** > **Grupos de consistencia**.
2. Seleccione el grupo de coherencia para el que desea crear una copia Snapshot bajo demanda.
3. Cambie a la pestaña **Copias de instantánea** y seleccione **+Agregar**.
4. Proporcione un **Nombre** y una **Etiqueta de SnapMirror**. En el menú desplegable de **Consistencia**, selecciona **Consistente a la aplicación** o **Consistente a la caída**.
5. Seleccione **Guardar**.

CLI

A partir de ONTAP 9.14.1, puede crear una copia Snapshot bajo demanda de un grupo de consistencia utilizando la CLI.

Paso

1. Cree la copia Snapshot:

   De forma predeterminada, el tipo de Snapshot es coherente con los fallos. Puede modificar el tipo de instantánea con el opcional `-type` parámetro.

   ```
   consistency-group snapshot create -vserver svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name
   ```

Cree Snapshots de grupo de consistencia de dos fases

A partir de ONTAP 9.11.1, los grupos de consistencia admiten confirmaciones de dos fases para la creación de Snapshot de grupos de consistencia (CG), que ejecutan una comprobación previa antes de confirmar la copia Snapshot. Esta función solo está disponible con la API de REST de ONTAP.

La creación de snapshots de dos fases de CG solo está disponible para la creación de snapshots, no para el aprovisionamiento de grupos de consistencia ni para la restauración de grupos de consistencia.

Una Snapshot CG de dos fases divide el proceso de creación de Snapshot en dos fases:

1. En la primera fase, la API ejecuta comprobaciones previas y activa la creación de copias Snapshot. La primera fase incluye un parámetro de tiempo de espera, lo que designa la cantidad de tiempo que tarda la copia Snapshot en realizarse correctamente.
2. Si la solicitud en la primera fase se completa correctamente, puede invocar la segunda fase dentro del intervalo designado desde la primera fase, confirmando la copia Snapshot en el punto final correspondiente.

Antes de empezar

- Para utilizar la creación Snapshot de CG de dos fases, todos los nodos del clúster deben ejecutar ONTAP 9.11.1 o una versión posterior.
- Solo se admite una llamada activa de una operación Snapshot de grupo de consistencia en una instancia de grupo de consistencia a la vez, ya sea una fase o dos fases. Al intentar invocar una operación de Snapshot mientras otra está en curso, se produce un error.
- Cuando invoca la creación de Snapshot, puede configurar un valor de tiempo de espera opcional de entre 5 y 120 segundos. Si no se proporciona ningún valor de tiempo de espera, se agota el tiempo de espera

de la operación en el valor predeterminado de 7 segundos. En la API, configure el valor de tiempo de espera en `action_timeout` parámetro. En la CLI, utilice `-timeout` bandera.

Pasos

Es posible completar una Snapshot en dos fases con la API de REST o, a partir de ONTAP 9.14.1, la CLI de ONTAP. Esta operación no es compatible con System Manager.

> Si invoca la creación de Snapshot con la API, debe confirmar la copia Snapshot con la API. Si invoca la creación de Snapshot con la CLI, debe confirmar la copia Snapshot con la CLI. No se admiten métodos de mezcla.

CLI

A partir de ONTAP 9.14.1, puede crear una copia Snapshot de dos fases con la CLI.

Pasos

1. Inicie la instantánea:

   ```
   consistency-group snapshot start -vserver svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name [-timeout time_in_seconds
   -write-fence {true|false}]
   ```

2. Compruebe que la instantánea se ha realizado:

   ```
   consistency-group snapshot show
   ```

3. Confirme la instantánea:

   ```
   consistency-group snapshot commit svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name
   ```

API

1. Invoque la creación de la instantánea. Envíe una solicitud POST al extremo del grupo de consistencia mediante el `action=start` parámetro.

   ```
   curl -k -X POST 'https://<IP_address>/application/consistency-
   groups/<cg-uuid>/snapshots?action=start&action_timeout=7' -H
   "accept: application/hal+json" -H "content-type: application/json"
   -d '
   {
     "name": "<snapshot_name>",
     "consistency_type": "crash",
     "comment": "<comment>",
     "snapmirror_label": "<SnapMirror_label>"
   }'
   ```

2. Si la solicitud POST se realiza correctamente, el resultado incluye un uuid de Snapshot. Con ese uuid, envíe una solicitud de REVISIÓN para confirmar la copia Snapshot.

```
curl -k -X PATCH 'https://<IP_address>/application/consistency-
groups/<cg_uuid>/snapshots/<snapshot_id>?action=commit' -H "accept:
application/hal+json" -H "content-type: application/json"

For more information about the ONTAP REST API, see
link:https://docs.netapp.com/us-en/ontap-
automation/reference/api_reference.html[API reference^] or the
link:https://devnet.netapp.com/restapi.php[ONTAP REST API page^] at
the NetApp Developer Network for a complete list of API endpoints.
```

Configurar la protección remota para un grupo de coherencia

Los grupos de coherencia ofrecen protección remota mediante SM-BC y, a partir de ONTAP 9.13.1, SnapMirror asíncrono.

Configurar la protección con SM-BC

Puede utilizar SM-BC para garantizar que las copias Snapshot de los grupos de consistencia creados en el grupo de consistencia se copien el destino. Para obtener más información sobre SM-BC o sobre cómo configurar SM-BC mediante la CLI, consulte Configure la protección para la continuidad del negocio.

Antes de empezar

- No se pueden establecer relaciones de SM-BC en volúmenes montados para el acceso NAS.
- Las etiquetas de políticas del clúster de origen y destino deben coincidir.
- SM-BC no replicará las copias Snapshot de forma predeterminada a menos que se añada una regla con una etiqueta de SnapMirror al valor predefinido `AutomatedFailOver` La política y las copias de Snapshot se crean con esa etiqueta.

  Para obtener más información sobre este proceso, consulte "Proteja con SM-BC".

- Implementaciones en cascada No son compatibles con SM-BC.
- A partir de ONTAP 9.13.1, se puede sin interrupciones añada volúmenes a un grupo de coherencia Con una relación SM-BC activa. Cualquier otro cambio en un grupo de consistencia requiere que rompa la relación de SM-BC, que modifique el grupo de consistencia y, a continuación, vuelva a establecer y resincronizar la relación.

Para configurar SM-BC con la CLI, consulte Proteja con SM-BC.

Pasos para System Manager

1. Asegúrese de haber cumplido con el "Requisitos previos para usar SM-BC".
2. Seleccione **almacenamiento > grupos de consistencia**.
3. Seleccione el grupo de consistencia que ha creado en el menú del grupo de consistencia.
4. En la parte superior derecha de la página de descripción general, seleccione **más** y, a continuación, **proteger**.
5. System Manager rellena automáticamente la información del origen. Seleccione la máquina virtual de almacenamiento y clúster apropiado para el destino. Seleccione una política de protección. Asegúrese de

que **Initialize Relationship** está activada.

6. Seleccione **Guardar**.
7. El grupo de consistencia debe inicializar y sincronizar. Confirme que la sincronización se ha completado correctamente volviendo al menú **Grupo de consistencia**. Se muestra el estado **SnapMirror (Remote)** `Protected` junto a. .

Configurar la protección asíncrona de SnapMirror

A partir de ONTAP 9.13.1, puede configurar la protección SnapMirror asíncrona para un único grupo de consistencia. A partir de ONTAP 9.14.1, se puede usar SnapMirror asíncrono para replicar copias Snapshot granulares de volúmenes en el clúster de destino mediante la relación del grupo de coherencia.

Acerca de esta tarea

Para replicar copias Snapshot granulares del volumen, debe ejecutar ONTAP 9.14.1 o una versión posterior. Para las políticas de MirrorAndVault y Vault, la etiqueta de SnapMirror de la política de Snapshot granular de volumen debe coincidir con la regla de política de SnapMirror del grupo de coherencia. Las snapshots granulares del volumen rigen el valor conservar de la política de SnapMirror del grupo de consistencia, que se calcula independientemente de las snapshots del grupo de consistencia. Por ejemplo, si tiene una política para conservar dos copias Snapshot en el destino, puede tener dos copias Snapshot granulares de volumen y dos copias Snapshot de grupo de consistencia.

Al volver a sincronizar la relación de SnapMirror con copias Snapshot granulares de volúmenes, se pueden conservar copias de Snapshot granulares de volúmenes con el `-preserve` bandera. Se conservan las copias Snapshot granulares de volúmenes más recientes que las copias Snapshot de grupo de consistencia. Si no existe una copia de Snapshot de grupo de consistencia, no se pueden transferir copias de Snapshot granulares de volumen en la operación de resincronización.

Antes de empezar

- La protección asíncrona SnapMirror solo está disponible para grupos de consistencia individuales. No se admite para grupos de coherencia jerárquicos. Para convertir un grupo de consistencia jerárquico en un grupo de consistencia único, consulte modificar la arquitectura del grupo de consistencia.
- Las etiquetas de políticas del clúster de origen y destino deben coincidir.
- Puede sin interrupciones añada volúmenes a un grupo de coherencia Con una relación de SnapMirror asíncrona activa. Cualquier otro cambio en un grupo de consistencia requiere que rompa la relación de SnapMirror, modifique el grupo de consistencia y, a continuación, vuelva a establecer y vuelva a sincronizar la relación.
- Si se configuró una relación de protección de SnapMirror asíncrono para varios volúmenes individuales, puede convertir dichos volúmenes en un grupo de coherencia y mantener las copias de Snapshot existentes. Para convertir volúmenes correctamente:
  - Debe haber una copia de Snapshot común de los volúmenes.
  - Debe interrumpir la relación de SnapMirror existente. añada los volúmenes a un único grupo de consistencia, a continuación, vuelva a sincronizar la relación mediante el siguiente flujo de trabajo.

Pasos

1. En el clúster de destino, seleccione **Almacenamiento > Grupos de consistencia**.
2. Seleccione el grupo de consistencia que ha creado en el menú del grupo de consistencia.
3. En la parte superior derecha de la página de descripción general, seleccione **más** y, a continuación, **proteger**.
4. System Manager rellena automáticamente la información del origen. Seleccione la máquina virtual de

almacenamiento y clúster apropiado para el destino. Seleccione una política de protección. Asegúrese de que **Initialize Relationship** está activada.

Al seleccionar una política asíncrona, tiene la opción de **Anular horario de transferencia**.

> La programación mínima admitida (objetivo de punto de recuperación o objetivo de punto de recuperación) para los grupos de consistencia con SnapMirror asíncrono es de 30 minutos.

5. Seleccione **Guardar**.
6. El grupo de consistencia debe inicializar y sincronizar. Confirme que la sincronización se ha completado correctamente volviendo al menú **Grupo de consistencia**. Se muestra el estado **SnapMirror (Remote)** `Protected` junto a. .

Configurar la recuperación ante desastres de la SVM

A partir de ONTAP 9.14.1, Recuperación ante desastres de SVM admite grupos de coherencia, lo que permite reflejar información del grupo de coherencia del origen al clúster de destino.

Si va a habilitar la recuperación ante desastres de SVM en una SVM que ya contiene un grupo de consistencia, a continuación los flujos de trabajo de configuración de la SVM para System Manager o la CLI de ONTAP.

Si va a añadir un grupo de coherencia a una SVM que esté en una relación de recuperación ante desastres de SVM activa y en buen estado, debe actualizar la relación de recuperación ante desastres de SVM desde el clúster de destino. Para obtener más información, consulte Actualice manualmente una relación de replicación. Debe actualizar la relación cada vez que expanda el grupo de consistencia.

Limitaciones

- La recuperación ante desastres de SVM no admite grupos de consistencia jerárquicos.
- La recuperación ante desastres de SVM no admite grupos de consistencia protegidos con SnapMirror asíncrono. Debe interrumpir la relación de SnapMirror antes de configurar la recuperación ante desastres de SVM.
- Ambos clústeres deben ejecutar ONTAP 9.14.1 o una versión posterior.
- Las relaciones de dispersión no se admiten para las configuraciones de recuperación ante desastres de SVM que contienen grupos de coherencia.
- Para ver otros límites, consulte límites del grupo de consistencia.

Visualizar relaciones

System Manager visualiza los mapas de LUN en el menú **Protección > Relaciones**. Cuando selecciona una relación de origen, System Manager muestra una visualización de las relaciones de origen. Al seleccionar un volumen, puede profundizar en estas relaciones para ver una lista de las LUN contenidas y las relaciones con el iGroup. Esta información se puede descargar como un libro de Excel desde la vista de volumen individual; la operación de descarga se ejecuta en segundo plano.

Información relacionada

- "Clonar un grupo de consistencia"
- "Configure las copias Snapshot"
- "Cree políticas de protección de datos personalizadas"

- "Recuperar desde copias Snapshot"
- "Restaurar un volumen de una copia de Snapshot anterior"
- "Información general sobre SM-BC"
- "Documentación de automatización de ONTAP"
- Conceptos básicos de la recuperación ante desastres de SnapMirror asíncrono

Modificar los volúmenes miembro en un grupo de coherencia

A partir de ONTAP 9.12.1, puede modificar un grupo de coherencia quitando volúmenes o añadiendo volúmenes (expandiendo el grupo de coherencia). A partir de ONTAP 9.13.1, se pueden mover volúmenes entre grupos de coherencia secundarios si comparten un volumen primario común.

Añadir volúmenes a un grupo de coherencia

A partir de ONTAP 9.12.1, es posible añadir volúmenes a un grupo de coherencia sin interrupciones.

Acerca de esta tarea

- No es posible añadir volúmenes asociados con otro grupo de coherencia.
- Los grupos de consistencia admiten los protocolos NAS, SAN y NVMe.
- Puede añadir hasta 16 volúmenes a la vez a un grupo de coherencia si los ajustes se encuentran dentro de la configuración general límites del grupo de consistencia.
- A partir de ONTAP 9.13.1, se pueden añadir volúmenes sin interrupciones a un grupo de coherencia con una política de continuidad del negocio con SnapMirror (SM-BC) activa o una política de protección SnapMirror asíncrona.
- Cuando se añaden volúmenes a un grupo de coherencia protegido por SM-BC, el estado de la relación de SM-BC cambiará a «Expansión» hasta que el mirroring y la protección se configuren para el volumen nuevo. Si se produce un desastre en el clúster primario antes de que se complete este proceso, el grupo de consistencia revierte a su composición original como parte de la operación de conmutación al nodo de respaldo.
- En ONTAP 9.12.1 y versiones anteriores, *no puede* añadir volúmenes a un grupo de coherencia de una relación SM-BC. Primero, debe interrumpir la relación de SM-BC, modificar el grupo de consistencia y, a continuación, restaurar la protección con SM-BC.
- A partir de ONTAP 9.12.1, la API DE REST DE ONTAP admite la adición *new* o volúmenes existentes a un grupo de coherencia. Para obtener más información sobre la API de REST de ONTAP, consulte "Documentación de referencia de la API DE REST de ONTAP".

  A partir de ONTAP 9.13.1, esta funcionalidad es compatible con System Manager.

- Al expandir un grupo de consistencia, las copias Snapshot del grupo de consistencia capturado antes de la modificación se considerarán parciales. Cualquier operación de restauración basada en esa copia Snapshot reflejará el grupo de consistencia en el momento específico de la Snapshot.
- Si utiliza ONTAP 9.10.1 a 9.11.1, no puede modificar un grupo de consistencia. Para cambiar la configuración de un grupo de coherencia en ONTAP 9.10.1 o 9.11.1, debe eliminar el grupo de coherencia y, a continuación, crear un nuevo grupo de coherencia con los volúmenes que desea incluir.
- A partir de ONTAP 9.14.1, se pueden replicar copias Snapshot granulares del volumen en el clúster de destino cuando se utiliza SnapMirror asíncrono. Cuando se amplía un grupo de consistencia con SnapMirror asíncrono, las copias Snapshot granulares de volúmenes solo se replican después de

expandir el grupo de coherencia cuando la política de SnapMirror es MirrorAll o MirrorAndVault. Solo se replican las copias Snapshot granulares del volumen más recientes que las copias Snapshot del grupo de consistencia base.

- Si añade volúmenes a un grupo de consistencia en una relación de recuperación ante desastres de SVM (compatible a partir de ONTAP 9.14.1), debe actualizar la relación de recuperación ante desastres de SVM desde el clúster de destino tras expandir el grupo de consistencia. Para obtener más información, consulte Actualice manualmente una relación de replicación.

Ejemplo 1. Pasos

System Manager

A partir de ONTAP 9.12.1, puede realizar esta operación con System Manager.

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de coherencia que desea modificar.
3. Si va a modificar un solo grupo de consistencia, en la parte superior del menú **Volumes**, seleccione **más** y, a continuación, **ampliar** para añadir un volumen.

   Si va a modificar un grupo de consistencia secundario, identifique el grupo de consistencia primario que desea modificar. Seleccione el botón **>** para ver los grupos de consistencia hijo y, a continuación, seleccione ⋮ junto al nombre del grupo de consistencia secundario que desea modificar. En ese menú, seleccione **ampliar**.
4. Seleccione hasta 16 volúmenes para añadir al grupo de coherencia.
5. Seleccione **Guardar**. Cuando la operación se complete, vea los volúmenes recién agregados en el menú **Volúmenes** del grupo de consistencia.

CLI

A partir de ONTAP 9.14.1, puede añadir volúmenes a un grupo de coherencia mediante la CLI de ONTAP.

Añadir volúmenes existentes

1. Ejecute el siguiente comando. La `-volumes` el parámetro acepta una lista de volúmenes separados por comas.

   > Incluya sólo el `-parent-consistency-group` el parámetro si el grupo de coherencia está en una relación jerárquica.

   ```
   consistency-group volume add -vserver svm_name -consistency-group
   consistency_group_name -parent-consistency-group parent_consistency_group
   -volume volumes
   ```

Añadir volúmenes nuevos

El procedimiento para añadir volúmenes nuevos depende del protocolo que utilice.

> Incluya sólo el `-parent-consistency-group` el parámetro si el grupo de coherencia está en una relación jerárquica.

- Para añadir volúmenes nuevos sin exportarlos, realice lo siguiente:

  ```
  consistency-group volume create -vserver SVM_name -consistency-group
  child_consistency_group -parent-consistency-group existingParentCg -volume
  volume_name -size size
  ```

- Para añadir volúmenes NFS nuevos:

  ```
  consistency-group volume create -vserver SVM_name -consistency-group
  consistency-group-name -volume volume-prefix -volume-count number -size
  ```

```
size -export-policy policy_name
```

- Para añadir nuevos volúmenes de SAN:

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency-group-name -lun lun_name -size size -lun-count number -igroup
igroup_name
```

- Para añadir nuevos espacios de nombres de NVMe:

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency_group_name -namespace namespace_name -volume-count number
-namespace-count number -size size -subsystem subsystem_name
```

Quite volúmenes de un grupo de coherencia

Los volúmenes que se quitan de un grupo de consistencia no se eliminan. Permanecen activos en el clúster.

Acerca de esta tarea

- No se pueden quitar volúmenes de un grupo de coherencia de una relación de recuperación ante desastres de SM-BC o SVM. Primero, debe romper la relación de SM-BC para modificar el grupo de consistencia y, a continuación, volver a establecer la relación.
- Si un grupo de coherencia no tiene volúmenes en él después de la operación de eliminación, se eliminará el grupo de coherencia.
- Cuando un volumen se elimina de un grupo de consistencia, las Snapshot existentes del grupo de consistencia permanecen, pero se consideran no válidas. Las snapshots existentes no se pueden utilizar para restaurar el contenido del grupo de consistencia. Siguen siendo válidas las copias Snapshot granulares en volúmenes.
- Si elimina un volumen del clúster, se elimina automáticamente del grupo de coherencia.
- Para cambiar la configuración de un grupo de coherencia en ONTAP 9.10.1 o 9.11.1, debe eliminar el grupo de coherencia y, a continuación, crear un grupo de coherencia nuevo con los volúmenes miembro deseados.
- Al eliminar un volumen del clúster, automáticamente lo quitará el grupo de coherencia.

System Manager

A partir de ONTAP 9.12.1, puede realizar esta operación con System Manager.

Pasos

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de consistencia único o secundario que desea modificar.
3. En el menú **volúmenes**, seleccione las casillas de verificación junto a los volúmenes individuales que desea quitar del grupo de consistencia.
4. Seleccione **Eliminar volúmenes del grupo de coherencia**.
5. Confirmar que comprende la eliminación de los volúmenes hará que todas las copias snapshot del grupo de consistencia no sean válidas y seleccione **Quitar**.

CLI

A partir de ONTAP 9.14.1, puede quitar volúmenes de un grupo de consistencia mediante la CLI.

Paso

1. Quite los volúmenes. La `-volumes` el parámetro acepta una lista de volúmenes separados por comas.

   Incluya sólo el `-parent-consistency-group` el parámetro si el grupo de coherencia está en una relación jerárquica.

   ```
   consistency-group volume remove -vserver SVM_name -consistency-group
   consistency_group_name -parent-consistency-group
   parent_consistency_group_name -volume volumes
   ```

Mover volúmenes entre grupos de coherencia

A partir de ONTAP 9.13.1, se pueden mover volúmenes entre grupos de coherencia secundarios que comparten un volumen primario.

Acerca de esta tarea

- Solo puede mover volúmenes entre grupos de coherencia anidados bajo el mismo grupo de consistencia primario.
- Las snapshots de grupo de consistencia existentes quedan no válidas y ya no se puede acceder a ellas como snapshots de grupo de consistencia. Las copias de Snapshot de volumen individuales siguen siendo válidas.
- Las copias Snapshot del grupo de consistencia primario siguen siendo válidas.
- Si mueve todos los volúmenes de un grupo de consistencia secundario, se eliminará ese grupo de coherencia.
- Las modificaciones a un grupo de consistencia deben respetar límites del grupo de consistencia.

System Manager

A partir de ONTAP 9.12.1, puede realizar esta operación con System Manager.

Pasos

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de coherencia primario que contiene los volúmenes que desea mover. Encuentre el grupo de consistencia secundario y luego expanda el menú **VOLUMES**. Seleccione los volúmenes que desea mover.
3. Selecciona **Mover**.
4. Seleccione si desea mover los volúmenes a un grupo de coherencia nuevo o a un grupo existente.
   a. Para desplazarse a un grupo de consistencia existente, seleccione **Grupo de consistencia secundario existente** y, a continuación, elija el nombre del grupo de consistencia en el menú desplegable.
   b. Para desplazarse a un nuevo grupo de consistencia, seleccione **Nuevo grupo de consistencia secundario**. Introduzca un nombre para el nuevo grupo de consistencia secundario y seleccione un tipo de componente.
5. Selecciona **Mover**.

CLI

A partir de ONTAP 9.14.1, puede mover volúmenes entre grupos de consistencia mediante la interfaz de línea de comandos de ONTAP.

Mueva volúmenes a un nuevo grupo de coherencia secundario

1. El siguiente comando crea un nuevo grupo de coherencia secundario que contiene los volúmenes designados.

   Cuando se crea el nuevo grupo de coherencia, se pueden designar nuevas políticas de Snapshot, calidad de servicio y organización en niveles.

   ```
   consistency-group volume reassign -vserver SVM_name -consistency-group
   source_child_consistency_group -parent-consistency-group
   parent_consistency_group -volume volumes -new-consistency-group
   consistency_group_name [-snapshot-policy policy -qos-policy policy -tiering
   -policy policy]
   ```

Mueva volúmenes a un grupo de coherencia secundario existente

1. Reasigne los volúmenes. La `-volumes` parameter acepta una lista de nombres de volúmenes separados por comas.

   ```
   consistency-group volume reassign -vserver SVM_name -consistency-group
   source_child_consistency_group -parent-consistency-group
   parent_consistency_group -volume volumes -to-consistency-group
   target_consistency_group
   ```

Información relacionada

- Límites del grupo de consistencia

- Clonar un grupo de consistencia

Modificar la geometría del grupo de consistencia

A partir de ONTAP 9.13.1, puede modificar la geometría de un grupo de consistencia. Modificar la geometría de un grupo de coherencia permite modificar la configuración de grupos de coherencia secundarios o primarios sin interrupciones en las operaciones de I/O en curso.

La modificación de la geometría del grupo de coherencia afectará a las copias Snapshot existentes.

> No puede modificar la geometría de un grupo de consistencia configurado con una política de protección remota. Primero debe romper la relación de protección, modificar la geometría y, a continuación, restaurar la protección remota.

Agregue un nuevo grupo de consistencia secundario

A partir de ONTAP 9.13.1, puede agregar un nuevo grupo de consistencia secundario a un grupo de consistencia primario existente.

Antes de empezar

- Un grupo de coherencia primario puede contener un máximo de cinco grupos de coherencia secundarios. Consulte límites del grupo de consistencia para otros límites.
- No puede agregar un grupo de consistencia secundario a un grupo de consistencia único. Usted debe primero [promocionar] el grupo de consistencia, luego puede agregar un grupo de consistencia secundario.
- Las copias Snapshot existentes del grupo de consistencia capturadas antes de la operación de ampliación se considerarán parciales. Cualquier operación de restauración basada en esa copia Snapshot reflejará el grupo de consistencia en el momento específico de la copia Snapshot.

Ejemplo 2. Pasos

System Manager

A partir de ONTAP 9.13.1, puede realizar esta operación con System Manager.

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de consistencia primario al que desea añadir un grupo de consistencia secundario.
3. Junto al nombre del grupo de consistencia primario, seleccione **Más** y luego **Agregar nuevo grupo de consistencia secundario**.
4. Introduzca un nombre para su grupo de consistencia.
5. Seleccione si desea añadir volúmenes nuevos o existentes.
   a. Si va a agregar volúmenes existentes, seleccione **Volúmenes existentes** y, a continuación, elija los volúmenes en el menú desplegable.
   b. Si va a agregar nuevos volúmenes, seleccione **Nuevos volúmenes** y luego designe el número de volúmenes y su tamaño.
6. Seleccione **Agregar**.

CLI

A partir de ONTAP 9.14.1, puede agregar un grupo de consistencia secundario mediante la CLI de ONTAP.

Añada un grupo de coherencia secundario con volúmenes nuevos

1. Cree el nuevo grupo de consistencia. Proporcionar valores para el nombre del grupo de coherencia, el prefijo del volumen, la cantidad de volúmenes, el tamaño de volumen, el servicio de almacenamiento, y el nombre de la política de exportación:

   ```
   consistency-group create -vserver SVM_name -consistency-group
   consistency_group -parent-consistency-group parent_consistency_group
   -volume-prefix prefix -volume-count number -size size -storage-service
   service -export-policy policy_name
   ```

Añada un grupo de coherencia secundario con volúmenes existentes

1. Cree el nuevo grupo de consistencia. La `volumes` parameter acepta una lista de nombres de volúmenes separados por comas.

   ```
   consistency-group create -vserver SVM_name -consistency-group
   new_consistency_group -parent-consistency-group parent_consistency_group
   -volumes volume
   ```

Desvincular un grupo de consistencia secundario

A partir de ONTAP 9.13.1, puede quitar un grupo de consistencia secundario de su primario, convirtiéndolo en un grupo de consistencia individual.

Antes de empezar

- Al desvincular un grupo de coherencia secundario, las snapshots del grupo de coherencia primario dejan de ser válidas y no se puede acceder a ellas. Las copias Snapshot granulares de volúmenes siguen

siendo válidas.

- Las copias Snapshot existentes del grupo de consistencia individual siguen siendo válidas.
- Se producirá un error en esta operación si existe un grupo de coherencia único existente con el mismo nombre que el grupo de coherencia secundario que se pretende desvincular. Si se encuentra con esta situación, debe cambiar el nombre del grupo de consistencia al desconectarlo.

Ejemplo 3. Pasos

System Manager

A partir de ONTAP 9.13.1, puede realizar esta operación con System Manager.

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de consistencia primario que contiene el secundario que desea desvincular.
3. Junto al grupo de consistencia hijo que desea separar, seleccione **Más** y luego **Desasociar del padre**.
4. Opcionalmente, cambie el nombre del grupo de coherencia y seleccione un tipo de aplicación.
5. Seleccione **Desasociar**.

CLI

A partir de ONTAP 9.14.1, puede desvincular un grupo de consistencia secundario mediante la CLI de ONTAP.

1. Desvincule el grupo de consistencia. De manera opcional, cambie el nombre del grupo de consistencia desvinculado con `-new-name` parámetro.

   ```
   consistency-group detach -vserver SVM_name -consistency-group
   child_consistency_group -parent-consistency-group parent_consistency_group
   [-new-name new_name]
   ```

Mueva un grupo de consistencia único existente bajo un grupo de consistencia primario

A partir de ONTAP 9.13.1, puede convertir un grupo de consistencia único existente en un grupo de consistencia secundario. Puede mover el grupo de consistencia por un grupo de consistencia primario existente o crear un grupo de consistencia primario nuevo durante la operación de movimiento.

Antes de empezar

- El grupo de coherencia primario debe tener cuatro o menos hijos. Un grupo de coherencia primario puede contener un máximo de cinco grupos de coherencia secundarios. Consulte límites del grupo de consistencia para otros límites.
- Las copias Snapshot existentes del grupo de consistencia *parent* capturadas antes de esta operación se considerarán parciales. Cualquier operación de restauración basada en una de esas copias Snapshot reflejará el grupo de consistencia en el momento específico de la copia Snapshot.
- Las copias de Snapshot de grupo de consistencia existentes del grupo de consistencia único siguen siendo válidas.

Ejemplo 4. Pasos

System Manager

A partir de ONTAP 9.13.1, puede realizar esta operación con System Manager.

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de consistencia que desea convertir.
3. Seleccione **Más** y luego **Mover bajo diferente grupo de consistencia**.
4. De manera opcional, introduzca un nuevo nombre para el grupo de consistencia y seleccione un tipo de componente. De forma predeterminada, el tipo de componente será Otro.
5. Elija si desea migrar a un grupo de consistencia primario existente o crear un nuevo grupo de consistencia primario:
   a. Para migrar a un grupo de consistencia primario existente, seleccione **Grupo de consistencia existente** y, a continuación, elija el grupo de consistencia en el menú desplegable.
   b. Para crear un grupo de consistencia primario nuevo, seleccione **Nuevo grupo de consistencia** y, a continuación, proporcione un nombre para el nuevo grupo de consistencia.
6. Selecciona **Mover**.

CLI

A partir de ONTAP 9.14.1, puede mover un solo grupo de consistencia debajo de un grupo de consistencia primario mediante la CLI de ONTAP.

Mover un grupo de consistencia debajo de un nuevo grupo de consistencia primario

1. Cree el nuevo grupo de consistencia primario. La `-consistency-groups` el parámetro migrará cualquier grupo de consistencia existente al nuevo elemento principal.

   ```
   consistency-group attach -vserver svm_name -consistency-group
   parent_consistency_group -consistency-groups child_consistency_group
   ```

Mueva un grupo de consistencia bajo un grupo de consistencia existente

1. Mueva el grupo de consistencia:

   ```
   consistency-group add -vserver SVM_name -consistency-group
   consistency_group -parent-consistency-group parent_consistency_group
   ```

Promover un grupo de consistencia secundario

A partir de ONTAP 9.13.1, puede promover un grupo de consistencia a un grupo de consistencia primario. Cuando se promociona el grupo de coherencia único a un elemento primario, también se crea un nuevo grupo de coherencia secundario que hereda todos los volúmenes del grupo de coherencia único original.

Antes de empezar

- Si desea convertir un grupo de consistencia secundario en un grupo de consistencia primario, primero debe [detach] el grupo de consistencia secundario y, a continuación, siga este procedimiento.
- Las copias Snapshot existentes del grupo de consistencia siguen siendo válidas después de promocionar el grupo de consistencia.

Ejemplo 5. Pasos

System Manager

A partir de ONTAP 9.13.1, puede realizar esta operación con System Manager.

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de coherencia que desea promocionar.
3. Seleccione **Más** y luego **Promocionar al grupo de consistencia primario**.
4. Introduzca un **Nombre** y seleccione un **Tipo de componente** para el grupo de consistencia hijo.
5. Selecciona **Promocionar**.

CLI

A partir de ONTAP 9.14.1, puede mover un solo grupo de consistencia debajo de un grupo de consistencia primario mediante la CLI de ONTAP.

1. Promocione el grupo de consistencia. Este comando creará un grupo de coherencia primario y un secundario.

   ```
   consistency-group promote -vserver SVM_name -consistency-group
   existing_consistency_group -new-name new_child_consistency_group
   ```

Degrade un elemento principal a un solo grupo de consistencia

A partir de ONTAP 9.13.1, puede degradar un grupo de consistencia primario a un solo grupo de consistencia. Al degradar el elemento primario, se abre la jerarquía del grupo de consistencia y se eliminan todos los grupos de coherencia secundarios asociados. Todos los volúmenes del grupo de coherencia permanecerán bajo el nuevo grupo de coherencia único.

Antes de empezar

- Las copias Snapshot existentes del grupo de consistencia primario siguen siendo válidas después de degradarlas a una sola consistencia. Las copias Snapshot existentes de cualquiera de los grupos de consistencia secundarios asociados de dicho grupo principal dejarán de ser válidas, pero las snapshots de volúmenes individuales que contienen siguen siendo accesibles como snapshots granulares para el volumen.

Ejemplo 6. Pasos

System Manager

A partir de ONTAP 9.13.1, puede realizar esta operación con System Manager.

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de consistencia primario que desea degradar.
3. Seleccione **Más** y luego **Descender a un solo grupo de consistencia**.
4. Una advertencia le aconsejará que se eliminen todos los grupos de coherencia secundarios asociados y que sus volúmenes se muevan al nuevo grupo de consistencia único. Selecciona **Descenso** para confirmar que entiendes el impacto.

CLI

A partir de ONTAP 9.14.1, puede degradar un grupo de consistencia mediante la CLI de ONTAP.

1. Degrade el grupo de consistencia. Utilice el opcional `-new-name` parámetro para cambiar el nombre del grupo de consistencia.

   ```
   consistency-group demote -vserver SVM_name -consistency-group
   parent_consistency_group [-new-name new_consistency_group_name]
   ```

Modificar etiquetas de aplicación y componentes

A partir de ONTAP 9.12.1, los grupos de consistencia admiten el etiquetado de componentes y aplicaciones. Las etiquetas de aplicaciones y componentes son una herramienta de gestión que le permite filtrar e identificar diferentes cargas de trabajo en sus grupos de consistencia.

Acerca de esta tarea

Los grupos de consistencia ofrecen dos tipos de etiquetas:

- **Etiquetas de aplicación**: Estas se aplican a grupos de consistencia individuales y padre. Las etiquetas de las aplicaciones proporcionan etiquetas para cargas de trabajo como MongoDB, Oracle o SQL Server. La etiqueta de aplicación predeterminada para los grupos de consistencia es otra.
- **Etiquetas de componentes**: Los niños de los grupos de consistencia jerárquicos tienen etiquetas de componentes en lugar de etiquetas de aplicación. Las opciones para etiquetas de componentes son "datos", "registros" u "otros". El valor predeterminado es Other.

Puede aplicar las etiquetas al crear grupos de consistencia o después de crear los grupos de consistencia.

> Si el grupo de consistencia tiene una relación SM-BC, debe utilizar **otros** como la aplicación o etiqueta de componente.

Pasos

A partir de ONTAP 9.12.1, puede modificar las etiquetas de componentes y aplicaciones mediante System Manager. A partir de ONTAP 9.14.1, puede modificar la aplicación y las etiquetas de los componentes mediante la CLI de ONTAP.

System Manager

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de consistencia cuya etiqueta desea modificar. Seleccione la ⋮ Junto al nombre del grupo de consistencia luego **Editar**.
3. En el menú desplegable, seleccione la aplicación o etiqueta de componente adecuada.
4. Seleccione **Guardar**.

CLI

A partir de ONTAP 9.14.1, puede modificar la aplicación o la etiqueta de componente de un grupo de consistencia existente mediante la CLI de ONTAP.

Modifique la etiqueta de aplicación

1. Las etiquetas de aplicación aceptan un número limitado de cadenas predefinidas. Para ver la lista de cadenas aceptadas, ejecute el siguiente comando:
   `consistency-group modify -vserver` *`svm_name`* `-consistency-group` *`consistency_group`* `-application-type ?`
2. Elija la cadena adecuada del resultado, el modifique el grupo de consistencia:
   `consistency-group modify -vserver` *`svm_name`* `-consistency-group` *`consistency_group`* `-application-type application_type`

Modifique la etiqueta de componente

1. Modifique el tipo de componente. El tipo de componente puede ser datos, registros u otros. Si está utilizando SM-BC, debe ser “Otro”.
   `consistency-group modify -vserver` *`svm`* `-consistency-group` *`child_consistency_group`* `-parent-consistency-group` *`parent_consistency_group`* `-application-component-type [data|logs|other]`

Clonar un grupo de consistencia

A partir de ONTAP 9.12.1, puede clonar un grupo de consistencia para crear una copia de un grupo de consistencia y su contenido. La clonación de un grupo de coherencia crea una copia de la configuración del grupo de coherencia, sus metadatos, como el tipo de aplicación, y todos los volúmenes y su contenido, como archivos, directorios, LUN o espacios de nombres NVMe.

Acerca de esta tarea

Al clonar un grupo de consistencia, puede clonarlo con su configuración actual, pero con el contenido del volumen como son o basado en una snapshot de grupo de consistencia existente.

La clonación de un grupo de consistencia solo se admite para todo el grupo de consistencia. No puede clonar un grupo de consistencia secundario individual en una relación jerárquica: Solo se puede clonar la configuración completa del grupo de consistencia.

Cuando clona un grupo de consistencia, no se clonan los siguientes componentes:

- Grupos de iniciadores
- Mapas de LUN

- Subsistemas NVMe
- Asignaciones del subsistema de espacio de nombres de NVMe

Antes de empezar

- Cuando se clona un grupo de coherencia, ONTAP no creará recursos compartidos de SMB para los volúmenes clonados si no se especifica un nombre de recurso compartido. * Los grupos de consistencia clonados no están montados si no se especifica una ruta de unión.
- Si intenta clonar un grupo de consistencia basado en una snapshot que no refleja los volúmenes constituyentes actuales del grupo de consistencia, se producirá un error en la operación.
- Después de clonar un grupo de consistencia, debe realizar la operación de asignación adecuada.

  Consulte Asigne iGroups a varias LUN o. Asignar un espacio de nombres NVMe a un subsistema si quiere más información.

- No se admite la clonado de un grupo de consistencia en una relación de continuidad empresarial de SnapMirror o con ningún volumen de DP asociado.

System Manager

Pasos

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de consistencia que desea clonar en el menú **Grupo de consistencia**.
3. En la parte superior derecha de la página de descripción general del grupo de consistencia, seleccione **Clonar**.
4. Introduzca un nombre para el nuevo grupo de consistencia clonado o acepte el nombre predeterminado.
   a. Elija si desea habilitar "**Thin Provisioning**".
   b. Elija **Split Clone** si desea disociar el grupo de consistencia de su origen y asignar espacio en disco adicional para el grupo de consistencia clonado.
5. Para clonar el grupo de consistencia en su estado actual, elija **Agregar una nueva copia Snapshot**.

   Para clonar el grupo de consistencia basado en una instantánea, seleccione **utilizar una copia Snapshot** existente. Si selecciona esta opción, se abrirá un nuevo submenú. Elija la copia de Snapshot que desea usar como base para la operación de clonado.
6. Seleccione **Clonar**.
7. Vuelva al menú **Grupo de consistencia** para confirmar que el grupo de consistencia ha sido clonado.

CLI

A partir de ONTAP 9.14.1, puede clonar un grupo de consistencia mediante la CLI.

Clonar un grupo de consistencia

1. La `consistency-group clone create` el comando clona el grupo de coherencia en su estado actual de un momento específico. Para basar la operación de clonación en una instantánea, incluya la `-source-snapshot` parámetro.

   ```
   consistency-group clone create -vserver svm_name -consistency-group
   clone_name -source-consistency-group consistency_group_name [-source-
   snapshot snapshot_name]
   ```

Siguientes pasos

- Asigne iGroups a varias LUN
- Asignar un espacio de nombres NVMe a un subsistema

Eliminar un grupo de consistencia

Si decide que ya no necesita un grupo de consistencia, puede eliminarlo.

Acerca de esta tarea

- Al eliminar un grupo de coherencia se elimina la instancia del grupo de coherencia y *no* afecta a los volúmenes constituyentes o las LUN. La eliminación de un grupo de consistencia no elimina las instantáneas presentes en cada volumen, pero ya no será accesible como copias Snapshot de grupo de consistencia. Sin embargo, las copias Snapshot pueden seguir gestionándose como snapshots granulares

de volumen normales.

- ONTAP elimina automáticamente un grupo de coherencia si todos los volúmenes del grupo de coherencia se eliminan.
- Al eliminar un grupo de consistencia primario, se eliminan todos los grupos de consistencia secundarios asociados.
- Si utiliza una versión de ONTAP entre 9.10.1 y 9.12.0, los volúmenes solo se pueden eliminar de un grupo de coherencia si el volumen se elimina, en cuyo caso, el volumen se elimina automáticamente del grupo de coherencia. A partir de ONTAP 9.12.1, es posible quitar volúmenes de un grupo de consistencia sin eliminar el grupo de consistencia. Para obtener más información sobre este proceso, consulte Modificar un grupo de consistencia.

Ejemplo 7. Pasos

System Manager

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de coherencia que desea eliminar.
3. Junto al nombre del grupo de consistencia, seleccione ⋮ Luego **Eliminar**.

CLI

A partir de ONTAP 9.14.1, puede eliminar un grupo de consistencia mediante la CLI.

Eliminar un grupo de consistencia

1. Elimine el grupo de consistencia:

```
consistency-group delete -vserver svm_name -consistency-group
consistency_group_name
```

Continuidad del negocio de SnapMirror

Información general sobre la continuidad del negocio de SnapMirror

SnapMirror Business Continuity (SM-BC), también conocido como SnapMirror sincronización activa, permite que los servicios empresariales continúen funcionando incluso si se produce un fallo completo en el sitio, lo que permite que las aplicaciones conmuten por error de forma transparente usando una copia secundaria. No se requiere intervención manual ni secuencias de comandos adicionales para activar una recuperación tras fallos con SM-BC.

SM-BC está disponible a partir de ONTAP 9,8. SM-BC se admite en clústeres AFF o en clústeres de cabinas all-flash de SAN (ASA), donde los clústeres primario y secundario pueden ser AFF o ASA. SM-BC protege las aplicaciones con LUN iSCSI o FCP.

Beneficios

SM-BC ofrece las siguientes ventajas:

- Disponibilidad continua para aplicaciones vitales para el negocio

- Capacidad de alojar aplicaciones críticas alternativamente desde la ubicación principal y la secundaria
- Gestión de aplicaciones simplificada usando grupos de consistencia para mantener la coherencia de los pedidos de escritura dependiente
- La capacidad de probar la recuperación tras fallos para cada aplicación
- Creación instantánea de clones duplicados sin afectar a la disponibilidad de las aplicaciones
- A partir de ONTAP 9.11.1, SM-BC admite SnapRestore de archivo único.
- A partir de ONTAP 9.14.1, SM-BC es compatible con los clústeres de conmutación al nodo de respaldo de Windows y "Reservas persistentes de SCSI 3", mejorando la alta disponibilidad.

Casos de uso

Puesta en marcha de aplicaciones para objeto de tiempo de recuperación cero (RTO)

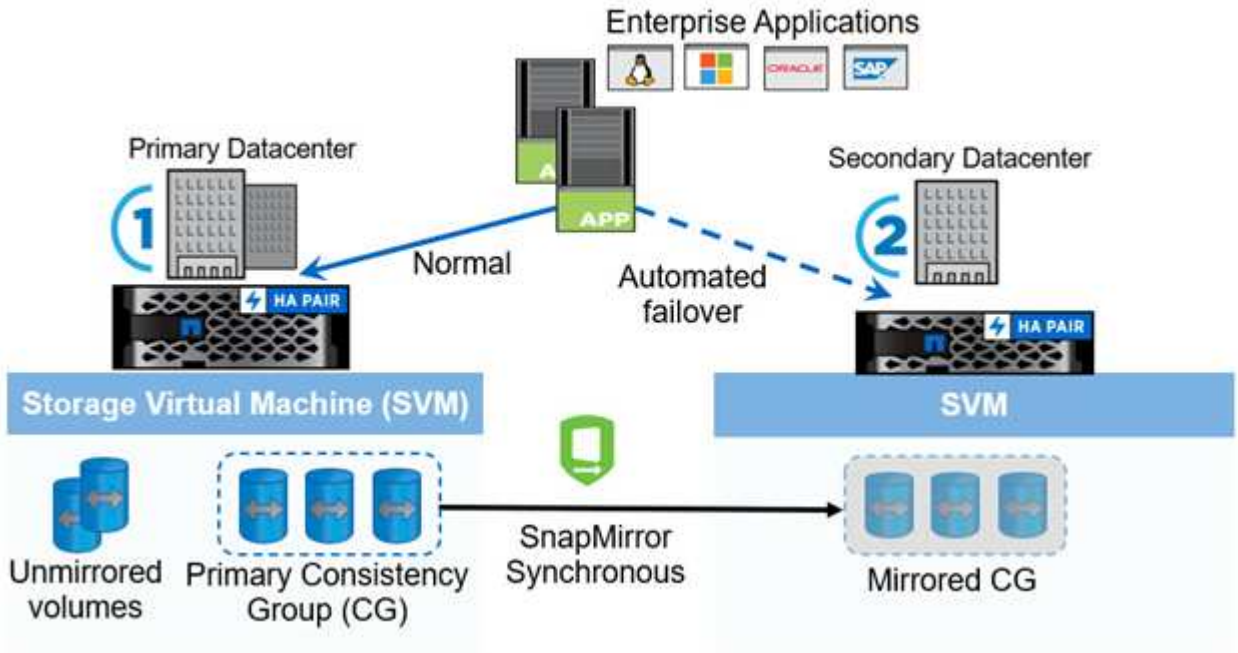
En una implementación de SM-BC, tendrá un clúster primario y secundario. Una LUN en el clúster primario `1LP`) tendrá un espejo (`L1s`) En el volumen secundario; ambas LUN comparten el mismo ID de serie y se notifican como LUN de lectura y escritura en el host. Sin embargo, las operaciones de lectura y escritura solo se realizan en la LUN principal, `1LP`. Cualquier escritura en el reflejo `L1S` son servidas por proxy.

Situación de desastre

Con SM-BC, puede replicar de forma síncrona varios volúmenes para una aplicación entre sitios en ubicaciones geográficamente dispersas. Puede conmutar automáticamente por respaldo a la copia secundaria en caso de interrupción del almacenamiento primario, con lo que se permite la continuidad del negocio para aplicaciones de nivel uno.

Arquitectura

La siguiente figura muestra el funcionamiento de la función de continuidad de negocio de SnapMirror a grandes rasgos.



En la sección uno del diagrama, se pone en marcha una aplicación en una SVM del centro de datos principal. Los volúmenes que se han añadido al grupo de coherencia primario están protegidos con SM-BC y se reflejan

en un grupo de coherencia secundario en un centro de datos secundario. Los volúmenes del grupo de coherencia primario se conmutarán al nodo de respaldo al grupo de coherencia reflejado en caso de interrupción. Los volúmenes que no están en un grupo de consistencia reflejada no se proporcionan en caso de conmutación al nodo de respaldo.

Más información

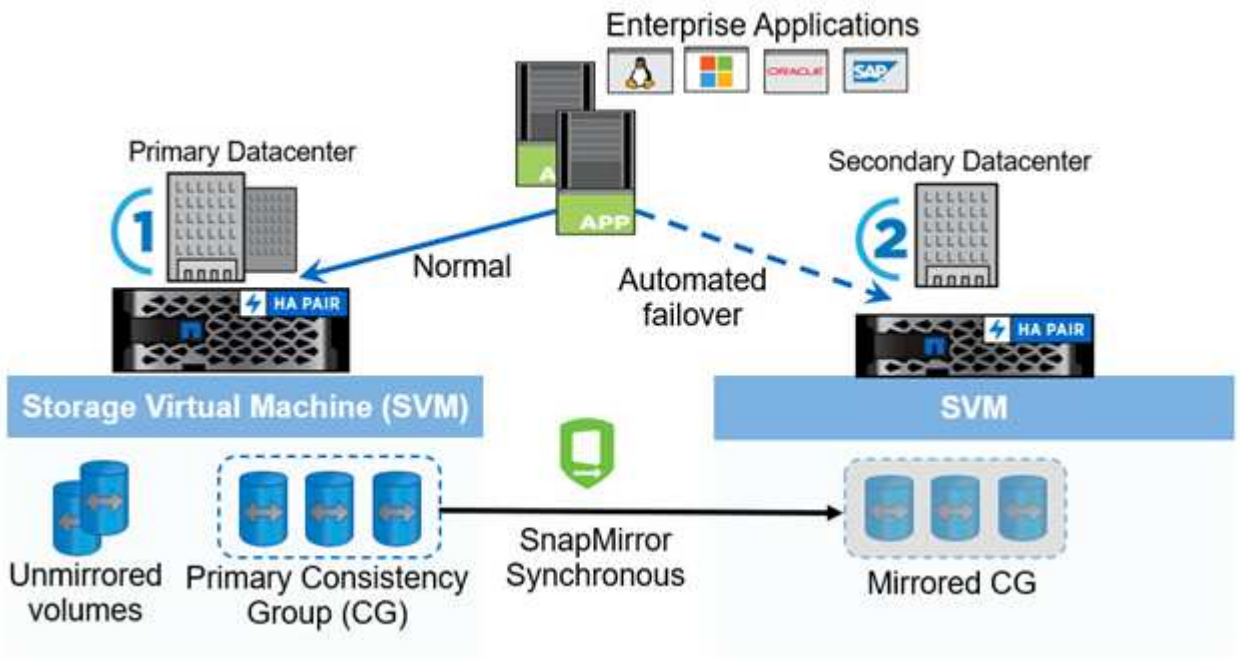
- "TR-4878: Continuidad del negocio de SnapMirror"

Conceptos clave

La continuidad del negocio de SnapMirror (SM-BC) utiliza funciones tales como grupos de consistencia y el mediador de ONTAP para garantizar que sus datos se repliquen y se sirvan incluso en caso de desastre. A la hora de planificar la implementación de SM-BC, es importante comprender los conceptos básicos de SM-BC y su arquitectura.

Arquitectura

En la siguiente figura se muestra una descripción general de la implementación de SM-BC.



El diagrama muestra una aplicación empresarial alojada en una máquina virtual de almacenamiento (SVM) en el centro de datos principal. La SVM contiene cinco volúmenes, tres de los cuales forman parte de un grupo de coherencia. Los tres volúmenes del grupo de coherencia se reflejan en un centro de datos secundario. En circunstancias normales, todas las operaciones de escritura se realizan en el centro de datos primario; en efecto, este centro de datos sirve como origen de operaciones de I/O, mientras que el centro de datos secundario sirve como destino.

En caso de que se produzca un desastre en el centro de datos primario, ONTAP Mediator dirigirá al centro de datos secundario para que actúe como primario y sirva todas las operaciones de I/O. Solo se servirá los volúmenes reflejados en el grupo de coherencia. Cualquier operación que pertenezca a los otros dos volúmenes en la SVM se verá afectada por el evento de desastre.

Conceptos esenciales

Comprender los siguientes términos le ayudará a implementar SM-BC.

Grupo de consistencia

Un grupo de coherencia es una colección de volúmenes o LUN que proporcionan una garantía de coherencia en orden de escritura para la carga de trabajo de la aplicación que debe protegerse para la continuidad del negocio. Un grupo de consistencia garantiza que todos los volúmenes de este conjunto de datos se pongan en modo inactivo y, a continuación, se snappean en el mismo momento específico, lo que proporciona un punto de restauración coherente con los datos en todos los volúmenes para ese conjunto de datos.

En SM-BC, creará un grupo de consistencia principal y secundario para la replicación y la protección de datos. El grupo de consistencia secundario servirá sus datos en caso de interrupción.

Para obtener más información sobre los grupos de consistencia, consulte "Información general sobre los grupos de consistencia".

Componente

Un volumen o LUN individual que forma parte de un grupo de coherencia, que está protegido por la relación de SM-BC.

Mediador ONTAP

Los mediadores de ONTAP supervisan los dos clústeres ONTAP y orquestan la conmutación por error en caso de que se produzca un error en el sistema de almacenamiento principal. Con Mediador de ONTAP, su aplicación se vuelve a conectar automáticamente con los recursos del sistema de almacenamiento secundario.

Con la información de estado de ONTAP Mediator, los clústeres pueden diferenciar entre fallos de LIF entre clústeres y fallos del sitio. Cuando el sitio falla, ONTAP Mediator transmite la información de estado al clúster del mismo nivel bajo demanda, lo que facilita el clúster del mismo nivel a la conmutación por error.

Obtenga más información sobre la "Mediador ONTAP".

Conmutación al respaldo planificada

Operación manual para cambiar los roles de las copias en una relación SM-BC. Los sitios primarios se convierten en los secundarios y los secundarios se convierten en los primarios.

Conmutación automática al respaldo no planificada (AUFO)

Una operación automática para ejecutar una conmutación por error a la copia de mirroring. La operación requiere ayuda de Mediator para detectar que la copia primaria no está disponible.

Fuera de sincronización (OOS)

Cuando las operaciones de I/O de aplicaciones no se replican en el sistema de almacenamiento secundario, se informará como **fuera de sincronización**. Un estado fuera de sincronización significa que los volúmenes secundarios no se sincronizan con el primario (origen) y que no se está produciendo la replicación de SnapMirror.

Si el estado de reflejo es `Snapmirrored`, esto indica un error de transferencia o un fallo debido a una operación no soportada.

RPO cero

RPO es la sigla en inglés para el objetivo de punto de recuperación, que es la cantidad de pérdida de datos que se considera aceptable durante un período de tiempo dado. El RPO de cero significa que no es aceptable ninguna pérdida de datos.

RTO CERO

El objetivo de tiempo de recuperación es el objetivo de tiempo de recuperación, que es la cantidad de tiempo que se considera aceptable para que una aplicación regrese a las operaciones normales tras una interrupción del servicio, un fallo u otro evento de pérdida de datos. El objetivo de tiempo de recuperación cero significa que no se acepta ningún tiempo de inactividad.

Planificación

Requisitos previos

Cuando planifique la puesta en marcha de continuidad del negocio de SnapMirror, asegúrese de haber cumplido los distintos requisitos de configuración de hardware, software y sistema.

Hardware subyacente

- Solo se admiten clústeres de alta disponibilidad de dos nodos
- Ambos clústeres deben ser AFF (incluido AFF C-Series) o ASA (sin combinación)

De NetApp

- ONTAP 9,8 o posterior
- Mediador ONTAP 1.2 o posterior
- Un servidor Linux o máquina virtual para el Mediador ONTAP que ejecuta uno de los siguientes:

Versión de ONTAP Mediator	Versiones de Linux compatibles
1,7	• Red Hat Enterprise Linux: 8,5, 8,6, 8,7, 8,8, 8,9, 9,0, 9,1, 9,2 y 9,3 • Rocky Linux 8 y 9
1,6	• Red Hat Enterprise Linux: 8,4, 8,5, 8,6, 8,7, 8,8, 9,0, 9,1, 9,2 • Rocky Linux 8 y 9
1,5	• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1 8.2, 8.3, 8.4, 8.5 • CentOS: 7.6, 7.7, 7.8, 7.9
1,4	• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1 8.2, 8.3, 8.4, 8.5 • CentOS: 7.6, 7.7, 7.8, 7.9
1,3	• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1 8.2, 8.3 • CentOS: 7.6, 7.7, 7.8, 7.9
1,2	• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 8.1 • CentOS: 7.6, 7.7, 7.8

Licencia

- Debe aplicarse la licencia síncrona de SnapMirror (SM-S) en ambos clústeres
- Debe aplicarse la licencia de SnapMirror en ambos clústeres

> Si sus sistemas de almacenamiento de ONTAP se adquirieron antes de junio de 2019, consulte "Claves de licencia maestra de ONTAP de NetApp" Para obtener la licencia SM-S necesaria.

Las licencias de SnapMirror Synchronous y SnapMirror Synchronous se incluyen en "ONTAP One".

Entorno de red

- El tiempo de ida y vuelta (RTT) de latencia entre clústeres debe ser inferior a 10 milisegundos.
- Las reservas persistentes SCSI-3 son **no** compatibles con SM-BC.

Protocolos compatibles

- Solo son compatibles los protocolos SAN (no NFS/SMB).
- Solo se admiten los protocolos Fibre Channel e iSCSI.
- El espacio IP predeterminado es necesario por SM-BC para las relaciones de paridad de clústeres. No se admite el espacio IP personalizado.

Estilo de seguridad NTFS

El estilo de seguridad NTFS **no** se admite en volúmenes SM-BC.

Mediador ONTAP

- El mediador ONTAP se aprovisiona externamente y se conecta a ONTAP para una recuperación transparente tras fallos de aplicaciones.
- Para que funcione completamente y habilitar la conmutación automática al respaldo no planificada, el mediador externo ONTAP se debería aprovisionar y configurar con clústeres de ONTAP.
- ONTAP Mediator debe instalarse en un tercer dominio de fallo, independiente de los dos clústeres de ONTAP.
- Al instalar el Mediador ONTAP, debe sustituir el certificado autofirmado por un certificado válido firmado por una CA confiable convencional.
- Para obtener más información sobre el Mediador ONTAP, consulte "Prepare la instalación del servicio Mediador ONTAP".

Volúmenes de destino de lectura y escritura

- No se admiten las relaciones de SM-BC en los volúmenes de destino de lectura/escritura. Para poder usar un volumen de lectura/escritura, debe convertirlo en un volumen de DP. Para ello, cree una relación de SnapMirror en el nivel de volumen y elimine la relación. Para obtener más información, consulte "Conversión de relaciones existentes a relaciones SM-BC"

Grandes LUN y grandes volúmenes

La compatibilidad con LUN de gran tamaño y volúmenes de gran tamaño (más de 100 TB) depende de la versión de ONTAP que utilice y de su plataforma.

ONTAP 9.12.1P2 y posterior

- Para ONTAP 9.12.1 P2 y versiones posteriores, SMBC admite LUN grandes y volúmenes grandes mayores de 100TB en ASA y AFF (incluido C-Series).

> Para las versiones 9.12.1P2 de ONTAP y versiones posteriores, debe asegurarse de que los clústeres primario y secundario sean cabinas All Flash SAN o cabina All Flash, y que ambos tengan instalado ONTAP 9.12.1 P2 o una versión posterior. Si el clúster secundario ejecuta una versión anterior a ONTAP 9.12.1P2, o si el tipo de cabina no es el mismo que el clúster primario, la relación síncrona puede desincronizarse si el volumen primario crece más de 100 TB.

ONTAP 9,8 - 9.12.1P1

- Para las versiones de ONTAP entre ONTAP 9,8 y 9.12.1 P1 (inclusive), las cabinas SAN all-flash solo admiten LUN de gran tamaño y volúmenes grandes superiores a 100TB TB.

> Para versiones de ONTAP entre ONTAP 9,8 y 9.12.1 P2, debe asegurarse de que los clústeres primario y secundario sean cabinas all-flash SAN, y que ambos tengan ONTAP 9,8 o una versión posterior instalada. Si el clúster secundario ejecuta una versión anterior a ONTAP 9,8, o si no es una cabina all-flash SAN, la relación síncrona puede desincronizarse si el volumen primario crece más de 100 TB.

Más información

- "Hardware Universe"
- "Descripción general de ONTAP Mediator"

Configuraciones y funciones compatibles

SnapMirror Business Continuity es compatible con numerosos sistemas operativos y otras funciones incluidas en ONTAP. Obtenga información sobre detalles y configuraciones recomendadas.

Configuraciones admitidas

SM-BC es compatible con numerosos sistemas operativos, incluyendo:

- AIX (a partir de ONTAP 9.11.1)
- HP-UX (a partir de ONTAP 9.10.1)
- Solaris 11,4 (a partir de ONTAP 9.10.1)

AIX

A partir de ONTAP 9.11.1, AIX es compatible con SM-BC. Con una configuración AIX, el clúster primario es el clúster "activo".

En una configuración AIX, las recuperaciones tras fallos son disruptivas. Con cada conmutación al nodo de respaldo, deberá realizar un nuevo análisis en el host para que se reanuden las operaciones de I/O.

Para configurar un host AIX con SM-BC, consulte el artículo de la base de conocimientos "Cómo configurar un

host AIX para la continuidad del negocio de SnapMirror (SM-BC)".

HP-UX

A partir de ONTAP 9.10.1, se admite SM-BC para HP-UX.

Limitaciones de HP-UX

Un evento de failover no planificado automático (AUFO) en el cluster maestro aislado puede deberse a un fallo de evento doble cuando se pierde la conexión entre el cluster primario y el secundario y también se pierde la conexión entre el cluster primario y el mediador. Esto se considera un evento raro, a diferencia de otros eventos de AUFO.

- En este escenario, podría tardar más de 120 segundos en reanudarse la E/S en el host HP-UX. En función de las aplicaciones que se estén ejecutando, esto puede no provocar ninguna interrupción de I/o o o mensajes de error.
- Para remediar, debe reiniciar las aplicaciones en el host de HP-UX que tengan una tolerancia de interrupción inferior a 120 segundos.

Recomendación de configuración de host de Solaris

A partir de ONTAP 9.10.1, SM-BC admite Solaris 11.4.

Para garantizar que las aplicaciones cliente de Solaris no son disruptivas cuando se produce una conmutación por error de sitio no planificada en un entorno SM-BC, modifique la configuración predeterminada del sistema operativo Solaris. Para configurar Solaris con la configuración recomendada, consulte el artículo de la base de conocimientos "Ajustes recomendados para el soporte de host Solaris en la configuración de continuidad empresarial de SnapMirror (SM-BC)".

Clustering de conmutación al nodo de respaldo de Windows

A partir de ONTAP 9.14.1, SM-BC es compatible con los clústeres de conmutación por error de Windows. Para obtener más información, consulte "TR-4878: Continuidad del negocio de SnapMirror".

Integraciones de ONTAP

SM-BC ofrece compatibilidad con otras funciones de ONTAP, como:

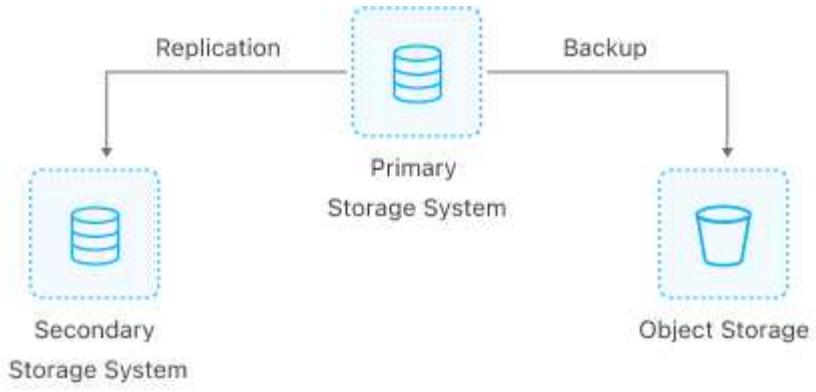
- Configuraciones de dispersión
- Copia NDMP (a partir de ONTAP 9.13.1)
- Restauración parcial de archivos (a partir de ONTAP 9.12.1)

FabricPool

SM-BC admite los volúmenes de origen y destino en agregados de FabricPool con la política de organización en niveles: Ninguno, Snapshot o Automático. SM-S SM-BC no es compatible con agregados FabricPool utilizando una política de organización en niveles de todos.

Configuraciones de dispersión

En una configuraciones de dispersión, Su volumen de origen se puede duplicar en un extremo de destino de SM-BC y en una o más relaciones asíncronas de SnapMirror.



Soportes SM-BC configuraciones de dispersión con la `MirrorAllSnapshots` Política y, a partir de ONTAP 9.11.1, el `MirrorAndVault` política. SM-BC no admite configuraciones de salida de ventilador con el `XDPDefault` política.

Si experimenta una conmutación al nodo de respaldo en el destino de SM-BC en una configuración de dispersión, deberá hacerlo de forma manual reanude la protección en la configuración de fan-out.

Restauración de NDMP

A partir de ONTAP 9.13.1, se puede usar NDMP para copiar y restaurar datos con SM-BC. El uso de NDMP permite mover datos a la fuente SM-BC para realizar una restauración sin pausar la protección. Esto resulta especialmente útil en configuraciones ramificadas.

Para obtener más información sobre este proceso, consulte Transferencia de datos mediante la copia ndmp.

Restauración parcial de archivos

A partir de ONTAP 9.12.1, se admite una restauración de LUN parcial para los volúmenes de SM-BC. Para obtener información sobre este proceso, consulte "Restaurar parte de un archivo desde una copia snapshot".

Límites de objetos para la continuidad del negocio de SnapMirror

Cuando se prepare para utilizar y gestionar SnapMirror Business Continuity, tenga en cuenta las siguientes limitaciones.

Grupos de consistencia en un clúster

Los límites de los grupos de consistencia para un clúster con SM-BC se calculan en función de las relaciones y dependen de la versión de ONTAP utilizada. Los límites son independientes de la plataforma.

Versión de ONTAP	Número máximo de relaciones
ONTAP 9,8-9.9.1	5
ONTAP 9.10.1	20
ONTAP 9.11.1 y versiones posteriores	50

Volúmenes por grupo de coherencia

El número máximo de volúmenes por grupo de coherencia con SM-BC es independiente de la plataforma.

Versión de ONTAP	Cantidad máxima de volúmenes admitidos en una relación de grupo de consistencia
ONTAP 9,8-9.9.1	12
ONTAP 9.10.1 y posteriores	16

Volúmenes

Los límites de volumen en SM-BC se calculan en función del número de puntos finales, no del número de relaciones. Un grupo de consistencia con 12 volúmenes contribuye con 12 extremos en el clúster primario y secundario. Tanto las relaciones de SM-BC como de SnapMirror Synchronous contribuyen al número total de extremos.

En la siguiente tabla se incluyen los puntos finales máximos por plataforma.

S. No	Plataforma	Extremos por ha para SM-BC			Sincronización general y extremos SM-BC por alta disponibilidad		
		ONTAP 9,8-9.9.1	ONTAP 9.10.1	ONTAP 9.11.1 y versiones posteriores	ONTAP 9,8-9.9.1	ONTAP 9.10.1	ONTAP 9.11.1 y versiones posteriores
1	AFF	60	200	400	80	200	400
2	ASA	60	200	400	80	200	400

Límites DE objetos DE SAN

En la siguiente tabla se incluyen los límites de objetos SAN. Los límites se aplican independientemente de la plataforma.

Objeto en una relación SM-BC	Cuente
LUN por volumen	256
Mapas de LUN por nodo	• 4096 (ONTAP 9,10 y posterior) • 2048 (ONTAP 9.9.1 y anterior)
Mapas de LUN por clúster	• 8192 (ONTAP 9,10 y posterior) • 4096 (ONTAP 9.9.1 y anterior)
LIF por SVM (con al menos un volumen en una relación SM-BC)	256
LIF entre clústeres por nodo	4
LIF entre clústeres por clúster	8

Información relacionada

- "Hardware Universe"
- "Límites del grupo de consistencia"

Instalar y configurar

Configurar el mediador de ONTAP y los clústeres para la continuidad del negocio con SnapMirror

SnapMirror Business Continuity (SM-BC) utiliza clústeres con conexión entre iguales para garantizar que los datos están disponibles en caso de conmutación por error. ONTAP Mediator es un recurso clave que garantiza la continuidad del negocio y supervisa el estado de cada clúster. Para configurar SM-BC, primero debe instalar ONTAP Mediator y asegurarse de que los clústeres primario y secundario están configurados correctamente.

Una vez que haya instalado ONTAP Mediator y configurado los clústeres, debe hacerlo [initialize-the-ontap-mediator] Mediador ONTAP para uso con SM-BC. Entonces debe hacerlo Cree, inicialice y asigne el grupo de consistencia para SM-BC

Mediador ONTAP

El Mediador ONTAP establece un quórum para los clústeres de ONTAP en una relación de SM-BC. Coordina la conmutación automática al nodo de respaldo cuando se detecta un fallo, al determinar qué clúster actúa como principal y garantizar que se sirven los datos a y desde el destino correcto.

Requisitos previos para el Mediador ONTAP

- El Mediador ONTAP incluye su propio conjunto de requisitos previos. Debe cumplir con estos requisitos previos antes de instalar el mediador.

  Para obtener más información, consulte "Prepare la instalación del servicio Mediador ONTAP".

- De forma predeterminada, el Mediador ONTAP proporciona servicio a través del puerto TCP 31784. Debe asegurarse de que el puerto 31784 esté abierto y disponible entre los clústeres de ONTAP y el mediador.

Instale ONTAP Mediator y confirme la configuración del cluster

Continúe con cada uno de los pasos siguientes. Para cada paso, debe confirmar que se ha realizado la configuración específica. Utilice el enlace que se incluye después de cada paso para obtener más información según sea necesario.

Pasos

1. Instale el servicio Mediator de ONTAP antes de asegurarse de que los clústeres de origen y destino están configurados correctamente.

   Prepárese para instalar o actualizar el servicio de Mediador de ONTAP

2. Confirme que existe una relación de paridad entre los clústeres.

   > El espacio IP predeterminado es necesario por SM-BC para las relaciones de paridad de clústeres. No se admite un espacio IP personalizado.

   Configure las relaciones de paridad

3. Confirmar que las máquinas virtuales de almacenamiento se crean en cada clúster.

   Creación de una SVM

4. Confirmar que existe una relación entre iguales entre las máquinas virtuales de almacenamiento en cada clúster.

   Creación de una relación de paridad de SVM

5. Confirme que los volúmenes existen para sus LUN.

   Creación de un volumen

6. Confirmar que se crea al menos un LIF SAN en cada nodo del clúster.

   "Consideraciones para los LIF en un entorno SAN de clúster"

   "Crear una LIF"

7. Confirmar que las LUN necesarias se crean y asignan a un igroup, que se utiliza para asignar las LUN al iniciador en el host de la aplicación.

   Cree LUN y asigne iGroups

8. Vuelva a analizar el host de la aplicación para detectar todos los LUN nuevos.

Inicialice el mediador ONTAP para SM-BC

Una vez que haya instalado ONTAP Mediator y confirmado la configuración del clúster, debe inicializar ONTAP Mediator para la supervisión del clúster. Puede inicializar ONTAP Mediator mediante System Manager o la CLI de ONTAP.

System Manager

Con System Manager, puede configurar el servidor ONTAP Mediator para una conmutación automática al respaldo. También puede reemplazar SSL y CA autofirmados por el certificado SSL y CA validados de terceros si aún no lo ha hecho.

Pasos

1. Vaya a **Protección > Descripción general > Mediador > Configurar**.
2. Seleccione **Agregar** e introduzca la siguiente información del servidor de ONTAP Mediator:
   - Dirección IPv4
   - Nombre de usuario
   - Contraseña
   - Certificado

CLI

Puede inicializar el mediador de ONTAP desde el clúster primario o secundario mediante la CLI de ONTAP. Cuando emita el `mediator add` Comando en un clúster, el Mediador ONTAP se agrega automáticamente al otro clúster.

Pasos

1. Inicialice Mediator en uno de los grupos:

   ```
   snapmirror mediator add -mediator-address IP_Address -peer-cluster
   cluster_name -username user_name
   ```

   ejemplo

   ```
   cluster1::> snapmirror mediator add -mediator-address 192.168.10.1
   -peer-cluster cluster2 -username mediatoradmin
   Notice: Enter the mediator password.

   Enter the password: ******
   Enter the password again: ******
   ```

2. Compruebe el estado de la configuración del Mediator:

   ```
   snapmirror mediator show
   ```

   ```
   Mediator Address Peer Cluster     Connection Status Quorum Status
   ---------------- ---------------- ----------------- -------------
   192.168.10.1     cluster-2        connected         true
   ```

   `Quorum Status` Indica si las relaciones del grupo de coherencia SnapMirror se sincronizan con el mediador, un estado de `true` indica una sincronización correcta.

Protección con SnapMirror Business Continuity

La configuración de la protección mediante SnapMirror Business Continuity implica seleccionar las LUN en el clúster de origen de ONTAP y añadirlas a un grupo de consistencia.

Antes de empezar

- Debe tener un "Licencia de SnapMirror Synchronous".
- Debe ser un administrador de clústeres o máquinas virtuales de almacenamiento.
- Todos los volúmenes constituyentes de un grupo de coherencia deben estar en una única máquina virtual de almacenamiento (SVM).
  - Los LUN pueden residir en distintos volúmenes.
- Los clústeres de origen y destino no pueden ser los mismos.
- No es posible establecer relaciones de grupos de consistencia SM-BC entre clústeres de ASA y clústeres no-ASA.
- El espacio IP predeterminado es necesario por SM-BC para las relaciones de paridad de clústeres. No se admite el espacio IP personalizado.
- El nombre del grupo de coherencia debe ser único.
- Los volúmenes en el clúster secundario (de destino) deben ser del tipo DP.
- Las SVM principales y secundarias deben estar en una relación entre iguales.

Pasos

Puede configurar un grupo de coherencia con la CLI de ONTAP o System Manager.

A partir de ONTAP 9.10.1, ONTAP ofrece un extremo y un menú de grupo de consistencia en System Manager, y ofrece utilidades de gestión adicionales. Si utiliza ONTAP 9.10.1 o posterior, consulte "Configurar un grupo de consistencia" a continuación "configure la protección" Para crear una relación SM-BC.

System Manager

1. En el clúster principal, navegue hasta **Protección > Descripción general > Proteger para continuidad empresarial > Proteger LUN**.
2. Seleccione las LUN que desea proteger y añádalas a un grupo de protección.
3. Seleccione el clúster y la SVM de destino.
4. **La opción inicializar relación** está seleccionada de forma predeterminada. Haga clic en **Guardar** para comenzar la protección.
5. Vaya a **Consola > rendimiento** para verificar la actividad de IOPS de las LUN.
6. En el clúster de destino, utilice System Manager para comprobar que la protección de la relación de continuidad de negocio está sincronizada: **Protección > Relaciones**.

CLI

1. Cree una relación de grupo de coherencia a partir del clúster de destino.
   `destination::> snapmirror create -source-path *source-path* -destination-path *destination-path* -cg-item -maps *volume-paths* -policy *policy-name*

   Puede asignar hasta 12 volúmenes constituyentes mediante el `cg-item-mappings` parámetro en la `snapmirror create` comando.

   El siguiente ejemplo crea dos grupos de consistencia: `cg_src_ on the source with `vol1` y.. `vol2` y un grupo de consistencia de destino de mirroring, `cg_dst`.

   ```
   destination::> snapmirror create -source-path vs1_src:/cg/cg_src
   -destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
   vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy AutomatedFailOver
   ```

2. Desde el clúster de destino, inicialice el grupo de coherencia.

   ```
   destination::>snapmirror initialize -destination-path destination-
   consistency-group
   ```

3. Confirme que la operación de inicialización se ha realizado correctamente. El estado debe ser `InSync`.

   ```
   snapmirror show
   ```

4. En cada clúster, cree un igroup para poder asignar las LUN al iniciador en el host de la aplicación.
   `lun igroup create -igroup *name* -protocol *fcp|iscsi* -ostype *os* -initiator *initiator_name*`
5. En cada clúster, asigne las LUN al igroup:

   ```
   lun map -path path_name -igroup igroup_name
   ```

6. Compruebe que la asignación de LUN se ha completado correctamente con el `lun map` comando. Luego, puede detectar las nuevas LUN en el host de la aplicación.

Gestión de SM-BC y protección de los datos

Cree una copia Snapshot común

Además de las operaciones de copia de Snapshot programadas regularmente, puede crear un común de forma manual "Copia Snapshot" Entre los volúmenes del grupo de coherencia de SnapMirror primario y los volúmenes en el grupo de coherencia de SnapMirror secundario.

Acerca de esta tarea

- En ONTAP 9.8, el intervalo de creación de snapshot programado es de una hora.

  A partir de ONTAP 9.9.1, ese intervalo es de 12 horas.

Antes de empezar

- La relación de grupo SnapMirror debe estar sincronizada.

Pasos

1. Cree una copia Snapshot común:

   ```
   destination::>snapmirror update -destination-path vs1_dst:/cg/cg_dst
   ```

2. Supervise el progreso de la actualización:

   ```
   destination::>snapmirror show -fields -newest-snapshot
   ```

Realizar una conmutación al respaldo planificada

En una conmutación al respaldo planificada, debe cambiar los roles de los clústeres primario y secundario, de modo que el clúster secundario asuma el control del clúster principal. Durante una conmutación por error, lo que normalmente funciona el clúster secundario procesa las solicitudes de entrada y salida localmente sin interrumpir las operaciones del cliente.

Quizás desee realizar una conmutación al respaldo planificada para probar el estado de la configuración de recuperación de desastres o realizar tareas de mantenimiento del clúster principal.

Acerca de esta tarea

El administrador del clúster secundario inicia una conmutación al respaldo planificada. La operación requiere cambiar los roles primario y secundario de manera que el clúster secundario asuma el control del primario. Después, el nuevo clúster principal puede comenzar a procesar solicitudes de entrada y salida de forma local sin interrumpir las operaciones del cliente.

Antes de empezar

- La relación SM-BC debe estar sincronizada.
- No puede iniciar una conmutación al respaldo planificada cuando hay una operación no disruptiva en proceso. Las operaciones no disruptivas incluyen movimientos de volúmenes, reubicaciones de agregaciones y recuperación tras fallos de almacenamiento.
- El mediador ONTAP debe estar configurado, conectado y en quórum.

Pasos

Puede realizar una conmutación al respaldo planificada con la interfaz de línea de comandos de ONTAP o System Manager.

System Manager

1. En System Manager, seleccione **Protección > Descripción general > Relaciones**.
2. Identifique la relación de SM-BC que desea conmutar al nodo de respaldo. Junto a su nombre, seleccione la … Junto al nombre de la relación, luego seleccione **Failover**.
3. Para supervisar el estado de la conmutación por error, utilice `snapmirror failover show` En la CLI de ONTAP.

CLI

1. Desde el clúster de destino, inicie la operación de conmutación por error:

   ```
   destination::>snapmirror failover start -destination-path
   vs1_dst:/cg/cg_dst
   ```

2. Supervise el progreso de la conmutación por error:

   ```
   destination::>snapmirror failover show
   ```

3. Una vez finalizada la operación de conmutación por error, puede supervisar el estado de la relación de protección de SnapMirror síncrono desde el destino:

   ```
   destination::>snapmirror show
   ```

Recuperarse de operaciones de conmutación al respaldo automáticas no planificadas

Una operación de conmutación por error no planificada automática (AUFO) se produce cuando el clúster primario está inactivo o aislado. El mediador ONTAP detecta cuándo se produce una conmutación por error y ejecuta una conmutación por error automática no planificada en el clúster secundario. El clúster secundario se convierte al principal y comienza a prestar servicio a los clientes. Esta operación se realiza sólo con la ayuda del Mediador ONTAP.

> Después de la conmutación automática al respaldo no planificada, es importante volver a analizar las rutas de I/o del LUN del host para que no se pierda las rutas de I/O.

Restablecer la relación de protección tras una conmutación al respaldo no planificada

Puede volver a establecer la relación de protección mediante System Manager o la CLI de ONTAP.

System Manager

Pasos

1. Vaya a **Protección > Relaciones** y espere a que el estado de la relación muestre “InSync”.
2. Para reanudar las operaciones en el clúster de origen original, haga clic en ⋮ Y seleccione **Failover**.

CLI

Puede supervisar el estado de la conmutación automática al respaldo no planificada mediante `snapmirror failover show` comando.

Por ejemplo:

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
         Source Path: vs1:/cg/scg3
    Destination Path: vs3:/cg/dcg3
     Failover Status: completed
        Error Reason:
            End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
       Failover Type: unplanned
  Error Reason codes: -
```

Consulte la "Referencia EMS" para obtener más información acerca de los mensajes de eventos y las acciones correctivas.

Reanude la protección en una configuración ramificada después de una conmutación al nodo de respaldo

Si experimenta una conmutación al respaldo en el clúster secundario en la relación de SM-BC, el destino asíncrono de SnapMirror queda en mal estado. Debe restaurar manualmente la protección eliminando y volviendo a crear la relación con el extremo asíncrono de SnapMirror.

Pasos

1. Compruebe que la conmutación por error se ha realizado correctamente:
   `snapmirror failover show`
2. En el extremo asíncrono de SnapMirror, elimine el extremo de dispersión:
   `snapmirror delete -destination-path` *`destination_path`*
3. En el tercer sitio, cree una relación asíncrona de SnapMirror entre el nuevo volumen primario de SM-BC y el volumen de destino de dispersión asíncrono:
   `snapmirror create -source-path` *`source_path`* `-destination-path` *`destination_path`* `-policy MirrorAllSnapshots -schedule` *`schedule`*
4. Resincronice la relación:
   `snapmirror resync -destination-path` *`destination_path`*
5. Verifique el estado y el estado de la relación:
   `snapmirror show`

Supervisar las operaciones de continuidad del negocio de SnapMirror

Puede supervisar las siguientes operaciones de continuidad del negocio de SnapMirror (SM-BC) para garantizar el estado de la configuración de SM-BC:

- Mediador ONTAP
- Operaciones de conmutación por error planificadas
- Operaciones automáticas de conmutación al respaldo no planificadas
- Disponibilidad de SM-BC

Mediador ONTAP

Durante las operaciones normales, el estado Mediador de ONTAP debe estar conectado. Si está en cualquier otro estado, esto puede indicar una condición de error. Puede revisar el "Mensajes del sistema de gestión de eventos (EMS)" para determinar el error y las acciones correctivas apropiadas.

Operaciones de conmutación por error planificadas

Puede supervisar el estado y el progreso de una operación de conmutación al nodo de respaldo planificada mediante el `snapmirror failover show` comando. Por ejemplo:

```
ClusterB::> snapmirror failover start -destination-path vs1:/cg/dcg1
```

Una vez finalizada la operación de conmutación al nodo de respaldo, puede supervisar el estado de protección de SnapMirror síncrono desde el nuevo clúster de destino. Por ejemplo:

```
ClusterA::> snapmirror show
```

Consulte la "Referencia EMS" para obtener más información acerca de los mensajes de eventos y las acciones correctivas.

Operaciones automáticas de conmutación al respaldo no planificadas

Durante una conmutación al respaldo automática no planificada, puede supervisar el estado de la operación mediante el `snapmirror failover show` comando.

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
         Source Path: vs1:/cg/scg3
    Destination Path: vs3:/cg/dcg3
     Failover Status: completed
        Error Reason:
            End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
       Failover Type: unplanned
  Error Reason codes: -
```

Consulte la "Referencia EMS" para obtener más información acerca de los mensajes de eventos y las acciones correctivas.

Disponibilidad de SM-BC

Puede comprobar la disponibilidad de la relación SM-BC mediante una serie de comandos, ya sea en el clúster principal, el clúster secundario o ambos.

Entre los comandos que utiliza se incluyen los `snapmirror mediator show` comando en el clúster principal y secundario para comprobar la conexión y el estado de quórum, la `snapmirror show` y la `volume show` comando. Por ejemplo:

```
SMBC_A::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_B           connected         true

SMBC_B::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_A           connected         true

SMBC_B::*> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/cg1 XDP  vs1:/cg/cg1_dp Snapmirrored InSync  -         true    -
vs0:vol1    XDP  vs1:vol1_dp  Snapmirrored InSync    -         true    -
2 entries were displayed.

SMBC_A::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------ -------------- ------------------------ --------------
vs0     vol1   true           false                      Consensus

SMBC_B::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1_dp
vserver volume  is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------- -------------- ------------------------ --------------
vs1     vol1_dp false          true                       No-consensus
```

Añada o quite volúmenes a un grupo de coherencia

A medida que cambian los requisitos de carga de trabajo de la aplicación, es posible que deba añadir o quitar volúmenes de un grupo de coherencia para garantizar la continuidad del negocio. El proceso de añadir y quitar volúmenes en una relación de SM-BC activa depende de la versión de ONTAP que utilice.

En la mayoría de los casos, este es un proceso disruptivo que requiere que se rompa la relación de SnapMirror, se modifique el grupo de consistencia y, a continuación, se reanude la protección. A partir de ONTAP 9.13.1, añadir volúmenes a un grupo de coherencia con una relación de SM-BC activa es una operación no disruptiva.

Acerca de esta tarea

- En ONTAP 9,8 a 9,9.1, es posible añadir o quitar volúmenes a un grupo de consistencia mediante la CLI de ONTAP.
- A partir de ONTAP 9.10.1, se recomienda que los gestione "grupos de consistencia" A través de System Manager o con la API DE REST de ONTAP.

  Si desea cambiar la composición del grupo de coherencia. Para ello, añada o quite un volumen, primero debe eliminar la relación original y, a continuación, volver a crear el grupo de coherencia con la nueva composición.

- A partir de ONTAP 9.13.1, se pueden añadir volúmenes a un grupo de coherencia con una relación de SM-BC activa desde el origen o el destino.

  Eliminar volúmenes es una operación disruptiva. Debe interrumpir la relación de SnapMirror antes de continuar eliminando los volúmenes.

ONTAP 9,8-9.13.0

Antes de empezar

- No puede comenzar a modificar el grupo de consistencia mientras está en la `InSync` estado.
- El volumen de destino debe ser del tipo DP.
- El nuevo volumen que añada para expandir el grupo de coherencia debe tener un par de copias de Snapshot comunes entre los volúmenes de origen y de destino.

Pasos

Los ejemplos que se muestran en dos asignaciones de volúmenes: `vol_src1` ←→ `vol_dst1` y.. `vol_src2` ←→ `vol_dst2`, en una relación de grupo de coherencia entre los puntos finales `vs1_src:/cg/cg_src` y.. `vs1_dst:/cg/cg_dst`.

1. En los clústeres de origen y destino, compruebe que hay una Snapshot común entre los clústeres de origen y destino con el comando `snapshot show -vserver` *`svm_name`* `-volume` *`volume_name`* `-snapshot` *`snapmirror`*

   ```
   source::>snapshot show -vserver vs1_src -volume vol_src3 -snapshot
   snapmirror*

   destination::>snapshot show -vserver vs1_dst -volume vol_dst3 -snapshot
   snapmirror*
   ```

2. Si no existe ninguna copia Snapshot común, cree e inicialice una relación de SnapMirror de FlexVol:

   ```
   destination::>snapmirror initialize -source-path vs1_src:vol_src3
   -destination-path vs1_dst:vol_dst3
   ```

3. Elimine la relación del grupo de consistencia:

   ```
   destination::>snapmirror delete -destination-path vs1_dst:vol_dst3
   ```

4. Libere la relación de SnapMirror de origen y conserve las copias Snapshot comunes:

   ```
   source::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol_dst3
   ```

5. Desasigne las LUN y elimine la relación de grupo de consistencia existente:

   ```
   destination::>lun mapping delete -vserver vs1_dst -path <lun_path> -igroup
   <igroup_name>
   ```

   > Se anula la asignación de las LUN de destino, mientras que las LUN de la copia principal siguen sirviendo la I/o del host

   ```
   destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst

   source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
   -relationship-info-only true
   ```

6. **Si está utilizando ONTAP 9.10.1 a 9.13.0,** elimine y recree y el grupo de consistencia en la fuente

con la composición correcta. Siga los pasos de Eliminar un grupo de consistencia y después Configure un único grupo de consistencia. En ONTAP 9.10.1 y versiones posteriores, debe realizar las operaciones de eliminación y creación en System Manager o con la API DE REST de ONTAP; no existe un procedimiento de la CLI.

Si está utilizando ONTAP 9.8, 9.0 o 9.9.1, vaya al paso siguiente.

7. Cree el nuevo grupo de consistencia en el destino con la nueva composición:

```
destination::>snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings vol_src1:@vol_dst1,
vol_src2:@vol_dst2, vol_src3:@vol_dst3
```

8. Resincronice la relación del grupo de consistencia de objetivo de tiempo de recuperación cero para garantizar que está sincronizada:

```
destination::>snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

9. Reasigne las LUN no asignadas en el paso 5:

```
destination::> lun map -vserver vs1_dst -path lun_path -igroup igroup_name
```

10. Vuelva a analizar las rutas de I/o del LUN del host para restaurar todas las rutas a los LUN.

ONTAP 9.13.1 y versiones posteriores

A partir de ONTAP 9.13.1, es posible añadir volúmenes de forma no disruptiva a un grupo de coherencia con una relación de SM-BC activa. SM-BC admite la adición de volúmenes de origen y destino.

Para obtener detalles sobre cómo añadir volúmenes del grupo de coherencia de origen, consulte Modificar un grupo de consistencia.

Añada un volumen desde el clúster de destino

1. En el clúster de destino, seleccione **Protección** > **Relaciones**.
2. Busque la relación de SM-BC a la que desea añadir volúmenes. Seleccione ⋮ Luego **Expandir**.
3. Seleccione las relaciones de volumen cuyos volúmenes se añadirán al grupo de coherencia
4. Seleccione **Expandir**.

Convertir relaciones existentes en relaciones SM-BC

Si tiene una relación de SnapMirror síncrono entre un clúster de origen y de destino, puede convertirlo en una relación de SM-BC. De este modo, se pueden asociar los volúmenes reflejados a un grupo de coherencia, garantizando un objetivo de punto de recuperación cero en una carga de trabajo de varios volúmenes. Además, puede conservar los snapshots de SnapMirror existentes si necesita revertir a un momento específico antes de establecer la relación SM-BC.

Antes de empezar

- Debe haber una relación de SnapMirror síncrono con un objetivo de punto de recuperación cero entre el clúster primario y el secundario.
- Se deben anular la asignación de todas las LUN del volumen de destino antes de crear la relación de

SnapMirror con objetivo de tiempo de recuperación cero.

- SM-BC solo admite protocolos SAN (no NFS/CIFS). Asegúrese de que no hay ningún componente del grupo de consistencia montado para el acceso NAS.

Acerca de esta tarea

- Debe ser un administrador de clústeres y de SVM en los clústeres principales y secundarios.
- No se puede convertir un objetivo de punto de recuperación de cero en una sincronización de objetivo de tiempo de recuperación de cero cambiando la política de SnapMirror.
- Debe asegurarse de quitar la asignación de las LUN antes de emitir el `snapmirror create` comando.

  Si las LUN existentes en el volumen secundario se asignan y el `AutomatedFailover` la política se configura, la `snapmirror create` desencadenará un error.

Pasos

1. Desde el clúster secundario, realice una actualización de SnapMirror en la relación existente:

   ```
   destination::>snapmirror update -destination-path vs1_dst:vol1
   ```

2. Compruebe que la actualización de SnapMirror se ha realizado correctamente:

   ```
   destination::>snapmirror show
   ```

3. Desactive cada una de las relaciones síncronas de RPO cero:

   ```
   destination::>snapmirror quiesce -destination-path vs1_dst:vol1

   destination::>snapmirror quiesce -destination-path vs1_dst:vol2
   ```

4. Elimine cada una de las relaciones síncronas de RPO cero:

   ```
   destination::>snapmirror delete -destination-path vs1_dst:vol1

   destination::>snapmirror delete -destination-path vs1_dst:vol2
   ```

5. Libere la relación de SnapMirror de origen, pero conserve las copias Snapshot comunes:

   ```
   source::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol1

   source::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol2
   ```

6. Cree un objetivo de tiempo de recuperación cero para grupo relación de SnapMirror síncrono:

   ```
   destination::> snapmirror create -source-path vs1_src:/cg/cg_src -destination
   -path vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy
   AutomatedFailover
   ```

7. Resincronice el grupo de consistencia:

   ```
   destination::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
   ```

8. Vuelva a analizar las rutas de I/o del LUN del host para restaurar todas las rutas a los LUN.

Actualice y revierta ONTAP con SM-BC

La continuidad del negocio con SnapMirror (SM-BC) es compatible a partir de ONTAP 9,8. Actualizar y revertir el clúster de ONTAP tiene implicaciones en su relación SM-BC dependiendo de la versión de ONTAP a la que actualice o revierta.

Actualice ONTAP con SM-BC

Para usar SM-BC, todos los nodos de los clústeres de origen y destino deben ejecutar ONTAP 9,8 o una versión posterior.

Al actualizar ONTAP con relaciones activas de SM-BC, debe utilizar Actualización automatizada no disruptiva (ANDU). El uso de ANDU garantiza que sus relaciones de SM-BC estén sincronizadas y en buen estado durante el proceso de actualización.

No hay pasos de configuración para preparar las implementaciones de SM-BC para las actualizaciones de ONTAP. Sin embargo, se recomienda que antes y después de la actualización, compruebe que:

- Las relaciones de SM-BC están sincronizadas.
- No hay errores relacionados con SnapMirror en el registro de eventos.
- El Mediador está en línea y en buen estado desde ambos clusters.
- Todos los hosts pueden ver todas las rutas correctamente para proteger los LUN.

> Cuando se actualizan clústeres de ONTAP 9,8 o 9.9.1 a ONTAP 9.10.1 y versiones posteriores, ONTAP crea nuevos grupos de consistencia En los clústeres de origen y de destino para las relaciones de SM-BC que se pueden configurar mediante System Manager.

> La `snapmirror quiesce` y.. `snampirror resume` Los comandos no son compatibles con SM-BC.

Vuelva a ONTAP 9.9.1 desde ONTAP 9.10.1

Para revertir las relaciones de la versión 9.10.1 a la 9.9.1, deben eliminarse las relaciones de SM-BC, seguido por la instancia del grupo de consistencia 9.10.1. Los grupos de consistencia con una relación de SM-BC activa no se pueden eliminar. Todos los volúmenes de FlexVol que se hayan actualizado a 9.10.1 asociados previamente con otro contenedor inteligente o aplicación empresarial en la versión 9.9.1 o anterior ya no se asociarán al revertir. Al eliminar grupos de consistencia no se eliminan los volúmenes constituyentes ni las snapshots granulares de volúmenes. Consulte "Eliminar un grupo de consistencia" Para obtener más información sobre esta tarea en ONTAP 9.10.1 y versiones posteriores.

Vuelva a ONTAP 9,7 desde ONTAP 9,8

> SM-BC no es compatible con clústeres mixtos de ONTAP 9.7 y ONTAP 9.8.

Al cambiar de ONTAP 9.8 a ONTAP 9.7, debe tener en cuenta lo siguiente:

- Si el clúster aloja un destino de SM-BC, no se permite revertir a ONTAP 9,7 hasta que se rompa y se elimine la relación.

- Si el clúster aloja un origen de SM-BC, no se permite revertir a ONTAP 9,7 hasta que se libere la relación.
- Todas las políticas personalizadas de SM-BC SnapMirror creadas por el usuario deben eliminarse antes de revertir a ONTAP 9.7.

Para cumplir estos requisitos, consulte "Quitar una configuración de SM-BC".

Pasos

1. Realice una comprobación de reversión desde uno de los clústeres de la relación de SM-BC:

   ```
   cluster::*> system node revert-to -version 9.7 -check-only
   ```

   Ejemplo:

   ```
   cluster::*> system node revert-to -version 9.7 -check-only
   Error: command failed: The revert check phase failed. The following
   issues must be resolved before revert can be completed. Bring the data
   LIFs down on running vservers. Command to list the running vservers:
   vserver show -admin-state running Command to list the data LIFs that are
   up: network interface show -role data -status-admin up Command to bring
   all data LIFs down: network interface modify {-role data} -status-admin
   down
   Disable snapshot policies.
       Command to list snapshot policies: "snapshot policy show".
       Command to disable snapshot policies: "snapshot policy modify
   -vserver
      * -enabled false"

      Break off the initialized online data-protection (DP) volumes and
   delete
      Uninitialized online data-protection (DP) volumes present on the
   local
      node.
       Command to list all online data-protection volumes on the local
   node:
      volume show -type DP -state online -node <local-node-name>
       Before breaking off the initialized online data-protection volumes,
      quiesce and abort transfers on associated SnapMirror relationships
   and
      wait for the Relationship Status to be Quiesced.
       Command to quiesce a SnapMirror relationship: snapmirror quiesce
       Command to abort transfers on a SnapMirror relationship: snapmirror
      abort
       Command to see if the Relationship Status of a SnapMirror
   relationship
      is Quiesced: snapmirror show
       Command to break off a data-protection volume: snapmirror break
       Command to break off a data-protection volume which is the
   ```

```
destination
   of a SnapMirror relationship with a policy of type "vault":
snapmirror
   break -delete-snapshots
    Uninitialized data-protection volumes are reported by the
"snapmirror
   break" command when applied on a DP volume.
    Command to delete volume: volume delete

   Delete current version snapshots in advanced privilege level.
    Command to list snapshots: "snapshot show -fs-version 9.8"
    Command to delete snapshots: "snapshot prepare-for-revert -node
   <nodename>"

   Delete all user-created policies of the type active-strict-sync-
mirror
   and active-sync-mirror.
   The command to see all active-strict-sync-mirror and active-sync-
mirror
   type policies is:
    snapmirror policy show -type
   active-strict-sync-mirror,active-sync-mirror
   The command to delete a policy is :
    snapmirror policy delete -vserver <SVM-name> -policy <policy-name>
```

Para obtener información sobre cómo revertir los clústeres, consulte "Revierte ONTAP".

Quitar una configuración de SM-BC

Si ya no necesita protección SnapMirror sincronizada con un objetivo de tiempo de recuperación cero, puede eliminar su relación SM-BC.

Acerca de esta tarea

- Antes de eliminar la relación SM-BC, se debe quitar la asignación de todas las LUN del clúster de destino.
- Una vez que se anula la asignación de las LUN y se vuelve a analizar el host, el destino SCSI notifica a los hosts que ha cambiado el inventario de LUN. Las LUN existentes en los volúmenes secundarios con objetivo de tiempo de recuperación cero cambian para reflejar una identidad nueva después de eliminar la relación con objetivo de tiempo de recuperación cero. Los hosts detectan los LUN del volumen secundario como nuevos LUN que no tienen relación con los LUN del volumen de origen.
- Los volúmenes secundarios permanecen en los volúmenes de recuperación ante desastres una vez que se elimina la relación. Puede emitir el `snapmirror break` comando para convertirlos a lectura/escritura.
- No se permite eliminar la relación en el estado fallido cuando no se invierte la relación.

Pasos

1. En el clúster secundario, quite la relación del grupo de consistencia de SM-BC entre el extremo de origen y el extremo de destino:

```
destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
```

2. En el clúster principal, liberar la relación del grupo de consistencia y las copias Snapshot creadas para la relación:

```
source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
```

3. Realice una detección repetida del host para actualizar el inventario de LUN.
4. A partir de ONTAP 9.10.1, al eliminar la relación SnapMirror no se elimina el grupo de consistencia. Si desea eliminar el grupo de coherencia, debe usar System Manager o la API DE REST de ONTAP. Consulte Eliminar un grupo de consistencia si quiere más información.

Retire el Mediador ONTAP

Si desea eliminar una configuración de Mediador ONTAP existente de los clústeres de ONTAP, puede hacerlo mediante el `snapmirror mediator remove` comando.

Pasos

1. Eliminar Mediador ONTAP:

```
snapmirror mediator remove -mediator-address 12.345.678.90 -peer-cluster
cluster_xyz
```

Solucionar problemas

Se produce un error en la operación de eliminación de SnapMirror en estado de takover

Tema:

Cuando se instala ONTAP 9.9.1 en un clúster, se ejecuta el `snapmirror delete` Error del comando cuando la relación del grupo de consistencia SM-BC se encuentra en estado de toma de control.

```
C2_cluster::> snapmirror delete  vs1:/cg/dd

Error: command failed: RPC: Couldn't make connection
```

Solución

Cuando los nodos de una relación SM-BC se encuentran en estado de toma de control, realice la operación de eliminación y lanzamiento de SnapMirror con la opción "-force" establecida en true.

```
C2_cluster::> snapmirror delete  vs1:/cg/dd -force true

Warning: The relationship between source "vs0:/cg/ss" and destination
         "vs1:/cg/dd" will be deleted, however the items of the
destination
         Consistency Group might not be made writable, deletable, or
modifiable
         after the operation. Manual recovery might be required.
Do you want to continue? {y|n}: y
Operation succeeded: snapmirror delete for the relationship with
destination "vs1:/cg/dd".
```

Error al crear una relación de SnapMirror e inicializar el grupo de consistencia

Tema:

Se produce un error en la creación de la relación de SnapMirror y en la inicialización del grupo de consistencia.

Solución:

Asegúrese de no haber superado el límite de grupos de consistencia por clúster. Los límites de los grupos de consistencia en SM-BC son independientes de la plataforma y difieren en función de la versión de ONTAP. Consulte "Restricciones y limitaciones adicionales" Para limitaciones basadas en la versión de ONTAP.

Error

Si el grupo de consistencia está inicializando, compruebe el estado de sus inicializaciones de grupo de consistencia con la API REST de ONTAP, System Manager o el comando `sn show -expand`.

Solución:

Si los grupos de consistencia no se inicializan, elimine la relación SM-BC, elimine el grupo de consistencia y luego vuelva a crear la relación e inicializarla. Este flujo de trabajo varía en función de la versión de ONTAP que se utilice.

Si utiliza ONTAP 9.8-9.9.1	Si utiliza ONTAP 9.10.1 o una versión posterior
1. "Retire la configuración de SM-BC" 2. "Cree una relación de grupo de coherencia" 3. "Inicialice la relación del grupo de coherencia"	1. En **Protección > Relaciones**, encuentre la relación SM-BC en el grupo de consistencia. Seleccione ⋮, Luego **Eliminar** para eliminar la relación SM-BC. 2. "Elimine el grupo de consistencia" 3. "Configure el grupo de consistencia"

Conmutación al nodo de respaldo planificada incorrecta

Tema:

Después de ejecutar el `snapmirror failover start` comando, el resultado del `snapmirror failover show` el comando muestra un mensaje que indica que hay

una operación no disruptiva en curso.

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-------- ----------- -------- --------- ---------- ---------- ----------
vs1:/cg/cg vs0:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
Failover cannot start because a volume move is running. Retry the command
once volume move has finished.
                                                        08:35:04
08:35:04
```

Causa:

Una conmutación al respaldo planificada no puede comenzar cuando exista una operación no disruptiva en curso, incluyendo el movimiento de volúmenes, la reubicación de agregados y la conmutación al respaldo de almacenamiento.

Solución:

Se debe esperar a que finalice la operación no disruptiva y volver a intentar la operación de conmutación al nodo de respaldo.

No se puede acceder a mediador ONTAP o el estado del quórum de mediador es FALSE

Tema:

Después de ejecutar el `snapmirror failover start` comando, el resultado del `snapmirror failover show` Comando muestra un mensaje que indica que Mediator no está configurado.

Consulte "Inicialice el Mediador ONTAP".

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-------- ----------- -------- --------- ---------- ---------- ----------
vs0:/cg/cg vs1:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
failover cannot start because the source-side precheck failed. reason:
Mediator not configured.
05:50:42 05:50:43
```

Causa:

Mediador no está configurado o existen problemas de conectividad de red.

Solución:

Si el Mediador ONTAP no está configurado, debe configurar el Mediador ONTAP antes de poder establecer una relación SM-BC. Solucione cualquier problema de conectividad de red. Asegúrese de que Mediator está conectado y que el estado de quórum es verdadero en el sitio de origen y de destino mediante el comando

snapmirror mediador show. Para obtener más información, consulte Configure el Mediador ONTAP.

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.234.10.143    cluster2         connected         true
```

Recuperación tras fallos no planificada automática no activada en el sitio B

Tema:

Un error en el sitio A no activa una conmutación por error no planificada en el sitio B.

Causa posible n.o 1:

El Mediador ONTAP no está configurado. Para determinar si esta es la causa, emita el `snapmirror mediator show` Comando en el clúster del sitio B.

```
Cluster2::*> snapmirror mediator show
This table is currently empty.
```

Este ejemplo indica que ONTAP Mediator no está configurado en el sitio B.

Solución:

Asegúrese de que ONTAP Mediator está configurado en ambos clusters, que el estado es Conectado y que el quórum está definido en Verdadero.

Posible causa n.o 2:

El grupo de consistencia de SnapMirror no está sincronizado. Para determinar si esta es la causa, consulte el registro de eventos para ver si el grupo de consistencia estaba sincronizado durante el momento en el que se produjo un error en el sitio.

```
cluster::*> event log show -event *out.of.sync*

Time                Node             Severity      Event
------------------- ---------------- -------------
---------------------------
10/1/2020 23:26:12  sti42-vsim-ucs511w ERROR       sms.status.out.of.sync:
Source volume "vs0:zrto_cg_556844_511u_RW1" and destination volume
"vs1:zrto_cg_556881_511w_DP1" with relationship UUID "55ab7942-03e5-11eb-
ba5a-005056a7dc14" is in "out-of-sync" status due to the following reason:
"Transfer failed."
```

Solución:

Realice los pasos siguientes para realizar una conmutación por error forzada en el sitio B.

1. Desasigne todas las LUN que pertenecen al grupo de consistencia desde el sitio B.

2. Elimine la relación del grupo de coherencia SnapMirror mediante `force` opción.
3. Introduzca el `snapmirror break` Comando en los volúmenes constituyentes del grupo de coherencia para convertir volúmenes de DP a R/W para habilitar I/o del sitio B.
4. Arranque los nodos del sitio A para crear una relación de objetivo de tiempo de recuperación cero desde el sitio B al sitio A.
5. Libere el grupo de consistencia con `relationship-info-only` En el sitio A para conservar una copia Snapshot común y desasignar las LUN que pertenecen al grupo de consistencia.
6. Convierta los volúmenes en el sitio A de R/W a DP mediante la configuración de una relación de nivel de volumen con la política de sincronización o la política asíncrona.
7. Emita el `snapmirror resync` para sincronizar las relaciones.
8. Elimine las relaciones de SnapMirror con la política de sincronización en el sitio A.
9. Libere las relaciones de SnapMirror con la política de Sync mediante `relationship-info-only true` En el sitio B.
10. Cree una relación de grupo de consistencia del Sitio B al Sitio A.
11. Realice una resincronización del grupo de consistencia del sitio A y, a continuación, compruebe que el grupo de consistencia está sincronizado.
12. Vuelva a analizar las rutas de I/o del LUN del host para restaurar todas las rutas a los LUN.

Enlace entre el sitio B y el mediador caído y el sitio A caído

Para comprobar la conexión del Mediador ONTAP, utilice el `snapmirror mediator show` comando. Si el estado de conexión es inaccesible y el sitio B no puede acceder al sitio A, tendrá una salida similar a la que se muestra a continuación. Siga los pasos de la solución para restaurar la conexión

```
cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.237.86.17     C1_cluster       unreachable       true
SnapMirror consistency group relationship status is out of sync.

C2_cluster::*> snapmirror show -expand
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/src_cg_1 XDP vs1:/cg/dst_cg_1 Snapmirrored OutOfSync - false   -
vs0:zrto_cg_655724_188a_RW1 XDP vs1:zrto_cg_655755_188c_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655733_188a_RW2 XDP vs1:zrto_cg_655762_188c_DP2 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655739_188b_RW1 XDP vs1:zrto_cg_655768_188d_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655748_188b_RW2 XDP vs1:zrto_cg_655776_188d_DP2 Snapmirrored
OutOfSync - false -
5 entries were displayed.

Site B cluster is unable to reach Site A.
C2_cluster::*> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
C1_cluster            1-80-000011           Unavailable    ok
```

Solución

Forzar una conmutación al respaldo para habilitar la I/o en el sitio B y, a continuación, establecer una relación de objetivo de tiempo de recuperación cero en el sitio B al sitio A. Realice los pasos siguientes para realizar una conmutación por error forzada en el sitio B.

1. Desasigne todas las LUN que pertenecen al grupo de consistencia desde el sitio B.
2. Elimine la relación del grupo de coherencia SnapMirror con la opción force.
3. Introduzca el comando snapmirror break (`snapmirror break -destination_path svm:_volume_`) En los volúmenes constituyentes del grupo de coherencia para convertir volúmenes de DP a RW, para habilitar I/O del sitio B.

   Debe emitir el comando snapmirror break para cada relación del grupo de coherencia. Por ejemplo, si hay tres volúmenes en el grupo de coherencia, emitirá el comando para cada volumen.

4. Arranque los nodos del sitio A para crear una relación de objetivo de tiempo de recuperación cero desde el sitio B al sitio A.
5. Libere el grupo de consistencia con Relationship-info-only en el sitio A para conservar una copia Snapshot común y desasignar las LUN que pertenecen al grupo de consistencia.
6. Convierta los volúmenes en el sitio A de RW a DP configurando una relación de nivel de volumen mediante una política de sincronización o una política asíncrona.
7. Emita el `snapmirror resync` comando para sincronizar las relaciones.
8. Elimine las relaciones de SnapMirror con la política de sincronización en el sitio A.
9. Lance las relaciones de SnapMirror con la política Sync mediante la relación-info-only true en el sitio B.
10. Cree una relación de grupo de consistencia entre el sitio B y el sitio A.
11. En el clúster de origen, resincronice el grupo de consistencia. Compruebe que el estado del grupo de consistencia esté sincronizado.
12. Vuelva a analizar las rutas de I/O del LUN del host para restaurar todas las rutas a las LUN.

Enlace entre el sitio A y el mediador caído y el sitio B caído

Cuando use SM-BC, puede perder la conectividad entre ONTAP Mediator o sus clústeres con conexión entre iguales. Puede diagnosticar el problema comprobando la conexión, la disponibilidad y el estado de consenso de las diferentes partes de la relación SM-BC y, a continuación, reanudando la conexión con fuerza.

Qué comprobar	Comando CLI	Indicador
Mediador del Sitio A	`snapmirror mediator show`	El estado de la conexión será `unreachable`
Conectividad del centro B.	`cluster peer show`	Se ofrecerá disponibilidad `unavailable`
Estado de consenso del volumen SM-BC	`volume show` *`volume_name`* `-fields smbc-consensus`	La `sm-bc consensus` el campo leerá `Awaiting-consensus`

Para obtener información adicional acerca del diagnóstico y la resolución de este problema, consulte el artículo de la base de conocimientos "Enlace entre el Sitio A y el Mediador abajo y el Sitio B inactivo al utilizar SM-BC".

Se produce un error en la operación de eliminación de SM-BC de SnapMirror cuando se establece la cerca en el volumen de destino

Tema:

Se produce un error en la operación de eliminación de SnapMirror cuando alguno de los volúmenes de destino tiene un conjunto de cerca de redirección.

Solución

Realizar las siguientes operaciones para volver a intentar la redirección y eliminar la cerca del volumen de destino.

- Resincronización de SnapMirror
- Actualización de SnapMirror

La operación de movimiento de volúmenes se atasca cuando la opción primaria está inactiva

Tema:

Una operación de movimiento de volumen se bloquea indefinidamente en un estado de transposición diferida cuando el sitio primario está inactivo en una relación de SM-BC. Cuando el sitio primario está inactivo, el sitio secundario realiza una conmutación por error automática no planificada (AUFO). Cuando hay una operación de movimiento de volumen en curso cuando se activa el AUFO, el movimiento de volumen se queda atascado.

Solución:

Cancele la instancia de movimiento de volumen que está bloqueada y reinicie la operación de movimiento de volumen.

Se produce un error en la versión de SnapMirror cuando no se puede eliminar la copia de Snapshot

Tema:

Se produce un error en la operación de versión de SnapMirror cuando no se puede eliminar la copia de Snapshot.

Solución:

La copia Snapshot contiene una etiqueta transitoria. Utilice la `snapshot delete` con el `-ignore-owners` Opción para quitar la copia Snapshot puntual.

```
snapshot delete -volume <volume_name> -snapshot <snapshot_name> -ignore-owners
true -force true
```

Vuelva a intentar el `snapmirror release` comando.

La copia Snapshot de referencia de traslado de volúmenes se muestra como la más reciente

Tema:

Después de ejecutar una operación de movimiento de volumen en un volumen de grupo de coherencia, la copia de Snapshot de referencia para movimiento de volumen puede aparecer como la más reciente de la relación de SnapMirror.

Puede ver la copia Snapshot más reciente con el siguiente comando:

```
snapmirror show -fields newest-snapshot status -expand
```

Solución:

Realizar manualmente un `snapmirror resync` también puede esperar a la próxima operación de resincronización automática una vez que finalice la operación de movimiento de volumen.

Servicio mediador para la continuidad empresarial de MetroCluster y SnapMirror

Descripción general de ONTAP Mediator

El Mediador ONTAP proporciona varias funciones para las funciones de ONTAP:

- Proporciona un almacén persistente y cercado para metadatos de alta disponibilidad.
- Funciona como proxy ping para la vida útil de la controladora.
- Proporciona funcionalidad de consulta de estado de nodo síncrono para ayudar a determinar el quórum.

ONTAP Mediator proporciona dos servicios adicionales de systemctl:

- **`ontap_mediator.service`**

  Mantiene el servidor API REST para gestionar las relaciones ONAP.

- **`mediator-scst.service`**

  Controla el inicio y el apagado del módulo iSCSI (SCST).

Herramientas proporcionadas para el administrador del sistema

Herramientas proporcionadas para el administrador del sistema:

- **`/usr/local/bin/mediator_change_password`**

  Establece una nueva contraseña de API cuando se proporcionan el nombre de usuario y la contraseña actuales de la API.

- **`/usr/local/bin/mediator_change_user`**

  Establece un nuevo nombre de usuario de API cuando se proporcionan el nombre de usuario y la contraseña actuales de la API.

- **`/usr/local/bin/mediator_generate_support_bundle`**

  Genera un archivo tgz local con toda la información de soporte útil necesaria para la comunicación con el soporte al cliente de NetApp. Esto incluye la configuración de la aplicación, los registros y cierta información del sistema. Los paquetes se generan en el disco local y se pueden transferir manualmente, según sea necesario. Ubicación de almacenamiento: /Opt/netapp/data/support_bundles/

- **`/usr/local/bin/uninstall_ontap_mediator`**

  Elimina el paquete ONTAP Mediator y el módulo del núcleo SCST. Esto incluye todos los datos de configuración, registros y buzón de correo.

- **`/usr/local/bin/mediator_unlock_user`**

  Libera un bloqueo en la cuenta de usuario de la API si se alcanzó el límite de reintentos de autenticación. Esta función se utiliza para evitar la derivación de contraseña de fuerza bruta. Solicita al usuario el nombre de usuario y la contraseña correctos.

- **`/usr/local/bin/mediator_add_user`**

  (Solo soporte) Se utiliza para agregar el usuario de la API durante la instalación.

Notas especiales

ONTAP Mediator confía en SCST para proporcionar iSCSI (consulte http://scst.sourceforge.net/index.html). Este paquete es un módulo del núcleo que se compila durante la instalación específicamente para el núcleo. Es posible que cualquier actualización del núcleo requiera la reinstalación de SCST. Como alternativa, desinstale y vuelva a instalar ONTAP Mediator y, a continuación, vuelva a configurar la relación ONTAP.

> Cualquier actualización del kernel del sistema operativo del servidor se debe coordinar con una ventana de mantenimiento de ONTAP.

Novedades del Mediador ONTAP

En cada versión se incluyen nuevas mejoras del Mediador de ONTAP. Esto es lo nuevo.

Mejoras

Versión de ONTAP Mediator	Mejoras
1,7	• Compatibilidad con RHEL 8,5, 8,6, 8,7, 8,8, 8,9, 9,0, 9,1, 9,2 y 9,3 • Compatibilidad con Rocky Linux 8 y 9
1,6	• Actualizaciones de Python 3,9. • Compatibilidad con RHEL 8,4-8,8, 9,0-9,2, Rocky Linux 8 y 9. • Interrupción del soporte para RHEL 7.x / CentOS todas las versiones.
1,5	• Optimiza la velocidad para sistemas SMBC a gran escala. • Firma de código criptográfico añadida al instalador. • Incluye advertencias de amortización para RHEL 7.x / CentOS 7.x.
1,4	• Compatibilidad con RHEL 8,4 y 8,5. • Incluye SCST versión 3,6.0. • Se ha añadido soporte para Secure Boot (SB) del firmware basado en UFEI.
1,3	• Compatibilidad con RHEL/CentOS 8,2 y 8,3. • Incluye SCST versión 3,5.0.
1,2	• Compatibilidad con buzones HTTPS. • Para uso con ONTAP 9,8+ MCC-IP AUSO y SM-BC ZRTO. • Incluye SCST versión 3,4.0.
1,1	• Compatibilidad con RHEL/CentOS 7,6, 7,7, 8,0 y 8,1. • Elimina las dependencias de Perl. • Incluye SCST versión 3,4.0.

1,0	• Compatibilidad con buzones de correo iSCSI. • Para uso con ONTAP 9,7+ MCC-IP AUSO. • Compatibilidad con RHEL/CentOS 7,6.

Matriz de compatibilidad de SO

OS for ONTAP Mediator	1,7	1,6	1,5	1,4	1,3	1,2	1,1	1,0
7,6	Obsoleto	Obsoleto	Sí	Sí	Sí	Sí	Sí	Sí (solo RHEL)
7,7	Obsoleto	Obsoleto	Sí	Sí	Sí	Sí	No	No
7,8	Obsoleto	Obsoleto	Sí	Sí	Sí	Sí	No	No
7,9	Obsoleto	Obsoleto	Sí	Sí	Sí	Implícita	No	No
RHEL 8,0	Obsoleto	Obsoleto	Sí	Sí	Sí	Sí	Sí	No
RHEL 8,1	Obsoleto	Obsoleto	Sí	Sí	Sí	Sí	No	No
RHEL 8,2	Obsoleto	Obsoleto	Sí	Sí	Sí	No	No	No
RHEL 8,3	Obsoleto	Obsoleto	Sí	Sí	Sí	No	No	No
RHEL 8,4	Obsoleto	Sí	Sí	Sí	No	No	No	No
RHEL 8,5	Sí	Sí	Sí	Sí	No	No	No	No
RHEL 8,6	Sí	Sí	No	No	No	No	No	No
RHEL 8,7	Sí	Sí	No	No	No	No	No	No
RHEL 8,8	Sí	Sí	No	No	No	No	No	No
RHEL 9,0	Sí	Sí	No	No	No	No	No	No
RHEL 9,1	Sí	Sí	No	No	No	No	No	No
RHEL 9,2	Sí	Sí	No	No	No	No	No	No
RHEL 9,3	Sí	No	No	No	No	No	No	No

CentOS 8 y STREAM	No	No	No	No	No	N.A.	N.A.	N.A.
Rocky Linux 8	Sí	Sí	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.
Rocky Linux 9	Sí	Sí	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.

- OS hace referencia a las versiones RedHat y CentOS, a menos que se especifique lo contrario.
- “No” significa que el sistema operativo y el Mediador ONTAP no son compatibles.
- CentOS 8 se eliminó para todas las versiones debido a su reramificación. CentOS Stream no se consideró un sistema operativo de destino de producción adecuado. No se ha planificado ningún soporte.
- ONTAP Mediator 1,5 fue la última versión admitida para los sistemas operativos de sucursal RHEL 7.x.
- ONTAP Mediator 1,6 añade soporte para Rocky Linux 8 y 9.

Problemas resueltos

Fecha del cambio	Cambiar ID	Descripción
10 de enero de 2023	6567145	Se realizaron los siguientes cambios: • Se ha añadido soporte para sistemas operativos adicionales para ONTAP Mediator: RHEL 9,6, 8,7, 9,0 y 9,1. • Se ha añadido la nueva versión 3.7.0 de SCST para desbloquear los problemas de los nuevos sistemas operativos admitidos. • Añadido soporte para Rocky Linux: Rocky 8 y 9.
24 de enero de 2023	6621319	Se permite la biblioteca SCST preinstalada para instalaciones de ONTAP Mediator.
27 de febrero de 2023	6623764	Se han implementado cambios para cargar siempre el módulo del núcleo scst_DISK cuando se reinicia el servicio mediator-scst. Estos cambios garantizan que el servicio siempre estará listo para crear nuevos destinos iSCSI utilizando la lógica estándar.
28 de febrero de 2023	6625194	Se ha añadido una nueva opción al instalador de ONTAP Mediator: `--skip-yum-dependencies`
24 de marzo de 2023	6652840	Se ha actualizado el instalador de ONTAP Mediator para que pueda reinstalar o reparar la instalación de SCST.

27 de marzo de 2023	6655179	Se corrigió un problema de análisis que se produjo al activar la recogida del bundle de soporte con una contraseña compleja.
28 de marzo de 2023	6656739	Se ha cambiado la lógica de comparación de SCST para que se instale la versión correcta cuando se actualice ONTAP Mediator.

Instale o actualice

Prepárese para instalar o actualizar el servicio de Mediador de ONTAP

Para instalar el servicio ONTAP Mediator, debe asegurarse de que se cumplen todos los requisitos previos, obtener el paquete de instalación y ejecutar el instalador en el host. Este procedimiento se utiliza para una instalación o actualización de una instalación existente.

Acerca de esta tarea

- A partir de ONTAP 9.7, puede utilizar cualquier versión de Mediator de ONTAP para supervisar una configuración IP de MetroCluster.
- A partir de ONTAP 9.8, puede utilizar cualquier versión de Mediator de ONTAP para supervisar una relación SM-BC.

Antes de empezar

Debe cumplir con los siguientes requisitos previos.

Versión de ONTAP Mediator	Versiones de Linux compatibles
1,7	• Red Hat Enterprise Linux: 8,5, 8,6, 8,7, 8,8, 8,9, 9,0, 9,1, 9,2 y 9,3 • Rocky Linux 8 y 9
1,6	• Red Hat Enterprise Linux: 8,4, 8,5, 8,6, 8,7, 8,8, 9,0, 9,1, 9,2 • Rocky Linux 8 y 9
1,5	• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1 8.2, 8.3, 8.4, 8.5 • CentOS: 7.6, 7.7, 7.8, 7.9
1,4	• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1 8.2, 8.3, 8.4, 8.5 • CentOS: 7.6, 7.7, 7.8, 7.9
1,3	• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1 8.2, 8.3 • CentOS: 7.6, 7.7, 7.8, 7.9
1,2	• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 8.1 • CentOS: 7.6, 7.7, 7.8

> La versión del kernel debe coincidir con la versión del sistema operativo.

- instalación física de 64 bits o máquina virtual
- 8 GB DE MEMORIA RAM
- 1 GB de espacio en disco (utilizado para la instalación de aplicaciones, registros del servidor y la base de datos)
- Usuario: Acceso raíz

Cualquier paquete de biblioteca, excepto el núcleo, se puede actualizar de forma segura, pero es posible que sea necesario reiniciarlo para que se vea afectado dentro de la aplicación ONTAP Mediator. Se recomienda una ventana de servicio cuando es necesario reiniciar.

Si instala el `yum-utils` paquete, puede utilizar el `needs-restarting` comando.

El núcleo central del núcleo se puede actualizar si se está actualizando a una versión que aún es compatible con la matriz de versiones de ONTAP Mediator. Un reinicio será obligatorio, por lo que se requiere una ventana de servicio.

El módulo del núcleo SCST debe desinstalarse antes del reinicio y, a continuación, volver a instalarse después del reinicio.

> No se admite la actualización a un núcleo más allá de la versión de SO admitida para la versión de ONTAP Mediator específica. (Esto probablemente indica que el módulo SCST probado no se compilará).

Registre una clave de seguridad cuando el arranque seguro de UEFI esté habilitado

Si el inicio seguro de UEFI está activado, para instalar ONTAP Mediator, tendrá que registrar una clave de seguridad antes de que el servicio ONTAP Mediator pueda iniciarse. Para determinar si el sistema está habilitado para UEFI y Secure Boot está activado, realice los siguientes pasos:

Pasos

1. Si mokutil no está instalado, ejecute el siguiente comando:

   ```
   yum install mokutil
   ```

2. Para determinar si UEFI Secure Boot está habilitado en su sistema, ejecute el siguiente comando:

   ```
   mokutil --sb-state
   ```

   Los resultados muestran si UEFI Secure Boot está habilitado en este sistema.

   > ONTAP Mediator 1.2.0 y las versiones anteriores no admiten este modo.

Desactive UEFI Secure Boot

También puede optar por deshabilitar el arranque seguro de UEFI antes de instalar ONTAP Mediator.

Pasos

1. En la configuración del BIOS de la máquina física, desactive la opción «Arranque seguro UEFI».

2. En la configuración de VMware para la máquina virtual, desactive la opción de inicio seguro para vSphere 6.x o la opción de arranque seguro para vSphere 7.x.

Actualice el sistema operativo del host y, a continuación, el Mediador de ONTAP

Para actualizar el sistema operativo host para ONTAP Mediator a una versión posterior, primero debe desinstalar ONTAP Mediator.

Antes de empezar

A continuación se enumeran las mejores prácticas para instalar Red Hat Enterprise Linux o Rocky Linux y los repositorios asociados en su sistema. Los sistemas instalados o configurados de forma diferente pueden requerir pasos adicionales.

- Debe instalar Red Hat Enterprise Linux o Rocky Linux de acuerdo con las mejores prácticas de Red Hat. Debido al soporte final de su vida útil para las versiones CentOS 8.x, no se recomienda utilizar versiones compatibles de CentOS 8.x.
- Al instalar el servicio ONTAP Mediator en Red Hat Enterprise Linux o Rocky Linux, el sistema debe tener acceso al repositorio adecuado para que el programa de instalación pueda acceder e instalar todas las dependencias de software necesarias.
- Para que el instalador de yum encuentre software dependiente en los repositorios de Red Hat Enterprise Linux, debe haber registrado el sistema durante la instalación de Red Hat Enterprise Linux o después mediante una suscripción válida de Red Hat.

  Consulte la documentación de Red Hat para obtener información acerca de Red Hat Subscription Manager.

- Los siguientes puertos deben no utilizarse y estar disponibles para el Mediator:
  - 31784
  - 3260
- Si utiliza un firewall de terceros: Consulte "Requisitos de firewall para ONTAP Mediator"
- Si el host Linux se encuentra en una ubicación sin acceso a Internet, debe asegurarse de que los paquetes requeridos estén disponibles en un repositorio local.

  Si utiliza el protocolo de control de agregación de enlaces (LACP) en un entorno de Linux, debe configurar correctamente el kernel y asegurarse de que `sysctl net.ipv4.conf.all.arp_ignore` está configurado en "2".

Lo que necesitará

El servicio Mediator de ONTAP requiere los siguientes paquetes:

Todas las versiones RHEL/CentOS	Paquetes adicionales para RHEL 8.x / Rocky Linux 8	Paquetes adicionales para RHEL 9.x / Rocky Linux 9

• openssl • openssl • kernel-devel-$ (uname -r) • gcc • marca • libselinux-utils • parche • bzip2 • perl-Data-Dumper • perl-Extls-MakeMaker • efibootmgr • mokutil	• python3-pip • elfutils-libelf-devel • policcoreutils-python-utils • redhat-lsb-core • python39 • python39-devel	• python3-pip • elfutils-libelf-devel • policcoreutils-python-utils • python3 • python3-devel

El paquete de instalación de Mediator es un archivo tar comprimido autoextraíble que incluye:

- Un archivo RPM que contiene todas las dependencias que no pueden obtenerse del repositorio de la versión compatible.
- Una secuencia de comandos de instalación.

Se recomienda una certificación SSL válida.

Acerca de esta tarea

Al actualizar el sistema operativo host para ONTAP Mediator a una versión principal posterior (por ejemplo, de 7.x a 8.x) con la herramienta leapp-upgrade, Debe desinstalar ONTAP Mediator porque la herramienta intenta detectar nuevas versiones de los RPM instalados en los repositorios registrados con el sistema.

Como se instaló un archivo .rpm como parte del instalador de ONTAP Mediator, se incluye en esa búsqueda. Sin embargo, como ese archivo .rpm se desempaquetó como parte del instalador y no se descargó de un repositorio registrado, no se puede encontrar una actualización. En este caso, la herramienta leapp-upgrade desinstala el paquete.

Para conservar los archivos de registro, que se utilizarán para clasificar los casos de soporte, debe realizar una copia de seguridad de los archivos antes de realizar una actualización del sistema operativo y restaurarlos después de una reinstalación del paquete ONTAP Mediator. Debido a que ONTAP Mediator se está reinstalando, todos los clústeres de ONTAP que estén conectados a él deberán volver a conectarse después de la nueva instalación.

> Los siguientes pasos deben realizarse en orden. Inmediatamente después de reinstalar ONTAP Mediator, debe detener el servicio ontap_mediator, reemplazar los archivos de registro y reiniciar el servicio. Esto asegurará que no se pierdan los registros.

Pasos

1. Realice una copia de seguridad de los archivos de registro.

```
[rootmediator-host ~]# tar -czf ontap_mediator_file_backup.tgz -C
/opt/netapp/lib/ontap_mediator ./log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]# tar -tf ontap_mediator_file_backup.tgz
./log/
./log/ontap_mediator.log
./log/scstadmin.log
./log/ontap_mediator_stdout.log
./log/ontap_mediator_requests.log
./log/install_20230419134611.log
./log/scst.log
./log/ontap_mediator_syslog.log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]#
```

2. Realice la actualización con la herramienta leapp-upgrade.

```
[rootmediator-host ~]# leapp preupgrade --target 8.4
  ..<snip upgrade checks>..
  ..<fix issues found>..
[rootmediator-host ~]# leapp upgrade --target 8.4
  ..<snip upgrade>..
[rootmediator-host ~]# cat /etc/os-release | head -2
NAME="Red Hat Enterprise Linux"
VERSION="8.4 (Ootpa)"
[rootmediator-host ~]#
```

3. Vuelva a instalar ONTAP Mediator.

> Realice el resto de los pasos inmediatamente después de volver a instalar ONTAP Mediator para evitar la pérdida de archivos de registro.

```
[rootmediator-host ~]# ontap-mediator-1.6.0/ontap-mediator-1.6.0

ONTAP Mediator: Self Extracting Installer

  ..<snip installation>..
[rootmediator-host ~]#
```

4. Detenga el servicio ontap_mediator.

```
[rootmediator-host ~]# systemctl stop ontap_mediator
[rootmediator-host ~]#
```

5. Sustituya los archivos de registro.

```
[rootmediator-host ~]# tar -xf ontap_mediator_log_backup.tgz -C
/opt/netapp/lib/ontap_mediator
[rootmediator-host ~]#
```

6. Inicie el servicio ontap_mediator.

```
[rootmediator-host ~]# systemctl start ontap_mediator
[rootmediator-host ~]#
```

7. Vuelva a conectar todos los clústeres de ONTAP con el Mediador de ONTAP actualizado

Procedimiento para MetroCluster sobre IP

```
siteA::> metrocluster configuration-settings mediator show
Mediator IP     Port    Node                    Configuration
Connection
                                                Status        Status
--------------- ------- ----------------------- -------------
-----------
172.31.40.122
                31784   siteA-node2             true          false
                        siteA-node1             true          false
                        siteB-node2             true          false
                        siteB-node2             true          false
siteA::> metrocluster configuration-settings mediator remove
Removing the mediator and disabling Automatic Unplanned Switchover.
It may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Automatic Unplanned Switchover is disabled for all nodes...
Removing mediator mailboxes...
Successfully removed the mediator.

siteA::> metrocluster configuration-settings mediator add -mediator
-address 172.31.40.122
Adding the mediator and enabling Automatic Unplanned Switchover. It
may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Successfully added the mediator.

siteA::> metrocluster configuration-settings mediator show
Mediator IP     Port    Node                    Configuration
Connection
                                                Status        Status
--------------- ------- ----------------------- -------------
-----------
172.31.40.122
                31784   siteA-node2             true          true
                        siteA-node1             true          true
                        siteB-node2             true          true
                        siteB-node2             true          true
siteA::>
```

Procedimiento de Continuidad del negocio con SnapMirror

Para la continuidad del negocio con SnapMirror, si instaló su certificado TLS fuera del directorio /opt/netapp, no será necesario reinstalarlo. Si estaba utilizando el certificado autofirmado generado por defecto o colocó el certificado personalizado en el directorio /opt/netapp, deberá realizar un backup y restaurarlo.

```
peer1::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
172.31.49.237    peer2            unreachable       true

peer1::> snapmirror mediator remove -mediator-address 172.31.49.237
-peer-cluster peer2

Info: [Job 39] 'mediator remove' job queued

peer1::> job show -id 39
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
39     mediator remove      peer1      peer1-node1    Success
     Description: Removing entry in mediator

peer1::> security certificate show -common-name ONTAPMediatorCA
Vserver    Serial Number   Certificate Name
Type
---------- --------------- ------------------------------------
------------
peer1
        4A790360081F41145E14C5D7CE721DC6C210007F
                        ONTAPMediatorCA
server-ca
    Certificate Authority: ONTAP Mediator CA
        Expiration Date: Mon Apr 17 10:27:54 2073

peer1::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

 peer1::> security certificate install -type server-ca -vserver
peer1

Please enter Certificate: Press <Enter> when done
  ..<snip ONTAP Mediator CA public key>..

You should keep a copy of the CA-signed digital certificate for
future reference.
```

```
The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

peer2::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

peer2::> security certificate install -type server-ca -vserver peer2

 Please enter Certificate: Press <Enter> when done
..<snip ONTAP Mediator CA public key>..


You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

peer1::> snapmirror mediator add -mediator-address 172.31.49.237
-peer-cluster peer2 -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 43] 'mediator add' job queued

peer1::> job show -id 43
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
43     mediator add         peer1      peer1-node2    Success
    Description: Creating a mediator entry

peer1::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
172.31.49.237    peer2            connected         true
```

```
peer1::>
```

Habilite el acceso a los repositorios

Debe activar el acceso a los repositorios para que ONTAP Mediator pueda acceder a los paquetes necesarios durante el proceso de instalación

Pasos

1. Determine a qué repositorios se debe acceder, como se muestra en la siguiente tabla:

Si su sistema operativo es…	Debe proporcionar acceso a estos repositorios…
RHEL 7.x	• rhel-7-server-optional-rpms
RHEL 8.x	• rhel-8-for-x86_64-baseos-rpms • rhel-8-for-x86_64-appstream-rpms
RHEL 9.x	• rhel-9-for-x86_64-baseos-rpms • rhel-9-for-x86_64-appstream-rpms
CentOS 7.x	• C7.6.1810 - repositorio base
Rocky Linux 8	• flujo de aplicación • baseos
Rocky Linux 9	• flujo de aplicación • baseos

2. Utilice uno de los siguientes procedimientos para habilitar el acceso a los repositorios enumerados anteriormente para que ONTAP Mediator pueda acceder a los paquetes necesarios durante el proceso de instalación.

Procedimiento para el sistema operativo RHEL 7.x.

Utilice este procedimiento si su sistema operativo es **RHEL 7.x** para permitir el acceso a los repositorios:

Pasos

1. Suscríbase al repositorio deseado:

   ```
   subscription-manager repos --enable rhel-7-server-optional-rpms
   ```

   En el ejemplo siguiente se muestra la ejecución de este comando:

   ```
   [root@localhost ~]# subscription-manager repos --enable rhel-7-
   server-optional-rpms
   Repository 'rhel-7-server-optional-rpms' is enabled for this system.
   ```

2. Ejecute el `yum repolist` comando.

   En el siguiente ejemplo, se muestra la ejecución de este comando. El repositorio "rhel-7-Server-optional-rpms" debe aparecer en la lista.

   ```
   [root@localhost ~]# yum repolist
   Loaded plugins: product-id, search-disabled-repos, subscription-
   manager
   rhel-7-server-optional-rpms | 3.2 kB  00:00:00
   rhel-7-server-rpms | 3.5 kB  00:00:00
   (1/3): rhel-7-server-optional-rpms/7Server/x86_64/group
   |  26 kB  00:00:00
   (2/3): rhel-7-server-optional-rpms/7Server/x86_64/updateinfo
   | 2.5 MB  00:00:00
   (3/3): rhel-7-server-optional-rpms/7Server/x86_64/primary_db
   | 8.3 MB  00:00:01
   repo id                                       repo name
   status
   rhel-7-server-optional-rpms/7Server/x86_64   Red Hat Enterprise
   Linux 7 Server - Optional (RPMs)   19,447
   rhel-7-server-rpms/7Server/x86_64            Red Hat Enterprise
   Linux 7 Server (RPMs)              26,758
   repolist: 46,205
   [root@localhost ~]#
   ```

Procedimiento para el sistema operativo RHEL 8.x.

Utilice este procedimiento si su sistema operativo es **RHEL 8.x** para permitir el acceso a los repositorios:

Pasos

1. Suscríbase al repositorio deseado:

   `subscription-manager repos --enable rhel-8-for-x86_64-baseos-rpms`

   `subscription-manager repos --enable rhel-8-for-x86_64-appstream-rpms`

   En el ejemplo siguiente se muestra la ejecución de este comando:

   ```
   [root@localhost ~]# subscription-manager repos --enable rhel-8-for-
   x86_64-baseos-rpms
   Repository 'rhel-8-for-x86_64-baseos-rpms' is enabled for this
   system.
   [root@localhost ~]# subscription-manager repos --enable rhel-8-for-
   x86_64-appstream-rpms
   Repository 'rhel-8-for-x86_64-appstream-rpms' is enabled for this
   system.
   ```

2. Ejecute el `yum repolist` comando.

   Los repositorios recientemente suscritos deben aparecer en la lista.

Procedimiento para el sistema operativo RHEL 9.x.

Utilice este procedimiento si su sistema operativo es **RHEL 9.x** para permitir el acceso a los repositorios:

Pasos

1. Suscríbase al repositorio deseado:

   `subscription-manager repos --enable rhel-9-for-x86_64-baseos-rpms`

   `subscription-manager repos --enable rhel-9-for-x86_64-appstream-rpms`

   En el ejemplo siguiente se muestra la ejecución de este comando:

   ```
   [root@localhost ~]# subscription-manager repos --enable rhel-9-for-
   x86_64-baseos-rpms
   Repository 'rhel-9-for-x86_64-baseos-rpms' is enabled for this
   system.
   [root@localhost ~]# subscription-manager repos --enable rhel-9-for-
   x86_64-appstream-rpms
   Repository 'rhel-9-for-x86_64-appstream-rpms' is enabled for this
   system.
   ```

2. Ejecute el `yum repolist` comando.

   Los repositorios recientemente suscritos deben aparecer en la lista.

Procedimiento para el sistema operativo CentOS 7.x.

Utilice este procedimiento si su sistema operativo es **CentOS 7.x** para permitir el acceso a los repositorios:

> Los siguientes ejemplos muestran un repositorio para CentOS 7,6 y es posible que no funcione para otras versiones de CentOS. Utilice el repositorio base para su versión de CentOS.

Pasos

1. Agregue el repositorio base C7.6.1810. El repositorio de almacén base C7,6.1810 contiene el paquete «kernel-devel» necesario para ONTAP Mediator.
2. Agregue las siguientes líneas a /etc/yum.repos.d/CentOS-Vault.repo.

```
[C7.6.1810-base]
name=CentOS-7.6.1810 - Base
baseurl=http://vault.centos.org/7.6.1810/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
enabled=1
```

3. Ejecute el `yum repolist` comando.

   En el siguiente ejemplo, se muestra la ejecución de este comando. El repositorio de CentOS-7.6.1810 - base debería aparecer en la lista.

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: distro.ibiblio.org
 * extras: distro.ibiblio.org
 * updates: ewr.edge.kernel.org
C7.6.1810-base                                  | 3.6 kB  00:00:00
(1/2): C7.6.1810-base/x86_64/group_gz           | 166 kB  00:00:00
(2/2): C7.6.1810-base/x86_64/primary_db         | 6.0 MB  00:00:04
repo id                      repo name                 status
C7.6.1810-base/x86_64        CentOS-7.6.1810 - Base    10,019
base/7/x86_64                CentOS-7 - Base           10,097
extras/7/x86_64              CentOS-7 - Extras         307
updates/7/x86_64             CentOS-7 - Updates        1,010
repolist: 21,433
[root@localhost ~]#
```

Procedimiento para sistemas operativos Rocky Linux 8 o 9

Utilice este procedimiento si su sistema operativo es **Rocky Linux 8** o **Rocky Linux 9** para permitir el acceso a los repositorios:

Pasos

1. Suscríbase a los repositorios requeridos:

   ```
   dnf config-manager --set-enabled baseos

   dnf config-manager --set-enabled appstream
   ```

2. Realice una `clean` operación:

   ```
   dnf clean all
   ```

3. Verifique la lista de repositorios:

   ```
   dnf repolist
   ```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                        repo name
appstream                      Rocky Linux 8 - AppStream
baseos                         Rocky Linux 8 - BaseOS
[root@localhost ~]#
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                        repo name
appstream                      Rocky Linux 9 - AppStream
baseos                         Rocky Linux 9 - BaseOS
[root@localhost ~]#
```

Descargue el paquete de instalación de Mediator

Descargue el paquete de instalación de Mediator como parte del proceso de instalación.

Pasos

1. Descargue el paquete de instalación del Mediador desde la página Mediador de ONTAP.

   "Página de descarga de Mediador ONTAP"

2. Confirme que el paquete de instalación de Mediator se encuentra en el directorio de trabajo actual:

   `ls`

   ```
   [root@mediator-host ~]#ls
   ontap-mediator-1.7.0.tgz
   ```

   > Para las versiones 1.4 y anteriores de Mediator de ONTAP, se denomina al instalador `ontap-mediator`.

   Si se encuentra en una ubicación sin acceso a Internet, debe asegurarse de que el instalador tiene acceso a los paquetes necesarios.

3. Si es necesario, mueva el paquete de instalación de Mediator del directorio de descarga al directorio de instalación del host Linux Mediator.
4. Descomprima el paquete del instalador:

   `tar xvfz ontap-mediator-1.7.0.tgz`

   ```
   [root@scs000099753 ~]# tar xvfz ontap-mediator-1.7.0.tgz
   ontap-mediator-1.7.0/
   ontap-mediator-1.7.0/ONTAP-Mediator-production.pub
   ontap-mediator-1.7.0/tsa-prod-chain-ONTAP-Mediator.pem
   ontap-mediator-1.7.0/tsa-prod-ONTAP-Mediator.pem
   ontap-mediator-1.7.0/csc-prod-ONTAP-Mediator.pem
   ontap-mediator-1.7.0/csc-prod-chain-ONTAP-Mediator.pem
   ontap-mediator-1.7.0/ontap-mediator-1.7.0
   ontap-mediator-1.7.0/ontap-mediator-1.7.0.sig.tsr
   ontap-mediator-1.7.0/ontap-mediator-1.7.0.tsr
   ontap-mediator-1.7.0/ontap-mediator-1.7.0.sig
   ```

Verifique la firma del código del Mediador ONTAP

Antes de instalar el paquete de instalación del Mediador, debe comprobar la firma del código del Mediador ONTAP.

Antes de empezar

Antes de comprobar la firma del código del Mediator, el sistema debe cumplir los siguientes requisitos.

- versiones de openssl 1.0.2 a 3.0 para verificación básica
- la versión de openssl 1.1.0 o posterior para las operaciones de la Autoridad de fijación temporal (TSA)
- Acceso público a Internet para verificación OCSP

En el paquete de descarga se incluyen los siguientes archivos:

Archivo	Descripción
`ONTAP-Mediator-development.pub`	Clave pública utilizada para verificar la firma
`csc-prod-chain-ONTAP-Mediator.pem`	La cadena de confianza de CA de certificación pública
`csc-prod-ONTAP-Mediator.pem`	El certificado utilizado para generar la clave
`ontap-mediator-1.7.0`	Ejecutable de instalación del producto para la versión 1.7.0
`ontap-mediator-1.7.0.sig`	El SHA-256 hash, luego RSA-firmado usando la clave csc-prod, firma para el instalador
`ontap-mediator-1.7.0.sig.tsr`	La solicitud de revocación para el uso por parte de OCSCP para la firma del instalador
`tsa-prod-ONTAP-Mediator.pem`	El certificado público para la TSR
`tsa-prod-chain-ONTAP-Mediator.pem`	El certificado público CA Chain para la TSR

Pasos

1. Realice la comprobación de revocación activada `csc-prod-ONTAP-Mediator.pem` Mediante el protocolo de estado de certificado en línea (OCSP).
   a. Busque la URL de OCSP utilizada para registrar el certificado porque los certificados de desarrollador pueden no proporcionar un uri.

   ```
   openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
   ```

   b. Genere una solicitud OCSP para el certificado.

   ```
   openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
   prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem
   -reqout req.der
   ```

   c. Conéctese al administrador de OCSP para enviar la solicitud OCSP:

   ```
   openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
   prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem  -url
   ${ocsp_uri} -resp_text -respout resp.der -verify_other csc-prod-
   chain-ONTAP-Mediator.pem
   ```

2. Verifique la cadena de confianza del CSC y las fechas de vencimiento con respecto al host local:

   `openssl verify`

   > La `openssl` La versión de LA RUTA de ACCESO debe ser válida `cert.pem` (no autofirmado).

   ```
   openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath
   ${OPENSSLDIR} csc-prod-ONTAP-Mediator.pem  # Failure action: The Code-
   Signature-Check certificate has expired or is invalid. Download a newer
   version of the ONTAP Mediator.
   openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath
   ${OPENSSLDIR} tsa-prod-ONTAP-Mediator.pem  # Failure action: The Time-
   Stamp certificate has expired or is invalid. Download a newer version of
   the ONTAP Mediator.
   ```

3. Compruebe el `ontap-mediator-1.6.0.sig.tsr` y.. `ontap-mediator-1.7.0.tsr` archivos que utilizan los certificados asociados:

   `openssl ts -verify`

   > `.tsr` los archivos contienen la respuesta de marca de tiempo asociada con el instalador y la firma del código. El procesamiento confirma que la Marca de tiempo tiene una firma válida de TSA y que su archivo de entrada no ha cambiado.
   > La verificación se realiza de forma local en su máquina. Independientemente, no hay necesidad de acceder a los servidores TSA.

   ```
   openssl ts -verify -data ontap-mediator-1.7.0.sig -in ontap-mediator-
   1.7.0.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
   prod-ONTAP-Mediator.pem
   openssl ts -verify -data ontap-mediator-1.7.0 -in ontap-mediator-
   1.7.0.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-prod-
   ONTAP-Mediator.pem
   ```

4. Verificar firmas con respecto a la clave:

   `openssl -dgst -verify`

   ```
   openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature
   ontap-mediator-1.7.0.sig ontap-mediator-1.7.0
   ```

Ejemplo de verificación de la firma del código del Mediador ONTAP (salida de consola)

```
[root@scspa2695423001 ontap-mediator-1.7.0]# pwd
/root/ontap-mediator-1.7.0
[root@scspa2695423001 ontap-mediator-1.7.0]# ls -l
total 63660
-r--r--r-- 1 root root     8582 Feb 19 15:02 csc-prod-chain-ONTAP-
Mediator.pem
-r--r--r-- 1 root root     2373 Feb 19 15:02 csc-prod-ONTAP-
Mediator.pem
-r-xr-xr-- 1 root root 65132818 Feb 20 15:17 ontap-mediator-1.7.0
-rw-r--r-- 1 root root      384 Feb 20 15:17 ontap-mediator-1.7.0.sig
-rw-r--r-- 1 root root     5437 Feb 20 15:17 ontap-mediator-
1.7.0.sig.tsr
-rw-r--r-- 1 root root     5436 Feb 20 15:17 ontap-mediator-1.7.0.tsr
-r--r--r-- 1 root root      625 Feb 19 15:02 ONTAP-Mediator-
production.pub
-r--r--r-- 1 root root     3323 Feb 19 15:02 tsa-prod-chain-ONTAP-
Mediator.pem
-r--r--r-- 1 root root     1740 Feb 19 15:02 tsa-prod-ONTAP-
Mediator.pem
[root@scspa2695423001 ontap-mediator-1.7.0]#
[root@scspa2695423001 ontap-mediator-1.7.0]#
/root/verify_ontap_mediator_signatures.sh
++ openssl version -d
++ cut -d '"' -f2
+ OPENSSLDIR=/etc/pki/tls
+ openssl version
OpenSSL 1.1.1k  FIPS 25 Mar 2021
++ openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
+ ocsp_uri=http://ocsp.entrust.net
+ echo http://ocsp.entrust.net
http://ocsp.entrust.net
+ openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -reqout
req.der
+ openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -url
http://ocsp.entrust.net -resp_text -respout resp.der -verify_other csc-
prod-chain-ONTAP-Mediator.pem
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
```

```
    Produced At: Feb 28 05:01:00 2023 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A
      Issuer Key Hash: CE894F8251AA15A28462CA312361D261FBF8FE78
      Serial Number: 511A542B57522AEB7295A640DC6200E5
    Cert Status: good
    This Update: Feb 28 05:00:00 2023 GMT
    Next Update: Mar  4 04:59:59 2023 GMT

    Signature Algorithm: sha512WithRSAEncryption
         3c:1d:49:b0:93:62:37:3e:c7:38:e3:9f:9f:62:82:73:ed:f4:
         ea:00:6b:f1:01:cd:79:57:92:f1:9d:5d:85:9b:60:59:f8:6c:
         e6:f4:50:51:f3:4c:8a:51:dd:50:68:16:8f:20:24:7e:39:b0:
         44:94:8d:b0:61:da:b9:08:36:74:2d:44:55:62:fb:92:be:4a:
         e7:6c:8c:49:dd:0c:fd:d8:ce:20:08:0d:0f:5a:29:a3:19:03:
         9f:d3:df:41:f4:89:0f:73:18:3f:ac:bb:a7:a3:96:7d:c5:70:
         4c:57:cd:17:17:c6:8a:60:d1:37:c9:2d:81:07:2a:d7:a6:02:
         ee:ce:88:16:22:db:e3:43:64:1e:9b:0d:4d:31:66:fa:ab:a5:
         52:99:94:4a:4a:d0:52:c5:34:f5:18:c7:15:5b:ce:74:c2:fc:
         61:ea:55:aa:f1:2f:82:a3:6a:95:8d:7e:2b:38:49:4f:bf:b1:
         68:7b:1b:24:8b:1f:4d:c5:77:f0:71:af:9c:34:c8:7a:82:50:
         09:a2:19:6e:c6:30:4f:da:a2:79:08:f9:d0:ff:85:d9:2a:84:
         cf:0c:aa:75:8f:72:c9:a7:a2:83:e8:8b:cf:ed:0c:69:75:b6:
         2a:7b:6b:58:99:01:d8:34:ad:e1:89:25:27:1b:fa:d9:6d:32:
         97:3a:0b:0a:8e:a3:9e:e3:f4:e0:d6:1a:c9:b5:14:8c:3e:54:
         3b:37:17:1a:93:44:84:8b:4a:87:97:1e:76:43:3e:d3:ec:8b:
         7e:56:4a:3f:01:31:c0:e5:58:fb:50:ce:6f:b1:e7:35:f9:b7:
         a3:ef:6b:3b:21:95:37:a6:5b:8f:f0:15:18:36:65:89:a1:9c:
         9b:69:00:b4:b1:65:6a:bc:11:2d:d4:9b:b4:97:cc:cb:7a:0c:
         16:11:c1:75:58:7e:13:ab:56:3c:3f:93:5b:95:24:c6:54:52:
         1f:86:a9:16:ce:d9:ea:8b:3a:f3:4f:c4:8f:ad:de:e8:3e:3c:
         d2:51:51:ad:33:7f:d8:c5:33:24:26:f1:2d:9d:0e:9f:55:d0:
         68:bf:af:bd:68:4a:40:08:bc:92:a0:62:54:7d:16:7b:36:29:
         15:b1:cd:58:8e:fb:4a:f2:3e:94:8b:fe:56:95:cc:24:32:af:
         5f:71:99:18:ed:0c:64:94:f7:54:48:87:48:d0:6d:b3:42:04:
         96:03:73:a2:8e:8a:6a:b2:af:ee:56:19:a1:c6:35:12:59:ad:
         19:6a:fe:e0:f1:27:cc:96:4e:f0:4f:fb:6a:bd:ce:05:2c:aa:
         79:7c:df:02:5c:ca:53:7d:60:12:88:7c:ce:15:c7:d4:02:27:
         c1:ab:cf:71:30:1e:14:ba
WARNING: no nonce in response
Response verify OK
csc-prod-ONTAP-Mediator.pem: good
        This Update: Feb 28 05:00:00 2023 GMT
        Next Update: Mar  4 04:59:59 2023 GMT
```

```
+ openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath
/etc/pki/tls csc-prod-ONTAP-Mediator.pem
csc-prod-ONTAP-Mediator.pem: OK
+ openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath
/etc/pki/tls tsa-prod-ONTAP-Mediator.pem
tsa-prod-ONTAP-Mediator.pem: OK
+ openssl ts -verify -data ontap-mediator-1.7.0.sig -in ontap-mediator-
1.7.0.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
Using configuration from /etc/pki/tls/openssl.cnf
Verification: OK
+ openssl ts -verify -data ontap-mediator-1.7.0 -in ontap-mediator-
1.7.0.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
Using configuration from /etc/pki/tls/openssl.cnf
Verification: OK
+ openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature
ontap-mediator-1.7.0.sig ontap-mediator-1.7.0
Verified OK
[root@scspa2695423001 ontap-mediator-1.7.0]#
```

Instale el paquete de instalación del Mediador ONTAP

Para instalar el servicio ONTAP Mediator, debe obtener el paquete de instalación y ejecutar el instalador en el host.

Pasos

1. Ejecute el instalador y responda a las indicaciones según sea necesario:

   `./ontap-mediator-1.7.0/ontap-mediator-1.7.0 -y`

   ```
   [root@scs000099753 ~]# ./ontap-mediator-1.5.0/ontap-mediator-1.7.0 -y
   ```

   El proceso de instalación permite crear las cuentas necesarias e instalar los paquetes necesarios. Si tiene instalada una versión anterior de Mediator en el host, se le pedirá que confirme que desea actualizar.

2. A partir de ONTAP Mediator 1.4, el mecanismo de arranque seguro está activado en los sistemas UEFI. Cuando Secure Boot está activado, debe realizar pasos adicionales para registrar la clave de seguridad después de la instalación:

   - Siga las instrucciones del archivo README para firmar el módulo del núcleo SCST.:

     `/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-signing`

   - Localice las claves que desee:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys
```

Después de la instalación, los archivos README y la ubicación de la clave también se proporcionan en la salida del sistema.

Ejemplo de instalación de ONTAP Mediator 1,6 (salida de la consola)

```
[root@scs000099753 ~]# ./ontap-mediator-1.6.0/ontap-mediator-1.6.0 -y
ONTAP Mediator: Self Extracting Installer


+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
   Using openssl from the path: /usr/bin/openssl configured for
CApath:/etc/pki/tls

+ Unpacking the ONTAP Mediator installer
ONTAP Mediator requires two user accounts. One for the service
(netapp), and one for use by ONTAP to the mediator API (mediatoradmin).
Using default account names: netapp + mediatoradmin

Enter ONTAP Mediator user account (mediatoradmin) password:

Re-Enter ONTAP Mediator user account (mediatoradmin) password:

+ Checking if SELinux is in enforcing mode


+ Checking for default Linux firewall
success
success
success


################################################################
Preparing for installation of ONTAP Mediator packages.


+ Installing required packages.


Last metadata expiration check: 0:25:24 ago on Fri 21 Oct 2022 04:00:13
PM EDT.
Package openssl-1:1.1.1k-4.el8.x86_64 is already installed.
Package gcc-8.4.1-1.el8.x86_64 is already installed.
Package python36-3.6.8-2.module+el8.1.0+3334+5cb623d7.x86_64 is already
installed.
Package libselinux-utils-2.9-5.el8.x86_64 is already installed.
Package perl-Data-Dumper-2.167-399.el8.x86_64 is already installed.
Package efibootmgr-16-1.el8.x86_64 is already installed.
Package mokutil-1:0.3.0-11.el8.x86_64 is already installed.
```

```
Package python3-pip-9.0.3-19.el8.noarch is already installed.
Package policycoreutils-python-utils-2.9-14.el8.noarch is already
installed.
Dependencies resolved.
=========================================================================
=========================================================================
========================================
 Package                                        Architecture
Version                                                   Repository
Size
=========================================================================
=========================================================================
========================================
Installing:
 bzip2                                          x86_64
1.0.6-26.el8                                              rhel-8-for-
x86_64-baseos-rpms                       60 k
 elfutils-libelf-devel                          x86_64
0.186-1.el8                                               rhel-8-for-
x86_64-baseos-rpms                       60 k
 kernel-devel                                   x86_64
4.18.0-348.el8                                            rhel-8-for-
x86_64-baseos-rpms                       20 M
 make                                           x86_64
1:4.2.1-11.el8                                            rhel-8-for-
x86_64-baseos-rpms                      498 k
 openssl-devel                                  x86_64
1:1.1.1k-7.el8_6                                          rhel-8-for-
x86_64-baseos-rpms                      2.3 M
 patch                                          x86_64
2.7.6-11.el8                                              rhel-8-for-
x86_64-baseos-rpms                      138 k
 perl-ExtUtils-MakeMaker                        noarch
1:7.34-1.el8                                              rhel-8-for-
x86_64-appstream-rpms                   301 k
 python36-devel                                 x86_64
3.6.8-38.module+el8.5.0+12207+5c5719bc                    rhel-8-for-
x86_64-appstream-rpms                    17 k
 redhat-lsb-core                                x86_64
4.1-47.el8                                                rhel-8-for-
x86_64-appstream-rpms                    45 k
Upgrading:
 cpp                                            x86_64
8.5.0-10.1.el8_6                                          rhel-8-for-
x86_64-appstream-rpms                    10 M
 elfutils-libelf                                x86_64
```

```
0.186-1.el8                                                 rhel-8-for-
x86_64-baseos-rpms                      229 k
 elfutils-libs                                  x86_64
0.186-1.el8                                                 rhel-8-for-
x86_64-baseos-rpms                      295 k
 gcc                                            x86_64
8.5.0-10.1.el8_6                                            rhel-8-for-
x86_64-appstream-rpms                    23 M
 libgcc                                         x86_64
8.5.0-10.1.el8_6                                            rhel-8-for-
x86_64-baseos-rpms                       80 k
 libgomp                                        x86_64
8.5.0-10.1.el8_6                                            rhel-8-for-
x86_64-baseos-rpms                      207 k
 libsemanage                                    x86_64
2.9-8.el8                                                   rhel-8-for-
x86_64-baseos-rpms                      168 k
 mokutil                                        x86_64
1:0.3.0-11.el8_6.1                                          rhel-8-for-
x86_64-baseos-rpms                       46 k
 openssl                                        x86_64
1:1.1.1k-7.el8_6                                            rhel-8-for-
x86_64-baseos-rpms                      709 k
 openssl-libs                                   x86_64
1:1.1.1k-7.el8_6                                            rhel-8-for-
x86_64-baseos-rpms                      1.5 M
 platform-python-pip                            noarch
9.0.3-22.el8                                                rhel-8-for-
x86_64-baseos-rpms                      1.6 M
 policycoreutils                                x86_64
2.9-19.el8                                                  rhel-8-for-
x86_64-baseos-rpms                      374 k
 policycoreutils-python-utils                   noarch
2.9-19.el8                                                  rhel-8-for-
x86_64-baseos-rpms                      253 k
 python3-libsemanage                            x86_64
2.9-8.el8                                                   rhel-8-for-
x86_64-baseos-rpms                      128 k
 python3-pip                                    noarch
9.0.3-22.el8                                                rhel-8-for-
x86_64-appstream-rpms                    20 k
 python3-policycoreutils                        noarch
2.9-19.el8                                                  rhel-8-for-
x86_64-baseos-rpms                      2.2 M
 python36                                       x86_64
3.6.8-38.module+el8.5.0+12207+5c5719bc                      rhel-8-for-
```

```
x86_64-appstream-rpms                    19 k
Installing dependencies:
 annobin                                         x86_64
10.29-3.el8                                               rhel-8-for-
x86_64-appstream-rpms                   117 k
 at                                              x86_64
3.1.20-11.el8                                             rhel-8-for-
x86_64-baseos-rpms                       81 k
 bc                                              x86_64
1.07.1-5.el8                                              rhel-8-for-
x86_64-baseos-rpms                      129 k
 cups-client                                     x86_64
1:2.2.6-38.el8                                            rhel-8-for-
x86_64-appstream-rpms                   169 k
 dwz                                             x86_64
0.12-10.el8                                               rhel-8-for-
x86_64-appstream-rpms                   109 k
 ed                                              x86_64
1.14.2-4.el8                                              rhel-8-for-
x86_64-baseos-rpms                       82 k
 efi-srpm-macros                                 noarch
3-3.el8                                                   rhel-8-for-
x86_64-appstream-rpms                    22 k
 esmtp                                           x86_64
1.2-15.el8                                                EPEL-8
57 k
 ghc-srpm-macros                                 noarch
1.4.2-7.el8                                               rhel-8-for-
x86_64-appstream-rpms                   9.4 k
 go-srpm-macros                                  noarch
2-17.el8                                                  rhel-8-for-
x86_64-appstream-rpms                    13 k
 keyutils-libs-devel                             x86_64
1.5.10-6.el8                                              rhel-8-for-
x86_64-baseos-rpms                       48 k
 krb5-devel                                      x86_64
1.18.2-14.el8                                             rhel-8-for-
x86_64-baseos-rpms                      560 k
 libcom_err-devel                                x86_64
1.45.6-2.el8                                              rhel-8-for-
x86_64-baseos-rpms                       38 k
 libesmtp                                        x86_64
1.0.6-18.el8                                              EPEL-8
70 k
 libkadm5                                        x86_64
1.18.2-14.el8                                             rhel-8-for-
```

```
x86_64-baseos-rpms                      187 k
 liblockfile                                    x86_64
1.14-1.el8                                              rhel-8-for-
x86_64-appstream-rpms                    32 k
 libselinux-devel                               x86_64
2.9-5.el8                                               rhel-8-for-
x86_64-baseos-rpms                      200 k
 libsepol-devel                                 x86_64
2.9-3.el8                                               rhel-8-for-
x86_64-baseos-rpms                       87 k
 libverto-devel                                 x86_64
0.3.0-5.el8                                             rhel-8-for-
x86_64-baseos-rpms                       18 k
 m4                                             x86_64
1.4.18-7.el8                                            rhel-8-for-
x86_64-baseos-rpms                      223 k
 mailx                                          x86_64
12.5-29.el8                                             rhel-8-for-
x86_64-baseos-rpms                      257 k
 ncurses-compat-libs                            x86_64
6.1-9.20180224.el8                                      rhel-8-for-
x86_64-baseos-rpms                      328 k
 ocaml-srpm-macros                              noarch
5-4.el8                                                 rhel-8-for-
x86_64-appstream-rpms                   9.5 k
 openblas-srpm-macros                           noarch
2-2.el8                                                 rhel-8-for-
x86_64-appstream-rpms                   8.0 k
 pcre2-devel                                    x86_64
10.32-2.el8                                             rhel-8-for-
x86_64-baseos-rpms                      605 k
 pcre2-utf16                                    x86_64
10.32-2.el8                                             rhel-8-for-
x86_64-baseos-rpms                      229 k
 pcre2-utf32                                    x86_64
10.32-2.el8                                             rhel-8-for-
x86_64-baseos-rpms                      220 k
 perl-CPAN-Meta-YAML                            noarch
0.018-397.el8                                           rhel-8-for-
x86_64-appstream-rpms                    34 k
 perl-ExtUtils-Command                          noarch
1:7.34-1.el8                                            rhel-8-for-
x86_64-appstream-rpms                    19 k
 perl-ExtUtils-Install                          noarch
2.14-4.el8                                              rhel-8-for-
x86_64-appstream-rpms                    46 k
```

```
 perl-ExtUtils-Manifest                          noarch
1.70-395.el8                                             rhel-8-for-
x86_64-appstream-rpms                    37 k
 perl-ExtUtils-ParseXS                           noarch
1:3.35-2.el8                                             rhel-8-for-
x86_64-appstream-rpms                    83 k
 perl-JSON-PP                                    noarch
1:2.97.001-3.el8                                         rhel-8-for-
x86_64-appstream-rpms                    68 k
 perl-Math-BigInt                                noarch
1:1.9998.11-7.el8                                        rhel-8-for-
x86_64-baseos-rpms                      196 k
 perl-Math-Complex                               noarch
1.59-421.el8                                             rhel-8-for-
x86_64-baseos-rpms                      109 k
 perl-Test-Harness                               noarch
1:3.42-1.el8                                             rhel-8-for-
x86_64-appstream-rpms                   279 k
 perl-devel                                      x86_64
4:5.26.3-419.el8_4.1                                     rhel-8-for-
x86_64-appstream-rpms                   599 k
 perl-srpm-macros                                noarch
1-25.el8                                                 rhel-8-for-
x86_64-appstream-rpms                    11 k
 perl-version                                    x86_64
6:0.99.24-1.el8                                          rhel-8-for-
x86_64-appstream-rpms                    67 k
 platform-python-devel                           x86_64
3.6.8-41.el8                                             rhel-8-for-
x86_64-appstream-rpms                   249 k
 python-rpm-macros                               noarch
3-41.el8                                                 rhel-8-for-
x86_64-appstream-rpms                    15 k
 python-srpm-macros                              noarch
3-41.el8                                                 rhel-8-for-
x86_64-appstream-rpms                    15 k
 python3-pyparsing                               noarch
2.1.10-7.el8                                             rhel-8-for-
x86_64-baseos-rpms                      142 k
 python3-rpm-generators                          noarch
5-7.el8                                                  rhel-8-for-
x86_64-appstream-rpms                    25 k
 python3-rpm-macros                              noarch
3-41.el8                                                 rhel-8-for-
x86_64-appstream-rpms                    14 k
 qt5-srpm-macros                                 noarch
```

```
5.15.2-1.el8                                                rhel-8-for-
x86_64-appstream-rpms                   11 k
 redhat-lsb-submod-security                     x86_64
4.1-47.el8                                                  rhel-8-for-
x86_64-appstream-rpms                   22 k
 redhat-rpm-config                              noarch
125-1.el8                                                   rhel-8-for-
x86_64-appstream-rpms                   87 k
 rust-srpm-macros                               noarch
5-2.el8                                                     rhel-8-for-
x86_64-appstream-rpms                  9.3 k
 spax                                           x86_64
1.5.3-13.el8                                                rhel-8-for-
x86_64-baseos-rpms                    217 k
 systemtap-sdt-devel                            x86_64
4.6-4.el8                                                   rhel-8-for-
x86_64-appstream-rpms                   86 k
 time                                           x86_64
1.9-3.el8                                                   rhel-8-for-
x86_64-baseos-rpms                      54 k
 unzip                                          x86_64
6.0-46.el8                                                  rhel-8-for-
x86_64-baseos-rpms                    196 k
 util-linux-user                                x86_64
2.32.1-28.el8                                               rhel-8-for-
x86_64-baseos-rpms                    100 k
 zip                                            x86_64
3.0-23.el8                                                  rhel-8-for-
x86_64-baseos-rpms                    270 k
 zlib-devel                                     x86_64
1.2.11-17.el8                                               rhel-8-for-
x86_64-baseos-rpms                      58 k
Installing weak dependencies:
 perl-CPAN-Meta                                 noarch
2.150010-396.el8                                            rhel-8-for-
x86_64-appstream-rpms                   191 k
 perl-CPAN-Meta-Requirements                    noarch
2.140-396.el8                                               rhel-8-for-
x86_64-appstream-rpms                   37 k
 perl-Encode-Locale                             noarch
1.05-10.module+el8.3.0+6498+9eecfe51                        rhel-8-for-
x86_64-appstream-rpms                   22 k
 perl-Time-HiRes                                x86_64
4:1.9758-2.el8                                              rhel-8-for-
x86_64-appstream-rpms                   61 k
```

```
Transaction Summary
================================================================================
================================================================================
==========================================
Install  69 Packages
Upgrade  17 Packages

Total download size: 72 M
Is this ok [y/N]: y
Downloading Packages:
(1/86): perl-ExtUtils-Install-2.14-4.el8.noarch.rpm
735 kB/s |  46 kB     00:00
(2/86): libesmtp-1.0.6-18.el8.x86_64.rpm
1.0 MB/s |  70 kB     00:00
(3/86): esmtp-1.2-15.el8.x86_64.rpm
747 kB/s |  57 kB     00:00
(4/86): rust-srpm-macros-5-2.el8.noarch.rpm
308 kB/s | 9.3 kB     00:00
(5/86): perl-ExtUtils-Manifest-1.70-395.el8.noarch.rpm
781 kB/s |  37 kB     00:00
(6/86): perl-CPAN-Meta-2.150010-396.el8.noarch.rpm
2.7 MB/s | 191 kB     00:00
(7/86): ocaml-srpm-macros-5-4.el8.noarch.rpm
214 kB/s | 9.5 kB     00:00
(8/86): perl-JSON-PP-2.97.001-3.el8.noarch.rpm
1.2 MB/s |  68 kB     00:00
(9/86): perl-ExtUtils-MakeMaker-7.34-1.el8.noarch.rpm
5.8 MB/s | 301 kB     00:00
(10/86): ghc-srpm-macros-1.4.2-7.el8.noarch.rpm
317 kB/s | 9.4 kB     00:00
(11/86): perl-Test-Harness-3.42-1.el8.noarch.rpm
4.5 MB/s | 279 kB     00:00
(12/86): perl-ExtUtils-Command-7.34-1.el8.noarch.rpm
520 kB/s |  19 kB     00:00

...

15 MB/s | 1.5 MB     00:00
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
------------------------------------------
Total
35 MB/s |  72 MB     00:02
Running transaction check
Transaction check succeeded.
Running transaction test
```

```
Transaction test succeeded.
Running transaction
  Preparing        :
1/1
  Running scriptlet: openssl-libs-1:1.1.1k-7.el8_6.x86_64
1/1
  Upgrading        : openssl-libs-1:1.1.1k-7.el8_6.x86_64
1/103
  Running scriptlet: openssl-libs-1:1.1.1k-7.el8_6.x86_64
1/103
  Upgrading        : libgcc-8.5.0-10.1.el8_6.x86_64
2/103
  Running scriptlet: libgcc-8.5.0-10.1.el8_6.x86_64
2/103
  Upgrading        : elfutils-libelf-0.186-1.el8.x86_64
3/103
  Installing       : perl-version-6:0.99.24-1.el8.x86_64
4/103
  Installing       : perl-CPAN-Meta-Requirements-2.140-396.el8.noarch
5/103
  Upgrading        : libsemanage-2.9-8.el8.x86_64
6/103
  Installing       : zlib-devel-1.2.11-17.el8.x86_64
7/103
  Installing       : python-srpm-macros-3-41.el8.noarch
8/103
  Installing       : python-rpm-macros-3-41.el8.noarch
9/103
  Installing       : python3-rpm-macros-3-41.el8.noarch
10/103
  Installing       : perl-Time-HiRes-4:1.9758-2.el8.x86_64
11/103
  Installing       : perl-ExtUtils-ParseXS-1:3.35-2.el8.noarch
12/103
  Installing       : perl-Test-Harness-1:3.42-1.el8.noarch
13/103
  Upgrading        : python3-libsemanage-2.9-8.el8.x86_64
14/103
  Upgrading        : policycoreutils-2.9-19.el8.x86_64
15/103
  Running scriptlet: policycoreutils-2.9-19.el8.x86_64
15/103
  Upgrading        : python3-policycoreutils-2.9-19.el8.noarch
16/103
  Installing       : dwz-0.12-10.el8.x86_64
17/103
```

```
  Installing       : ncurses-compat-libs-6.1-9.20180224.el8.x86_64
18/103
  Installing       : libesmtp-1.0.6-18.el8.x86_64
19/103
  Installing       : mailx-12.5-29.el8.x86_64
20/103
  Installing       : libkadm5-1.18.2-14.el8.x86_64
21/103
  Upgrading        : libgomp-8.5.0-10.1.el8_6.x86_64
22/103
  Running scriptlet: libgomp-8.5.0-10.1.el8_6.x86_64
22/103
  Upgrading        : platform-python-pip-9.0.3-22.el8.noarch
23/103
  Upgrading        : python3-pip-9.0.3-22.el8.noarch
24/103
  Upgrading        : python36-3.6.8-
38.module+el8.5.0+12207+5c5719bc.x86_64
25/103
  Running scriptlet: python36-3.6.8-
38.module+el8.5.0+12207+5c5719bc.x86_64
25/103
  Upgrading        : cpp-8.5.0-10.1.el8_6.x86_64
26/103
  Running scriptlet: cpp-8.5.0-10.1.el8_6.x86_64
26/103
  Upgrading        : gcc-8.5.0-10.1.el8_6.x86_64
27/103
  Running scriptlet: gcc-8.5.0-10.1.el8_6.x86_64
27/103
  Installing       : annobin-10.29-3.el8.x86_64
28/103
  Installing       : unzip-6.0-46.el8.x86_64
29/103
  Installing       : zip-3.0-23.el8.x86_64
30/103
  Installing       : perl-Math-Complex-1.59-421.el8.noarch
31/103
  Installing       : perl-Math-BigInt-1:1.9998.11-7.el8.noarch
32/103
  Installing       : perl-JSON-PP-1:2.97.001-3.el8.noarch
33/103
  Installing       : make-1:4.2.1-11.el8.x86_64
34/103
  Running scriptlet: make-1:4.2.1-11.el8.x86_64
34/103
```

```
  Installing       : libcom_err-devel-1.45.6-2.el8.x86_64
35/103
  Installing       : util-linux-user-2.32.1-28.el8.x86_64
36/103
  Installing       : libsepol-devel-2.9-3.el8.x86_64
37/103
  Installing       : pcre2-utf32-10.32-2.el8.x86_64
38/103
  Installing       : pcre2-utf16-10.32-2.el8.x86_64
39/103
  Installing       : pcre2-devel-10.32-2.el8.x86_64
40/103
  Installing       : libselinux-devel-2.9-5.el8.x86_64
41/103
  Installing       : patch-2.7.6-11.el8.x86_64
42/103
  Installing       : python3-pyparsing-2.1.10-7.el8.noarch
43/103
  Installing       : systemtap-sdt-devel-4.6-4.el8.x86_64
44/103
  Installing       : spax-1.5.3-13.el8.x86_64
45/103
  Running scriptlet: spax-1.5.3-13.el8.x86_64
45/103
  Installing       : m4-1.4.18-7.el8.x86_64
46/103
  Running scriptlet: m4-1.4.18-7.el8.x86_64
46/103
  Installing       : libverto-devel-0.3.0-5.el8.x86_64
47/103
  Installing       : bc-1.07.1-5.el8.x86_64
48/103
  Running scriptlet: bc-1.07.1-5.el8.x86_64
48/103
  Installing       : at-3.1.20-11.el8.x86_64
49/103
  Running scriptlet: at-3.1.20-11.el8.x86_64
49/103
  Installing       : keyutils-libs-devel-1.5.10-6.el8.x86_64
50/103
  Installing       : krb5-devel-1.18.2-14.el8.x86_64
51/103
  Installing       : time-1.9-3.el8.x86_64
52/103
  Running scriptlet: time-1.9-3.el8.x86_64
52/103
```

```
  Upgrading        : policycoreutils-python-utils-2.9-19.el8.noarch
80/103
  Installing       : elfutils-libelf-devel-0.186-1.el8.x86_64
81/103
  Upgrading        : elfutils-libs-0.186-1.el8.x86_64
82/103
  Upgrading        : mokutil-1:0.3.0-11.el8_6.1.x86_64
83/103
  Upgrading        : openssl-1:1.1.1k-7.el8_6.x86_64
84/103
  Installing       : kernel-devel-4.18.0-348.el8.x86_64
85/103
  Running scriptlet: kernel-devel-4.18.0-348.el8.x86_64

  ...

85/103
  Installing       : bzip2-1.0.6-26.el8.x86_64
86/103
  Cleanup          : policycoreutils-python-utils-2.9-14.el8.noarch
87/103
  Cleanup          : python3-policycoreutils-2.9-14.el8.noarch
88/103
  Cleanup          : python36-3.6.8-
2.module+el8.1.0+3334+5cb623d7.x86_64
89/103
  Running scriptlet: python36-3.6.8-
2.module+el8.1.0+3334+5cb623d7.x86_64
89/103
  Cleanup          : elfutils-libs-0.185-1.el8.x86_64
90/103
  Cleanup          : openssl-1:1.1.1k-4.el8.x86_64
91/103
  Cleanup          : python3-libsemanage-2.9-6.el8.x86_64
92/103
  Running scriptlet: gcc-8.4.1-1.el8.x86_64
93/103
  Cleanup          : gcc-8.4.1-1.el8.x86_64
93/103
  Running scriptlet: policycoreutils-2.9-14.el8.x86_64
94/103
  Cleanup          : policycoreutils-2.9-14.el8.x86_64
94/103
  Cleanup          : mokutil-1:0.3.0-11.el8.x86_64
95/103
```

```
  Cleanup          : python3-pip-9.0.3-19.el8.noarch
96/103
  Cleanup          : platform-python-pip-9.0.3-19.el8.noarch
97/103
  Cleanup          : openssl-libs-1:1.1.1k-4.el8.x86_64
98/103
  Running scriptlet: openssl-libs-1:1.1.1k-4.el8.x86_64
98/103
  Cleanup          : libsemanage-2.9-6.el8.x86_64
99/103
  Running scriptlet: cpp-8.4.1-1.el8.x86_64
100/103
  Cleanup          : cpp-8.4.1-1.el8.x86_64
100/103
  Cleanup          : libgcc-8.5.0-3.el8.x86_64
101/103
  Running scriptlet: libgcc-8.5.0-3.el8.x86_64
101/103
  Running scriptlet: libgomp-8.4.1-1.el8.x86_64
102/103
  Cleanup          : libgomp-8.4.1-1.el8.x86_64
102/103
  Running scriptlet: libgomp-8.4.1-1.el8.x86_64
102/103
  Cleanup          : elfutils-libelf-0.185-1.el8.x86_64
103/103
  Running scriptlet: elfutils-libelf-0.185-1.el8.x86_64
103/103
  Verifying        : esmtp-1.2-15.el8.x86_64
1/103
  Verifying        : libesmtp-1.0.6-18.el8.x86_64

  ...

Upgraded:
  cpp-8.5.0-10.1.el8_6.x86_64                              elfutils-
libelf-0.186-1.el8.x86_64     elfutils-libs-0.186-1.el8.x86_64
gcc-8.5.0-10.1.el8_6.x86_64
  libgcc-8.5.0-10.1.el8_6.x86_64                           libgomp-
8.5.0-10.1.el8_6.x86_64        libsemanage-2.9-8.el8.x86_64
mokutil-1:0.3.0-11.el8_6.1.x86_64
  openssl-1:1.1.1k-7.el8_6.x86_64                          openssl-
libs-1:1.1.1k-7.el8_6.x86_64   platform-python-pip-9.0.3-22.el8.noarch
policycoreutils-2.9-19.el8.x86_64
  policycoreutils-python-utils-2.9-19.el8.noarch           python3-
libsemanage-2.9-8.el8.x86_64   python3-pip-9.0.3-22.el8.noarch
```

```
python3-policycoreutils-2.9-19.el8.noarch
  python36-3.6.8-38.module+el8.5.0+12207+5c5719bc.x86_64
Installed:
  annobin-10.29-3.el8.x86_64                                          at-
3.1.20-11.el8.x86_64                              bc-1.07.1-5.el8.x86_64
  bzip2-1.0.6-26.el8.x86_64
cups-client-1:2.2.6-38.el8.x86_64                   dwz-0.12-
10.el8.x86_64
  ed-1.14.2-4.el8.x86_64
efi-srpm-macros-3-3.el8.noarch                      elfutils-libelf-
devel-0.186-1.el8.x86_64
  esmtp-1.2-15.el8.x86_64
ghc-srpm-macros-1.4.2-7.el8.noarch                  go-srpm-macros-2-
17.el8.noarch
  kernel-devel-4.18.0-348.el8.x86_64
keyutils-libs-devel-1.5.10-6.el8.x86_64             krb5-devel-1.18.2-
14.el8.x86_64
  libcom_err-devel-1.45.6-2.el8.x86_64
libesmtp-1.0.6-18.el8.x86_64                        libkadm5-1.18.2-
14.el8.x86_64
  liblockfile-1.14-1.el8.x86_64
libselinux-devel-2.9-5.el8.x86_64                   libsepol-devel-2.9-
3.el8.x86_64
  libverto-devel-0.3.0-5.el8.x86_64                                   m4-
1.4.18-7.el8.x86_64                               mailx-12.5-
29.el8.x86_64
  make-1:4.2.1-11.el8.x86_64
ncurses-compat-libs-6.1-9.20180224.el8.x86_64       ocaml-srpm-macros-
5-4.el8.noarch
  openblas-srpm-macros-2-2.el8.noarch
openssl-devel-1:1.1.1k-7.el8_6.x86_64               patch-2.7.6-
11.el8.x86_64
  pcre2-devel-10.32-2.el8.x86_64
pcre2-utf16-10.32-2.el8.x86_64                      pcre2-utf32-10.32-
2.el8.x86_64
  perl-CPAN-Meta-2.150010-396.el8.noarch
perl-CPAN-Meta-Requirements-2.140-396.el8.noarch    perl-CPAN-Meta-
YAML-0.018-397.el8.noarch
  perl-Encode-Locale-1.05-10.module+el8.3.0+6498+9eecfe51.noarch
perl-ExtUtils-Command-1:7.34-1.el8.noarch           perl-ExtUtils-
Install-2.14-4.el8.noarch
  perl-ExtUtils-MakeMaker-1:7.34-1.el8.noarch
perl-ExtUtils-Manifest-1.70-395.el8.noarch          perl-ExtUtils-
ParseXS-1:3.35-2.el8.noarch
  perl-JSON-PP-1:2.97.001-3.el8.noarch
perl-Math-BigInt-1:1.9998.11-7.el8.noarch           perl-Math-Complex-
```

```
1.59-421.el8.noarch
  perl-Test-Harness-1:3.42-1.el8.noarch
perl-Time-HiRes-4:1.9758-2.el8.x86_64               perl-devel-
4:5.26.3-419.el8_4.1.x86_64
  perl-srpm-macros-1-25.el8.noarch
perl-version-6:0.99.24-1.el8.x86_64                 platform-python-
devel-3.6.8-41.el8.x86_64
  python-rpm-macros-3-41.el8.noarch
python-srpm-macros-3-41.el8.noarch                  python3-pyparsing-
2.1.10-7.el8.noarch
  python3-rpm-generators-5-7.el8.noarch
python3-rpm-macros-3-41.el8.noarch                  python36-devel-
3.6.8-38.module+el8.5.0+12207+5c5719bc.x86_64
  qt5-srpm-macros-5.15.2-1.el8.noarch
redhat-lsb-core-4.1-47.el8.x86_64                   redhat-lsb-submod-
security-4.1-47.el8.x86_64
  redhat-rpm-config-125-1.el8.noarch
rust-srpm-macros-5-2.el8.noarch                     spax-1.5.3-
13.el8.x86_64
  systemtap-sdt-devel-4.6-4.el8.x86_64
time-1.9-3.el8.x86_64                               unzip-6.0-
46.el8.x86_64
  util-linux-user-2.32.1-28.el8.x86_64
zip-3.0-23.el8.x86_64                               zlib-devel-1.2.11-
17.el8.x86_64

Complete!
OS package installations finished
+ Installing ONTAP Mediator. (Log: /tmp/ontap_mediator.JixKGP/ontap-
mediator-1.6.0/ontap-mediator-1.6.0/install_20221021155929.log)
    This step will take several minutes. Use the log file to view
progress.
    Sudoer config verified
    ONTAP Mediator rsyslog and logging rotation enabled
+ Install successful. (Moving log to
/opt/netapp/lib/ontap_mediator/log/install_20221021155929.log)
+ WARNING: This system supports UEFI
           Secure Boot (SB) is currently disabled on this system.
           If SB is enabled in the future, SCST will not work unless
the following action is taken:
           Using the keys in
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys follow
           instructions in
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.modu
le-signing
           to sign the SCST kernel module. Note that reboot will be
```

```
needed.
     SCST will not start automatically when Secure Boot is enabled and
not configured properly.
+ Note: ONTAP Mediator uses a kernel module compiled specifically for
the current
        OS. Using 'yum update' to upgrade the kernel might cause
service interruption.
    For more information, see /opt/netapp/lib/ontap_mediator/README
[root@scs000099753 ~]# cat /etc/redhat-release
Red Hat Enterprise Linux release 8.5 (Ootpa)
[root@scs000099753 ~]#
```

Compruebe la instalación

Después de instalar ONTAP Mediator, debe verificar que los servicios de ONTAP Mediator se están ejecutando.

Pasos

1. Ver el estado de los servicios de mediador de ONTAP:
   a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

 ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
      ├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      ├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      └─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
   Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
  Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
 Main PID: 286662 (iscsi-scstd)
    Tasks: 1 (limit: 49473)
   Memory: 1.2M
   CGroup: /system.slice/mediator-scst.service
           └─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. Confirme los puertos que utiliza el servicio ONTAP Mediator:

`netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

         tcp   0   0 0.0.0.0:31784   0.0.0.0:*      LISTEN

         tcp   0   0 0.0.0.0:3260    0.0.0.0:*      LISTEN

         tcp6  0   0 :::3260         :::*           LISTEN
```

Configuración posterior a la instalación

Una vez instalado y en ejecución el servicio ONTAP Mediator, se deben llevar a cabo tareas de configuración adicionales en el sistema de almacenamiento de ONTAP para utilizar las siguientes funciones:

- Para utilizar el servicio Mediator de ONTAP en una configuración IP de MetroCluster, consulte "Configuración del servicio Mediador ONTAP desde una configuración IP de MetroCluster".
- Para utilizar la continuidad del negocio de SnapMirror, consulte "Instale el Servicio Mediador ONTAP y confirme la configuración del clúster ONTAP".

Configurar las políticas de seguridad de ONTAP Mediator

El servidor ONTAP Mediator admite varios ajustes de seguridad configurables. Los valores por defecto para todos los valores se proporcionan en un archivo low_space_threshold_mib: 10read-only:

`/opt/netapp/lib/ontap_mediator/server_config/ontap_mediator.user_config.yaml`

Todos los valores que se colocan en el `ontap_mediator.user_config.yaml` Sustituirá los valores predeterminados y se mantendrá en todas las actualizaciones de ONTAP Mediator.

Después de modificar `ontap_mediator.user_config.yaml`, Reinicie el servicio ONTAP Mediator:

```
systemctl restart ontap_mediator
```

Modificar los atributos de ONTAP Mediator

Se pueden configurar los siguientes atributos:

> Otros valores predeterminados en la `ontap_mediator.config.yaml` no se debe modificar.

- **Configuración utilizada para instalar certificados SSL de terceros como reemplazos para los certificados autofirmados predeterminados**

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_media
tor_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_media
tor_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
cert_valid_days: '1095'                   # Used to set the expiration
on client certs to 3 years
x509_passin_pwd: 'pass:ontap'             # passphrase for the signed
client cert
```

- **Configuraciones que proporcionan protección contra ataques de adivinación de contraseñas de fuerza bruta**

  Para activar la función, configure un valor para `window_seconds` y la `retry_limit`

  Ejemplos:

  - Proporcione un intervalo de 5 minutos para las conjeturas y, a continuación, restablezca el recuento a cero fallos:

    ```
    authentication_lock_window_seconds: 300
    ```

  - Bloquee la cuenta si se producen cinco fallos dentro del marco temporal de la ventana:

    ```
    authentication_retry_limit: 5
    ```

- Reduzca el impacto de los ataques de adivinación de contraseñas de fuerza bruta estableciendo un retraso que se produce antes de rechazar cada intento, lo que ralentiza los ataques.

  `authentication_failure_delay_seconds: 5`

  ```
  authentication_failure_delay_seconds: 0   # seconds (float) to delay
  failed auth attempts prior to response, 0 = no delay
  authentication_lock_window_seconds: null  # seconds (int) since the
  oldest failure before resetting the retry counter, null = no window
  authentication_retry_limit: null          # number of retries to
  allow before locking API access, null = unlimited
  ```

- **Campos que controlan las reglas de complejidad de la contraseña de la cuenta de usuario de la API de Mediador de ONTAP**

  ```
  password_min_length: 8

  password_max_length: 64

  password_uppercase_chars: 0    # min. uppercase characters

  password_lowercase_chars: 1    # min. lowercase character

  password_special_chars: 1      # min. non-letter, non-digit

  password_nonletter_chars: 2    # min. non-letter characters (digits,
  specials, anything)
  ```

- **Configuración que controla el espacio libre requerido en el `/opt/netapp/lib/ontap_mediator` disco.**

  Si el espacio es inferior al umbral establecido, el servicio emitirá un evento de advertencia.

  ```
  low_space_threshold_mib: 10
  ```

- **Configuración que controla RESERVE_LOG_SPACE.**

  El servidor de ONTAP Mediator por defecto crea un espacio de disco independiente para los registros. El instalador crea un nuevo archivo de tamaño fijo con un total de 700 MB de espacio en disco que se utilizará explícitamente para el registro de Mediator.

  Para desactivar esta función y utilizar el espacio en disco predeterminado, realice los siguientes pasos:

  a. Cambie el valor de RESERVE_LOG_SPACE de «`1`» a «`0`» en el siguiente archivo:

     `/opt/netapp/lib/ontap_mediator/tools/mediator_env`

b. Reinicie Mediator:

i. `cat /opt/netapp/lib/ontap_mediator/tools/mediator_env | grep "RESERVE_LOG_SPACE"`

```
RESERVE_LOG_SPACE=0
```

ii. `systemctl restart ontap_mediator`

Para volver a habilitar la función, cambie el valor de “`0`” a “`1`” y reinicie el Mediador.

> Al alternar entre espacios de disco no se depuran los logs existentes. Se realiza una copia de seguridad de todos los registros anteriores y, a continuación, se mueve al espacio de disco actual después de alternar y reiniciar Mediator.

Gestione el servicio de mediación de ONTAP

Después de instalar el servicio Mediator de ONTAP, es posible que desee cambiar el nombre de usuario o la contraseña. También puede desinstalar el servicio de mediador de ONTAP.

Cambie el nombre de usuario

Acerca de estas tareas

Esta tarea se realiza en el host Linux en el que está instalado el servicio Mediator de ONTAP.

Si no puede alcanzar este comando, puede que deba ejecutar el comando con la ruta completa como se muestra en el ejemplo siguiente:

`/usr/local/bin/mediator_username`

Procedimiento

Cambie el nombre de usuario eligiendo una de las siguientes opciones:

- Ejecute el comando mediador_change_user y responda a las indicaciones como se muestra en el ejemplo siguiente:

```
[root@mediator-host ~]# mediator_change_user
Modify the Mediator API username by entering the following values:
    Mediator API User Name: mediatoradmin
                   Password:
New Mediator API User Name: mediator
The account username has been modified successfully.
[root@mediator-host ~]#
```

- Ejecute el siguiente comando:

```
MEDIATOR_USERNAME=mediator MEDIATOR_PASSWORD=mediator2
MEDIATOR_NEW_USERNAME=mediatoradmin mediator_change_user
```

```
 [root@mediator-host ~]# MEDIATOR_USERNAME= mediator
MEDIATOR_PASSWORD='mediator2' MEDIATOR_NEW_USERNAME= mediatoradmin
mediator_change_user
 The account username has been modified successfully.
 [root@mediator-host ~]#
```

Cambie la contraseña

Acerca de esta tarea

Esta tarea se realiza en el host Linux en el que está instalado el servicio Mediator de ONTAP.

Si no puede alcanzar este comando, puede que deba ejecutar el comando con la ruta completa como se muestra en el ejemplo siguiente:

```
/usr/local/bin/mediator_change_password
```

Procedimiento

Cambie la contraseña eligiendo una de las siguientes opciones:

- Ejecute el `mediator_change_password` y responda a las indicaciones como se muestra en el ejemplo siguiente:

```
[root@mediator-host ~]# mediator_change_password
Change the Mediator API password by entering the following values:
   Mediator API User Name: mediatoradmin
             Old Password:
             New Password:
         Confirm Password:
The password has been updated successfully.
[root@mediator-host ~]#
```

- Ejecute el siguiente comando:

```
MEDIATOR_USERNAME= mediatoradmin MEDIATOR_PASSWORD=mediator1
MEDIATOR_NEW_PASSWORD=mediator2 mediator_change_password
```

  El ejemplo muestra que la contraseña se cambia de “mediator1” a “mediator2”.

```
 [root@mediator-host ~]# MEDIATOR_USERNAME=mediatoradmin
MEDIATOR_PASSWORD=mediator1 MEDIATOR_NEW_PASSWORD=mediator2
mediator_change_password
 The password has been updated successfully.
 [root@mediator-host ~]#
```

Detenga el servicio ONTAP Mediator

Para detener el servicio ONTAP Mediator, realice los siguientes pasos:

Pasos

1. Detenga el Mediador ONTAP.

   ```
   systemctl stop ontap_mediator
   ```

2. Detener SCST.

   ```
   systemctl stop mediator-scst
   ```

3. Desactive ONTAP Mediator y SCST.

   ```
   systemctl diable ontap_mediator mediator-scst
   ```

Vuelva a habilitar el servicio ONTAP Mediator

Para volver a activar el servicio ONTAP Mediator, realice los siguientes pasos:

Pasos

1. Active el Mediador ONTAP y el SCST.

   ```
   systemctl enable ontap_mediator mediator-scst
   ```

2. Inicie SCST.

   ```
   systemctl start mediator-scst
   ```

3. Inicie Mediador ONTAP.

   ```
   systemctl start ontap_mediator
   ```

Compruebe que el mediador ONTAP está en buen estado

Después de instalar ONTAP Mediator, debe verificar que los servicios de ONTAP Mediator se están ejecutando.

Pasos

1. Ver el estado de los servicios de mediador de ONTAP:

   a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

 ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
      ├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      ├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      └─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
   Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
  Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
 Main PID: 286662 (iscsi-scstd)
    Tasks: 1 (limit: 49473)
   Memory: 1.2M
   CGroup: /system.slice/mediator-scst.service
           └─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. Confirme los puertos que utiliza el servicio ONTAP Mediator:

   `netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

         tcp   0   0 0.0.0.0:31784   0.0.0.0:*      LISTEN

         tcp   0   0 0.0.0.0:3260    0.0.0.0:*      LISTEN

         tcp6  0   0 :::3260         :::*           LISTEN
```

Desinstale manualmente SCST para realizar el mantenimiento del host

Para desinstalar SCST, necesita el paquete tar de SCST que se utiliza para la versión instalada de ONTAP Mediator.

Pasos

1. Descargue el paquete SCST adecuado (como se muestra en la siguiente tabla) y desmóntelo.

Para esta versión…	Usar este paquete tar…
Mediador ONTAP 1,7	scst-3,7.0.tar.bz2
Mediador ONTAP 1,6	scst-3,7.0.tar.bz2
Mediador ONTAP 1,5	scst-3,6.0.tar.bz2
Mediador ONTAP 1,4	scst-3,6.0.tar.bz2
Mediador ONTAP 1,3	scst-3,5.0.tar.bz2
Mediador ONTAP 1,1	scst-3,4.0.tar.bz2
Mediador ONTAP 1,0	scst-3,3.0.tar.bz2

2. Emita los siguientes comandos en el directorio scst:
   a. `systemctl stop mediator-scst`
   b. `make scstadm_uninstall`
   c. `make iscsi_uninstall`
   d. `make usr_uninstall`
   e. `make scst_uninstall`
   f. `depmod`

Instale manualmente SCST para realizar el mantenimiento del host

Para instalar manualmente SCST, necesita el paquete tar de SCST que se utiliza para la versión instalada de ONTAP Mediator (consulte la tabla anterior).

1. Emita los siguientes comandos en el directorio scst:
   a. `make 2release`
   b. `make scst_install`
   c. `make usr_install`
   d. `make iscsi_install`
   e. `make scstadm_install`
   f. `depmod`
   g. `cp scst/src/certs/scst_module_key.der /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/.`
   h. `cp scst/src/certs/scst_module_key.der /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/.`
   i. `patch /etc/init.d/scst < /opt/netapp/lib/ontap_mediator/systemd/scst.patch`
2. (Opcional) Si Secure Boot está activado, antes de reiniciar, realice los siguientes pasos:
   a. Determine cada nombre de archivo para los módulos «scst_vdisk», «scst» e «iscsi_scst».

      ```
      [root@localhost ~]# modinfo -n scst_vdisk
      [root@localhost ~]# modinfo -n scst
      [root@localhost ~]# modinfo -n iscsi_scst
      ```

   b. Determine la versión del kernel.

      ```
      [root@localhost ~]# uname -r
      ```

   c. Firmar cada archivo con el núcleo.

      ```
      [root@localhost ~]# /usr/src/kernels/<KERNEL-RELEASE>/scripts/sign-file \sha256 \
      /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.priv \
      /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.der \
      _module-filename_
      ```

   d. Instale la clave correcta con el firmware UEFI.

      Las instrucciones para instalar la clave UEFI se encuentran en:

      `/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-signing`

      La clave UEFI generada se encuentra en:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de
r
```

3. Reinicie.

```
reboot
```

Desinstale el servicio Mediator de ONTAP

Antes de empezar

Si es necesario, puede eliminar el servicio Mediador ONTAP. El Mediador debe desconectarse de ONTAP antes de quitar el servicio Mediator.

Acerca de esta tarea

Esta tarea se realiza en el host Linux en el que está instalado el servicio Mediator de ONTAP.

Si no puede alcanzar este comando, puede que deba ejecutar el comando con la ruta completa como se muestra en el ejemplo siguiente:

```
/usr/local/bin/uninstall_ontap_mediator
```

Paso

1. Desinstale el servicio Mediator de ONTAP:

```
uninstall_ontap_mediator
```

```
 [root@mediator-host ~]# uninstall_ontap_mediator

 ONTAP Mediator: Self Extracting Uninstaller

 + Removing ONTAP Mediator. (Log:
/tmp/ontap_mediator.GmRGdA/uninstall_ontap_mediator/remove.log)
 + Remove successful.
 [root@mediator-host ~]#
```

Vuelva a generar un certificado autofirmado temporal

Acerca de esta tarea

- Esta tarea se realiza en el host Linux en el que está instalado el servicio ONTAP Mediator.
- Puede realizar esta tarea solo si los certificados autofirmados generados se han vuelto obsoletos debido a cambios en el nombre de host o la dirección IP del host después de instalar ONTAP Mediator.
- Una vez que el certificado autofirmado temporal ha sido reemplazado por un certificado de terceros de confianza, *NOT* use esta tarea para regenerar un certificado. La ausencia de un certificado autofirmado provocará que falle este procedimiento.

Paso

Para regenerar un nuevo certificado autofirmado temporal para el host actual, realice el siguiente paso:

1. Reinicie el Mediador ONTAP:

```
./make_self_signed_certs.sh overwrite
```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................
.....................................................................
..................++++
.......................................................++++
e is 65537 (0x010001)
Generating a RSA private key
...............................................++++
.....................................................................
.....................................................................+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key
```

Mantener el host del sistema operativo para ONTAP Mediator

Para obtener un rendimiento óptimo, debe mantener regularmente el sistema operativo host para ONTAP Mediator.

Reinicie el host

Reinicie el host cuando el estado de los clústeres sea bueno. Mientras que ONTAP Mediator no está conectado, los clústeres corren el riesgo de no poder reaccionar correctamente ante fallos. Se recomienda una ventana de servicio si es necesario reiniciar.

ONTAP Mediator se reanudará automáticamente durante un reinicio y volverá a introducir las relaciones que se hayan configurado previamente con los clústeres de ONTAP.

Actualizaciones del paquete de host

Cualquier biblioteca o paquete yum (excepto el kernel) se puede actualizar de forma segura, pero puede requerir un reinicio para que surta efecto. Se recomienda una ventana de servicio si es necesario reiniciar.

Si instala el `yum-utils` paquete, utilice el `needs-restarting` comando para detectar si algún cambio de paquete requiere un reinicio.

Debe reiniciar si se actualiza alguna de las dependencias de Mediador de ONTAP porque no surtirán efecto inmediato en los procesos en ejecución.

Actualizaciones del kernel inferiores del sistema operativo host

Se debe compilar SCST para el núcleo que se está utilizando. Para actualizar el sistema operativo, se necesita una ventana de mantenimiento.

Pasos

Realice los siguientes pasos para actualizar el kernel del sistema operativo host.

1. Detenga el Mediador ONTAP
2. Desinstale el paquete SCST. (SCST no proporciona un mecanismo de actualización.)
3. Actualice el sistema operativo y reinicie.
4. Vuelva a instalar el paquete SCST.
5. Vuelva a habilitar los servicios de ONTAP Mediator.

El host cambia al nombre de host o IP

Acerca de esta tarea

- Esta tarea se realiza en el host Linux en el que está instalado el servicio ONTAP Mediator.
- Puede realizar esta tarea solo si los certificados autofirmados generados se han vuelto obsoletos debido a cambios en el nombre de host o la dirección IP del host después de instalar ONTAP Mediator.
- Una vez que el certificado autofirmado temporal ha sido reemplazado por un certificado de terceros de confianza, *NOT* use esta tarea para regenerar un certificado. La ausencia de un certificado autofirmado provocará que falle este procedimiento.

Paso

Para regenerar un nuevo certificado autofirmado temporal para el host actual, realice el siguiente paso:

1. Reinicie el Mediador ONTAP:

   ```
   ./make_self_signed_certs.sh overwrite
   ```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................
.....................................................................
..................++++
.......................................................++++
e is 65537 (0x010001)
Generating a RSA private key
...............................................++++
.....................................................................
.....................................................................+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key

[root@xyz000123456 server_config]# systemctl restart ontap_mediator
```

Gestione sitios de MetroCluster con System Manager

Información general sobre la gestión de sitios de MetroCluster con System Manager

A partir de ONTAP 9.8, es posible usar System Manager como interfaz simplificado para gestionar una configuración de MetroCluster.

Una configuración MetroCluster permite que dos clústeres reflejen datos entre sí por lo que si un clúster deja de funcionar, los datos no se pierden.

Normalmente, una organización configura los clústeres en dos ubicaciones geográficas independientes. Un administrador en cada ubicación establece un clúster y lo configura. A continuación, uno de los administradores puede configurar la relación entre iguales entre los clústeres para que puedan compartir datos.

La organización también puede instalar un Mediador ONTAP en una tercera ubicación. El servicio Mediador

ONTAP supervisa el estado de cada clúster. Cuando uno de los clústeres detecta que no puede comunicarse con el clúster asociado, consulta al monitor para determinar si el error es un problema con el sistema del clúster o con la conexión de red.

Si el problema está relacionado con la conexión de red, el administrador del sistema realiza métodos de solución de problemas para corregir el error y volver a conectarlo. Si el clúster de partners está inactivo, el otro clúster inicia un proceso de conmutación por sitios para controlar las operaciones de I/o de datos de ambos clústeres.

También puede realizar una conmutación de sitios para desconectar uno de los sistemas de clúster para el mantenimiento planificado. El clúster de partners gestiona todas las operaciones de I/o de datos de ambos clústeres hasta que se ponga en marcha el clúster en el cual usted llevó a cabo el mantenimiento y lleva a cabo una operación de conmutación de estado.

Es posible gestionar las siguientes operaciones:

- "Configure un sitio MetroCluster IP"
- "Configurar IP MetroCluster peering"
- "Configure un sitio MetroCluster IP"
- "Lleve a cabo conmutación de sitios y conmutación de estado de MetroCluster IP"
- "Solucionar problemas relacionados con la configuración de MetroCluster IP"
- "Actualice ONTAP en clústeres de MetroCluster"

Configure un sitio MetroCluster IP

A partir de ONTAP 9.8, puede usar System Manager para configurar una configuración IP de un sitio de MetroCluster.

Un sitio MetroCluster consta de dos clústeres. Normalmente, los clústeres se encuentran en diferentes ubicaciones geográficas.

Antes de empezar

- El sistema ya debe estar instalado y cableado de acuerdo con "Instrucciones de instalación y configuración" eso vino con el sistema.
- Las interfaces de red de clúster se deben configurar en cada nodo de cada clúster para la comunicación dentro del clúster.

Asigne una dirección IP de gestión de nodos

Sistema Windows

Debe conectar el equipo con Windows a la misma subred que las controladoras. De este modo se asignará automáticamente una dirección IP de gestión de nodos al sistema.

Pasos

1. Desde el sistema Windows, abra la unidad **Network** para descubrir los nodos.
2. Haga doble clic en el nodo para iniciar el asistente de configuración de clúster.

Otros sistemas

Debe configurar la dirección IP de gestión de nodos para uno de los nodos del clúster. Puede usar esta dirección IP de gestión de nodos para iniciar el asistente de configuración del clúster.

Consulte "Creación del clúster en el primer nodo" Para obtener información sobre la asignación de una dirección IP de gestión de nodos.

Inicialice y configure el clúster

Para inicializar el clúster, debe establecer una contraseña de administrador para el clúster y configurar las redes de gestión de clústeres y nodos. También puede configurar servicios como un servidor DNS para resolver nombres de host y un servidor NTP para sincronizar la hora.

Pasos

1. En un navegador web, introduzca la dirección IP de gestión de nodos que haya configurado: "https://node-management-IP"

   System Manager detecta automáticamente los nodos restantes del clúster.

2. En la ventana **inicializar sistema de almacenamiento**, realice lo siguiente:
   a. Introduzca los datos de configuración de la red de gestión del clúster.
   b. Introduzca las direcciones IP de gestión de nodos para todos los nodos.
   c. Proporcione detalles sobre los servidores de nombres de dominio (DNS).
   d. En la sección **otros**, active la casilla de verificación con la etiqueta **usar servicio de hora (NTP)** para agregar los servidores de hora.

Al hacer clic en **Enviar**, espere a que se cree y configure el clúster. A continuación, se produce un proceso de validación.

El futuro

Una vez que se hayan configurado, inicializado y configurado ambos clústeres, siga el siguiente procedimiento:

- "Configurar IP MetroCluster peering"

Configure ONTAP en un vídeo de clúster nuevo

Configurar IP MetroCluster peering

A partir de ONTAP 9.8, es posible gestionar una configuración IP de una operación de MetroCluster con System Manager. Después de configurar dos clústeres, debe configurar la configuración de paridad entre ellos.

Antes de empezar

Debe haber completado el siguiente procedimiento para configurar dos clústeres:

- "Configure un sitio MetroCluster IP"

Diferentes administradores del sistema ubicados en los sitios geográficos de cada clúster llevan a cabo algunos pasos de este proceso. Para explicar este proceso, los clústeres se denominan "clúster del sitio A" y "clúster del sitio B".

Realización del proceso de relaciones entre iguales desde el sitio A

Este proceso lo realiza un administrador del sistema en el Sitio A.

Pasos

1. Inicie sesión en Site A cluster.
2. En System Manager, seleccione **Dashboard** en la columna de navegación de la izquierda para mostrar la descripción general del clúster.

   La consola muestra los detalles de este clúster (Sitio A). En la sección **MetroCluster**, Site A se muestra un clúster a la izquierda.

3. Haga clic en **Adjuntar clúster de partners**.
4. Introduzca los detalles de las interfaces de red que permiten que los nodos del clúster del sitio A se

comuniquen con los nodos del clúster del sitio B.

5. Haga clic en **Guardar y continuar**.
6. En la ventana **Adjuntar clúster de socios**, seleccione **no tengo una contraseña**, lo que le permite generar una frase de contraseña.
7. Copie la frase de contraseña generada y compártela con el administrador del sistema en el sitio B.
8. Seleccione **Cerrar**.

Realización del proceso de relaciones entre iguales desde el sitio B

Este proceso lo lleva a cabo un administrador del sistema en el Sitio B.

Pasos

1. Inicie sesión en el clúster del sitio B.
2. En System Manager, seleccione **Dashboard** para mostrar la descripción general del clúster.

   La consola muestra los detalles de este clúster (sitio B). En la sección MetroCluster, el clúster del sitio B se muestra a la izquierda.

3. Haga clic en **Adjuntar clúster de socios** para iniciar el proceso de relaciones entre iguales.
4. Introduzca los detalles de las interfaces de red que permiten que los nodos del clúster del sitio B se comuniquen con los nodos del clúster del sitio A.
5. Haga clic en **Guardar y continuar**.
6. En la ventana **Adjuntar clúster de socios**, seleccione **Tengo una contraseña**, que le permite introducir la frase de contraseña que recibió del administrador del sistema en el sitio A.
7. Seleccione **Peer** para completar el proceso de comparación.

El futuro

Una vez que el proceso de relaciones entre iguales se haya completado correctamente, puede configurar los clústeres. Consulte "Configure un sitio MetroCluster IP".

Configure un sitio MetroCluster IP

A partir de ONTAP 9.8, es posible gestionar una configuración IP de una operación de MetroCluster con System Manager. Después de configurar dos clústeres y realizar una conexión entre iguales, debe configurar cada clúster.

Antes de empezar

Debe haber completado los siguientes procedimientos:

- "Configure un sitio MetroCluster IP"
- "Configurar IP MetroCluster peering"

Configure la conexión entre clústeres

Pasos

1. Inicie sesión en System Manager en uno de los sitios y seleccione **Panel**.

   En la sección **MetroCluster**, el gráfico muestra los dos clústeres que ha configurado y tiene una relación

entre iguales para los sitios MetroCluster. El clúster del que está trabajando desde (clúster local) se muestra a la izquierda.

2. Haga clic en **Configurar MetroCluster**. Desde esta ventana, puede realizar las siguientes tareas:
   a. Se muestran los nodos para cada clúster en la configuración de MetroCluster. Use las listas desplegables para seleccionar qué nodos del clúster local serán partners de recuperación ante desastres con los que se encuentre el clúster remoto.
   b. Haga clic en la casilla de verificación si desea configurar un servicio Mediador ONTAP. Consulte Configure el servicio Mediator de ONTAP.
   c. Si ambos clústeres tienen una licencia para habilitar el cifrado, se muestra la sección **cifrado**.

      Para habilitar el cifrado, introduzca una frase de contraseña.

   d. Haga clic en la casilla de verificación si desea configurar MetroCluster con una red de capa 3 compartida.

      Los nodos asociados de alta disponibilidad y los switches de red que se conectan a los nodos deben tener una configuración coincidente.

3. Haga clic en **Guardar** para configurar los sitios MetroCluster.

   En la sección **Tablero**, en la sección **MetroCluster**, el gráfico muestra una Marca de verificación en el enlace entre los dos grupos, lo que indica una conexión en buen estado.

Configure el servicio Mediator de ONTAP

El servicio Mediador ONTAP se instala normalmente en una ubicación geográfica independiente de cualquiera de las ubicaciones de los clusters. Los clústeres se comunican regularmente con el servicio para indicar que están activos y en ejecución. Si uno de los clústeres de la configuración de MetroCluster detecta que la comunicación con su clúster asociado está inactiva, se comprueba con el Mediador de ONTAP para determinar si el propio clúster asociado está inactivo.

Antes de empezar

Los dos clústeres de los sitios de MetroCluster deben tener una relación entre iguales.

Pasos

1. En el Administrador del sistema de ONTAP 9.8, seleccione **clúster > Configuración**.
2. En la sección **Mediator**, haga clic en ⚙.
3. En la ventana **Configurar Mediator**, haga clic en **Agregar+**.
4. Introduzca los detalles de configuración del Mediador ONTAP.

   Puede introducir los siguientes detalles al configurar un mediador de ONTAP con System Manager.

   - La dirección IP del Mediador.
   - El nombre de usuario.
   - La contraseña.

Gestiona el Mediador con System Manager

Con System Manager, puede realizar tareas para gestionar Mediator.

Acerca de estas tareas

A partir de ONTAP 9,8, puede usar System Manager como una interfaz simplificada para gestionar una configuración IP de cuatro nodos de una configuración de MetroCluster, que puede incluir un Mediator ONTAP instalado en una tercera ubicación.

A partir de ONTAP 9.14.1, se puede usar System Manager para realizar también estas operaciones para una configuración IP de ocho nodos de un sitio MetroCluster. Aunque no puede configurar o expandir un sistema de ocho nodos con System Manager, si ya configuró un sistema MetroCluster IP de ocho nodos, podrá realizar estas operaciones.

Realice las siguientes tareas para gestionar el Mediador.

Para realizar esta tarea…	Realice estas acciones…
Configure el servicio de Mediator	Siga los pasos de "Configure el servicio Mediator de ONTAP".
Activar o desactivar el cambio automático asistido por mediador (MAUSO)	1. En System Manager, haga clic en **Panel**. 2. Desplácese hasta la sección MetroCluster. 3. Haga clic en ⋮ Junto al nombre del sitio MetroCluster. 4. Seleccione **Activar** o **Desactivar**. 5. Introduzca el nombre de usuario y la contraseña del administrador, luego haga clic en **Habilitar** o **Deshabilitar**. ⓘ Puede activar o desactivar el Mediador cuando se puede acceder a él y ambos sitios están en modo “Normal”. El Mediador sigue estando disponible cuando MAUSO está activado o desactivado si el sistema MetroCluster está en buen estado.
Elimine Mediator de la configuración de MetroCluster	1. En System Manager, haga clic en **Panel**. 2. Desplácese hasta la sección MetroCluster. 3. Haga clic en ⋮ Junto al nombre del sitio MetroCluster. 4. Selecciona **Eliminar Mediador**. 5. Introduzca el nombre de usuario y la contraseña del administrador, luego haga clic en **Eliminar**.
Compruebe el estado del Mediador	Siga los pasos de "Solucionar problemas relacionados con la configuración de MetroCluster IP".
Realice una conmutación de sitios y una conmutación de retorno	Siga los pasos de "Lleve a cabo conmutación de sitios y conmutación de estado de MetroCluster IP".

Lleve a cabo conmutación de sitios y conmutación de estado de MetroCluster IP

Puede conmutar el control de un sitio IP MetroCluster al otro para realizar tareas de mantenimiento o recuperación de un problema.

> Los procedimientos de conmutación de sitios y conmutación de estado solo son compatibles con las configuraciones de MetroCluster IP.

Información general sobre conmutación de sitios y conmutación de estado

Un cambio puede producirse en dos instancias:

- **Un cambio planificado**

  Este cambio lo inicia un administrador del sistema mediante System Manager. La conmutación planificada permite al administrador de sistema de un clúster local controlar los switches de manera que los servicios de datos del clúster remoto se puedan gestionar mediante el clúster local. A continuación, un administrador del sistema en la ubicación de clúster remoto puede realizar tareas de mantenimiento en el clúster remoto.

- **Un cambio no planificado**

  En algunos casos, cuando un clúster MetroCluster cae o las conexiones entre los clústeres están inhabilitadas, ONTAP iniciará automáticamente un procedimiento de conmutación de modo que el clúster que aún se esté ejecutando gestione las responsabilidades de gestión de datos del clúster inactivo.

  Otras veces, cuando ONTAP no puede determinar el estado de uno de los clústeres, el administrador del sistema del sitio que está trabajando inicia el procedimiento de conmutación para tomar el control de las responsabilidades de manejo de datos del otro sitio.

En el caso de cualquier tipo de procedimiento de conmutación, la funcionalidad de servicio de datos vuelve al clúster usando un proceso *regresar*.

Usted lleva a cabo distintos procesos de conmutación de sitios y conmutación de estado para ONTAP 9.7 y 9.8:

- Use System Manager en ONTAP 9.7 para conmutación y conmutación de estado
- Utilice System Manager en ONTAP 9,8 para conmutación de sitios y conmutación de estado

Use System Manager en ONTAP 9.7 para conmutación y conmutación de estado

Pasos

1. Inicie sesión en System Manager en ONTAP 9.7.
2. Haga clic en **(Volver a la versión clásica)**.
3. Haga clic en **Configuración > MetroCluster**.

   System Manager verifica si es posible una conmutación negociada.

4. Realice uno de los siguientes subpasos cuando el proceso de validación haya finalizado:
   a. Si la validación falla, pero el sitio B está activo, se ha producido un error. Por ejemplo, es posible que haya un problema con un subsistema o que la duplicación de NVRAM no se sincronice.

i. Solucione el problema que está causando el error, haga clic en **Cerrar** y, a continuación, vuelva a comenzar en el paso 2.

ii. Detenga los nodos del sitio B, haga clic en **Cerrar** y, a continuación, realice los pasos en "Realizar una conmutación de sitios no planificada".

b. Si la validación falla y el sitio B está inactivo, lo más probable es que haya un problema de conexión. Compruebe que el sitio B está realmente inactivo y, a continuación, realice los pasos de "Realizar una conmutación de sitios no planificada".

5. Haga clic en **Cambio del sitio B al sitio A** para iniciar el proceso de cambio.
6. Haga clic en **Cambiar a la nueva experiencia**.

Utilice System Manager en ONTAP 9,8 para conmutación de sitios y conmutación de estado

Realizar una conmutación de sitios planificada (ONTAP 9.8)

Pasos

1. Inicie sesión en System Manager en ONTAP 9,8.
2. Seleccione **Panel**. En la sección **MetroCluster**, los dos clústeres se muestran con una conexión.
3. En el clúster local (que se muestra a la izquierda), haga clic en ⋮Y seleccione **Cambio de servicios de datos remotos al sitio local**.

   Una vez validada la solicitud de conmutación, el control se transfiere del sitio remoto al sitio local, que ejecuta solicitudes de servicio de datos de ambos clústeres.

   El clúster remoto se reinicia, pero los componentes de almacenamiento no están activos y el clúster no ofrece servicio a las solicitudes de datos. Ahora está disponible para el mantenimiento planificado.

> El clúster remoto no se debe utilizar para el mantenimiento de datos hasta que lleve a cabo una conmutación de estado.

Realizar una conmutación de sitios no planificada (ONTAP 9.8)

ONTAP puede iniciar automáticamente un cambio no planificado. Si ONTAP no puede determinar si es necesaria una conmutación de estado, el administrador del sistema del sitio de MetroCluster que aún se ejecuta inicia la conmutación de sitios con los siguientes pasos:

Pasos

1. Inicie sesión en System Manager en ONTAP 9,8.
2. Seleccione **Panel**.

   En la sección **MetroCluster**, la conexión entre los dos clústeres se muestra con una "X", lo que significa que no se puede detectar una conexión. Las conexiones o el clúster están inactivos.

3. En el clúster local (que se muestra a la izquierda), haga clic en ⋮Y seleccione **Cambio de servicios de datos remotos al sitio local**.

   Si se produce un error en la conmutación, haga clic en el enlace "View details" en el mensaje de error y confirme la conmutación no planificada.

   Una vez validada la solicitud de conmutación, el control se transfiere del sitio remoto al sitio local, que ejecuta solicitudes de servicio de datos de ambos clústeres.

El clúster se debe reparar antes de que vuelva a estar conectado.

> Una vez que el clúster remoto vuelve a estar en línea, no se debe usar para el servicio de datos hasta que vuelva a realizar una conmutación de estado.

Lleve a cabo una conmutación de estado (ONTAP 9.8)

Antes de empezar

Ya sea que el clúster remoto no estaba disponible debido a un mantenimiento planificado o debido a un desastre, ahora debería estar listo y en funcionamiento y esperar a que se produzca la conmutación de estado.

Pasos

1. En el clúster local, inicie sesión en System Manager en ONTAP 9.8.
2. Seleccione **Panel**.

   En la sección **MetroCluster**, se muestran los dos clústeres.

3. En el clúster local (que se muestra a la izquierda), haga clic en ⋮Y seleccione **recuperar control**.

   Los datos son *sanated* en primer lugar, para garantizar que los datos se sincronizan y se duplican entre ambos clústeres.

4. Cuando se complete la reparación de los datos, haga clic en ⋮Y seleccione **Iniciar regreso**.

   Una vez finalizada la conmutación de estado, ambos clústeres están activos y prestan servicio a las solicitudes de datos. Además, los datos se están reflejando y sincronizando entre los clústeres.

Modificar la dirección, la máscara de red y la pasarela en una IP de MetroCluster

A partir de ONTAP 9.10.1, puede cambiar las siguientes propiedades de una interfaz IP de MetroCluster: Dirección IP, máscara y puerta de enlace. Puede usar cualquier combinación de parámetros para actualizar.

Es posible que deba actualizar estas propiedades, por ejemplo, si se detecta una dirección IP duplicada o si una puerta de enlace necesita cambiar en el caso de una red de capa 3 debido a cambios en la configuración del enrutador. Sólo puede cambiar una interfaz a la vez. Habrá interrupciones en el tráfico en esa interfaz hasta que se actualicen las otras interfaces y se restablezcan las conexiones.

> Debe realizar los cambios en cada puerto. De igual modo, los switches de red también deben actualizar su configuración. Por ejemplo, si la puerta de enlace se actualiza, lo ideal es que cambie en ambos nodos de un par de alta disponibilidad, ya que son los mismos. Además, el switch conectado a dichos nodos también debe actualizar su puerta de enlace.

Paso

Actualice la dirección IP, la máscara de red y la pasarela de cada nodo e interfaz.

Solucionar problemas relacionados con la configuración de MetroCluster IP

A partir de ONTAP 9.8, System Manager supervisa el estado de las configuraciones de

MetroCluster IP y ayuda a identificar y corregir los problemas que pueden ocurrir.

Descripción general de la comprobación del estado de MetroCluster

System Manager comprueba periódicamente el estado de la configuración de MetroCluster IP. Cuando ve la sección MetroCluster en la Consola, normalmente el mensaje es "los sistemas MetroCluster están en buen estado".

Sin embargo, cuando se produce un problema, el mensaje mostrará el número de eventos. Puede hacer clic en ese mensaje y ver los resultados de la comprobación de estado de los siguientes componentes:

- Nodo
- Interfaz de red
- Nivel (almacenamiento)
- Clúster
- Conexión
- Volumen
- Replicación de la configuración

La columna **Estado** identifica qué componentes tienen problemas, y la columna **Detalles** sugiere cómo corregir el problema.

Resolución de problemas de MetroCluster

Pasos

1. En System Manager, seleccione **Panel**.
2. En la sección **MetroCluster**, observe el mensaje.
   a. Si el mensaje indica que la configuración de MetroCluster es correcta y que las conexiones entre los clústeres y el Mediador ONTAP están en buen estado (se muestra con marcas de comprobación), no tiene problemas para corregir.
   b. Si el mensaje enumera el número de eventos o las conexiones han caído (se muestra con una "X"), continúe con el paso siguiente.
3. Haga clic en el mensaje que muestra el número de eventos.

   Aparecerá el Informe de estado de MetroCluster.
4. Solucione los problemas que aparecen en el informe con las sugerencias de la columna **Detalles**.
5. Una vez corregidos todos los problemas, haga clic en **comprobar estado de MetroCluster**.

   > La comprobación del estado de MetroCluster utiliza una cantidad intensiva de recursos, por lo que se recomienda realizar todas las tareas de solución de problemas antes de ejecutar la comprobación.

   La comprobación del estado de MetroCluster se ejecuta en segundo plano. Puede trabajar en otras tareas mientras espera a que finalice.

Protección de datos mediante backup en cinta

Información general sobre backup a cinta de volúmenes de FlexVol

ONTAP es compatible con los procesos de backup y restauración a cinta mediante el protocolo de gestión de datos de red (NDMP). NDMP le permite realizar backups de datos en sistemas de almacenamiento directamente en cinta, lo cual resulta en un uso más eficiente del ancho de banda de la red. ONTAP es compatible con los motores de volcado y SMTape para backups a cinta.

Puede realizar backups o restauraciones de volcado o SMTape mediante aplicaciones de backup compatibles con NDMP. Solo se admite la versión 4 de NDMP.

Copia de seguridad en cinta mediante volcado

Dump es un backup basado en copias snapshot en el cual se realiza un backup de los datos del sistema de archivos en cinta. El motor de volcado ONTAP realiza copias de seguridad de los archivos, directorios y la información de la lista de control de acceso (ACL) aplicable a la cinta. Puede realizar un backup de un volumen completo, de un qtree completo o de un subárbol que no sea un volumen completo o un qtree completo. El volcado admite copias de seguridad de línea base, diferencial e incrementales.

Backup en cinta con SMTape

SMTape es una solución de recuperación ante desastres basada en copias de Snapshot de ONTAP que realiza backup de bloques de datos a cinta. Puede usar SMTape para realizar backups de volúmenes a las cintas. Sin embargo, no puede realizar un backup en el nivel qtree o subárbol. SMTape admite copias de seguridad de línea base, diferenciales e incrementales.

A partir de ONTAP 9.13.1, el backup en cinta con SMTape admite con Continuidad del negocio de SnapMirror.

Flujo de trabajo de backup y restauración a cinta

Es posible realizar operaciones de backup y restauración a cinta con una aplicación de backup habilitada para NDMP.

Acerca de esta tarea

El flujo de trabajo de backup y restauración a cinta ofrece información general de las tareas relacionadas con las operaciones de backup y restauración en cinta. Para obtener información detallada sobre cómo realizar una operación de backup y restauración, consulte la documentación de la aplicación de backup.

Pasos

1. Configure una biblioteca de cintas eligiendo una topología de cinta compatible con NDMP.
2. Active los servicios NDMP en el sistema de almacenamiento.

   Puede habilitar los servicios NDMP en el nivel del nodo o en el nivel de la máquina virtual de almacenamiento (SVM). Esto depende del modo NDMP en el que elija ejecutar las operaciones de backup y restauración a cinta.

3. Utilice las opciones NDMP para gestionar NDMP en su sistema de almacenamiento.

   Puede usar las opciones de NDMP a nivel de nodo o de SVM. Esto depende del modo NDMP en el que

elija ejecutar las operaciones de backup y restauración a cinta.

Puede modificar las opciones de NDMP en el nivel de nodo mediante el `system services ndmp modify` Y en el nivel de SVM mediante el `vserver services ndmp modify` comando. Para obtener más información sobre estos comandos, consulte las páginas man.

4. Realizar un backup a cinta o una restauración de datos mediante una aplicación de backup compatible con NDMP.

   ONTAP es compatible con los motores de volcado y SMTape para backup y restauración a cinta.

   Para obtener más información acerca del uso de la aplicación de copia de seguridad (también denominada *Data Management Applications* o *DMAs*) para realizar operaciones de copia de seguridad o restauración, consulte la documentación de la aplicación de copia de seguridad.

Información relacionada

Topologías habituales de backup en cinta NDMP

Motor de volcado para volúmenes FlexVol

Casos de uso a la hora de elegir un motor de backup en cinta

ONTAP admite dos motores de respaldo: SMTape y dump. Debe conocer los casos de uso de los motores de copia de seguridad SMTape y de volcado para ayudarle a elegir el motor de copia de seguridad para realizar operaciones de copia de seguridad en cinta y restauración.

El volcado se puede utilizar en los siguientes casos:

- Recuperación de acceso directo (DAR) de ficheros y directorios
- Copia de seguridad de un subconjunto de subdirectorios o archivos en una ruta de acceso específica
- Exclusión de archivos y directorios específicos durante las copias de seguridad
- Conservación del backup a largo plazo

SMTape se puede utilizar en los siguientes casos:

- Solución de recuperación tras siniestros
- Conservación del ahorro de la deduplicación y de la configuración de deduplicación en los datos de backup durante la operación de restauración
- Backup de grandes volúmenes

Gestión de unidades de cinta

Descripción general de la administración de unidades de cinta

Puede verificar las conexiones de la biblioteca de cintas y ver la información de la unidad de cinta antes de realizar una operación de backup o restauración de cinta. Puede utilizar una unidad de cinta no cualificada emulando esta unidad a una unidad de cinta cualificada. También puede asignar y eliminar alias de cinta además de ver los alias

existentes.

Cuando se realiza el backup de los datos en cinta, estos se almacenan en archivos de cinta. Las marcas de archivo separan los archivos de cinta y los archivos no tienen nombres. Especifique un archivo de cinta por su posición en la cinta. Se escribe un archivo de cinta mediante un dispositivo de cinta. Cuando lea el archivo de cinta, debe especificar un dispositivo que tenga el mismo tipo de compresión que utilizó para escribir ese archivo de cinta.

Comandos para gestionar unidades de cinta, cambiadores de medios y operaciones de unidades de cinta

Hay comandos para ver información acerca de las unidades de cinta y los intercambiadores de medios en un clúster, conectar una unidad de cinta y desconectarla, modificar la posición del cartucho de la unidad de cinta, configurar y borrar el nombre del alias de la unidad de cinta y restablecer una unidad de cinta. También es posible ver y restablecer las estadísticas de la unidad de cinta.

Si desea…	Se usa este comando…
Conectar una unidad de cinta	`storage tape online`
Borre un nombre de alias para la unidad de cinta o el cambiador de medios	`storage tape alias clear`
Activar o desactivar una operación de rastreo de cinta para una unidad de cinta	`storage tape trace`
Modifique la posición del cartucho de la unidad de cinta	`storage tape position`
Restablezca una unidad de cinta	`storage tape reset` Este comando solo está disponible en el nivel de privilegios avanzados.
Defina un nombre de alias para la unidad de cinta o el cambiador de medios	`storage tape alias set`
Desconectar una unidad de cinta	`storage tape offline`
Ver información acerca de todas las unidades de cinta e intercambiadores de medios	`storage tape show`
Ver información acerca de las unidades de cinta conectadas al clúster	• `storage tape show-tape-drive` • `system node hardware tape drive show`

Si desea…	Se usa este comando…
Ver información acerca de los cambiadores de medios conectados al clúster	`storage tape show-media-changer`
Ver información de errores sobre las unidades de cinta conectadas al clúster	`storage tape show-errors`
Ver todas las unidades de cinta cualificadas y compatibles de ONTAP conectadas a cada nodo del clúster	`storage tape show-supported-status`
Vea alias de todas las unidades de cinta e intercambiadores de medios conectados a cada nodo del clúster	`storage tape alias show`
Restablece la lectura de estadísticas de una unidad de cinta a cero	`storage stats tape zero tape_name` Debe utilizar este comando en el nodeshell.
Vea las unidades de cinta compatibles con ONTAP	`storage show tape supported [-v]` Debe utilizar este comando en el nodeshell. Puede utilizar el `-v` opción para ver más detalles sobre cada unidad de cinta.
Vea las estadísticas de dispositivos de cinta para comprender el rendimiento de la cinta y comprobar los patrones de uso	`storage stats tape tape_name` Debe utilizar este comando en el nodeshell.

Para obtener más información sobre estos comandos, consulte las páginas man.

Utilice una unidad de cinta no cualificada

Puede utilizar una unidad de cinta no cualificada en un sistema de almacenamiento si puede emular una unidad de cinta cualificada. Luego se trata como una unidad de cinta cualificada. Para utilizar una unidad de cinta no cualificada, primero debe determinar si emula cualquiera de las unidades de cinta cualificadas.

Acerca de esta tarea

Una unidad de cinta no cualificada es una unidad conectada al sistema de almacenamiento, pero que ONTAP no admite ni reconoce.

Pasos

1. Consulte las unidades de cinta no cualificadas conectadas a un sistema de almacenamiento mediante la `storage tape show-supported-status` comando.

   El siguiente comando muestra las unidades de cinta conectadas al sistema de almacenamiento y el estado de soporte y cualificación de cada unidad de cinta. También se enumeran las unidades de cinta no

cualificadas. `tape_drive_vendor_name` Es una unidad de cinta no cualificada conectada al sistema de almacenamiento, pero que no es compatible con ONTAP.

```
cluster1::> storage tape show-supported-status -node Node1

          Node: Node1
                                    Is
          Tape Drive                Supported  Support Status
          --------------------      ---------  --------------
          "tape_drive_vendor_name"  false      Nonqualified tape drive
          Hewlett-Packard C1533A    true       Qualified
          Hewlett-Packard C1553A    true       Qualified
          Hewlett-Packard Ultrium 1 true       Qualified
          Sony SDX-300C             true       Qualified
          Sony SDX-500C             true       Qualified
          StorageTek T9840C         true       Dynamically Qualified
          StorageTek T9840D         true       Dynamically Qualified
          Tandberg LTO-2 HH         true       Dynamically Qualified
```

2. Emular la unidad de cinta cualificada.

   "Descargas de NetApp: Archivos de configuración de dispositivo de cinta"

Información relacionada

Qué son las unidades de cinta adecuadas

Asigne alias de cinta

Para facilitar la identificación del dispositivo, puede asignar alias de cinta a una unidad de cinta o a un cambiador de medios. Los alias proporcionan una correspondencia entre los nombres lógicos de los dispositivos de copia de seguridad y un nombre asignado permanentemente a la unidad de cinta o al cambiador de medios.

Pasos

1. Asigne un alias a una unidad de cinta o a un cambiador de medios mediante el `storage tape alias set` comando.

   Para obtener más información acerca de este comando, consulte las páginas man.

   Puede ver la información sobre el número de serie (SN) de las unidades de cinta mediante el `system node hardware tape drive show` y acerca de las bibliotecas de cintas mediante el `system node hardware tape library show` comandos.

   El siguiente comando establece un nombre de alias en una unidad de cinta con el número de serie SN[123456]L4 conectado al nodo, cluster1-01:

```
cluster-01::> storage tape alias set  -node cluster-01 -name st3
-mapping SN[123456]L4
```

El siguiente comando establece un nombre de alias en un cambiador de medios con el número de serie SN[65432] conectado al nodo, cluster1-01:

```
cluster-01::> storage tape alias set  -node cluster-01 -name mc1
-mapping SN[65432]
```

Información relacionada

Qué es el solapamiento de cinta

Eliminación de alias de cinta

Elimine los alias de cinta

Puede eliminar alias utilizando `storage tape alias clear` comando cuando ya no se necesitan alias persistentes para una unidad de cinta o un cambiador de medios.

Pasos

1. Retire un alias de una unidad de cinta o de un cambiador de medios mediante el `storage tape alias clear` comando.

   Para obtener más información acerca de este comando, consulte las páginas man.

   El siguiente comando elimina los alias de todas las unidades de cinta especificando el ámbito de la operación de alias Clear `tape`:

   ```
   cluster-01::>storage tape alias clear -node cluster-01 -clear-scope tape
   ```

Después de terminar

Si va a realizar una operación de backup o restauración de cinta mediante NDMP, después de eliminar un alias de una unidad de cinta o un cambiador de medios, debe asignar un nuevo nombre de alias a la unidad de cinta o al cambiador de medios para continuar accediendo al dispositivo de cinta.

Información relacionada

Qué es el solapamiento de cinta

Asignación de alias de cinta

Activación o desactivación de reservas de cinta

Puede controlar cómo ONTAP administra las reservas de dispositivos de cinta mediante la `tape.reservations` opción. De forma predeterminada, la reserva de cinta está desactivada.

Acerca de esta tarea

La activación de la opción de reservas de cintas puede ocasionar problemas si las unidades de cinta, los cambiadores de medios, los puentes o las bibliotecas no funcionan correctamente. Si los comandos de cinta indican que el dispositivo está reservado cuando no hay otros sistemas de almacenamiento que utilicen el dispositivo, esta opción debería estar desactivada.

Pasos

1. Para utilizar el mecanismo de reserva/liberación SCSI o la reserva persistente SCSI para desactivar las reservas en cinta, introduzca el siguiente comando en el clustershell:

   `options -option-name tape.reservations -option-value {scsi | persistent | off}`

   `scsi` Selecciona el mecanismo de reserva/liberación SCSI.

   `persistent` Selecciona Reservas persistentes SCSI.

   `off` desactiva las reservas de cinta.

Información relacionada

Qué reservas de cinta son

Comandos para verificar las conexiones de la biblioteca de cintas

Puede ver información acerca de la ruta de conexión entre un sistema de almacenamiento y una configuración de biblioteca de cintas conectada al sistema de almacenamiento. Puede utilizar esta información para verificar la ruta de conexión a la configuración de la biblioteca de cintas o para solucionar problemas relacionados con las rutas de conexión.

Puede ver los siguientes detalles de la biblioteca de cintas para verificar las conexiones de la biblioteca de cintas después de agregar o crear una biblioteca de cintas nueva, o después de restaurar una ruta de acceso fallida en una ruta única o acceso multivía a una biblioteca de cintas. También puede utilizar esta información al solucionar errores relacionados con la ruta de acceso o si el acceso a una biblioteca de cintas falla.

- Nodo al que está conectada la biblioteca de cintas
- ID del dispositivo
- Ruta NDMP
- Nombre de la biblioteca de cintas
- ID de puerto de destino e puerto de iniciador
- Acceso de ruta única o multivía a una biblioteca de cintas para cada puerto iniciador FC o de destino
- Detalles de la integridad de los datos relacionados con la ruta, como «'errores de ruta'» y «'Manual de ruta'».
- Los grupos LUN y el número de LUN

Si desea…	Se usa este comando…
Ver información sobre una biblioteca de cintas en un clúster	`system node hardware tape library show`

Si desea…	Se usa este comando…
Ver información de ruta de una biblioteca de cintas	`storage tape library path show`
Vea la información de ruta de una biblioteca de cintas para cada puerto iniciador	`storage tape library path show-by-initiator`
Vea la información de conectividad entre una biblioteca de cinta de almacenamiento y un clúster	`storage tape library config show`

Para obtener más información sobre estos comandos, consulte las páginas man.

Acerca de las unidades de cinta

Descripción general de las unidades de cinta cualificadas

Debe utilizar una unidad de cinta cualificada que se haya probado y encontrado para funcionar correctamente en un sistema de almacenamiento. Puede seguir el solapamiento de cintas y activar reservas de cinta para asegurarse de que sólo un sistema de almacenamiento accede a una unidad de cinta en un momento determinado.

Una unidad de cinta cualificada es una unidad de cinta que se ha probado y que funciona correctamente en sistemas de almacenamiento. Puede calificar las unidades de cinta para las versiones de ONTAP existentes mediante el archivo de configuración de cinta.

Formato del archivo de configuración de cinta

El formato de archivo de configuración de cinta consta de campos como el ID de proveedor, el ID de producto y los detalles de los tipos de compresión de una unidad de cinta. Este archivo también consta de campos opcionales para activar la función de carga automática de una unidad de cinta y cambiar los valores de tiempo de espera de comando de una unidad de cinta.

La siguiente tabla muestra el formato del archivo de configuración de cinta:

Elemento	Tamaño	Descripción
`vendor_id` (cadena)	hasta 8 bytes	El ID del proveedor según lo informa la `SCSI Inquiry` comando.
`product_id`(cadena)	hasta 16 bytes	El ID de producto indicado por la `SCSI Inquiry` comando.

Elemento	Tamaño	Descripción
`id_match_size`(número)		El número de bytes del ID de producto que se va a utilizar para la coincidencia para detectar la unidad de cinta que se va a identificar, comenzando por el primer carácter del ID de producto en los datos de consulta.
`vendor_pretty` (cadena)	hasta 16 bytes	Si este parámetro está presente, se especifica mediante la cadena mostrada por el comando, `storage tape show -device -names`; De lo contrario, se mostrará INQ_VENDOR_ID.
`product_pretty`(cadena)	hasta 16 bytes	Si este parámetro está presente, se especifica mediante la cadena mostrada por el comando, `storage tape show -device -names`; De lo contrario, aparecerá INQ_PRODUCT_ID.

La `vendor_pretty` y.. `product_pretty` los campos son opcionales, pero si uno de estos campos tiene un valor, el otro también debe tener un valor.

En la siguiente tabla se explica la descripción, el código de densidad y el algoritmo de compresión de los distintos tipos de compresión, como `l`, `m`, `h`, y. `a`:

Elemento	Tamaño	Descripción
`{l	m	h
a}_description=(string)`	hasta 24 bytes	La cadena que se va a imprimir para el comando nodeshell, `sysconfig -t`, que describe las características de la configuración de densidad determinada.
`{l	m	h
a}_density=(hex codes)`		El código de densidad que se va a establecer en el descriptor de bloque de página del modo SCSI correspondiente al código de densidad deseado para l, m, h o a..
`{l	m	h

Elemento	Tamaño	Descripción
a}_algorithm=(hex codes)`		El algoritmo de compresión que se establecerá en la página del modo de compresión SCSI correspondiente al código de densidad y la característica de densidad deseada.

En la siguiente tabla se describen los campos opcionales disponibles en el archivo de configuración de cinta:

Campo	Descripción
`autoload=(Boolean yes/no)`	Este campo está establecido en `yes` si la unidad de cinta tiene una función de carga automática, es decir, después de insertar el cartucho de cinta, la unidad de cinta estará lista sin necesidad de ejecutar un `SCSI load` (unidad de arranque/parada). El valor predeterminado de este campo es `no`.
`cmd_timeout_0x`	Valor de tiempo de espera individual. Debe utilizar este campo sólo si desea especificar un valor de tiempo de espera diferente del que está utilizando como valor predeterminado el controlador de cinta. El archivo de ejemplo enumera los valores de tiempo de espera predeterminados del comando SCSI que utiliza la unidad de cinta. El valor de tiempo de espera puede expresarse en minutos (m), segundos (s) o milisegundos (ms). No debe cambiar este campo.

Puede descargar y ver el archivo de configuración de cinta desde el sitio de soporte de NetApp.

Ejemplo de formato de archivo de configuración de cinta

El formato de archivo de configuración de cinta para la unidad de cinta HP LTO5 ULTRIUM es el siguiente:

`vendor_id`="HP"

`product_id`="Ultrium 5-SCSI"

`id_match_size`=9

`vendor_pretty`="Hewlett-Packard"

`product_pretty`="LTO-5"

`l_description`="LTO-3(ro)/4 4/800 GB"

`l_density`=0x00

`l_algorithm`=0x00

`m_description`="LTO-3(ro)/4 8/1600 GB cmp"

`m_density`=0x00

`m_algorithm`=0x01

`h_description`="LTO-5 1600 GB"

`h_density`=0x58

`h_algorithm`=0x00

`a_description`="LTO-5 3200 GB cmp"

`a_density`=0x58

`a_algorithm`=0x01

`autoload`="sí"

Información relacionada

"Herramientas de NetApp: Archivos de configuración de dispositivos de cinta"

Cómo el sistema de almacenamiento dota a una nueva unidad de cinta de forma dinámica

El sistema de almacenamiento califica una unidad de cinta de forma dinámica emparejando su ID de proveedor y su ID de producto con la información contenida en la tabla de calificación de cinta.

Cuando conecta una unidad de cinta al sistema de almacenamiento, busca una identificación del proveedor y una coincidencia de ID de producto entre la información obtenida durante la detección de cinta y la información de la tabla de calificación de cinta interna. Si el sistema de almacenamiento detecta una coincidencia, Marca la unidad de cinta como cualificada y puede acceder a la unidad de cinta. Si el sistema de almacenamiento no encuentra una coincidencia, la unidad de cinta permanece en estado no cualificado y no se accede a ella.

Descripción general de los dispositivos de cinta

Descripción general de los dispositivos de cinta

Un dispositivo de cinta es una representación de una unidad de cinta. Es una combinación específica de tipo de rebobinado y capacidad de compresión de una unidad de cinta.

Se crea un dispositivo de cinta para cada combinación de tipo de rebobinado y capacidad de compresión. Por tanto, una unidad de cinta o una biblioteca de cintas pueden tener asociados varios dispositivos de cinta. Debe especificar un dispositivo de cinta para mover, escribir o leer cintas.

Al instalar una unidad de cinta o una biblioteca de cintas en un sistema de almacenamiento, ONTAP crea dispositivos de cinta asociados con la unidad de cinta o la biblioteca de cintas.

ONTAP detecta unidades de cinta y bibliotecas de cintas y asigna números lógicos y dispositivos de cinta a ellos. ONTAP detecta las bibliotecas y unidades de cinta SCSI paralelas, SAS y Fibre Channel cuando están conectadas a los puertos de interfaz. ONTAP detecta estas unidades cuando sus interfaces están habilitadas.

Formato de nombre de dispositivo de cinta

Cada dispositivo de cinta tiene un nombre asociado que aparece en un formato definido. El formato incluye información acerca del tipo de dispositivo, el tipo de rebobinado, el alias y el tipo de compresión.

El formato de un nombre de dispositivo de cinta es el siguiente:

`rewind_type st alias_number compression_type`

`rewind_type` es el tipo de rebobinado.

En la siguiente lista se describen los distintos valores de tipo de rebobinado:

- **r**

  ONTAP rebobina la cinta después de que termine de escribir el archivo de cinta.

- **no**

  ONTAP no rebobinará la cinta después de que termine de escribir el archivo de cinta. Debe utilizar este tipo de rebobinado cuando desee escribir varios archivos de cinta en la misma cinta.

- **ur**

  Este es el tipo de rebobinado de descarga/recarga. Cuando se utiliza este tipo de rebobinado, la biblioteca de cintas descarga la cinta cuando llega al final de un archivo de cinta y, a continuación, carga la cinta siguiente, si existe una.

  Debe utilizar este tipo de rebobinado sólo en las siguientes circunstancias:

  - La unidad de cinta asociada con este dispositivo se encuentra en una biblioteca de cintas o en un cambiador de medios que se encuentra en el modo de biblioteca.
  - La unidad de cinta asociada con este dispositivo está conectada a un sistema de almacenamiento.
  - Las cintas suficientes para la operación que está realizando están disponibles en la secuencia de cintas de biblioteca definida para esta unidad de cinta.

> Si graba una cinta con un dispositivo de no rebobinado, debe rebobinar la cinta antes de leerla.

`st` es la designación estándar de una unidad de cinta.

`alias_number` Es el alias que ONTAP asigna a la unidad de cinta. Cuando ONTAP detecta una nueva unidad de cinta, ONTAP asigna un alias a la unidad de cinta.

`compression_type` es un código específico de una unidad para la densidad de datos en la cinta y el tipo de compresión.

La siguiente lista describe los distintos valores para `compression_type`:

- **a**

  Mayor compresión

- **h**

  Alta compresión

- **m**

  Compresión media

- **l**

  Baja compresión

Ejemplos

`nrst0a` especifica un dispositivo sin rebobinar en la unidad de cinta 0 utilizando la compresión más alta.

Ejemplo de una lista de dispositivos de cinta

En el siguiente ejemplo se muestran los dispositivos de cinta asociados con HP Ultrium 2-SCSI:

```
        Tape drive (fc202_6:2.126L1)  HP      Ultrium 2-SCSI
rst0l  -  rewind device,        format is: HP (200GB)
nrst0l -  no rewind device,     format is: HP (200GB)
urst0l -  unload/reload device, format is: HP (200GB)
rst0m  -  rewind device,        format is: HP (200GB)
nrst0m -  no rewind device,     format is: HP (200GB)
urst0m -  unload/reload device, format is: HP (200GB)
rst0h  -  rewind device,        format is: HP (200GB)
nrst0h -  no rewind device,     format is: HP (200GB)
urst0h -  unload/reload device, format is: HP (200GB)
rst0a  -  rewind device,        format is: HP (400GB w/comp)
nrst0a -  no rewind device,     format is: HP (400GB w/comp)
urst0a -  unload/reload device, format is: HP (400GB w/comp)
```

En la siguiente lista se describen las abreviaturas del ejemplo anterior:

- GB—Gigabytes; esta es la capacidad de la cinta.
- con compresión; esto muestra la capacidad de cinta con compresión.

Compatible con el número de dispositivos de cinta simultáneos

ONTAP admite un máximo de 64 conexiones simultáneas de unidad de cinta, 16 cambiadores de soporte y 16 dispositivos de puente o router para cada sistema de almacenamiento (por nodo) en cualquier combinación de conexiones Fibre Channel, SCSI o SAS.

Las unidades de cinta o los cambiadores de medios pueden ser dispositivos en bibliotecas de cintas físicas o

virtuales o dispositivos independientes.

> Aunque un sistema de almacenamiento puede detectar 64 conexiones a unidades de cinta, la cantidad máxima de sesiones de backup y restauración que pueden realizarse de forma simultánea depende de los límites de escalabilidad del motor de backup.

Información relacionada

Límites de escalabilidad para sesiones de backup y restauración de volcado

Solapamiento de cinta

Descripción general de solapamiento de cinta

Aliasing simplifica el proceso de identificación del dispositivo. Aliasing enlaza un nombre de ruta física (PPN) o un número de serie (SN) de una cinta o un cambiador de soporte a un nombre de alias persistente pero modificable.

La siguiente tabla describe cómo el aliasing de cinta le permite asegurarse de que una unidad de cinta (o biblioteca de cintas o cambiador de medios) está siempre asociada con un único nombre de alias:

Situación	Reasignar el alias
Cuando se reinicia el sistema	La unidad de cinta se reasigna automáticamente su alias anterior.
Cuando un dispositivo de cinta se mueve a otro puerto	El alias se puede ajustar para que apunte a la nueva dirección.
Cuando más de un sistema utiliza un dispositivo de cinta concreto	El usuario puede configurar el alias para que sea el mismo en todos los sistemas.

> Al actualizar de Data ONTAP 8.1.x a Data ONTAP 8.2.x, la función de alias de cinta de Data ONTAP 8.2.x modifica los nombres de alias de cinta existentes. En tal caso, es posible que tenga que actualizar los nombres de alias de cinta en la aplicación de copia de seguridad.

La asignación de alias de cinta proporciona una correspondencia entre los nombres lógicos de los dispositivos de copia de seguridad (por ejemplo, st0 o mc1) y un nombre asignado permanentemente a un puerto, una unidad de cinta o un cambiador de medios.

> st0 y st00 son nombres lógicos diferentes.

> Los nombres lógicos y números de serie se utilizan sólo para acceder a un dispositivo. Después de acceder al dispositivo, devuelve todos los mensajes de error utilizando el nombre de ruta física.

Hay dos tipos de nombres disponibles para el solapamiento: Nombre de ruta física y número de serie.

Qué son los nombres de ruta física

Los nombres de rutas físicas (PNP) son las secuencias de direcciones numéricas que

ONTAP asigna a unidades de cinta y bibliotecas de cintas basadas en el adaptador o switch SCSI-2/3 (ubicación específica) que están conectados al sistema de almacenamiento. Los PPNS también se conocen como nombres eléctricos.

Los PPNS de dispositivos de conexión directa utilizan el siguiente formato: `host_adapter. device_id_lun`

> El valor de LUN se muestra solo para los dispositivos de cinta y cambio medio cuyos valores de LUN no son cero; es decir, si el valor de LUN es cero el `lun` No se muestra parte de la PPN.

Por ejemplo, PPN 8.6 indica que el número de adaptador de host es 8, el ID de dispositivo es 6 y el número de unidad lógica (LUN) es 0.

Los dispositivos de cinta SAS también son dispositivos de conexión directa. Por ejemplo, el PPN 5c.4 indica que en un sistema de almacenamiento, el SAS HBA está conectado en la ranura 5, la cinta SAS está conectada al puerto C del SAS HBA y el identificador de dispositivo es 4.

Los PPNS de los dispositivos conectados mediante conmutador Fibre Channel utilizan el siguiente formato: `switch:port_id. device_id_lun`

Por ejemplo, el PPN MY_SWITCH:5.3L2 indica que la unidad de cinta conectada al puerto 5 de un switch llamado MY_SWITCH está establecida con el ID de dispositivo 3 y tiene el LUN 2.

La unidad determina el LUN (número de unidad lógica). Fibre Channel, bibliotecas y unidades de cinta SCSI, así como discos, tienen VPN.

Los PPNS de unidades de cinta y bibliotecas no cambian a menos que cambie el nombre del conmutador, se mueva la unidad de cinta o la biblioteca o se reconfigure la unidad de cinta o la biblioteca. Los PPNS permanecen sin cambios después del reinicio. Por ejemplo, si se retira una unidad de cinta denominada MY_SWITCH:5.3L2 y SE conecta una nueva unidad de cinta con el mismo ID de dispositivo y LUN al puerto 5 del conmutador MY_SWITCH, se podrá acceder a la nueva unidad de cinta mediante MY_SWITCH:5.3L2.

Qué son los números de serie

Un número de serie (SN) es un identificador único para una unidad de cinta o un cambiador de medios. ONTAP genera alias basados en SN en lugar de WWN.

Dado que el SN es un identificador único para una unidad de cinta o un cambiador de medios, el alias permanece igual independientemente de las múltiples rutas de conexión a la unidad de cinta o al cambiador de medios. Esto ayuda a los sistemas de almacenamiento a realizar un seguimiento de la misma unidad de cinta o cambiador de medios en una configuración de biblioteca de cintas.

El número de serie de una unidad de cinta o un cambiador de medios no cambia aunque cambie el nombre del conmutador Fibre Channel al que está conectada la unidad de cinta o el cambiador de medios. Sin embargo, en una biblioteca de cintas si reemplaza una unidad de cinta existente con una nueva, ONTAP genera nuevos alias porque cambia el número de serie de la unidad de cinta. Además, si mueve una unidad de cinta existente a una nueva ranura de una biblioteca de cintas o reasigna el LUN de la unidad de cinta, ONTAP genera un nuevo alias para esa unidad de cinta.

> Debe actualizar las aplicaciones de backup con los alias recién generados.

El número de serie de un dispositivo de cinta utiliza el siguiente formato: `SN[xxxxxxxxxx]L[X]`

`x` Es un carácter alfanumérico y L`x` Es el LUN del dispositivo de cinta. Si el LUN es 0, la L.`x` no se muestra parte de la cadena.

Cada SN consta de hasta 32 caracteres; el formato para el SN no distingue entre mayúsculas y minúsculas.

Consideraciones que tener en cuenta al configurar el acceso a cinta multivía

Puede configurar dos rutas desde el sistema de almacenamiento para acceder a las unidades de cinta de una biblioteca de cintas. Si falla una ruta, el sistema de almacenamiento puede utilizar las otras rutas para acceder a las unidades de cinta sin tener que reparar inmediatamente la ruta con error. Esto garantiza que se puedan reiniciar las operaciones de cinta.

Al configurar el acceso a cinta multivía desde el sistema de almacenamiento, debe tener en cuenta lo siguiente:

- En bibliotecas de cintas que admiten la asignación de LUN, para acceder de varias rutas a un grupo LUN, la asignación de LUN debe ser simétrica en cada ruta.

  Las unidades de cinta e intercambiadores de medios se asignan a grupos de LUN (conjunto de LUN que comparten el mismo conjunto de rutas del iniciador) en una biblioteca de cintas. Todas las unidades de cinta de un grupo LUN deben estar disponibles para las operaciones de backup y restauración en todas las rutas múltiples.

- Se puede configurar un máximo de dos rutas desde el sistema de almacenamiento para acceder a las unidades de cinta de una biblioteca de cintas.
- El acceso a cinta multivía es compatible con el equilibrio de carga. El equilibrio de carga está deshabilitado de forma predeterminada.

En el ejemplo siguiente, el sistema de almacenamiento accede al grupo LUN 0 a través de dos rutas de iniciador: 0b y 0d. En estas dos rutas, el grupo de LUN tiene el mismo número de LUN, 0 y el número de LUN, 5. El sistema de almacenamiento accede al grupo LUN 1 a través de solo una ruta de iniciador, 3d.

```
STSW-3070-2_cluster::> storage tape library config show

Node                     LUN Group   LUN Count  Library Name  Library
Target Port  Initiator
----------------------- ----------- ---------- -------------
-------------------- -----
STSW-3070-2_cluster-01        0      5         IBM 3573-TL_1
510a09800000412d     0b

0d
                              1      2         IBM 3573-TL_2
50050763124b4d6f     3d

3 entries were displayed
```

Para obtener más información, consulte las páginas de manual.

Cómo se añaden unidades y bibliotecas de cinta a los sistemas de almacenamiento

Puede agregar bibliotecas y unidades de cinta al sistema de almacenamiento de forma dinámica (sin desconectar el sistema).

Al añadir un nuevo cambiador de medios, el sistema de almacenamiento detecta su presencia y la añade a la configuración. Si ya se hace referencia al cambiador de medios en la información del alias, no se crea ningún nombre lógico nuevo. Si no se hace referencia a la biblioteca, el sistema de almacenamiento crea un nuevo alias para el cambiador de medios.

En una configuración de biblioteca de cintas, debe configurar una unidad de cinta o un cambiador de medios en el LUN 0 de un puerto de destino para ONTAP para descubrir todos los cambiadores de medios y unidades de cinta en ese puerto de destino.

Qué reservas de cinta son

Múltiples sistemas de almacenamiento pueden compartir el acceso a unidades de cinta, cambiadores de medio, puentes o bibliotecas de cintas. Las reservas de cintas garantizan que sólo un sistema de almacenamiento pueda acceder a un dispositivo en cualquier momento, ya sea habilitando el mecanismo de reserva/versión SCSI o las reservas persistentes SCSI para todas las unidades de cinta, cambiadores medianos, puentes y bibliotecas de cintas.

> Todos los sistemas que comparten dispositivos en una biblioteca, incluidos o no conmutadores, deben utilizar el mismo método de reserva.

El mecanismo de reserva/liberación SCSI para reservar dispositivos funciona bien en condiciones normales. Sin embargo, durante los procedimientos de recuperación de errores de interfaz, se pueden perder las reservas. Si esto sucede, los iniciadores que no son el propietario reservado pueden acceder al dispositivo.

Las reservas realizadas con reservas persistentes SCSI no se ven afectadas por mecanismos de recuperación de errores, como el restablecimiento de bucle o el restablecimiento de objetivos; sin embargo, no todos los dispositivos implementan correctamente las reservas persistentes SCSI.

Transferir datos mediante ndmpcopy

Transfiera los datos utilizando la descripción general de ndmpcopy

La `ndmpcopy` Nodesinfierno Command transfiere datos entre sistemas de almacenamiento que admiten NDMP v4. Puede realizar transferencias de datos completas e incrementales. Puede transferir volúmenes completos o parciales, qtrees, directorios o archivos individuales.

Acerca de esta tarea

Gracias al uso de ONTAP 8.x y versiones anteriores, las transferencias incrementales están limitadas a un máximo de dos niveles (uno completo y hasta dos backups incrementales).

A partir de ONTAP 9.0 y versiones posteriores, las transferencias incrementales están limitadas a un máximo de nueve niveles (uno completo y hasta nueve backups incrementales).

Puede ejecutar `ndmpcopy` en la línea de comandos nodesinfierno de los sistemas de almacenamiento de

origen y destino, o un sistema de almacenamiento que no es el origen ni el destino de la transferencia de datos. También puede ejecutar `ndmpcopy` en un único sistema de almacenamiento que sea el origen y el destino de la transferencia de datos.

Las direcciones IPv4 o IPv6 de los sistemas de almacenamiento de origen y destino en el `ndmpcopy` comando. El formato de ruta es `/vserver_name/volume_name \[path\]`.

Pasos

1. Active el servicio NDMP en los sistemas de almacenamiento de origen y destino:

Si realiza transferencia de datos en el origen o el destino en…	Usar el siguiente comando…
Modo de NDMP con ámbito SVM	`vserver services ndmp on` Para la autenticación NDMP en la SVM de administrador, la cuenta de usuario es `admin` y el rol de usuario es `admin` o. `backup`. En la SVM de datos, la cuenta de usuario es `vsadmin` y el rol de usuario es `vsadmin` o. `vsadmin-backup` función.
Modo de NDMP con ámbito del nodo	`system services ndmp on`

2. Transferir datos dentro de un sistema de almacenamiento o entre sistemas de almacenamiento mediante el `ndmpcopy` mando en el nodesinfierno:

```
::> system node run -node <node_name> < ndmpcopy [options]
source_IP:source_path destination_IP:destination_path [-mcs {inet|inet6}] [-
mcd {inet|inet6}] [-md {inet|inet6}]
```

> Los nombres DNS no son compatibles con ndmpcopy. Debe proporcionar la dirección IP del origen y del destino. La dirección de bucle invertido (127.0.0.1) no es compatible con la dirección IP de origen ni con la dirección IP de destino.

   - La `ndmpcopy` command determina el modo de dirección para las conexiones de control de la siguiente manera:
     - El modo de dirección para la conexión de control corresponde a la dirección IP proporcionada.
     - Puede anular estas reglas mediante el `-mcs` y.. `-mcd` opciones.
   - Si el origen o el destino son el sistema ONTAP, entonces según el modo NDMP (ámbito del nodo o ámbito de la SVM), utilice una dirección IP que permita el acceso al volumen de destino.
   - `source_path` y.. `destination_path` son los nombres de ruta absolutos hasta el nivel granular de volumen, qtree, directorio o archivo.
   - `-mcs` especifica el modo de direccionamiento preferido para la conexión de control al sistema de almacenamiento de origen.

`inet` Indica un modo de dirección IPv4 y. `inet6` Indica un modo de dirección IPv6.

- `-mcd` especifica el modo de direccionamiento preferido para la conexión de control al sistema de almacenamiento de destino.

  `inet` Indica un modo de dirección IPv4 y. `inet6` Indica un modo de dirección IPv6.

- `-md` especifica el modo de direccionamiento preferido para transferencias de datos entre los sistemas de almacenamiento de origen y destino.

  `inet` Indica un modo de dirección IPv4 y. `inet6` Indica un modo de dirección IPv6.

  Si no utiliza la `-md` en la `ndmpcopy` comando, el modo de direccionamiento de la conexión de datos se determina de la siguiente manera:

  - Si alguna de las direcciones especificadas para las conexiones de control es una dirección IPv6, el modo de dirección para la conexión de datos es IPv6.
  - Si las dos direcciones especificadas para las conexiones de control son direcciones IPv4, el `ndmpcopy` En primer lugar, Command intenta utilizar un modo de dirección IPv6 para la conexión de datos.

    Si no es así, el comando utiliza un modo de dirección IPv4.

    > Una dirección IPv6, si se especifica, debe escribirse entre corchetes.

    Este comando de ejemplo migra datos de una ruta de acceso de origen (`source_path`) a una ruta de destino (`destination_path`).

```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password>
 -st md5 -dt md5 192.0.2.129:/<src_svm>/<src_vol>
192.0.2.131:/<dst_svm>/<dst_vol>
```

+
Este comando de ejemplo establece explícitamente las conexiones de control y la conexión de datos para utilizar el modo de dirección IPv6:

```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password> -st md5
-dt md5 -mcs inet6 -mcd inet6 -md
 inet6 [2001:0db8:1:1:209:6bff:feae:6d67]:/<src_svm>/<src_vol>
[2001:0ec9:1:1:200:7cgg:gfdf:7e78]:/<dst_svm>/<dst_vol>
```

Opciones para el comando ndmpcopy

Debe comprender las opciones disponibles para el `ndmpcopy` nodeshell comando para transferir datos con éxito.

En la siguiente tabla se enumeran las opciones disponibles. Para obtener más información, consulte

`ndmpcopy` páginas de manual disponibles a través del nodesinfierno.

Opción	Descripción
`-sa` `username`:[`password`]	Esta opción configura el nombre de usuario y la contraseña de autenticación de origen para conectarse con el sistema de almacenamiento de origen. Esta es una opción obligatoria. Para un usuario sin privilegios de administrador, debe especificar la contraseña específica de NDMP generada por el sistema del usuario. La contraseña que genera el sistema es obligatoria tanto para los usuarios administradores como para los que no son de administrador.
`-da` `username`:[`password`]	Esta opción establece el nombre de usuario y la contraseña de autenticación de destino para conectarse al sistema de almacenamiento de destino. Esta es una opción obligatoria.
`-st` {`md5`	`text`}
Esta opción establece el tipo de autenticación de origen que se va a utilizar al conectarse al sistema de almacenamiento de origen. Esta es una opción obligatoria y, por lo tanto, el usuario debe proporcionar una `text` o. `md5` opción.	`-dt` {`md5`
`text`}	Esta opción establece el tipo de autenticación de destino que se utilizará al conectarse al sistema de almacenamiento de destino.
`-l`	Esta opción establece el nivel de volcado utilizado para la transferencia al valor especificado de level.Valid are `0`, `1`, a. `9`, donde `0` indica una transferencia completa y. `1` para `9` especifica una transferencia incremental. El valor predeterminado es `0`.
`-d`	Esta opción permite la generación de mensajes de registro de depuración ndmpcopy. Los archivos de registro de depuración ndmpcopy se encuentran en la `/mroot/etc/log` volumen raíz. Los nombres de los archivos de registro de depuración ndmpcopy se encuentran en la `ndmpcopy.yyyymmdd` formato.
`-f`	Esta opción activa el modo forzado. Este modo permite que los archivos del sistema se sobrescriban en la `/etc` directorio en la raíz del volumen 7-Mode.

Opción	Descripción
`-h`	Esta opción imprime el mensaje de ayuda.
`-p`	Esta opción le pide que introduzca la contraseña para la autorización de origen y destino. Esta contraseña anula la contraseña especificada para `-sa` y.. `-da` opciones. Esta opción solo se puede utilizar cuando el comando se ejecuta en una consola interactiva.
`-exclude`	Esta opción excluye los archivos o directorios especificados de la ruta de acceso especificada para la transferencia de datos. El valor puede ser una lista separada por comas de nombres de directorio o de archivo como **`.pst`** `o. .txt`.

NDMP para volúmenes FlexVol

Acerca de NDMP para volúmenes FlexVol

El protocolo de gestión de datos de red (NDMP) es un protocolo estandarizado para controlar el backup, la recuperación y otros tipos de transferencia de datos entre dispositivos de almacenamiento primarios y secundarios, como sistemas de almacenamiento y bibliotecas de cintas.

Al habilitar la compatibilidad con NDMP en un sistema de almacenamiento, permite que ese sistema de almacenamiento se comunique con aplicaciones de backup conectadas a la red compatibles con NDMP (también denominadas *Data Management Applications* o *DMAs*), servidores de datos y servidores de cinta que participan en operaciones de backup o recuperación. Todas las comunicaciones de red se producen a través de la red TCPIP o TCP/IPv6. NDMP también proporciona un control de bajo nivel de unidades de cinta e intercambiadores de tamaño medio.

Puede realizar operaciones de backup y restauración de cinta en el modo NDMP de ámbito del nodo o en el modo NDMP de la máquina virtual de almacenamiento (SVM) con ámbito.

Debe saber cuáles son las consideraciones que debe tener en cuenta a la hora de utilizar NDMP, la lista de variables de entorno y las topologías de backup en cinta de NDMP admitidas. También puede habilitar o deshabilitar la funcionalidad DAR mejorada. Los dos métodos de autenticación compatibles con ONTAP para autenticar el acceso NDMP a un sistema de almacenamiento son: Sin formato y sin reto.

Información relacionada

Variables de entorno compatibles con ONTAP

Acerca de los modos de funcionamiento de NDMP

Puede optar por realizar operaciones de backup y restauración a cinta, ya sea en el nivel de nodo o en el nivel de la máquina virtual de almacenamiento (SVM). Para ejecutar

estas operaciones correctamente en el nivel de SVM, el servicio NDMP debe estar habilitado en la SVM.

Si actualiza de Data ONTAP 8.2 a Data ONTAP 8.3, seguirá reteniendo el modo de funcionamiento NDMP usado en 8.2 después de la actualización de 8.2 a 8.3.

Si instala un clúster nuevo con Data ONTAP 8.2 o posterior, NDMP se encuentra en el modo NDMP de ámbito SVM de manera predeterminada. Para realizar operaciones de backup y restauración de cinta en el modo de NDMP de ámbito del nodo, debe habilitar explícitamente el modo de NDMP de ámbito del nodo.

Información relacionada

Comandos para gestionar el modo NDMP de ámbito de nodo

Gestionar el modo NDMP de ámbito del nodo para volúmenes FlexVol

Gestionar el modo NDMP de ámbito SVM para volúmenes FlexVol

Lo que es el modo NDMP de ámbito del nodo

En el modo NDMP de ámbito del nodo, puede realizar operaciones de backup y restauración a cinta en el nivel del nodo. Se seguirá reteniendo el modo de funcionamiento NDMP usado en Data ONTAP 8.2 después de la actualización de 8.2 a 8.3.

En el modo NDMP de ámbito del nodo, puede realizar operaciones de backup y restauración de cinta en un nodo que posea el volumen. Para realizar estas operaciones, debe establecer conexiones de control NDMP en una LIF alojada en el nodo propietario de los dispositivos de volumen o cinta.

Este modo quedó obsoleto y se quitará en un lanzamiento principal futuro.

Información relacionada

Gestionar el modo NDMP de ámbito del nodo para volúmenes FlexVol

Qué es el modo NDMP con ámbito SVM

Se pueden ejecutar operaciones de backup y restauración de cinta en el nivel de máquina virtual de almacenamiento (SVM) correctamente si el servicio NDMP está habilitado en la SVM. Puede realizar backups y restauraciones de todos los volúmenes alojados en diferentes nodos en la SVM de un clúster si la aplicación de backup admite la extensión CAB.

Se puede establecer una conexión de control NDMP en diferentes tipos de LIF. En el modo NDMP con ámbito SVM, estas LIF pertenecen a la SVM de datos o a la SVM de administrador. La conexión puede establecerse en un LIF solo si el servicio NDMP está habilitado en la SVM propietaria de este LIF.

Una LIF de datos pertenece a la SVM de datos y la LIF entre clústeres, la LIF de gestión de nodos y la LIF de gestión de clúster pertenecen a la SVM de administrador.

En el modo NDMP de ámbito SVM, la disponibilidad de volúmenes y dispositivos de cinta para operaciones de backup y restauración depende del tipo de LIF en el que se establezca la conexión de control NDMP y el estado de la extensión CAB. Si su aplicación de backup admite la extensión CAB y un volumen y el dispositivo de cinta comparten la misma afinidad, la aplicación de backup puede realizar una operación de backup o

restauración local, en lugar de una operación de backup o restauración triple.

Información relacionada

Gestionar el modo NDMP de ámbito SVM para volúmenes FlexVol

Consideraciones que tener en cuenta al utilizar NDMP

Debe tener en cuenta una serie de consideraciones que se deben tener en cuenta al iniciar el servicio NDMP en el sistema de almacenamiento.

- Cada nodo admite un máximo de 16 backups, restauraciones o combinación simultáneas de los dos mediante unidades de cinta conectadas.
- Los servicios NDMP pueden generar datos del historial de ficheros si así lo solicitan las aplicaciones de backup NDMP.

  El historial de archivos se utiliza en las aplicaciones de copia de seguridad para permitir la recuperación optimizada de subconjuntos seleccionados de datos de una imagen de copia de seguridad. La generación y el procesamiento del historial de archivos pueden requerir mucho tiempo y requerir gran cantidad de CPU tanto en el sistema de almacenamiento como en la aplicación de backup.

  SMTape no admite el historial de archivos.

  Si la protección de datos está configurada para la recuperación ante desastres, donde se recuperará toda la imagen de copia de seguridad, puede deshabilitar la generación del historial de archivos para reducir el tiempo de copia de seguridad. Consulte la documentación de la aplicación de copia de seguridad para determinar si es posible desactivar la generación del historial de archivos NDMP.

- La política de firewall para NDMP está habilitada de forma predeterminada en todos los tipos de LIF.
- En el modo NDMP de ámbito del nodo, el backup de un volumen FlexVol requiere que utilice la aplicación de backup para iniciar un backup en un nodo propietario del volumen.

  Sin embargo, no puede realizar backups de un volumen raíz de nodo.

- Puede realizar un backup NDMP desde cualquier LIF de la forma permitida por las políticas de firewall.

  Si utiliza una LIF de datos, debe seleccionar una LIF que no esté configurada para la conmutación por error. Si una LIF de datos conmuta al nodo de respaldo durante una operación de NDMP, la operación de NDMP falla y debe volver a ejecutarse.

- En el modo NDMP de ámbito del nodo y la máquina virtual de almacenamiento (SVM) en modo NDMP sin soporte de extensión CAB, la conexión de datos NDMP usa la misma LIF que la conexión de control NDMP.
- Durante la migración de LIF, las operaciones de backup y restauración continuas se interrumpen.

  Debe iniciar las operaciones de backup y restauración después de la migración de LIF.

- La ruta de backup NDMP tiene el formato `/vserver_name/volume_name/path_name`.

  `path_name` Es opcional y especifica la ruta del directorio, el archivo o la copia Snapshot.

- Cuando se realiza un backup de un destino de SnapMirror a cinta mediante el motor de volcado, solo se realiza un backup de los datos del volumen.

Sin embargo, si se realiza un backup de un destino de SnapMirror en cinta con SMTape, también se realiza el backup de los metadatos. Las relaciones de SnapMirror y los metadatos asociados no se realizan en un backup a cinta. Por lo tanto, durante la restauración, solo se restauran los datos de ese volumen, pero no se restauran las relaciones de SnapMirror asociadas.

Información relacionada

Qué hace la extensión Cluster Aware Backup

"Conceptos de ONTAP"

"Administración del sistema"

Variable de entorno

Información general de las variables de entorno

Las variables de entorno se utilizan para comunicar información sobre una operación de backup o restauración entre una aplicación de backup habilitada para NDMP y un sistema de almacenamiento.

Por ejemplo, si un usuario especifica que una aplicación de backup debe realizar un backup `/vserver1/vol1/dir1`, La aplicación de copia de seguridad establece la variable de entorno DEL SISTEMA de ARCHIVOS `/vserver1/vol1/dir1`. Del mismo modo, si un usuario especifica que una copia de seguridad debe ser una copia de seguridad de nivel 1, la aplicación de copia de seguridad establece la variable DE entorno DE NIVEL en 1 (una).

> La configuración y examen de las variables de entorno suelen ser transparentes para los administradores de backup, es decir, la aplicación de backup las establece automáticamente.

Un administrador de backup rara vez especifica variables de entorno; no obstante, se puede cambiar el valor de una variable de entorno de la cual establece la aplicación de backup para caracterizar o trabajar en torno a un problema funcional o de rendimiento. Por ejemplo, es posible que un administrador desee deshabilitar temporalmente la generación del historial de archivos para determinar si el procesamiento de la información del historial de archivos de la aplicación de copia de seguridad está contribuyendo a problemas de rendimiento o de funcionamiento.

Muchas aplicaciones de backup proporcionan un medio para anular o modificar variables de entorno o especificar variables de entorno adicionales. Para obtener información, consulte la documentación de la aplicación de copia de seguridad.

Variables de entorno compatibles con ONTAP

Las variables de entorno se utilizan para comunicar información sobre una operación de backup o restauración entre una aplicación de backup habilitada para NDMP y un sistema de almacenamiento. ONTAP admite variables de entorno, con un valor predeterminado asociado. Sin embargo, puede modificar manualmente estos valores predeterminados.

Si modifica manualmente los valores establecidos por la aplicación de backup, la aplicación podría comportarse de forma impredecible. Esto se debe a que es posible que las operaciones de backup o restauración no hagan lo que la aplicación de backup esperaba que hicieran. Pero en algunos casos, una modificación juiciosa podría ayudar a identificar o a solucionar problemas.

En las tablas siguientes se enumeran las variables de entorno cuyo comportamiento es común para el volcado y SMTape y las variables que sólo se admiten para el volcado y SMTape. Estas tablas también contienen descripciones de cómo funcionan las variables de entorno compatibles con ONTAP si se utilizan:

> En la mayoría de los casos, variables que tienen el valor, `Y` también aceptar `T` y.. `N` también aceptar `F`.

Variables de entorno compatibles para volcado y SMTape

Variable de entorno	Valores válidos	Predeterminado	Descripción
DEPURAR	`Y` o. `N`	`N`	Especifica que se imprime la información de depuración.
SISTEMA DE ARCHIVOS	`string`	`none`	Especifica el nombre de la ruta de acceso de la raíz de los datos de los que se va a realizar una copia de seguridad.
VERSIÓN_NDMP	`return_only`	`none`	No debe modificar la variable NDMP_VERSION. Creada por la operación de backup, la variable NDMP_VERSION devuelve la versión de NDMP. ONTAP establece la variable NDMP_VERSION durante un backup para uso interno y para pasar a una aplicación de backup con fines informativos. La versión NDMP de una sesión NDMP no está configurada con esta variable.

Variable de entorno	Valores válidos	Predeterminado	Descripción
SEPARADOR_NOMBRE_RUTA	`return_value`	`none`	Especifica el carácter separador del nombre de ruta de acceso. Este carácter depende del sistema de archivos del que se va a realizar el backup. En el caso de ONTAP, el carácter «»/» se asignará a esta variable. El servidor NDMP configura esta variable antes de iniciar una operación de backup a cinta.
TIPO	`dump` o. `smtape`	`dump`	Especifica el tipo de backup admitido para realizar operaciones de backup y restauración a cinta.
VERBOSE	`Y` o. `N`	`N`	Aumenta los mensajes de registro mientras se realiza una operación de copia de seguridad o restauración de cinta.

Variables de entorno compatibles con el volcado

Variable de entorno	Valores válidos	Predeterminado	Descripción
ACL_START	`return_only`	`none`	Creada por la operación de backup, la variable ACL_START es un valor de desplazamiento que utilizan una operación de restauración de acceso directo o de backup NDMP reiniciable. El valor de desplazamiento es el desplazamiento de bytes en el archivo de volcado donde comienzan los datos de ACL (pase V) y se devuelven al final de una copia de seguridad. Para que una operación de restauración de acceso directo restaure correctamente los datos de los que se ha realizado un backup, el valor de ACL_START debe pasarse a la operación de restauración cuando se inicia. Una operación de backup reiniciable de NDMP utiliza el valor ACL_START para comunicarse con la aplicación de backup donde comienza la parte no reiniciable del flujo de backup.

Variable de entorno	Valores válidos	Predeterminado	Descripción
FECHA_BASE	`0`, `-1`, o. `DUMP_DATE` valor	`-1`	Especifica la fecha de inicio de las copias de seguridad incrementales. Cuando se establece en `-1`, El especificador incremental BASE_DATE está desactivado. Cuando se establece en `0` en un backup de nivel 0, se habilitan los backups incrementales. Después de la copia de seguridad inicial, el valor de la variable DUMP_DATE de la copia de seguridad incremental anterior se asigna a la variable BASE_DATE. Estas variables son una alternativa a las copias de seguridad incrementales basadas en NIVEL/ACTUALIZACIÓN.
DIRECTO	`Y` o. `N`	`N`	Especifica que una restauración se debe reenviar directamente a la ubicación de la cinta en la que residen los datos del archivo en lugar de analizar la cinta completa. Para que la recuperación de acceso directo funcione, la aplicación de backup debe proporcionar información de posicionamiento. Si esta variable está establecida en `Y`, la aplicación de copia de seguridad especifica los nombres de archivo o directorio y la información de posicionamiento.

Variable de entorno	Valores válidos	Predeterminado	Descripción
NOMBRE_DMP	`string`	`none`	Especifica el nombre de una copia de seguridad de varios subárboles. Esta variable es obligatoria para varias copias de seguridad de subárbol.
FECHA_DE_VOLCADO	`return_value`	`none`	No se cambia esta variable directamente. Lo crea el backup si la variable BASE_DATE se establece en un valor distinto de `-1`. LA variable DUMP_DATE se deriva prependiente el valor de nivel de 32 bits a un valor de tiempo de 32 bits calculado por el software de volcado. El nivel se incrementa desde el valor del último nivel pasado a la variable BASE_DATE. El valor resultante se utiliza como valor BASE_DATE en un backup incremental posterior.

Variable de entorno	Valores válidos	Predeterminado	Descripción
MEJORADO_DAR_HABILITADO	`Y` o. `N`	`N`	Especifica si la funcionalidad DAR mejorada está activada. La funcionalidad DAR mejorada es compatible con DAR de directorios y DAR de ficheros con secuencias NT. Proporciona mejoras de rendimiento. Las mejoras DE DAR durante la restauración solo son posibles si se cumplen las siguientes condiciones: • ONTAP admite DAR mejorado. • El historial de archivos está activado (HIST=y) durante la copia de seguridad. • La `ndmpd.offset_map.enable` opción establecida en `on`. • La variable ENHANCED_DAR_ENABLED se establece en `Y` durante la restauración.

Variable de entorno	Valores válidos	Predeterminado	Descripción
EXCLUIR	`pattern_string`	`none`	Especifica los archivos o directorios que se excluyen al realizar una copia de seguridad de los datos. La lista de exclusión es una lista de nombres de archivos o directorios separados por comas. Si el nombre de un archivo o directorio coincide con uno de los nombres de la lista, se excluye de la copia de seguridad. Las siguientes reglas se aplican al especificar nombres en la lista excluir: • Debe utilizarse el nombre exacto del archivo o directorio. • El asterisco (*), un carácter comodín, debe ser el primer carácter o el último de la cadena. Cada cadena puede tener hasta dos asteriscos. • Una coma en un nombre de archivo o directorio debe ir precedida de una barra invertida. • La lista de exclusión puede contener hasta 32 nombres.

Variable de entorno	Valores válidos	Predeterminado	Descripción
EXTRAER	`Y`, `N`, o. `E`	`N`	Especifica que se van a restaurar los subárboles de un conjunto de datos de copia de seguridad. La aplicación de copia de seguridad especifica los nombres de los subárboles que se van a extraer. Si un archivo especificado coincide con un directorio cuyo contenido se hizo una copia de seguridad, el directorio se extrae recursivamente. Para cambiar el nombre de un archivo, directorio o qtree durante la restauración sin usar DAR, debe configurar la variable de entorno DE EXTRACCIÓN en `E`.
EXTRAER_ACL	`Y` o. `N`	`Y`	Especifica que las ACL del archivo de copia de seguridad se restauran en una operación de restauración. El valor predeterminado es restaurar las ACL cuando se restauran los datos, excepto para DARS (DIRECT=y).

Variable de entorno	Valores válidos	Predeterminado	Descripción
FUERZA	`Y` o. `N`	`N`	Determina si la operación de restauración debe comprobar la disponibilidad de espacio de volumen y de nodos de información en el volumen de destino. Estableciendo esta variable en `Y` hace que la operación de restauración omita las comprobaciones del espacio del volumen y de la disponibilidad de nodos de información en la ruta de destino. Si no hay suficiente espacio o inodos en el volumen de destino, la operación de restauración recupera la cantidad de datos permitidos por el espacio del volumen de destino y la disponibilidad de nodos de información. La operación de restauración se detiene cuando el espacio del volumen o los inodos no están disponibles.

Variable de entorno	Valores válidos	Predeterminado	Descripción
HIST	`Y` o. `N`	`N`	Especifica que la información del historial de archivos se envía a la aplicación de copia de seguridad. La mayoría de las aplicaciones de copia de seguridad comerciales establecen la variable HIST como `Y`. Si desea aumentar la velocidad de una operación de copia de seguridad o desea solucionar un problema con la colección de historial de archivos, puede establecer esta variable en `N`. No debe establecer la variable HIST en `Y` si la aplicación de copia de seguridad no admite el historial de archivos.

Variable de entorno	Valores válidos	Predeterminado	Descripción
IGNORE_CTIME	`Y` o. `N`	`N`	Especifica que no se realiza una copia de seguridad incremental de un archivo si sólo ha cambiado su valor ctime desde la copia de seguridad incremental anterior. Algunas aplicaciones, como el software de análisis de virus, cambian el valor de ctime de un archivo dentro del inodo, aunque el archivo o sus atributos no hayan cambiado. Como resultado, una copia de seguridad incremental puede hacer una copia de seguridad de los archivos que no han cambiado. La `IGNORE_CTIME` la variable debe especificarse solo si los backups incrementales están tomando una cantidad de tiempo o espacio inaceptable debido a que se ha modificado el valor ctime. La `NDMP dump` conjuntos de comandos `IGNORE_CTIME` para `false` de forma predeterminada. Configuración en `true` puede provocar la siguiente pérdida de datos: 1. Si `IGNORE_CTIME` se estable

Variable de entorno	Valores válidos	Predeterminado	Descripción
IGNORE_QTREES	`Y` o. `N`	`N`	Especifica que la operación de restauración no restaura la información de qtree a partir de qtrees de los que se ha realizado un backup.
NIVEL	`0-31`	`0`	Especifica el nivel de backup. El nivel 0 copia todo el conjunto de datos. Niveles de copia de seguridad incrementales, especificados por valores superiores a 0, copie todos los archivos (nuevos o modificados) desde la última copia de seguridad incremental. Por ejemplo, un nivel 1 realiza una copia de seguridad de los archivos nuevos o modificados desde la copia de seguridad de nivel 0, un nivel 2 realiza una copia de seguridad de los archivos nuevos o modificados desde la copia de seguridad de nivel 1, etc.
LISTA	`Y` o. `N`	`N`	Enumera los nombres de los archivos de backup y los números de nodos de información sin restaurar los datos realmente.
QTREES_DE_LISTAS	`Y` o. `N`	`N`	Enumera los qtrees de los que se ha realizado backup sin restaurar realmente los datos.

archivos, que se mueven entre qtrees de origen durante la restaur

Variable de entorno	Valores válidos	Predeterminado	Descripción
NOMBRES DE MULTIÁRBOL_	`string`	`none`	Especifica que la copia de seguridad es una copia de seguridad de varios subárboles. Se especifican varios subárboles en la cadena, que es una lista de nombres de subárboles separados por nuevas líneas y terminados en nulo. Los subárboles se especifican mediante nombres de ruta relativos a su directorio raíz común, que deben especificarse como último elemento de la lista. Si se usa esta variable, también se debe usar la variable DMP_NAME.
NDMP_UNICODE_ FH	`Y` o. `N`	`N`	Especifica que se incluye un nombre Unicode además del nombre NFS del archivo en la información del historial de archivos. Esta opción no la utilizan la mayoría de las aplicaciones de copia de seguridad y no debe establecerse a menos que la aplicación de copia de seguridad esté diseñada para recibir estos nombres de archivo adicionales. También se debe establecer la variable HIST.
NO_ACL	`Y` o. `N`	`N`	Especifica que las ACL no se deben copiar al realizar copias de seguridad de datos.

Variable de entorno	Valores válidos	Predeterminado	Descripción
ÁRBOL_NO_CUOTA	`Y` o. `N`	`N`	Especifica que los archivos y directorios en qtrees deben ignorarse al realizar una copia de seguridad de los datos. Cuando se establece en `Y`, No se realiza una copia de seguridad de los elementos de qtrees del conjunto de datos especificado por la variable DEL SISTEMA de ARCHIVOS. Esta variable solo tiene un efecto si la variable FILESYSTEM especifica un volumen completo. La variable NON_QUOTA_TREE sólo funciona en una copia de seguridad de nivel 0 y no funciona si se especifica la variable MULTI_SUBTREE_NAMES. Los archivos o directorios especificados para ser excluidos para la copia de seguridad no se excluyen si se establece NON_QUOTA_TREE en `Y` al mismo tiempo.

Variable de entorno	Valores válidos	Predeterminado	Descripción
NOWRITE	`Y` o. `N`	`N`	Especifica que la operación de restauración no debe escribir datos en el disco. Esta variable se utiliza para la depuración.

Variable de entorno	Valores válidos	Predeterminado	Descripción
RECURSIVA	`Y` o. `N`	`Y`	Especifica que se amplíen las entradas de directorio durante una restauración DE DAR. Deben habilitarse las variables de entorno DIRECT y ENHANCED_DAR_ENABLED (establecer en) `Y`) también. Si la variable RECURSIVA está desactivada (establecida en `N`), sólo los permisos y las ACL de todos los directorios de la ruta de origen original se restauran desde cinta, no el contenido de los directorios. Si la variable RECURSIVA está establecida en `N` O BIEN, LA variable RECOVER_FULL_PATHS está establecida en `Y`, la ruta de recuperación debe terminar con la ruta original. Si la variable RECURSIVA está deshabilitada y hay más de una ruta de recuperación, todas las rutas de recuperación deben estar contenidas en el más largo de las rutas de recuperación. De lo contrario, se mostrará un mensaje de error.

Por ejemplo, las

Variable de entorno	Valores válidos	Predeterminado	Descripción
RECUPERE_FULL_PATHS	`Y` o. `N`	`N`	Especifica que la ruta de recuperación completa tendrá sus permisos y ACL restaurados después del DAR. DIRECT y ENHANCED_DAR_ENABLED deben estar habilitados (establecer en `Y`) también. Si RECOVER_FULL_PATHS está establecido en `Y`, la ruta de recuperación debe terminar con la ruta original. Si ya hay directorios en el volumen de destino, sus permisos y ACL no se restaurarán a partir de la cinta.
ACTUALIZAR	`Y` o. `N`	`Y`	Actualiza la información de los metadatos para permitir la realización de backups incrementales basados EN NIVELES.

- `/foo/dir2/myfile`

Variables de entorno compatibles con SMTape

Variable de entorno	Valores válidos	Predeterminado	Descripción

FECHA_BASE	`DUMP_DATE`	`-1`	Especifica la fecha de inicio de las copias de seguridad incrementales.
			
			`` `BASE_DATE` Es una representación de cadena de los identificadores de instantánea de referencia. Con el `BASE_DATE` String, SMTape localiza la copia Snapshot de referencia. ``
			
			`` `BASE_DATE` no se requiere para backups básicos. Para un backup incremental, el valor de `DUMP_DATE` la variable de la base anterior o la copia de seguridad incremental se asigna a `BASE_DATE` variable. ``
			
			La aplicación de backup asigna el `DUMP_DATE` Valor de un backup incremental o base de SMTape anterior.

Variable de entorno	Valores válidos	Predeterminado	Descripción
FECHA_DE_VOLCADO	`return_value`	`none`	Al final de un backup de SMTape, DUMP_DATE contiene un identificador de cadena que identifica la copia Snapshot utilizada para ese backup. Esta copia Snapshot se puede utilizar como copia Snapshot de referencia para realizar un backup incremental posterior. El valor resultante de DUMP_DATE se utiliza como valor BASE_DATE para las copias de seguridad incrementales subsiguientes.
SMTAPE_BACKUP_SET_ID	`string`	`none`	Identifica la secuencia de backups incrementales asociados con el backup de referencia. El ID del conjunto de backup es un ID exclusivo de 128 bits que se genera durante una copia de seguridad de línea de base. La aplicación de copia de seguridad asigna este ID como entrada a `SMTAPE_BACKUP_SET_ID` variable durante una copia de seguridad incremental.

Variable de entorno	Valores válidos	Predeterminado	Descripción
SMTAPE_SNAPSHOT_NAME	Cualquier copia Snapshot válida que esté disponible en el volumen	`Invalid`	Cuando la variable SMTAPE_SNAPSHOT_NAME se establece en una copia de Snapshot, se realiza un backup de esa copia de Snapshot y de sus copias de Snapshot anteriores a cinta. Para backups incrementales, esta variable especifica la copia Snapshot incremental. La variable BASE_DATE proporciona la copia Snapshot de referencia.
SMTAPE_DELETE_SNAPSHOT	`Y` o. `N`	`N`	Para una copia Snapshot creada automáticamente por SMTape, cuando la variable SMTAPE_DELETE_SNAPSHOT se establece en `Y`, Después de completar la operación de copia de seguridad, SMTape elimina esta copia snapshot. Sin embargo, no se eliminará una copia Snapshot creada por la aplicación de backup.
SMTAPE_BREAK_MIRROR	`Y` o. `N`	`N`	Cuando la variable SMTAPE_BREAK_MIRROR se establece en `Y`, el volumen del tipo `DP` se cambia a a. `RW` volumen después de una restauración correcta.

Topologías habituales de backup en cinta NDMP

NDMP admite una serie de topologías y configuraciones entre aplicaciones de backup y sistemas de almacenamiento u otros servidores NDMP que proporcionan datos (sistemas de archivos) y servicios de cinta.

Del sistema de almacenamiento a la cinta local

En la configuración más simple, una aplicación de copia de seguridad realiza una copia de seguridad de los datos de un sistema de almacenamiento a un subsistema de cinta conectado al sistema de almacenamiento. La conexión de control NDMP existe en el límite de la red. La conexión de datos NDMP que existe dentro del sistema de almacenamiento entre los servicios de datos y cinta se denomina configuración local NDMP.

Sistema de almacenamiento a cinta conectado a otro sistema de almacenamiento

Una aplicación de backup también puede realizar backups de datos de un sistema de almacenamiento en una librería de cintas (un cambiador medio con una o varias unidades de cinta) conectada a otro sistema de almacenamiento. En este caso, la conexión de datos NDMP entre los servicios de datos y la cinta se proporciona mediante una conexión de red TCP o TCP/IPv6. Esto se denomina configuración de sistema de almacenamiento triple NDMP.

Librería de cintas conectada a la red y del sistema de almacenamiento

Las bibliotecas de cinta compatibles con NDMP proporcionan una variación de la configuración triple. En este caso, la biblioteca de cintas se conecta directamente a la red TCP/IP y se comunica con la aplicación de backup y el sistema de almacenamiento a través de un servidor NDMP interno.

Almacenamiento del sistema al servidor de datos, a cinta o servidor de datos al sistema de almacenamiento a cinta

NDMP también admite configuraciones triples de sistemas de almacenamiento para servidores de datos y sistemas de datos-servidor-almacenamiento, aunque estas variantes se implementan menos en gran medida. El sistema de almacenamiento al servidor permite realizar backups de los datos del sistema de almacenamiento en una biblioteca de cintas conectada al host de aplicaciones de backup o a otro sistema servidor de datos. La configuración de servidor a sistema de almacenamiento permite realizar copias de seguridad de los datos del servidor en una biblioteca de cintas conectada al sistema de almacenamiento.

Métodos de autenticación NDMP compatibles

Puede especificar un método de autenticación para permitir solicitudes de conexión NDMP. ONTAP es compatible con dos métodos para autenticar el acceso NDMP a un sistema de almacenamiento: Texto sin formato y el reto.

En el modo NDMP de ámbito nodo, tanto el reto como el texto sin formato están habilitados de forma predeterminada. Sin embargo, no puede desactivar el desafío. Puede activar y desactivar texto sin formato. En el método de autenticación de texto sin formato, la contraseña de inicio de sesión se transmite como texto sin cifrar.

En el modo NDMP de ámbito de la máquina virtual de almacenamiento (SVM), el método de autenticación es el reto de forma predeterminada. A diferencia del modo NDMP de ámbito de nodo, en este modo puede habilitar y deshabilitar los métodos de autenticación de texto sin formato y de desafío.

Información relacionada

Autenticación de usuario en un modo NDMP de ámbito de nodo

Autenticación de usuario en el modo NDMP con ámbito de SVM

Extensiones NDMP compatibles con ONTAP

NDMP v4 proporciona un mecanismo para crear extensiones de protocolo NDMP v4 sin tener que modificar el protocolo NDMP v4 de núcleo. Debe conocer las extensiones de

NDMP v4 compatibles con ONTAP.

Las siguientes extensiones de NDMP v4 son compatibles con ONTAP:

- Respaldo para clúster (CAB)

  Esta extensión solo es compatible con el modo NDMP con el ámbito de la SVM.

- Extensión de dirección de conexión (cae) para compatibilidad con IPv6
- Clase de extensión 0x2050

  Esta extensión admite operaciones de backup reiniciables y extensiones de administración de Snapshot.

  La `NDMP_SNAP_RECOVER` El mensaje, que forma parte de las extensiones de administración Snapshot, se utiliza para iniciar una operación de recuperación y transferir los datos recuperados de una copia Snapshot local a una ubicación del sistema de archivos local. En ONTAP, este mensaje solo permite la recuperación de volúmenes y archivos normales.

  La `NDMP_SNAP_DIR_LIST` Message le permite examinar a través de las copias Snapshot de un volumen. Si se realiza una operación no disruptiva mientras hay una operación de exploración en curso, la aplicación de backup debe volver a iniciar la operación de exploración.

Extensión de backup reiniciable de NDMP para un volcado compatible con ONTAP

Puede utilizar la funcionalidad de extensión de backup reiniciable (RBE) de NDMP para reiniciar un backup desde un punto de control conocido en el flujo de datos antes del fallo.

Qué es la funcionalidad DAR mejorada

Puede utilizar la funcionalidad DE recuperación DE acceso directo (DAR) mejorada para DAR de directorios y DAR de ficheros y secuencias NT. De forma predeterminada, la función DAR mejorada está activada.

Habilitar una funcionalidad DAR mejorada puede tener un impacto en el rendimiento de backup, ya que es necesario crear y escribir un mapa offset en cinta. Puede habilitar o deshabilitar EL DAR mejorado en los modos NDMP de ámbito de nodos y de máquinas virtuales de almacenamiento (SVM).

Límites de escalabilidad para sesiones NDMP

Debe tener en cuenta el número máximo de sesiones NDMP que se pueden establecer de manera simultánea en sistemas de almacenamiento de diferentes capacidades de memoria del sistema. Este número máximo depende de la memoria del sistema de un sistema de almacenamiento.

Los límites mencionados en la siguiente tabla son para el servidor NDMP. Los límites mencionados en la sección "límites de disponibilidad para sesiones de copia de seguridad y restauración de volcado" corresponden a la sesión de descarga y restauración.

Límites de escalabilidad para sesiones de backup y restauración de volcado

Memoria del sistema de un sistema de almacenamiento	Número máximo de sesiones NDMP
Menos de 16 GB	8
Mayor o igual que 16 GB pero menor que 24 GB	20
Mayor o igual que 24 GB	36

Puede obtener la memoria del sistema del sistema de almacenamiento mediante el `sysconfig -a` comando (disponible a través del nodeshell). Para obtener más información acerca de cómo utilizar este comando, consulte las páginas man.

Acerca de NDMP para volúmenes FlexGroup

A partir de ONTAP 9.7, NDMP es compatible con los volúmenes FlexGroup.

A partir de ONTAP 9.7, se admite el comando ndmpcopy para la transferencia de datos entre volúmenes FlexVol y FlexGroup.

Si se revierte de ONTAP 9.7 a una versión anterior, la información de transferencia incremental de las transferencias anteriores no se conserva y, por lo tanto, se debe realizar una copia básica después de revertir.

A partir de ONTAP 9.8, las siguientes funciones NDMP son compatibles con los volúmenes FlexGroup:

- El mensaje NDMP_SNAP_RECOVER de la clase de extensión 0x2050 se puede utilizar para recuperar archivos individuales de un volumen FlexGroup.
- Se admite la extensión de backup NDMP restartable (RBE) para los volúmenes de FlexGroup.
- Las variables de entorno EXCLUDE y MULTI_SUBTREE_NAMES son compatibles con los volúmenes FlexGroup.

Acerca de NDMP con volúmenes SnapLock

La creación de varias copias de datos regulados le proporciona escenarios de recuperación redundantes y, al utilizar el volcado y la restauración NDMP, es posible conservar las características DE escritura única y lectura múltiple (WORM) de los archivos de origen en un volumen SnapLock.

Los atributos WORM de los archivos de un volumen de SnapLock se conservan al realizar backups, restaurar y copiar datos; sin embargo, los atributos WORM solo se aplican al restaurar a un volumen de SnapLock. Si se restaura un backup de un volumen SnapLock en un volumen distinto a un volumen SnapLock, se conservan los atributos WORM, pero se ignoran y ONTAP no los aplica.

Gestione el modo NDMP de ámbito del nodo para volúmenes FlexVol

Gestione la información general del modo NDMP de ámbito del nodo para FlexVol Volumes

Puede administrar NDMP en el nivel de nodo mediante los comandos y las opciones de

NDMP. Las opciones de NDMP se pueden modificar mediante el `options` comando. Es necesario usar credenciales específicas de NDMP para acceder a un sistema de almacenamiento a fin de ejecutar operaciones de backup y restauración a cinta.

Para obtener más información acerca de `options` consulte las páginas de manual.

Información relacionada

Comandos para gestionar el modo NDMP de ámbito de nodo

Lo que es el modo NDMP de ámbito del nodo

Comandos para gestionar el modo NDMP de ámbito de nodo

Puede utilizar el `system services ndmp` Comandos para gestionar NDMP en el nivel de un nodo. Algunos de estos comandos quedan obsoletos y se quitarán en una versión principal futura.

Puede utilizar los siguientes comandos NDMP solamente en el nivel de privilegio avanzado:

- `system services ndmp service terminate`
- `system services ndmp service start`
- `system services ndmp service stop`
- `system services ndmp log start`
- `system services ndmp log stop`

Si desea…	Se usa este comando…
Active el servicio NDMP	`system services ndmp on*`
Desactive el servicio NDMP	`system services ndmp off*`
Mostrar la configuración de NDMP	`system services ndmp show*`
Modifique la configuración de NDMP	`system services ndmp modify*`
Muestra la versión predeterminada de NDMP	`system services ndmp version*`
Mostrar la configuración del servicio NDMP	`system services ndmp service show`
Modifique la configuración del servicio NDMP	`system services ndmp service modify`
Mostrar todas las sesiones de NDMP	`system services ndmp status`
Mostrar información detallada acerca de todas las sesiones NDMP	`system services ndmp probe`

Si desea…	Se usa este comando…
Finalice la sesión NDMP especificada	`system services ndmp kill`
Finalice todas las sesiones NDMP	`system services ndmp kill-all`
Cambie la contraseña NDMP	`system services ndmp password*`
Habilite el modo de NDMP de ámbito del nodo	`system services ndmp node-scope-mode on*`
Deshabilite el modo NDMP de ámbito del nodo	`system services ndmp node-scope-mode off*`
Muestra el estado del modo NDMP de ámbito del nodo	`system services ndmp node-scope-mode status*`
Cierre todas las sesiones NDMP con fuerza	`system services ndmp service terminate`
Inicie el demonio del servicio NDMP	`system services ndmp service start`
Detenga el demonio del servicio NDMP	`system services ndmp service stop`
Inicie el registro para la sesión NDMP especificada	`system services ndmp log start*`
Detenga el registro de la sesión NDMP especificada	`system services ndmp log stop*`

- Estos comandos quedaron obsoletos y se quitarán en una versión principal futura.

Para obtener más información sobre estos comandos, consulte las páginas de manual de `system services ndmp` comandos.

Autenticación de usuario en un modo NDMP de ámbito de nodo

En el modo NDMP de ámbito del nodo, debe utilizar credenciales específicas de NDMP para acceder a un sistema de almacenamiento a fin de realizar operaciones de backup y restauración a cinta.

El ID de usuario predeterminado es "'root'". Antes de usar NDMP en un nodo, debe asegurarse de cambiar la contraseña de NDMP predeterminada asociada con el usuario NDMP. También es posible cambiar el ID de usuario predeterminado de NDMP.

Información relacionada

Comandos para gestionar el modo NDMP de ámbito de nodo

Gestione el modo NDMP de ámbito SVM para volúmenes FlexVol

Gestione la información general sobre el modo NDMP de ámbito SVM para FlexVol Volumes

Puede gestionar NDMP por SVM usando las opciones y los comandos de NDMP. Las opciones de NDMP se pueden modificar mediante el `vserver services ndmp modify` comando. En el modo NDMP con ámbito SVM, la autenticación del usuario está integrada con el mecanismo de control de acceso basado en roles.

Puede agregar NDMP a la lista de protocolos permitidos o no permitidos utilizando el `vserver modify` comando. De forma predeterminada, NDMP se encuentra en la lista de protocolos permitidos. Si se agrega NDMP a la lista de protocolos no permitidos, no se podrán establecer sesiones NDMP.

Puede controlar el tipo de LIF en el que se establece una conexión de datos NDMP mediante el `-preferred-interface-role` opción. Durante una conexión de datos NDMP, NDMP elige una dirección IP que pertenece al tipo de LIF tal como especifica esta opción. Si las direcciones IP no pertenecen a ninguno de estos tipos de LIF, no se puede establecer la conexión de datos NDMP. Para obtener más información acerca de `-preferred-interface-role` consulte las páginas man.

Para obtener más información acerca de `vserver services ndmp modify` consulte las páginas de manual.

Información relacionada

Comandos para gestionar el modo NDMP con ámbito de la SVM

Qué hace la extensión Cluster Aware Backup

"Conceptos de ONTAP"

Qué es el modo NDMP con ámbito SVM

"Administración del sistema"

Comandos para gestionar el modo NDMP con ámbito de la SVM

Puede utilizar el `vserver services ndmp` Comandos para gestionar NDMP en cada máquina virtual de almacenamiento (SVM, antes denominada Vserver).

Si desea…	Se usa este comando…
Active el servicio NDMP	`vserver services ndmp on` El servicio NDMP siempre debe estar habilitado en todos los nodos de un clúster. Puede habilitar el servicio NDMP en un nodo mediante el `system services ndmp on` comando. De manera predeterminada, el servicio NDMP siempre está habilitado en un nodo.

Si desea…	Se usa este comando…
Desactive el servicio NDMP	`vserver services ndmp off`
Mostrar la configuración de NDMP	`vserver services ndmp show`
Modifique la configuración de NDMP	`vserver services ndmp modify`
Muestra la versión NDMP predeterminada	`vserver services ndmp version`
Mostrar todas las sesiones de NDMP	`vserver services ndmp status`
Mostrar información detallada acerca de todas las sesiones NDMP	`vserver services ndmp probe`
Terminar una sesión NDMP especificada	`vserver services ndmp kill`
Finalice todas las sesiones NDMP	`vserver services ndmp kill-all`
Genere la contraseña NDMP	`vserver services ndmp generate-password`
Mostrar el estado de la extensión NDMP	`vserver services ndmp extensions show` Este comando solo está disponible en el nivel de privilegios avanzado.
Modifique el estado de la extensión NDMP (enable o disable)	`vserver services ndmp extensions modify` Este comando solo está disponible en el nivel de privilegios avanzado.
Inicie el registro para la sesión NDMP especificada	`vserver services ndmp log start` Este comando solo está disponible en el nivel de privilegios avanzado.
Detenga el registro de la sesión NDMP especificada	`vserver services ndmp log stop` Este comando solo está disponible en el nivel de privilegios avanzado.

Para obtener más información sobre estos comandos, consulte las páginas de manual de `vserver services ndmp` comandos.

Qué hace la extensión Cluster Aware Backup

CAB (Backup para Cluster Aware) es una extensión del protocolo NDMP v4. Esta extensión permite que el servidor NDMP establezca una conexión de datos en un nodo propietario de un volumen. Esto también permite a la aplicación de backup determinar si hay volúmenes y dispositivos de cinta ubicados en el mismo nodo de un clúster.

Para permitir que el servidor NDMP identifique el nodo propietario de un volumen y establezca una conexión de datos en dicho nodo, la aplicación de backup debe admitir la extensión CAB. La extensión CAB requiere que la aplicación de copia de seguridad informe al servidor NDMP del volumen que se va a realizar una copia de seguridad o restaurar antes de establecer la conexión de datos. Esto permite que el servidor NDMP determine el nodo que aloja el volumen y establezca la conexión de datos correctamente.

Con la extensión CAB que admite la aplicación de backup, el servidor NDMP proporciona información de afinidad acerca de los volúmenes y los dispositivos de cinta. Con esta información de afinidad, la aplicación de backup puede realizar un backup local en lugar de un backup triple si un volumen y un dispositivo de cinta están ubicados en el mismo nodo de un clúster.

Disponibilidad de volúmenes y dispositivos de cinta para realizar backups y restauraciones en diferentes tipos de LIF

Puede configurar una aplicación de backup para establecer una conexión de control NDMP en cualquiera de los tipos de LIF de un clúster. En el modo NDMP de la máquina virtual de almacenamiento (SVM), puede determinar la disponibilidad de volúmenes y dispositivos de cinta para las operaciones de backup y restauración, en función de estos tipos de LIF y el estado de la extensión CAB.

En las siguientes tablas, se muestra la disponibilidad de volúmenes y dispositivos de cinta para los tipos de LIF de conexión de control NDMP y el estado de la extensión CAB:

La disponibilidad de volúmenes y dispositivos de cinta cuando la aplicación de backup no admite la extensión CAB

Tipo de LIF de conexión de control NDMP	Volúmenes disponibles para backup o restauración	Dispositivos de cinta disponibles para backup o restauración
LIF de gestión de nodos	Todos los volúmenes alojados por un nodo	Los dispositivos de cinta conectados al nodo que aloja el LIF de gestión del nodo
LIF de datos	Solo los volúmenes que pertenecen a la SVM alojada por un nodo que aloja la LIF de datos	Ninguno
LIF de gestión de clústeres	Todos los volúmenes alojados por un nodo que aloja el LIF de gestión de clústeres	Ninguno
LIF entre clústeres	Todos los volúmenes alojados por un nodo que aloja la LIF de interconexión de clústeres	Los dispositivos de cinta conectados al nodo que aloja la LIF de interconexión de clústeres

Disponibilidad de volúmenes y dispositivos de cinta cuando la aplicación de backup admite la extensión CAB

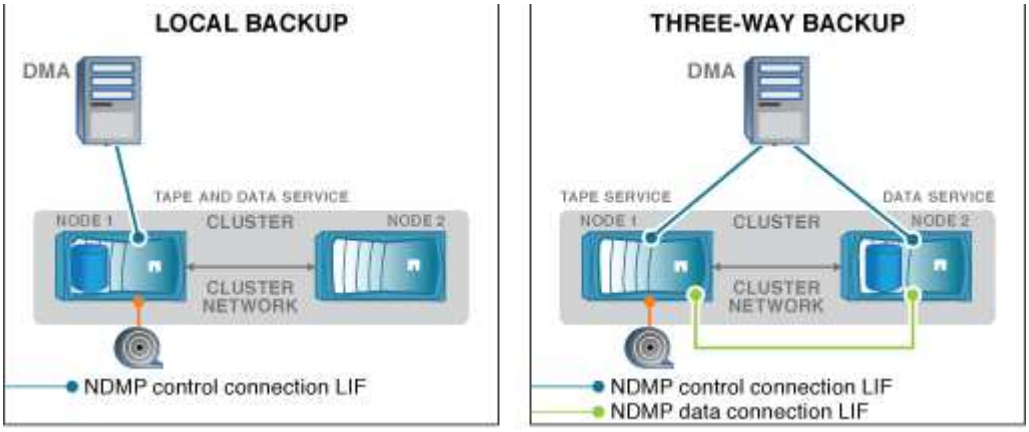
Tipo de LIF de conexión de control NDMP	Volúmenes disponibles para backup o restauración	Dispositivos de cinta disponibles para backup o restauración
LIF de gestión de nodos	Todos los volúmenes alojados por un nodo	Los dispositivos de cinta conectados al nodo que aloja el LIF de gestión del nodo
LIF de datos	Todos los volúmenes que pertenecen a la SVM que aloja la LIF de datos	Ninguno
LIF de gestión de clústeres	Todos los volúmenes del clúster	Todos los dispositivos de cinta del cluster
LIF entre clústeres	Todos los volúmenes del clúster	Todos los dispositivos de cinta del cluster

Qué es la información de afinidad

Una vez que la aplicación de backup se detecta EN CABINA, el servidor NDMP proporciona información única sobre la ubicación de los volúmenes y los dispositivos de cinta. Mediante el uso de esta información de afinidad, la aplicación de backup puede realizar un backup local en lugar de un backup triple si un volumen y un dispositivo de cinta comparten la misma afinidad.

Si la conexión de control NDMP se establece en una LIF de gestión de nodos, LIF de gestión de clústeres, O mediante LIF de interconexión de clústeres, la aplicación de backup puede usar la información de afinidad para determinar si un volumen y un dispositivo de cinta están ubicados en el mismo nodo y, a continuación, realizar una operación de backup o restauración local o triple. Si la conexión del control NDMP se establece en una LIF de datos, la aplicación de backup siempre realiza un backup triple.

Backup NDMP local y backup NDMP triple



Mediante la información de afinidad con los volúmenes y los dispositivos de cinta, DMA (aplicación de backup) realiza un backup NDMP local en el volumen y el dispositivo de cinta ubicados en el nodo 1 del clúster. Si el volumen se mueve del nodo 1 al nodo 2, cambia la información de afinidad sobre el volumen y el dispositivo

de cinta. Por lo tanto, para un backup posterior, DMA realiza una operación de backup NDMP triple. De este modo se garantiza la continuidad de la política de backup del volumen independientemente del nodo al que se traslade el volumen.

Información relacionada

Qué hace la extensión Cluster Aware Backup

El servidor NDMP admite conexiones de control seguras en el modo SVM-scoped

Se puede establecer una conexión de control segura entre la aplicación de administración de datos (DMA) y el servidor NDMP utilizando sockets seguros (SSL/TLS) como mecanismo de comunicación. Esta comunicación SSL se basa en los certificados del servidor. El servidor NDMP escucha en el puerto 30000 (asignado por IANA para el servicio "'ndmps'").

Tras establecer la conexión desde el cliente en este puerto, el protocolo de enlace SSL estándar se produce cuando el servidor presenta el certificado al cliente. Cuando el cliente acepta el certificado, se completa el apretón de manos SSL. Una vez completado este proceso, toda la comunicación entre el cliente y el servidor se cifra. El flujo de trabajo del protocolo NDMP sigue siendo exactamente igual que antes. La conexión NDMP segura sólo requiere autenticación de certificado del servidor. Un DMA puede optar por establecer una conexión mediante la conexión al servicio NDMP seguro o al servicio NDMP estándar.

De manera predeterminada, el servicio NDMP seguro está deshabilitado para una máquina virtual de almacenamiento (SVM). Puede habilitar o deshabilitar el servicio NDMP seguro en una SVM determinada mediante el `vserver services ndmp modify -vserver vserver -is-secure-control -connection-enabled [true|false]` comando.

Tipos de conexión de datos NDMP

En el modo NDMP de la máquina virtual de almacenamiento (SVM), los tipos de conexión de datos NDMP admitidos dependen del tipo de LIF de conexión de control NDMP y el estado de la extensión CAB. Este tipo de conexión de datos NDMP indica si se puede ejecutar una operación de backup o restauración NDMP local o triple.

Puede realizar un backup o una operación de restauración NDMP triple a través de una red TCP o TCP/IPv6. En las siguientes tablas, se muestran los tipos de conexión de datos NDMP según el tipo de LIF de conexión de control NDMP y el estado de la extensión CAB.

Tipo de conexión de datos NDMP cuando la aplicación de backup admite una extensión CAB

Tipo de LIF de conexión de control NDMP	Tipo de conexión de datos NDMP
LIF de gestión de nodos	LOCAL, TCP Y TCP/IPV6
LIF de datos	TCP/TCP
LIF de gestión de clústeres	LOCAL, TCP Y TCP/IPV6
LIF entre clústeres	LOCAL, TCP Y TCP/IPV6

Tipo de conexión de datos NDMP cuando la aplicación de backup no admite la extensión CAB

Tipo de LIF de conexión de control NDMP	Tipo de conexión de datos NDMP
LIF de gestión de nodos	LOCAL, TCP Y TCP/IPV6
LIF de datos	TCP/TCP
LIF de gestión de clústeres	TCP/TCP
LIF entre clústeres	LOCAL, TCP Y TCP/IPV6

Información relacionada

Qué hace la extensión Cluster Aware Backup

"Gestión de redes"

Autenticación de usuario en el modo NDMP con ámbito de SVM

En el modo NDMP de la máquina virtual de almacenamiento (SVM), la autenticación de usuario NDMP está integrada con el control de acceso basado en roles. En el contexto de la SVM, el usuario NDMP debe tener el rol "'vsadmin'" o "'vsadmin-backup'". En un contexto de cluster, el usuario NDMP debe tener el rol «'admin'» o «'backup'».

Además de estas funciones predefinidas, una cuenta de usuario asociada a una función personalizada también puede utilizarse para la autenticación NDMP siempre y cuando la función personalizada tenga la carpeta «'vserver Services ndmp'» en su directorio de comandos y el nivel de acceso de la carpeta no sea «'none'». En este modo, debe generar una contraseña NDMP para una cuenta de usuario determinada, que se crea mediante el control de acceso basado en roles. Los usuarios de clúster con un rol de administrador o backup pueden acceder a una LIF de gestión de nodos, una LIF de gestión de clústeres o una LIF de interconexión de clústeres. Los usuarios de un rol de vsadmin o de vsadmin pueden acceder solo a la LIF de datos para esa SVM. Por lo tanto, según la función de un usuario, la disponibilidad de volúmenes y dispositivos de cinta para las operaciones de backup y restauración varía.

Este modo también admite la autenticación de usuario para usuarios NIS y LDAP. Por lo tanto, los usuarios NIS y LDAP pueden acceder a varias SVM con un ID de usuario y una contraseña comunes. Sin embargo, la autenticación NDMP no admite usuarios de Active Directory.

En este modo, una cuenta de usuario debe estar asociada a la aplicación SSH y al método de autenticación «'Contraseña de usuario'».

Información relacionada

Comandos para gestionar el modo NDMP con ámbito de la SVM

"Administración del sistema"

"Conceptos de ONTAP"

Genere una contraseña específica de NDMP para los usuarios de NDMP

En el modo NDMP de la máquina virtual de almacenamiento (SVM), debe generar una

contraseña para un ID de usuario específico. La contraseña generada se basa en la contraseña de inicio de sesión real para el usuario NDMP. Si cambia la contraseña de inicio de sesión real, deberá generar de nuevo la contraseña específica de NDMP.

Pasos

1. Utilice la `vserver services ndmp generate-password` Para generar una contraseña específica de NDMP.

   Puede utilizar esta contraseña en cualquier operación NDMP actual o futura que requiera la introducción de la contraseña.

   > Desde el contexto de la máquina virtual de almacenamiento (SVM, antes denominada Vserver), puede generar contraseñas de NDMP para usuarios que solo pertenecen a esa SVM.

   El ejemplo siguiente muestra cómo generar una contraseña específica de NDMP para un ID de usuario usuario1:

   ```
   cluster1::vserver services ndmp> generate-password -vserver vs1 -user
   user1

   Vserver: vs1
   User: user1
   Password: jWZiNt57huPOoD8d
   ```

2. Si cambia la contraseña a su cuenta de sistema de almacenamiento normal, repita este procedimiento para obtener su nueva contraseña específica de NDMP.

Cómo se ven afectadas las operaciones de backup y restauración de cinta durante la recuperación ante desastres en la configuración de MetroCluster

Se pueden ejecutar operaciones de backup y restauración a cinta simultáneamente durante la recuperación ante desastres en una configuración de MetroCluster. Debe entender cómo se ven afectadas estas operaciones durante la recuperación de desastres.

Si las operaciones de backup y restauración de cinta se llevan a cabo en un volumen de anSVM en una relación de recuperación ante desastres, puede continuar con las operaciones de backup y restauración de cinta incrementales después de una conmutación de sitios y conmutación de estado.

Acerca del motor de volcado para volúmenes FlexVol

Acerca del motor de volcado para volúmenes FlexVol

Dump es una solución de backup y recuperación basada en copias de Snapshot de ONTAP que ayuda a realizar backups de archivos y directorios desde una copia Snapshot a un dispositivo de cinta y restaura los datos del backup en un sistema de almacenamiento.

Puede realizar una copia de seguridad de los datos del sistema de archivos, como directorios, archivos y su configuración de seguridad asociada, en un dispositivo de cinta mediante la copia de seguridad de volcado. Puede realizar backup de un volumen completo, de un qtree completo o de un subárbol que no sea ni un volumen completo ni un qtree completo.

Puede realizar un backup o una restauración de volcado utilizando aplicaciones de backup compatibles con NDMP.

Cuando se realiza un backup de volcado, es posible especificar la copia Snapshot que se usará para un backup. Si no se especifica una copia Snapshot para el backup, el motor de volcado crea una copia Snapshot para el backup. Una vez completada la operación de copia de seguridad, el motor de volcado elimina esta copia snapshot.

Puede realizar copias de seguridad de nivel 0, incrementales o diferenciales en cinta utilizando el motor de descarga.

> Después de revertir a una versión anterior a Data ONTAP 8.3, debe ejecutar una operación de backup base antes de realizar una operación de backup incremental.

Información relacionada

"Actualización, reversión o degradación"

Cómo funciona un backup de volcado

Una copia de seguridad de volcado escribe los datos del sistema de archivos del disco a la cinta mediante un proceso predefinido. Puede realizar un backup de un volumen, un qtree o un subárbol que no sea ni un volumen completo ni un qtree completo.

En la siguiente tabla se describe el proceso que ONTAP utiliza para realizar un backup del objeto indicado por la ruta de volcado:

Etapa	Acción
1	Para un volumen completo menor que los backups qtree o los backups completos de qtree, ONTAP atraviesa directorios para identificar los archivos en los que se va a realizar el backup. Si va a realizar el backup de un volumen o qtree completo, ONTAP combina esta fase con la fase 2.
2	Para un backup de volumen completo o de qtree completo, ONTAP identifica los directorios en los volúmenes o qtrees de los que se va a realizar un backup.
3	ONTAP escribe los directorios en la cinta.
4	ONTAP escribe los archivos en la cinta.
5	ONTAP escribe la información de ACL (si corresponde) en la cinta.

El backup de volcado utiliza una copia Snapshot de los datos para el backup. Por lo tanto, no es necesario desconectar el volumen antes de iniciar el backup.

El backup de volcado asigna nombres a cada copia Snapshot que crea `snapshot_for_backup.n`, donde `n`

es un entero que comienza en 0. Cada vez que el backup volcado crea una copia Snapshot, incrementa el número entero en 1. El entero se restablece a 0 después de reiniciar el sistema de almacenamiento. Una vez completada la operación de copia de seguridad, el motor de volcado elimina esta copia snapshot.

Cuando ONTAP realiza varios backups de volcado de manera simultánea, el motor de volcado crea varias copias Snapshot. Por ejemplo, si ONTAP ejecuta dos backups de volcado de manera simultánea, puede encontrar las siguientes copias Snapshot en los volúmenes desde los cuales se realiza el backup de los datos: `snapshot_for_backup.0` y.. `snapshot_for_backup.1`.

> Cuando se realiza un backup de una copia Snapshot, el motor de volcado no crea una copia Snapshot adicional.

Tipos de datos de los que el motor de descarga realiza una copia de seguridad

El motor de volcado permite lanzar backups de los datos a cinta como protección ante desastres o interrupciones en la controladora. Además de realizar backups de objetos de datos como archivos, directorios, qtrees o volúmenes completos, el motor de volcado puede realizar backups de muchos tipos de información acerca de cada archivo. Conocer los tipos de datos que el motor de volcado puede realizar y las restricciones que se deben tener en cuenta puede ayudarle a planificar su método de recuperación ante desastres.

Además de realizar una copia de seguridad de los datos de los archivos, el motor de volcado puede realizar una copia de seguridad de la siguiente información acerca de cada archivo, según corresponda:

- GID de UNIX, UID del propietario y permisos de archivo
- Acceso UNIX, creación y tiempo de modificación
- Tipo de archivo
- Tamaño de archivo
- Nombre dos, atributos dos y hora de creación
- Listas de control de acceso (ACL) con 1,024 entradas de control de acceso (ACE)
- Información de Qtree
- Rutas de unión

Las rutas de unión se copian como enlaces simbólicos.

- Clones LUN y LUN

  Puede realizar backups de un objeto de LUN completo; sin embargo, no puede realizar backups de un único archivo dentro del objeto LUN. De igual modo, puede restaurar un objeto de LUN completo, pero no un solo archivo dentro de la LUN.

  > El motor de volcado realiza una copia de seguridad de los clones de LUN como LUN independientes.

- Archivos alineados con equipos virtuales

  Las versiones anteriores a Data ONTAP 8.1.2 no admiten la copia de seguridad de archivos alineados con equipos virtuales.

> Cuando se realiza la transición de un clon de LUN respaldado por snapshots de Data ONTAP operativo en 7-Mode a ONTAP, se convierte en una LUN inconsistente. El motor de volcado no realiza copias LUN incoherentes.

Cuando restaura datos en un volumen, las operaciones de I/o del cliente están restringidas en las LUN que se restauran. La restricción de LUN se elimina solo cuando se completa la operación de restauración de volcado. De forma similar, durante una operación de restauración de archivos o LUN únicos de SnapMirror, las I/o del cliente están restringidas a ambos archivos y LUN que se van a restaurar. Esta restricción se elimina solo cuando se completa la operación de restauración de archivos o LUN. Si se realiza un backup de volcado en un volumen en el que se está realizando una operación de restauración de volcado o restauración de archivo único de SnapMirror o LUN, los archivos o LUN que tienen restricción de I/o del cliente no se incluyen en el backup. Estos archivos o LUN se incluyen en una operación de copia de seguridad posterior si la restricción de I/o del cliente se elimina.

> Una LUN que se ejecute en Data ONTAP 8.3 y que se realice un backup a cinta solo se podrá restaurar a las versiones 8.3 y posteriores, y no a una versión anterior. Si la LUN se restaura a una versión anterior, la LUN se restaura como un archivo.

Cuando se realiza un backup de un volumen secundario de SnapVault o de un destino de SnapMirror para volúmenes a cinta, solo se realiza un backup de los datos del volumen. No se realiza un backup de los metadatos asociados. Por lo tanto, cuando intenta restaurar el volumen, solo se restauran los datos de ese volumen. La información sobre las relaciones de SnapMirror para volúmenes no está disponible en el backup y, por lo tanto, no se restaura.

Si vuelca un archivo que sólo tiene permisos de Windows NT y lo restaura a un qtree o volumen de estilo UNIX, el archivo obtiene los permisos UNIX predeterminados para ese qtree o volumen.

Si vuelca un archivo que solo tiene permisos de UNIX y lo restaura a un qtree o volumen de estilo NTFS, el archivo obtiene los permisos de Windows predeterminados para ese qtree o volumen.

Otros volcados y restauraciones conservan los permisos.

Puede realizar un backup de los archivos alineados con las máquinas virtuales y del `vm-align-sector` opción. Para obtener más información sobre los archivos alineados con equipos virtuales, consulte "Gestión de almacenamiento lógico".

Qué cadenas de incremento son

Una cadena de incremento es una serie de copias de seguridad incrementales de la misma ruta. Como puede especificar cualquier nivel de backup en cualquier momento, debe comprender las cadenas de incremento para poder realizar backups y restauraciones de manera efectiva. Es posible ejecutar 31 niveles de operaciones de backup incrementales.

Existen dos tipos de cadenas de incremento:

- Una cadena de incremento consecutiva, que es una secuencia de backups incrementales que comienza con el nivel 0 y se eleva por 1 en cada backup posterior.
- Una cadena de incremento no consecutiva, donde las copias de seguridad incrementales omiten niveles o tienen niveles que están fuera de secuencia, como 0, 2, 3, 1, 4 o más comúnmente 0, 1, 1, 1 o 0, 1, 2, 1, 2.

Los backups incrementales se basan en los backups más recientes de bajo nivel. Por ejemplo, la secuencia

de niveles de backup 0, 2, 3, 1, 4 proporciona dos cadenas de incremento: 0, 2, 3 y 0, 1, 4. La siguiente tabla explica las bases de los backups incrementales:

Orden de copia de seguridad	Incrementar el nivel	Cadena de incremento	Base	Archivos de copia de seguridad
1	0	Ambas	De los archivos del sistema de almacenamiento	Todos los archivos de la ruta de copia de seguridad
2	2	0, 2, 3	Backup de nivel 0	Archivos en la ruta de copia de seguridad creada desde la copia de seguridad de nivel 0
3	3	0, 2, 3	Backup de nivel 2	Archivos en la ruta de copia de seguridad creada desde la copia de seguridad de nivel 2
4	1	0, 1, 4	Backup de nivel 0, porque es el nivel más reciente inferior al backup de nivel 1	Archivos en la ruta de copia de seguridad creados desde la copia de seguridad de nivel 0, incluidos los archivos que se encuentran en las copias de seguridad de nivel 2 y nivel 3
5	4	0, 1, 4	El backup de nivel 1, porque es un nivel inferior y es más reciente que los backups de nivel 0, nivel 2 o nivel 3	Archivos creados desde la copia de seguridad de nivel 1

Qué es el factor de bloqueo

Un bloque de cinta es 1,024 bytes de datos. Durante un backup o una restauración de cinta, es posible especificar la cantidad de bloques de cinta que se transfieren en cada operación de lectura/escritura. Este número se llama el *factor de bloqueo*.

Puede utilizar un factor de bloqueo de 4 a 256. Si tiene previsto restaurar una copia de seguridad en un sistema distinto al del que hizo la copia de seguridad, el sistema de restauración debe admitir el factor de bloqueo que se utilizó para la copia de seguridad. Por ejemplo, si se utiliza un factor de bloqueo de 128, el sistema en el que se restaura ese backup debe admitir un factor de bloqueo de 128.

Durante una copia de seguridad NDMP, EL OBJETO MOVER_RECORD_SIZE determina el factor de bloqueo. ONTAP permite un valor máximo de 256 KB para MOVER_RECORD_SIZE.

Cuándo reiniciar una copia de seguridad de volcado

En ocasiones, un backup de volcado no finaliza a causa de errores internos o externos, como errores de escritura en cinta, interrupciones del suministro eléctrico, interrupciones accidentales de los usuarios o incoherencias internas en el sistema de almacenamiento. Si falla el backup por uno de estos motivos, puede reiniciarlo.

Puede optar por interrumpir y reiniciar un backup para evitar periodos de gran tráfico en el sistema de almacenamiento o competir por otros recursos limitados del sistema de almacenamiento, como una unidad de cinta. Puede interrumpir una copia de seguridad larga y reiniciarla más tarde si una restauración (o copia de seguridad) más urgente requiere la misma unidad de cinta. Los backups reiniciables persisten durante los reinicios. Sólo puede reiniciar una copia de seguridad anulada en cinta si se cumplen las siguientes condiciones:

- La copia de seguridad anulada se encuentra en la fase IV
- Están disponibles todas las copias Snapshot asociadas que estaban bloqueadas por el comando dump.
- El historial de archivos debe estar activado.

Cuando se cancela una operación de volcado y se deja en un estado reiniciable, las copias Snapshot asociadas se bloquean. Estas copias Snapshot se liberan después de que se elimine el contexto de los backups. Puede ver la lista de contextos de copia de seguridad mediante la `vserver services ndmp restartable backup show` comando.

```
cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                   Is Cleanup Pending?
----------- ------------------------------------ -------------------
vserver1 330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1 481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2 5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::> vserver services ndmpd restartable-backup show -vserver
vserver1 -context-id 330e6739-0179-11e6-a299-005056bb4bc9

                      Vserver: vserver1
            Context Identifier: 330e6739-0179-11e6-a299-005056bb4bc9
                   Volume Name: /vserver1/vol1
           Is Cleanup Pending?: false
            Backup Engine Type: dump
Is Snapshot Copy Auto-created?: true
                     Dump Path: /vol/vol1
   Incremental Backup Level ID: 0
                     Dump Name: /vserver1/vol1
     Context Last Updated Time: 1460624875
               Has Offset Map?: true
                 Offset Verify: true
       Is Context Restartable?: true
              Is Context Busy?: false
                  Restart Pass: 4
              Status of Backup: 2
            Snapshot Copy Name: snapshot_for_backup.1
          State of the Context: 7

cluster::>"
```

Cómo funciona una restauración de volcado

Una restauración de volcado escribe los datos del sistema de archivos de una cinta a un disco mediante un proceso predefinido.

El proceso de la siguiente tabla muestra el funcionamiento de la restauración de volcado:

Etapa	Acción
1	ONTAP cataloga los archivos que deben extraerse de la cinta.
2	ONTAP crea directorios y archivos vacíos.

Etapa	Acción
3	ONTAP lee un archivo desde una cinta, lo escribe en el disco y establece los permisos (incluidas las ACL) en él.
4	ONTAP repite las fases 2 y 3 hasta que todos los archivos especificados se copien de la cinta.

Tipos de datos que restaura el motor de volcado

Cuando se produce un desastre o una interrupción de la controladora, el motor de volcado ofrece diversos métodos para recuperar todos los datos de los que se hizo backup, desde archivos individuales a atributos de archivo, a directorios completos. Conocer los tipos de datos que el motor de volcado puede restaurar y cuándo utilizar qué método de recuperación puede ayudar a minimizar el tiempo de inactividad.

Puede restaurar datos a una LUN asignada en línea. Sin embargo, las aplicaciones host no pueden acceder a esta LUN hasta que se complete la operación de restauración. Una vez finalizada la operación de restauración, la caché del host de los datos de LUN se debe vaciar para ofrecer coherencia con los datos restaurados.

El motor de descarga puede recuperar los siguientes datos:

- Contenido de los archivos y directorios
- Permisos de archivos UNIX
- ACL

  Si restaura un archivo que solo tiene permisos de archivo UNIX a un qtree o volumen NTFS, el archivo no tiene ACL de Windows NT. El sistema de almacenamiento utiliza sólo los permisos de archivo UNIX en este archivo hasta que se crea una ACL de Windows NT en él.

  > Si restaura ACL respaldados de sistemas de almacenamiento que ejecutan Data ONTAP 8.2 a sistemas de almacenamiento que ejecutan Data ONTAP 8.1.x y versiones anteriores que tienen un límite de ACE inferior a 1,024, se restaura una ACL predeterminada.

- Información de Qtree

  La información de qtree se utiliza solo si un qtree se restaura en la raíz de un volumen. La información de qtree no se utiliza si un qtree se restaura a un directorio inferior, como `/vs1/vol1/subdir/lowerdir`, y deja de ser un qtree.

- Todos los demás atributos de archivo y directorio
- Secuencias de Windows NT
- LUN
  - Es necesario restaurar una LUN a nivel de volumen o un nivel de qtree para que permanezca como una LUN.

    Si se restaura a un directorio, se restaura como un archivo porque no contiene metadatos válidos.

    - Un LUN de 7-Mode se restaura como LUN en un volumen ONTAP.
- Un volumen de 7-Mode se puede restaurar en un volumen de ONTAP.
- Los archivos alineados con máquinas virtuales restaurados en un volumen de destino heredan las propiedades de alineación de máquinas virtuales del volumen de destino.
- El volumen de destino de una operación de restauración puede tener archivos con bloqueos obligatorios o de asesoramiento.

  Mientras se realiza una operación de restauración en dicho volumen de destino, el motor de volcado ignora estos bloqueos.

Consideraciones que tener en cuenta antes de restaurar datos

Puede restaurar los datos de los que se ha realizado una copia de seguridad en su ruta original o en otro destino. Si va a restaurar datos con un backup en otro destino, debe preparar el destino para la operación de restauración.

Antes de restaurar datos en su ruta original o en un destino diferente, debe disponer de la siguiente información y cumplir los requisitos siguientes:

- El nivel de la restauración
- La ruta a la que se van a restaurar los datos
- El factor de bloqueo utilizado durante el backup
- Si realiza una restauración incremental, todas las cintas deben estar en la cadena de backup
- Una unidad de cinta disponible y compatible con la cinta a restaurar

Antes de restaurar los datos en otro destino, debe ejecutar las operaciones siguientes:

- Si va a restaurar un volumen, debe crear un volumen nuevo.
- Si va a restaurar un qtree o un directorio, debe cambiar el nombre de los archivos que probablemente tengan los mismos nombres que los archivos que va a restaurar.

> En ONTAP 9, los nombres de qtree admiten el formato Unicode. Las versiones anteriores de ONTAP no admiten este formato. Si un qtree con nombres Unicode en ONTAP 9 se copia en una versión anterior de ONTAP mediante `ndmpcopy` O mediante la restauración desde una imagen de copia de seguridad en una cinta, el qtree se restaura como un directorio normal y no como un qtree con formato Unicode.

> Si un archivo restaurado tiene el mismo nombre que un archivo existente, el archivo existente se sobrescribe con el archivo restaurado. Sin embargo, los directorios no se sobrescriben.

Para cambiar el nombre de un archivo, directorio o qtree durante la restauración sin usar DAR, debe configurar la variable de entorno DE EXTRACCIÓN en `E`.

Espacio requerido en el sistema de almacenamiento de destino

Necesita aproximadamente 100 MB de espacio en el sistema de almacenamiento de destino que la cantidad de datos que se van a restaurar.

La operación de restauración comprueba la disponibilidad de espacio de los volúmenes y de nodos de información en el volumen de destino cuando se inicia la operación de restauración. Establecer la variable de entorno FORCE a. `Y` hace que la operación de restauración omita las comprobaciones del espacio del volumen y de la disponibilidad de nodos de información en la ruta de destino. Si no hay suficiente espacio o inodos disponibles en el volumen de destino, la operación de restauración recupera la cantidad de datos permitidos por el espacio del volumen de destino y la disponibilidad del inodo. La operación de restauración se detiene cuando no queda más espacio del volumen o inodos.

Límites de escalabilidad para sesiones de backup y restauración de volcado

Es necesario conocer la cantidad máxima de sesiones de backup y restauración de volcado que se pueden ejecutar simultáneamente en sistemas de almacenamiento de diferentes capacidades de memoria del sistema. Este número máximo depende de la memoria del sistema de un sistema de almacenamiento.

Los límites mencionados en la tabla siguiente son para el motor de descarga o restauración. Los límites mencionados en los límites de escalabilidad para las sesiones NDMP son para el servidor NDMP, que son más altos que los límites del motor.

Memoria del sistema de un sistema de almacenamiento	Cantidad total de sesiones de backup y restauración de volcado
Menos de 16 GB	4
Mayor o igual que 16 GB pero menor que 24 GB	16
Mayor o igual que 24 GB	32

Si utiliza `ndmpcopy` Comando para copiar datos dentro de los sistemas de almacenamiento, se establecen dos sesiones NDMP, una para backup de volcado y la otra para restauración de volcado.

Puede obtener la memoria del sistema del sistema de almacenamiento mediante el `sysconfig -a` comando (disponible a través del nodeshell). Para obtener más información acerca de cómo utilizar este comando, consulte las páginas man.

Información relacionada

Límites de escalabilidad para sesiones NDMP

Compatibilidad con backup y restauración a cinta entre Data ONTAP operando en 7-Mode y ONTAP

Es posible restaurar datos de los que se ha realizado un backup desde un sistema de almacenamiento operativo en 7-Mode o donde se ejecuta ONTAP en un sistema de almacenamiento que funciona en 7-Mode o en ONTAP.

Las siguientes operaciones de backup y restauración de cinta son compatibles entre Data ONTAP en 7-Mode y ONTAP:

- Realizar un backup de un volumen de 7-Mode a una unidad de cinta conectada a un sistema de almacenamiento que ejecuta ONTAP
- Realizar backups de un volumen de ONTAP en una unidad de cinta conectada a un sistema 7-Mode
- Restaurar los datos con backup de un volumen de 7-Mode a partir de una unidad de cinta conectada a un sistema de almacenamiento que ejecuta ONTAP
- Restaurar datos con backup de un volumen ONTAP a partir de una unidad de cinta conectada a un sistema 7-Mode
- Restaurar un volumen de 7-Mode en un volumen de ONTAP

```
-   A 7-Mode LUN is restored as a LUN on an ONTAP volume.
-   You should retain the ONTAP LUN identifiers when
restoring a 7-Mode LUN to an existing ONTAP LUN.
```

- Restaurar un volumen ONTAP en un volumen de 7-Mode

Un LUN de ONTAP se restaura como un archivo normal en un volumen de 7-Mode.

Eliminar contextos reiniciables

Si desea iniciar un backup en lugar de reiniciar un contexto, puede eliminar el contexto.

Acerca de esta tarea

Puede eliminar un contexto reiniciable mediante el `vserver services ndmp restartable-backup delete` Para proporcionar el nombre de SVM y el ID de contexto.

Pasos

1. Eliminar un contexto reiniciable:

   `vserver services ndmp restartable-backup delete -vserver` *`vserver-name`* `-context -id` *`context_identifier`*.

```
cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                   Is Cleanup Pending?
----------- ------------------------------------ -------------------
vserver1    330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1    481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2    5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>
cluster::> vserver services ndmp restartable-backup delete -vserver
vserver1 -context-id 481025c1-0179-11e6-a299-005056bb4bc9

cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                   Is Cleanup Pending?
----------- ------------------------------------ -------------------
vserver1    330e6739-0179-11e6-a299-005056bb4bc9 false
vserver2    5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>"
```

Cómo funciona el volcado en un volumen secundario de SnapVault

Es posible realizar operaciones de backup a cinta en datos que estén reflejados en el volumen secundario de SnapVault. Puede realizar un backup únicamente de los datos que se reflejan en el volumen secundario de SnapVault a cinta, y no los metadatos de la relación de SnapVault.

Cuando se rompe la relación de reflejo de protección de datos (`snapmirror break`) O cuando se produce una resincronización de SnapMirror, siempre es necesario ejecutar un backup básico.

Cómo funciona el volcado con la recuperación tras fallos del almacenamiento y las operaciones ARL

Antes de ejecutar operaciones de backup de volcado o restauración, debe comprender cómo funcionan estas operaciones con las operaciones de conmutación por error (toma de control y devolución) de almacenamiento o reubicación de agregados (ARL). La `-override-vetoes` Option determina el comportamiento de un motor de volcado durante una operación de ARL o una conmutación por error del almacenamiento.

Cuando se ejecuta una operación de volcado de backup o restauración, y la `-override-vetoes` opción establecida en `false`, Se detiene una operación ARL o una recuperación tras fallos de almacenamiento iniciada por el usuario. Sin embargo, si la `-override-vetoes` opción establecida en `true`, La operación de recuperación tras fallos de almacenamiento o ARL continúa y se cancela la operación de copia de seguridad o restauración de volcado. Cuando el sistema de almacenamiento inicia automáticamente una conmutación por error o una operación de ARL del almacenamiento, siempre se cancela una operación de backup o restauración de volcado activa. No es posible reiniciar las operaciones de volcado de backup y restauración

incluso después de la conmutación por error de almacenamiento o de la finalización de las operaciones de ARL.

Operaciones de descarga cuando se admite la extensión DE LA CABINA

Si la aplicación de backup admite la extensión CAB, puede seguir realizando operaciones de backup de volcado y restauración incrementales sin tener que volver a configurar las políticas de backup tras una conmutación por error del almacenamiento o una operación ARL.

Operaciones de volcado cuando la extensión DE LA CABINA no es compatible

Si la aplicación de backup no admite la extensión CAB, puede seguir realizando operaciones de backup y restauración de volcado incrementales si migra la LIF configurada en la política de backup al nodo que aloja el agregado de destino. De lo contrario, una vez realizada la conmutación por error del almacenamiento y la operación ARL, debe realizar un backup básico antes de realizar la operación de backup incremental.

> Para las operaciones de recuperación tras fallos de almacenamiento, el LIF configurado en la política de backup se debe migrar al nodo compañero.

Información relacionada

"Conceptos de ONTAP"

"Alta disponibilidad"

Cómo funciona el volcado con el movimiento de volúmenes

El sistema de almacenamiento puede ejecutar en paralelo las operaciones de backup y restauración de cinta y el movimiento de volúmenes hasta que el sistema de almacenamiento intente la fase final de transposición. Una vez completada esta fase, no se permiten nuevas operaciones de backup y restauración en cinta en el volumen que se mueve. No obstante, las operaciones actuales siguen en ejecución hasta que se complete.

En la siguiente tabla se describe el comportamiento de las operaciones de backup a cinta y restauración después de la operación de movimiento de volúmenes:

Si realiza operaciones de backup y restauración en cinta en…	Realice lo siguiente…
La aplicación de backup admite la extensión CAB del modo NDMP de las máquinas virtuales de almacenamiento (SVM)	Puede seguir realizando operaciones incrementales de backup a cinta y restauración en volúmenes de lectura/escritura y solo lectura sin tener que reconfigurar las políticas de backup.

Si realiza operaciones de backup y restauración en cinta en…	Realice lo siguiente…
El modo NDMP con ámbito SVM cuando la aplicación de backup no admite la extensión CAB	Puede seguir realizando operaciones incrementales de backup a cinta y restauración en volúmenes de lectura/escritura y solo lectura si migra la LIF configurada en la política de backup al nodo que aloja el agregado de destino. De lo contrario, después del movimiento de volumen, debe ejecutar un backup básico antes de ejecutar la operación de backup incremental.

Cuando se produce un movimiento de volúmenes, si el volumen que pertenece a una SVM diferente del nodo de destino tiene el mismo nombre que el del volumen movido, no se pueden ejecutar operaciones de backup incrementales del volumen movido.

Información relacionada

"Conceptos de ONTAP"

Cómo funciona el volcado cuando un volumen FlexVol está lleno

Antes de realizar una operación de backup de volcado incremental, debe asegurarse de que haya suficiente espacio libre en el volumen FlexVol.

Si se produce un error en la operación, debe aumentar el espacio libre en el volumen FlexVol aumentando su tamaño o eliminando las copias de Snapshot. A continuación, vuelva a realizar la operación de copia de seguridad incremental.

Cómo funciona el volcado cuando cambia el tipo de acceso de volúmenes

Cuando un volumen de destino de SnapMirror o un volumen secundario de SnapVault cambian el estado de lectura/escritura a solo lectura o de solo lectura a lectura/escritura, se debe ejecutar una operación de backup o restauración de cinta de referencia.

Los volúmenes secundarios de destino de SnapMirror y SnapVault son volúmenes de solo lectura. Si realiza operaciones de backup y restauración de cinta en dichos volúmenes, se debe ejecutar una operación de backup o restauración de línea base siempre que el volumen cambie el estado de solo lectura a lectura/escritura o de lectura/escritura a solo lectura.

Información relacionada

"Conceptos de ONTAP"

Cómo funciona el volcado con la restauración de archivos únicos o LUN de SnapMirror

Antes de realizar operaciones de volcado de backup o restauración en un volumen en el que se restaura un solo archivo o LUN mediante la tecnología SnapMirror, debe entender cómo funcionan las operaciones de volcado con una sola operación de restauración de archivos o LUN.

Durante una operación de restauración de un único archivo o LUN de SnapMirror, las I/o del cliente están

restringidas en el archivo o LUN que se van a restaurar. Cuando la operación de restauración de archivos o LUN individuales finaliza, se elimina la restricción de I/o del archivo o LUN. Si se realiza un backup de volcado en un volumen para el que se restaura un solo archivo o LUN, el archivo o el LUN que tiene restricción de I/o del cliente no se incluye en el backup de volcado. En una operación de copia de seguridad posterior, se realiza una copia de seguridad de este archivo o LUN en cinta después de eliminar la restricción de E/S.

No se puede realizar una restauración de volcado y una operación de restauración de archivos o LUN de SnapMirror simultáneamente en el mismo volumen.

Cómo las operaciones de volcado de backup y restauración se ven afectadas por las configuraciones de MetroCluster

Antes de llevar a cabo operaciones de backup de volcado y restauración en una configuración de MetroCluster, debe comprender cómo se ven afectadas las operaciones de volcado cuando se produzca una operación de conmutación de sitios o conmutación de estado.

Operación de copia de seguridad o restauración de volcado seguida de la conmutación

Considere dos clústeres: El clúster 1 y el clúster 2. Durante una operación de backup de volcado o restauración en el clúster 1, si se inicia una conmutación por error desde el clúster 1 al clúster 2, se produce lo siguiente:

- Si el valor de `override-vetoes` la opción es `false`, a continuación, se cancela la operación de switchover y continúa la operación de copia de seguridad o restauración.
- Si el valor de la opción es `true`, la operación de copia de seguridad de volcado o restauración se cancela y la operación de switchover continúa.

Operación de copia de seguridad o restauración de volcado seguida de una conmutación de estado

Una conmutación de sitios se realiza desde el clúster 1 al clúster 2 y se inicia una operación de backup de volcado o restauración en el clúster 2. La operación de volcado realiza un backup o restaura un volumen ubicado en el clúster 2. En este punto, si se inicia una conmutación de estado del clúster 2 al clúster 1, sucede lo siguiente:

- Si el valor de `override-vetoes` la opción es `false`, a continuación, la conmutación de regreso se cancela y la operación de copia de seguridad o restauración continúa.
- Si el valor de la opción es `true`, a continuación, la operación de copia de seguridad o restauración se cancela y la conmutación de regreso continúa.

La operación de backup o restauración de volcado se inició durante una conmutación de sitios o una conmutación de estado

Durante una conmutación de sitios del clúster 1 al clúster 2, si se inicia una operación de backup de volcado o restauración en el clúster 1, las operaciones de backup o restauración fallan y la conmutación continúa.

Durante una conmutación de estado del clúster 2 al clúster 1, si se inicia una operación de backup o restauración de volcado desde el clúster 2, la operación de backup o restauración dará error y esta continuará.

Acerca del motor SMTape para volúmenes de FlexVol

Acerca del motor SMTape para volúmenes de FlexVol

SMTape es una solución de recuperación ante desastres de ONTAP que realiza backup de bloques de datos a cinta. Puede usar SMTape para realizar backups de volúmenes a las cintas. Sin embargo, no puede realizar un backup en el nivel qtree o subárbol. SMTape admite copias de seguridad de línea base, diferenciales e incrementales. SMTape no requiere una licencia.

Puede realizar una operación de backup y restauración de SMTape mediante una aplicación de backup compatible con NDMP. Puede elegir SMTape para realizar operaciones de backup y restauración solo en el modo de NDMP de las máquinas virtuales de almacenamiento (SVM) con ámbito.

> No se admite el proceso de reversión cuando hay una sesión de copia de seguridad o restauración de SMTape en curso. Debe esperar hasta que finalice la sesión o debe anular la sesión NDMP.

Con SMTape, puede realizar backups de 255 copias Snapshot. Para obtener backups completos, incrementales o diferenciales posteriores, debe eliminar las copias Snapshot con backup más antiguas.

Antes de ejecutar una restauración básica, debe ser del tipo el volumen al que se van a restaurar los datos `DP` y este volumen debe estar en estado restringido. Después de una restauración correcta, este volumen está en línea automáticamente. Se pueden realizar restauraciones posteriores incrementales o diferenciales en este volumen en el orden en que se ejecutaron los backups.

Use las copias Snapshot durante el backup de SMTape

Debe comprender cómo se utilizan las copias Snapshot durante un backup básico de SMTape y un backup incremental. También hay que tener en cuenta al realizar un backup con SMTape.

Backup de línea de base

Al realizar un backup de referencia, es posible especificar el nombre de la copia Snapshot de la que se realizará un backup en cinta. Si no se especifica ninguna copia Snapshot, según el tipo de acceso del volumen (lectura/escritura o solo lectura), se crea automáticamente una copia Snapshot o se utilizan copias Snapshot existentes. Cuando especifica una copia Snapshot para el backup, también se realiza un backup en cinta de todas las copias Snapshot más antiguas de la copia Snapshot especificada.

Si no se especifica una copia Snapshot para el backup, ocurre lo siguiente:

- En el caso de un volumen de lectura/escritura, se crea automáticamente una copia Snapshot.

  La copia Snapshot recién creada y se realiza un backup en cinta de todas las copias Snapshot más antiguas.

- Para un volumen de solo lectura, todas las copias Snapshot, incluida la última copia de Snapshot, se copian en cinta.

  No se realiza un backup de ninguna copia Snapshot nueva creada después de comenzar el backup.

Backup incremental

Para las operaciones de backup incremental o diferencial de SMTape, las aplicaciones de backup compatibles con NDMP crean y gestionan las copias Snapshot.

Siempre debe especificar una copia de Snapshot mientras realiza una operación de backup incremental. Para que la operación de backup incremental se realice correctamente, la copia de Snapshot de la que se realizó un backup durante la operación de backup anterior (de referencia o incremental) debe estar en el volumen a partir del cual se ejecutó el backup. Para garantizar que usa esta copia Snapshot con backup, debe tener en cuenta la política de Snapshot asignada en este volumen al configurar la política de backup.

Consideraciones sobre backups de SMTape en destinos de SnapMirror

- Una relación de mirroring de protección de datos crea copias Snapshot temporales en el volumen de destino para la replicación.

  No debe usar estas copias Snapshot para backup de SMTape.

- Si se produce una actualización de SnapMirror en un volumen de destino en una relación de reflejo de protección de datos durante una operación de backup de SMTape en el mismo volumen, la copia de Snapshot de la que SMTape se realiza el backup no debe eliminarse en el volumen de origen.

  Durante la operación de backup, SMTape bloquea la copia Snapshot en el volumen de destino y si se elimina la copia de Snapshot correspondiente en el volumen de origen, se producirá un error en la operación de actualización de SnapMirror posterior.

- No debe utilizar estas copias Snapshot durante un backup incremental.

Capacidades SMTape

Las funcionalidades de SMTape como el backup de copias Snapshot, backups incrementales y diferenciales, la conservación de las funciones de deduplicación y compresión en volúmenes restaurados y de propagación en cinta ayudan a optimizar las operaciones de backup y restauración en cinta.

SMTape ofrece las siguientes capacidades:

- Ofrece una solución de recuperación tras siniestros
- Permite backups incrementales y diferenciales
- Realiza un backup de copias Snapshot
- Permite realizar backups y restauraciones de volúmenes deduplicados y mantiene la deduplicación en los volúmenes restaurados
- Realiza backups de volúmenes comprimidos y mantiene la compresión en los volúmenes restaurados
- Permite siembra de cintas

SMTape admite el factor de bloqueo en múltiplos de 4 KB, dentro del intervalo de 4 KB a 256 KB.

> Es posible restaurar datos en volúmenes creados solo en dos versiones principales consecutivas de ONTAP.

Funciones no admitidas en SMTape

SMTape no admite backups reiniciables ni la verificación de archivos con backup.

Límites de escalabilidad para las sesiones de backup y restauración de SMTape

Al ejecutar operaciones de backup y restauración de SMTape mediante NDMP o interfaz de línea de comandos (propagación de cintas), debe tener en cuenta la cantidad máxima de sesiones de backup y restauración de SMTape que pueden realizarse de manera simultánea en sistemas de almacenamiento con diferentes capacidades de memoria del sistema. Este número máximo depende de la memoria del sistema de un sistema de almacenamiento.

> Los límites de escalabilidad de las sesiones de backup y restauración de SMTape son diferentes de los límites de sesiones de NDMP y los límites de sesiones de volcado.

Memoria del sistema de almacenamiento	Cantidad total de sesiones de backup y restauración de SMTape
Menos de 16 GB	6
Mayor o igual que 16 GB pero menor que 24 GB	16
Mayor o igual que 24 GB	32

Puede obtener la memoria del sistema del sistema de almacenamiento mediante el `sysconfig -a` comando (disponible a través del nodeshell). Para obtener más información acerca de cómo utilizar este comando, consulte las páginas man.

Información relacionada

Límites de escalabilidad para sesiones NDMP

Límites de escalabilidad para sesiones de backup y restauración de volcado

Qué es la siembra de cintas

La propagación de cintas es una funcionalidad SMTape que ayuda a inicializar un volumen de FlexVol de destino en una relación de mirroring de protección de datos.

La propagación de cintas permite establecer una relación de mirroring para la protección de datos entre un sistema de origen y un sistema de destino a través de una conexión de ancho de banda bajo.

El mirroring incremental de las copias Snapshot del origen al destino es factible gracias a una conexión de ancho de banda bajo. Sin embargo, un mirroring inicial de la copia Snapshot base demora mucho tiempo en una conexión de ancho de banda bajo. En estos casos, se puede realizar un backup de SMTape del volumen de origen a una cinta y usar la cinta para transferir la copia Snapshot básica inicial al destino. A continuación, puede configurar las actualizaciones incrementales de SnapMirror en el sistema de destino mediante la conexión con un ancho de banda bajo.

Información relacionada

"Conceptos de ONTAP"

Funcionamiento de SMTape con la recuperación tras fallos de almacenamiento y las operaciones de ARL

Antes de ejecutar operaciones de backup o restauración de SMTape, debe comprender cómo funcionan estas operaciones con la operación de conmutación al nodo de respaldo (toma de control y retorno al nodo primario) de almacenamiento o la operación de reubicación de agregados (ARL). La `-override-vetoes` Option determina el comportamiento del motor de SMTape durante una recuperación tras fallos de almacenamiento o una operación de ARL.

Cuando se ejecuta una operación de backup o restauración de SMTape y la `-override-vetoes` opción establecida en `false`, Se detiene una operación de ARL o una conmutación por error del almacenamiento iniciada por el usuario y se completa la operación de copia de seguridad o restauración. Si la aplicación de backup admite la extensión CAB, puede seguir realizando operaciones incrementales de backup y restauración de datos SMTape sin tener que reconfigurar las políticas de backup. Sin embargo, si la `-override-vetoes` opción establecida en `true`, La operación de recuperación tras fallos de almacenamiento o ARL continúa y se anula la operación de copia de seguridad o restauración de SMTape.

Información relacionada

"Gestión de redes"

"Alta disponibilidad"

Funcionamiento de SMTape con el movimiento de volúmenes

Las operaciones de backup de SMTape y las operaciones de movimiento de volúmenes se pueden ejecutar en paralelo hasta que el sistema de almacenamiento intente la fase final de la transición. Una vez pasada esta fase, no se pueden ejecutar nuevas operaciones de backup de SMTape en el volumen que se va a mover. No obstante, las operaciones actuales siguen en ejecución hasta que se complete.

Antes de iniciar la fase de transición de un volumen, la operación de movimiento de volúmenes comprueba las operaciones de backup de SMTape activas en el mismo volumen. Si hay operaciones de backup de SMTape activas, la operación de movimiento de volúmenes pasa al estado de transposición diferida y permite que se completen las operaciones de backup de SMTape. Una vez completadas estas operaciones de backup, debe reiniciar manualmente la operación de movimiento de volúmenes.

Si la aplicación de backup admite la extensión CAB, puede seguir realizando operaciones incrementales de backup y restauración de cinta en volúmenes de lectura/escritura y solo lectura sin tener que reconfigurar las políticas de backup.

No se pueden ejecutar las operaciones de restauración básica y movimiento de volúmenes de forma simultánea; sin embargo, la restauración incremental puede ejecutarse en paralelo con las operaciones de movimiento de volúmenes, con un comportamiento similar al de las operaciones de backup de SMTape durante las operaciones de movimiento de volúmenes.

Información relacionada

"Conceptos de ONTAP"

Cómo funciona SMTape con las operaciones de realojamiento de volúmenes

No se pueden iniciar las operaciones de SMTape cuando hay una operación de realojamiento de volumen en curso en un volumen. Cuando un volumen está implicado en una operación de realojamiento de volúmenes, no debe iniciarse la sesión de SMTape en ese volumen.

Si hay alguna operación de rehost de volumen en curso, se produce un error en el backup o la restauración de SMTape. Si hay un backup o una restauración de SMTape en curso, se producirá un error en las operaciones de rehost de volúmenes con el mensaje de error correspondiente. Esta condición se aplica tanto a las operaciones de backup o restauración basadas en NDMP como a las basadas en CLI.

Cómo se ve afectada la política de backup NDMP durante el Bad

Cuando se habilita el equilibrador automático de datos (ADB), el equilibrador analiza las estadísticas de uso de agregados para identificar el agregado que ha superado el porcentaje de uso de umbral alto configurado.

Tras identificar el agregado que ha superado el umbral, el equilibrador identifica un volumen que se puede mover a agregados que residen en otro nodo del clúster e intenta mover dicho volumen. Esta situación afecta a la política de backup configurada para este volumen porque si la aplicación de gestión de datos (DMA) no tiene en CUENTA LA CABINA, el usuario debe volver a configurar la política de backup y ejecutar la operación de backup de referencia.

> Si el DMA es compatible CON CAB y la política de respaldo se ha configurado utilizando una interfaz específica, el ADB no se ve afectado.

Cómo se ven afectadas las operaciones de backup y restauración de SMTape en las configuraciones de MetroCluster

Antes de ejecutar operaciones de backup y restauración de SMTape en una configuración de MetroCluster, debe comprender cómo se ven afectadas las operaciones de SMTape cuando se produce una operación de conmutación de sitios o conmutación de estado.

Operación de backup o restauración de SMTape seguida de una conmutación

Considere dos clústeres: El clúster 1 y el clúster 2. Durante una operación de backup o restauración de SMTape en el clúster 1, si se inicia una conmutación entre el clúster 1 y el clúster 2, se produce lo siguiente:

- Si el valor de `-override-vetoes` la opción es `false`, a continuación, el proceso de switchover se cancela y la operación de copia de seguridad o restauración continúa.
- Si el valor de la opción es `true`, La operación de copia de seguridad o restauración de SMTape se cancela y el proceso de cambio continúa.

Operación de copia de seguridad o restauración de SMTape seguida de una conmutación de estado

Se realiza una conmutación de sitios desde el clúster 1 al clúster 2 y se inicia una operación de backup o restauración de SMTape en el clúster 2. La operación SMTape realiza backups o restaura un volumen ubicado en el clúster 2. En este punto, si se inicia una conmutación de estado del clúster 2 al clúster 1, sucede lo siguiente:

- Si el valor de `-override-vetoes` la opción es `false`, a continuación, el proceso de regreso se cancela y la operación de copia de seguridad o restauración continúa.
- Si el valor de la opción es `true`, la operación de copia de seguridad o restauración se cancela y el proceso de regreso continúa.

La operación de backup o restauración de SMTape se inició durante una conmutación de sitios o conmutación de estado

Durante un proceso de conmutación de sitios del clúster 1 al clúster 2, si se inicia una operación de backup o restauración de SMTape en el clúster 1, la operación de backup o restauración falla y la conmutación continúa.

Durante un proceso de conmutación de estado del clúster 2 al clúster 1, si se inicia una operación de backup o restauración SMTape desde el clúster 2, la operación de backup o restauración falla y la conmutación de estado continúa.

Supervisar las operaciones de backup y restauración a cinta para volúmenes de FlexVol

Supervisar la información general sobre las operaciones de backup y restauración a cinta para volúmenes de FlexVol

Es posible ver los archivos de registro de eventos para supervisar las operaciones de backup a cinta y restauración. ONTAP registra automáticamente los eventos de backup y restauración importantes, así como el momento en que se producen en un archivo de registro denominado `backup` en las controladoras `/etc/log/` directorio. De forma predeterminada, el registro de eventos está establecido en `on`.

Es posible que desee ver los archivos de registro de eventos por los siguientes motivos:

- Comprobar si un backup nocturno se ha realizado correctamente
- Recopilación de estadísticas sobre operaciones de backup
- Para usar la información de los archivos de registro de eventos anteriores con el fin de ayudar a diagnosticar problemas con las operaciones de backup y restauración

Una vez cada semana, los archivos de registro de eventos se rotan. La `/etc/log/backup` se cambia el nombre del archivo a. `/etc/log/backup.0`, la `/etc/log/backup.0` se cambia el nombre del archivo a. `/etc/log/backup.1`, y así sucesivamente. El sistema guarda los archivos de registro durante un máximo de seis semanas; por lo tanto, puede tener hasta siete archivos de mensaje (`/etc/log/backup.[0-5]` y la corriente `/etc/log/backup` archivo).

Acceda a los archivos de registro de eventos

Es posible acceder a los archivos de registro de eventos para las operaciones de backup a cinta y restauración en la `/etc/log/` mediante el directorio `rdfile` orden en el nodesinfierno. Es posible ver estos archivos de registro de eventos para supervisar las operaciones de backup a cinta y restauración.

Acerca de esta tarea

Con configuraciones adicionales, como una función de control de acceso con acceso al `spi` servicio web o una cuenta de usuario configurada con `http` método de acceso, también puede utilizar un explorador web

para acceder a estos archivos de registro.

Pasos

1. Para acceder a nodeshell, introduzca el siguiente comando:

   `node run -node node_name`

   `node_name` es el nombre del nodo.

2. Para acceder a los archivos del registro de eventos para las operaciones de backup a cinta y restauración, escriba el siguiente comando:

   `rdfile /etc/log/backup`

Información relacionada

"Administración del sistema"

"Conceptos de ONTAP"

Qué es el formato de mensaje de volcado y restauración del registro de eventos

Información general sobre el formato del mensaje de registro de eventos de volcado y restauración

Para cada evento de volcado y restauración, se escribe un mensaje en el archivo de registro de copia de seguridad.

El formato del mensaje de volcado y restauración del registro de eventos es el siguiente:

`type timestamp identifier event (event_info)`

En la lista siguiente se describen los campos en el formato de mensaje del registro de eventos:

- Cada mensaje de registro comienza con uno de los indicadores de tipo descritos en la siguiente tabla:

Tipo	Descripción
registro	Evento de registro
dmp	Evento de volcado
rst	Evento de restauración

- `timestamp` muestra la fecha y la hora del evento.
- La `identifier` El campo de un evento de volcado incluye la ruta de volcado y el ID exclusivo del volcado. La `identifier` el campo de un evento de restauración solo utiliza el nombre de ruta de destino de restauración como identificador único. Los mensajes de eventos relacionados con el registro no incluyen un `identifier` campo.

Qué son los eventos de registro

El campo de evento de un mensaje que comienza con un registro especifica el comienzo de un registro o el final de un registro.

Contiene uno de los eventos que se muestran en la siguiente tabla:

Evento	Descripción
Inicio_registro	Indica el comienzo del registro o que el registro se ha vuelto a activar después de estar desactivado.
Stop_Logging	Indica que se ha desactivado el registro.

¿Qué eventos de volcado son

El campo de evento de un evento de volcado contiene un tipo de evento seguido de información específica del evento entre paréntesis.

En la siguiente tabla se describen los eventos, sus descripciones y la información de eventos relacionada que puede registrarse para una operación de volcado:

Evento	Descripción	Información del evento
Comenzar	Se ha iniciado el volcado NDMP	Nivel de descarga y tipo de volcado
Fin	Volcados completados correctamente	Cantidad de datos procesados
Anular	Se cancela la operación	Cantidad de datos procesados
Opciones	Se muestran las opciones especificadas	Todas las opciones y sus valores asociados, incluidas las opciones NDMP
Tape_open	La cinta está abierta para lectura y escritura	Nombre del nuevo dispositivo de cinta
Tape_close	La cinta se cierra para lectura/escritura	El nombre del dispositivo de cinta
Cambio de fase	Un volcado está entrando en una nueva fase de procesamiento	El nombre de la nueva fase
Error	Un volcado ha encontrado un evento inesperado	Mensaje de error
Snapshot	Se crea o se encuentra una copia Snapshot	El nombre y la hora de la copia Snapshot

Evento	Descripción	Información del evento
Volcado_base	Se ha localizado una entrada de volcado base en el metarchivo interno	El nivel y la hora del volcado base (sólo para volcados incrementales)

Qué eventos de restauración son

El campo de evento de restauración contiene un tipo de evento seguido de información específica del evento entre paréntesis.

En la siguiente tabla, se proporciona información sobre los eventos, sus descripciones y la información de eventos relacionada que se puede registrar para una operación de restauración:

Evento	Descripción	Información del evento
Comenzar	Se ha iniciado la restauración NDMP	Nivel de restauración y tipo de restauración
Fin	Las restauraciones se completaron correctamente	Número de archivos y cantidad de datos procesados
Anular	Se cancela la operación	Número de archivos y cantidad de datos procesados
Opciones	Se muestran las opciones especificadas	Todas las opciones y sus valores asociados, incluidas las opciones NDMP
Tape_open	La cinta está abierta para lectura y escritura	Nombre del nuevo dispositivo de cinta
Tape_close	La cinta se cierra para lectura/escritura	El nombre del dispositivo de cinta
Cambio de fase	Restore está entrando en una nueva fase de procesamiento	El nombre de la nueva fase
Error	La restauración encuentra un evento inesperado	Mensaje de error

Habilitar o deshabilitar el registro de eventos

Puede activar o desactivar el registro de eventos.

Pasos

1. Para habilitar o deshabilitar el registro de eventos, introduzca el siguiente comando en el clustershell:

```
options -option_name backup.log.enable -option-value {on | off}
```

`on` activa el inicio de sesión de eventos.

`off` desactiva la sesión de eventos.

> El registro de eventos está activado de forma predeterminada.

Mensajes de error para backup y restauración a cinta de volúmenes de FlexVol

Mensajes de error de copia de seguridad y restauración

Limitación de recursos: No hay ningún subproceso disponible

- **Mensaje**

  ```
  Resource limitation: no available thread
  ```

- **Causa**

  El número máximo de subprocesos de E/S de cinta local activos está actualmente en uso. Puede tener un máximo de 16 unidades de cinta locales activas.

- **Acción Correctiva**

  Espere a que finalicen algunos trabajos de cinta antes de iniciar una nueva tarea de copia de seguridad o restauración.

Reserva de cintas prehecha

- **Mensaje**

  ```
  Tape reservation preempted
  ```

- **Causa**

  La unidad de cinta está en uso por otra operación o la cinta se ha cerrado prematuramente.

- **Acción Correctiva**

  Asegúrese de que la unidad de cinta no esté en uso en otra operación y de que la aplicación DMA no haya cancelado el trabajo y vuelva a intentarlo.

No se pudo inicializar el medio

- **Mensaje**

  ```
  Could not initialize media
  ```

- **Causa**

  Puede obtener este error por uno de los siguientes motivos:

  - La unidad de cinta utilizada para la copia de seguridad está dañada o dañada.

- La cinta no contiene la copia de seguridad completa o está dañada.
- El número máximo de subprocesos de E/S de cinta local activos está actualmente en uso.

  Puede tener un máximo de 16 unidades de cinta locales activas.

- **Acción Correctiva**
  - Si la unidad de cinta está dañada o dañada, vuelva a intentar la operación con una unidad de cinta válida.
  - Si la cinta no contiene la copia de seguridad completa o está dañada, no podrá realizar la operación de restauración.
  - Si no hay recursos de cinta disponibles, espere a que finalicen algunos de los trabajos de backup o restauración y vuelva a intentar la operación.

Número máximo de volcados o restauraciones permitidos (límite máximo de sesión) en curso

- **Mensaje**

  `Maximum number of allowed dumps or restores` *`(maximum session limit)`* `in progress`

- **Causa**

  Ya se está ejecutando la cantidad máxima de trabajos de backup o restauración.

- **Acción Correctiva**

  Vuelva a intentar la operación después de que finalicen algunos de los trabajos en ejecución actualmente.

Error de soporte al escribir la cinta

- **Mensaje**

  `Media error on tape write`

- **Causa**

  La cinta utilizada para la copia de seguridad está dañada.

- **Acción Correctiva**

  Sustituya la cinta y vuelva a intentar la tarea de copia de seguridad.

Error al escribir en la cinta

- **Mensaje**

  `Tape write failed`

- **Causa**

  La cinta utilizada para la copia de seguridad está dañada.

- **Acción Correctiva**

  Sustituya la cinta y vuelva a intentar la tarea de copia de seguridad.

Error al escribir la cinta: La nueva cinta encontró un error de soporte

- **Mensaje**

  ```
  Tape write failed - new tape encountered media error
  ```

- **Causa**

  La cinta utilizada para la copia de seguridad está dañada.

- **Acción Correctiva**

  Sustituir la cinta y volver a intentar la copia de seguridad.

Error al escribir en la cinta: La nueva cinta está rota o está protegida contra escritura

- **Mensaje**

  ```
  Tape write failed - new tape is broken or write protected
  ```

- **Causa**

  La cinta utilizada para el backup está dañada o protegida contra escritura.

- **Acción Correctiva**

  Sustituir la cinta y volver a intentar la copia de seguridad.

Error al escribir en cinta: La nueva cinta ya está al final del soporte

- **Mensaje**

  ```
  Tape write failed - new tape is already at the end of media
  ```

- **Causa**

  No hay suficiente espacio en la cinta para completar la copia de seguridad.

- **Acción Correctiva**

  Sustituir la cinta y volver a intentar la copia de seguridad.

Error de escritura de cinta

- **Mensaje**

  ```
  Tape write error - The previous tape had less than the required minimum
  capacity, size MB, for this tape operation, The operation should be restarted
  from the beginning
  ```

- **Causa**

  La capacidad de la cinta no es suficiente para contener los datos de copia de seguridad.

- **Acción Correctiva**

  Utilice cintas con mayor capacidad y vuelva a intentar realizar la tarea de backup.

Error de soporte en la cinta de lectura

- **Mensaje**

  ```
  Media error on tape read
  ```

- **Causa**

  La cinta de la que se van a restaurar los datos está dañada y puede que no contenga los datos de copia de seguridad completos.

- **Acción Correctiva**

  Si está seguro de que la cinta tiene la copia de seguridad completa, vuelva a intentar la operación de restauración. Si la cinta no contiene la copia de seguridad completa, no se puede ejecutar la operación de restauración.

Error de lectura de cinta

- **Mensaje**

  ```
  Tape read error
  ```

- **Causa**

  La unidad de cinta está dañada o la cinta no contiene la copia de seguridad completa.

- **Acción Correctiva**

  Si la unidad de cinta está dañada, utilice otra unidad de cinta. Si la cinta no contiene la copia de seguridad completa, no podrá restaurar los datos.

Ya al final de la cinta

- **Mensaje**

  ```
  Already at the end of tape
  ```

- **Causa**

  La cinta no contiene datos o debe rebobinarse.

- **Acción Correctiva**

  Si la cinta no contiene datos, utilice la cinta que contiene la copia de seguridad y vuelva a intentar la tarea de restauración. De lo contrario, rebobine la cinta y vuelva a intentar el trabajo de restauración.

El tamaño del registro de cinta es demasiado pequeño. Pruebe con un tamaño mayor.

- **Mensaje**

  ```
  Tape record size is too small. Try a larger size.
  ```

- **Causa**

  El factor de bloqueo especificado para la operación de restauración es menor que el factor de bloqueo que se utilizó durante el backup.

- **Acción Correctiva**

  Utilice el mismo factor de bloqueo que se especificó durante la copia de seguridad.

El tamaño del registro de cinta debe ser block_Siz1 y no Block_Size2

- **Mensaje**

  ```
  Tape record size should be block_size1 and not block_size2
  ```

- **Causa**

  El factor de bloqueo especificado para la restauración local es incorrecto.

- **Acción Correctiva**

  Vuelva a intentar la tarea de restauración con `block_size1` como factor de bloqueo.

El tamaño del registro de la cinta debe estar comprendido entre 4 KB y 256 KB

- **Mensaje**

  ```
  Tape record size must be in the range between 4KB and 256KB
  ```

- **Causa**

  El factor de bloqueo especificado para la operación de backup o restauración no se encuentra dentro del rango permitido.

- **Acción Correctiva**

  Especifique un factor de bloqueo entre 4 KB y 256 KB.

Mensajes de error de NDMP

Error de comunicación de red

- **Mensaje**

  ```
  Network communication error
  ```

- **Causa**

Se produjo un error en la comunicación a una cinta remota en una conexión triple NDMP.

- **Acción Correctiva**

  Compruebe la conexión de red al mando a distancia.

Mensaje de Read Socket: Error_string

- **Mensaje**

  ```
  Message from Read Socket: error_string
  ```

- **Causa**

  Restaurar la comunicación desde la cinta remota en la conexión NDMP 3-way tiene errores.

- **Acción Correctiva**

  Compruebe la conexión de red al mando a distancia.

Mensaje de Write Dirnet: Error_string

- **Mensaje**

  ```
  Message from Write Dirnet: error_string
  ```

- **Causa**

  Se produjo un error en la comunicación de backup a una cinta remota en una conexión triple NDMP.

- **Acción Correctiva**

  Compruebe la conexión de red al mando a distancia.

Leer el conector hembra EOF recibido

- **Mensaje**

  ```
  Read Socket received EOF
  ```

- **Causa**

  El intento de comunicarse con una cinta remota en una conexión triple NDMP ha alcanzado el fin de la Marca de archivo. Es posible que se intente realizar una restauración triple desde una imagen de backup con un tamaño de bloque mayor.

- **Acción Correctiva**

  Especifique el tamaño de bloque correcto y vuelva a intentar la operación de restauración.

ndmpd número de versión no válido: version_number "

- **Mensaje**

```
ndmpd invalid version number: version_number
```

- **Causa**

  La versión NDMP especificada no es compatible con el sistema de almacenamiento.

- **Acción Correctiva**

  Especifique la versión 4 de NDMP.

Ndmpd session_ID no activo

- **Mensaje**

```
ndmpd session session_ID not active
```

- **Causa**

  Es posible que la sesión NDMP no exista.

- **Acción Correctiva**

  Utilice la `ndmpd status` Comando para ver las sesiones NDMP activas.

No se puede obtener la referencia de volumen para Volume_name

- **Mensaje**

```
Could not obtain vol ref for Volume vol_name
```

- **Causa**

  No se pudo obtener la referencia del volumen debido a que este puede estar en uso por parte de otras operaciones.

- **Acción Correctiva**

  Volver a intentar la operación más tarde.

El tipo de conexión de datos ["NDMP4_ADDR_TCP"|"NDMP4_ADDR_TCP_IPv6"] no es compatible con las conexiones de control ["IPv6"|"IPv4"]

- **Mensaje**

```
Data connection type ["NDMP4_ADDR_TCP"|"NDMP4_ADDR_TCP_IPv6"] not supported
for ["IPv6"|"IPv4"] control connections
```

- **Causa**

  En el modo NDMP de ámbito de nodo, la conexión de datos NDMP establecida debe ser del mismo tipo de dirección de red (IPv4 o IPv6) que la conexión de control NDMP.

- **Acción Correctiva**

Póngase en contacto con el proveedor de sus aplicaciones de backup.

ESCUCHA DE DATOS: Error de condición de preparación de la conexión DE datos DE LA CABINA

- **Mensaje**

  ```
  DATA LISTEN: CAB data connection prepare precondition error
  ```

- **Causa**

  Se produce un error en la escucha de datos NDMP cuando la aplicación de backup ha negociado la extensión CAB con el servidor NDMP y el tipo de dirección de conexión de datos NDMP especificado no coincide entre los mensajes NDMP_CAB_DATA_CONN_PREPARE y NDMP_DATA_LISTEN.

- **Acción Correctiva**

  Póngase en contacto con el proveedor de sus aplicaciones de backup.

CONEXIÓN DE DATOS: Error de condición de preparación de la conexión DE datos DE LA CABINA

- **Mensaje**

  ```
  DATA CONNECT: CAB data connection prepare precondition error
  ```

- **Causa**

  Se produce un error en la conexión de datos NDMP cuando la aplicación de backup ha negociado la extensión CAB con el servidor NDMP y el tipo de dirección de conexión de datos NDMP especificado no coincide entre los mensajes NDMP_CAB_DATA_CONN_PREPARE y NDMP_DATA_CONNECT.

- **Acción Correctiva**

  Póngase en contacto con el proveedor de sus aplicaciones de backup.

Error:error al mostrar: No se puede obtener la contraseña del usuario '<username>'

- **Mensaje**

  ```
  Error: show failed: Cannot get password for user '<username>'
  ```

- **Causa**

  Configuración de cuenta de usuario incompleta para NDMP

- **Acción Correctiva**

  Asegúrese de que la cuenta de usuario esté asociada con el método de acceso SSH y que el método de autenticación sea la contraseña de usuario.

Mensajes de error de volcado

El volumen de destino es de solo lectura

- **Mensaje**

  `Destination volume is read-only`

- **Causa**

  La ruta a la que se intenta realizar la operación de restauración es de solo lectura.

- **Acción Correctiva**

  Intente restaurar los datos en una ubicación diferente.

El qtree de destino es de solo lectura

- **Mensaje**

  `Destination qtree is read-only`

- **Causa**

  El qtree al que se intenta restaurar es de solo lectura.

- **Acción Correctiva**

  Intente restaurar los datos en una ubicación diferente.

Vuelca temporalmente desactivado en el volumen, vuelva a intentarlo

- **Mensaje**

  `Dumps temporarily disabled on volume, try again`

- **Causa**

  Se intenta realizar un backup de volcado NDMP en un volumen de destino de SnapMirror que forma parte de cualquiera de los dos `snapmirror break` o a `snapmirror resync` funcionamiento.

- **Acción Correctiva**

  Espere a que el `snapmirror break` o. `snapmirror resync` operación para finalizar y después realizar la operación de volcado.

  > Siempre que el estado de un volumen de destino de SnapMirror cambie de lectura/escritura a solo lectura o de solo lectura a lectura/escritura, debe ejecutar un backup de referencia.

Etiquetas de NFS no reconocidas

- **Mensaje**

  `Error: Aborting: dump encountered NFS security labels in the file system`

- **Causa**

  Las etiquetas de seguridad NFS son compatibles a partir de ONTAP 9.9.1 cuando NFSv4.2 está habilitado. Sin embargo, el motor de volcado no reconoce actualmente las etiquetas de seguridad NFS. Si encuentra alguna etiqueta de seguridad NFS en los archivos, directorios o cualquier archivo especial en cualquier formato de volcado, el volcado falla.

- **Acción Correctiva**

  Compruebe que ningún archivo o directorio tiene etiquetas de seguridad NFS.

No se crearon archivos

- **Mensaje**

  ```
  No files were created
  ```

- **Causa**

  Se intentó un DAR de directorio sin permitir la funcionalidad DAR mejorada.

- **Acción Correctiva**

  Active la funcionalidad DAR mejorada y vuelva a intentar DAR.

Error en la restauración del <file name> de archivo

- **Mensaje**

  ```
  Restore of the file file name failed
  ```

- **Causa**

  Cuando SE realiza UN DAR (recuperación de acceso directo) de un archivo cuyo nombre de archivo es el mismo que el de un LUN del volumen de destino, se produce un error EN EL DAR.

- **Acción Correctiva**

  Vuelva a intentar DAR del archivo.

Error de truncamiento para el inode <inode number> src…

- **Mensaje**

  ```
  Truncation failed for src inode <inode number>. Error <error number>. Skipping
  inode.
  ```

- **Causa**

  El inodo de un archivo se elimina cuando se restaura el archivo.

- **Acción Correctiva**

  Espere a que se complete la operación de restauración en un volumen antes de usar ese volumen.

No se puede bloquear una snapshot necesaria mediante el volcado

- **Mensaje**

  ```
  Unable to lock a snapshot needed by dump
  ```

- **Causa**

  La copia Snapshot especificada para el backup no está disponible.

- **Acción Correctiva**

  Vuelva a intentar el backup con una copia Snapshot diferente.

  Utilice la `snap list` Comando para ver la lista de copias Snapshot disponibles.

No se pueden localizar los archivos de mapa de bits

- **Mensaje**

  ```
  Unable to locate bitmap files
  ```

- **Causa**

  Es posible que se hayan eliminado los archivos de mapa de bits necesarios para la operación de copia de seguridad. En este caso, no se puede reiniciar el backup.

- **Acción Correctiva**

  Vuelva a ejecutar la copia de seguridad.

El volumen se encuentra temporalmente en estado transitorio

- **Mensaje**

  ```
  Volume is temporarily in a transitional state
  ```

- **Causa**

  El volumen del que se realiza el backup se encuentra temporalmente en el estado desmontado.

- **Acción Correctiva**

  Espere algún tiempo y vuelva a realizar la copia de seguridad.

Mensajes de error de SMTape

Trozos fuera de servicio

- **Mensaje**

  ```
  Chunks out of order
  ```

- **Causa**

Las cintas de copia de seguridad no se restauran en el orden correcto.

- **Acción Correctiva**

  Vuelva a intentar la operación de restauración y cargue las cintas en la secuencia correcta.

Formato de fragmento no compatible

- **Mensaje**

  ```
  Chunk format not supported
  ```

- **Causa**

  La imagen de copia de seguridad no es de SMTape.

- **Acción Correctiva**

  Si la imagen de copia de seguridad no es de SMTape, vuelva a intentar la operación con una cinta que tenga la copia de seguridad de SMTape.

Error al asignar memoria

- **Mensaje**

  ```
  Failed to allocate memory
  ```

- **Causa**

  El sistema se ha quedado sin memoria.

- **Acción Correctiva**

  Vuelva a intentar el trabajo más tarde cuando el sistema no esté demasiado ocupado.

Error al obtener el búfer de datos

- **Mensaje**

  ```
  Failed to get data buffer
  ```

- **Causa**

  El sistema de almacenamiento se agotó de los búferes.

- **Acción Correctiva**

  Espere a que algunas operaciones del sistema de almacenamiento finalicen y luego vuelva a intentar la tarea.

Error al encontrar la snapshot

- **Mensaje**

```
Failed to find snapshot
```

- **Causa**

  La copia Snapshot especificada para el backup no está disponible.

- **Acción Correctiva**

  Compruebe si la copia Snapshot especificada está disponible. En caso contrario, vuelva a intentarlo con la copia de Snapshot correcta.

No se puede crear la snapshot

- **Mensaje**

  ```
  Failed to create snapshot
  ```

- **Causa**

  El volumen ya contiene el número máximo de copias snapshot.

- **Acción Correctiva**

  Elimine algunas copias de Snapshot y vuelva a intentar la operación de backup.

Error al bloquear la snapshot

- **Mensaje**

  ```
  Failed to lock snapshot
  ```

- **Causa**

  La copia Snapshot está en uso o se ha eliminado.

- **Acción Correctiva**

  Si otra operación utiliza la copia de Snapshot, espere a que finalice y vuelva a intentar el backup. Si la copia Snapshot se ha eliminado, no puede realizar el backup.

Error al eliminar la snapshot

- **Mensaje**

  ```
  Failed to delete snapshot
  ```

- **Causa**

  No se pudo eliminar la copia automática de Snapshot porque está en uso en otras operaciones.

- **Acción Correctiva**

  Utilice la `snap` Comando para determinar el estado de la copia Snapshot. Si no es necesaria la copia Snapshot, elimínela manualmente.

Error al obtener la snapshot más reciente

- **Mensaje**

  ```
  Failed to get latest snapshot
  ```

- **Causa**

  Es posible que la copia Snapshot más reciente no exista porque SnapMirror inicializa el volumen.

- **Acción Correctiva**

  Vuelva a intentarlo una vez completada la inicialización.

No se pudo cargar la nueva cinta

- **Mensaje**

  ```
  Failed to load new tape
  ```

- **Causa**

  Error en unidad de cinta o soporte.

- **Acción Correctiva**

  Sustituya la cinta y vuelva a intentar la operación.

Error al inicializar la cinta

- **Mensaje**

  ```
  Failed to initialize tape
  ```

- **Causa**

  Puede obtener este mensaje de error por uno de los siguientes motivos:

  - La imagen de copia de seguridad no es de SMTape.
  - El factor de bloqueo de cinta especificado es incorrecto.
  - La cinta está dañada o dañada.
  - Se ha cargado una cinta incorrecta para la restauración.

- **Acción Correctiva**
  - Si la imagen de copia de seguridad no es de SMTape, vuelva a intentar la operación con una cinta que tiene una copia de seguridad de SMTape.
  - Si el factor de bloqueo es incorrecto, especifique el factor de bloqueo correcto y vuelva a intentar la operación.
  - Si la cinta está dañada, no podrá realizar la operación de restauración.
  - Si se carga la cinta incorrecta, vuelva a intentar la operación con la cinta correcta.

Error al inicializar el flujo de restauración

- **Mensaje**

  ```
  Failed to initialize restore stream
  ```

- **Causa**

  Puede obtener este mensaje de error por uno de los siguientes motivos:

  - La imagen de copia de seguridad no es de SMTape.
  - El factor de bloqueo de cinta especificado es incorrecto.
  - La cinta está dañada o dañada.
  - Se ha cargado una cinta incorrecta para la restauración.

- **Acción Correctiva**
  - Si la imagen de copia de seguridad no es de SMTape, vuelva a intentar la operación con una cinta que tenga la copia de seguridad de SMTape.
  - Si el factor de bloqueo es incorrecto, especifique el factor de bloqueo correcto y vuelva a intentar la operación.
  - Si la cinta está dañada, no podrá realizar la operación de restauración.
  - Si se carga la cinta incorrecta, vuelva a intentar la operación con la cinta correcta.

Error al leer la imagen de la copia de seguridad

- **Mensaje**

  ```
  Failed to read backup image
  ```

- **Causa**

  La cinta está dañada.

- **Acción Correctiva**

  Si la cinta está dañada, no podrá realizar la operación de restauración.

Falta el encabezado de la imagen o está dañado

- **Mensaje**

  ```
  Image header missing or corrupted
  ```

- **Causa**

  La cinta no contiene una copia de seguridad de SMTape válida.

- **Acción Correctiva**

  Vuelva a intentarlo con una cinta que contenga un backup válido.

Afirmación interna

- **Mensaje**

  ```
  Internal assertion
  ```

- **Causa**

  Hay un error interno de SMTape.

- **Acción Correctiva**

  Informe del error y envíe el `etc/log/backup` archivar para soporte técnico.

Número mágico de imagen de copia de seguridad no válido

- **Mensaje**

  ```
  Invalid backup image magic number
  ```

- **Causa**

  La imagen de copia de seguridad no es de SMTape.

- **Acción Correctiva**

  Si la imagen de copia de seguridad no es de SMTape, vuelva a intentar la operación con una cinta que tenga la copia de seguridad de SMTape.

Suma de comprobación de imagen de backup no válida

- **Mensaje**

  ```
  Invalid backup image checksum
  ```

- **Causa**

  La cinta está dañada.

- **Acción Correctiva**

  Si la cinta está dañada, no podrá realizar la operación de restauración.

Cinta de entrada no válida

- **Mensaje**

  ```
  Invalid input tape
  ```

- **Causa**

  La firma de la imagen de copia de seguridad no es válida en el encabezado de la cinta. La cinta tiene datos dañados o no contiene una imagen de copia de seguridad válida.

- **Acción Correctiva**

  Vuelva a intentar el trabajo de restauración con una imagen de backup válida.

La ruta de volumen no es válida

- **Mensaje**

  `Invalid volume path`

- **Causa**

  No se encuentra el volumen especificado para la operación de backup o restauración.

- **Acción Correctiva**

  Vuelva a intentar el trabajo con una ruta de volumen y un nombre de volumen válidos.

El ID del conjunto de copia de seguridad no coincide

- **Mensaje**

  `Mismatch in backup set ID`

- **Causa**

  La cinta cargada durante un cambio de cinta no forma parte del conjunto de copia de seguridad.

- **Acción Correctiva**

  Cargue la cinta correcta y vuelva a intentar el trabajo.

No coincide con la Marca de tiempo de backup

- **Mensaje**

  `Mismatch in backup time stamp`

- **Causa**

  La cinta cargada durante un cambio de cinta no forma parte del conjunto de copia de seguridad.

- **Acción Correctiva**

  Utilice la `smtape restore -h` comando para verificar la información de encabezado de una cinta.

Trabajo anulado debido a cierre

- **Mensaje**

  `Job aborted due to shutdown`

- **Causa**

El sistema de almacenamiento se está reiniciando.

- **Acción Correctiva**

  Vuelva a intentar el trabajo después de que se reinicie el sistema de almacenamiento.

Trabajo anulado debido a la eliminación automática de snapshot

- **Mensaje**

  ```
  Job aborted due to Snapshot autodelete
  ```

- **Causa**

  El volumen no tiene suficiente espacio y ha activado la eliminación automática de copias Snapshot.

- **Acción Correctiva**

  Libere espacio en el volumen y vuelva a intentar el trabajo.

En la actualidad, la cinta se está utilizando en otras operaciones

- **Mensaje**

  ```
  Tape is currently in use by other operations
  ```

- **Causa**

  La unidad de cinta está en uso por otro trabajo.

- **Acción Correctiva**

  Se debe reintentar la copia de seguridad una vez finalizado el trabajo actualmente activo.

Las cintas están fuera de servicio

- **Mensaje**

  ```
  Tapes out of order
  ```

- **Causa**

  La primera cinta de la secuencia de cinta para la operación de restauración no tiene el encabezado de la imagen.

- **Acción Correctiva**

  Cargue la cinta con el encabezado de la imagen y vuelva a intentar el trabajo.

Error de transferencia (se canceló debido a una operación de MetroCluster)

- **Mensaje**

  ```
  Transfer failed (Aborted due to MetroCluster operation)
  ```

- **Causa**

  La operación SMTape se cancela debido a una operación de conmutación de sitios o conmutación de estado.

- **Acción Correctiva**

  Lleve a cabo la operación SMTape después de que finalice la operación de conmutación o conmutación de regreso.

Error en la transferencia (ARL Initiated abort)

- **Mensaje**

  ```
  Transfer failed (ARL initiated abort)
  ```

- **Causa**

  Mientras se está realizando una operación SMTape si se inicia una reubicación de agregado, se cancela la operación SMTape.

- **Acción Correctiva**

  Realice la operación SMTape después de que finalice la operación de reubicación de agregados.

Error en la transferencia (interrupción iniciada por el CFO)

- **Mensaje**

  ```
  Transfer failed (CFO initiated abort)
  ```

- **Causa**

  La operación SMTape se cancela debido a una operación de recuperación tras fallos (toma de control y retorno al nodo primario) del almacenamiento de un agregado CFO.

- **Acción Correctiva**

  Ejecutar la operación de SMTape tras la recuperación tras la recuperación tras fallos del agregado CFO de almacenamiento.

Error en la transferencia (interrupción iniciada por SFO)

- **Mensaje**

  ```
  Transfer failed (SFO initiated abort)
  ```

- **Causa**

  La operación SMTape se cancela debido a una operación de conmutación al nodo de respaldo (toma de control y retorno al nodo primario) del almacenamiento.

- **Acción Correctiva**

Realice la operación SMTape después de que termine la operación de recuperación tras fallos (toma de control y devolución) del almacenamiento.

Agregado subyacente durante la migración

- **Mensaje**

  ```
  Underlying aggregate under migration
  ```

- **Causa**

  Si se inicia una operación SMTape en un agregado que se está realizando la migración (conmutación por error del almacenamiento o reubicación de agregados), la operación SMTape falla.

- **Acción Correctiva**

  Realice la operación SMTape una vez finalizada la migración de agregado.

El volumen se encuentra actualmente en proceso de migración

- **Mensaje**

  ```
  Volume is currently under migration
  ```

- **Causa**

  La migración de volúmenes y el backup de SMTape no se pueden ejecutar simultáneamente.

- **Acción Correctiva**

  Vuelva a intentar el trabajo de backup después de completar la migración del volumen.

Volumen sin conexión

- **Mensaje**

  ```
  Volume offline
  ```

- **Causa**

  El volumen del cual se realiza el backup está sin conexión.

- **Acción Correctiva**

  Coloque el volumen en línea y vuelva a intentar el backup.

Volumen no restringido

- **Mensaje**

  ```
  Volume not restricted
  ```

- **Causa**

No está restringido el volumen de destino al que se restauran los datos.

- **Acción Correctiva**

  Restrinja el volumen y vuelva a intentar la operación de restauración.

Configuración de NDMP

Información general de la configuración de NDMP

Puede configurar rápidamente un clúster ONTAP 9 para utilizar el protocolo de gestión de datos de red (NDMP) con el fin de realizar backups de los datos directamente en cinta mediante una aplicación de backup de terceros.

Si la aplicación de backup admite Cluster Aware Backup (CAB), puede configurar NDMP como *SVM-scoped* o *node-scoped*:

- Con el ámbito de SVM en el nivel del clúster (SVM de administrador), puede realizar backup de todos los volúmenes alojados en diferentes nodos del clúster. Siempre que sea posible, se recomienda utilizar NDMP con ámbito SVM.
- NDMP de ámbito de nodo le permite realizar backup de todos los volúmenes alojados en ese nodo.

Si la aplicación de backup no admite CAB, debe utilizar NDMP de ámbito de nodo.

El protocolo NDMP de ámbito SVM y el de ámbito de nodo son mutuamente exclusivos; no se pueden configurar en el mismo clúster.

NDMP de ámbito del nodo está obsoleto en ONTAP 9.

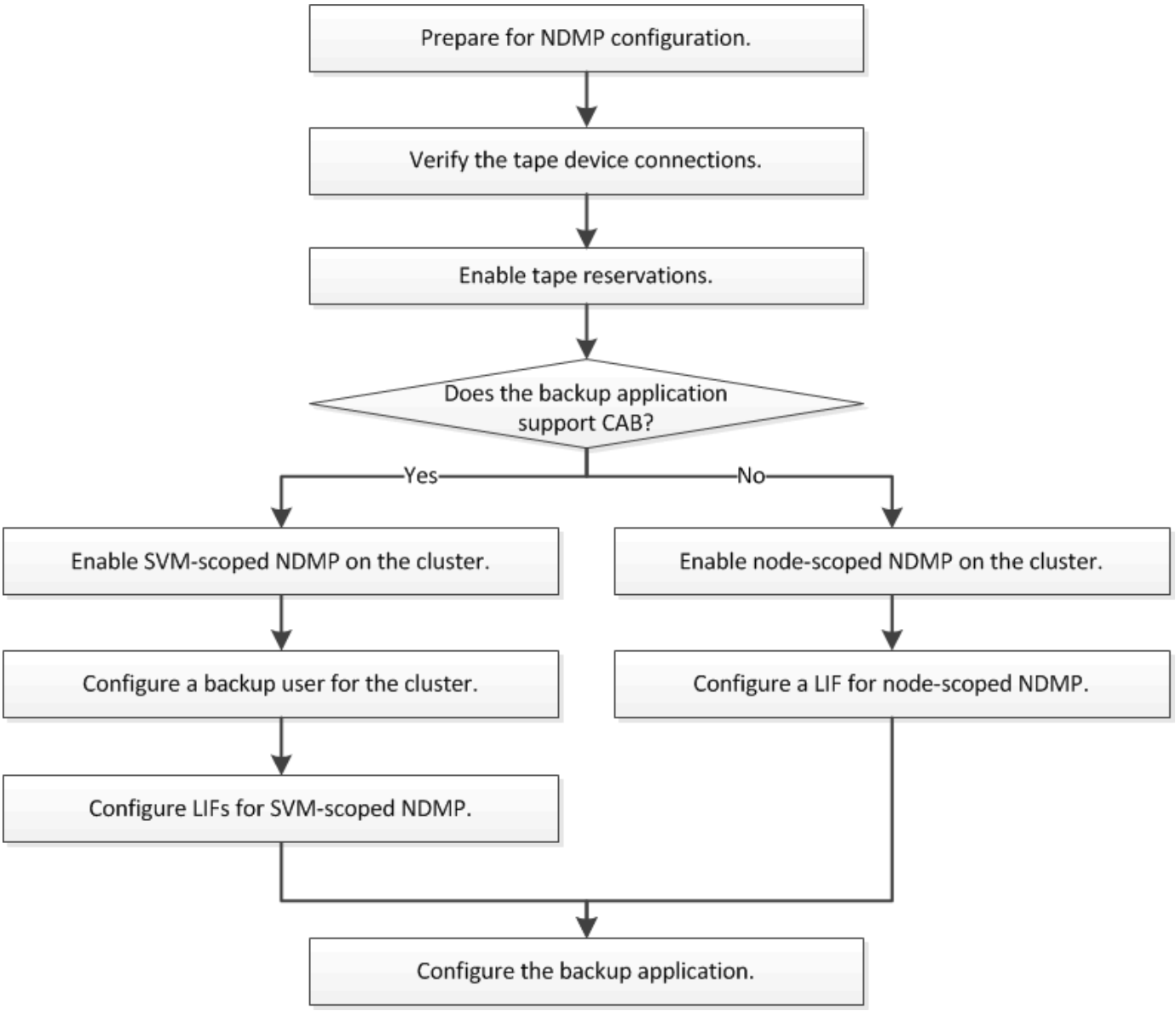
Más información acerca de "Respaldo para clúster (CAB)".

Antes de configurar NDMP, compruebe lo siguiente:

- Tiene una aplicación de copia de seguridad de terceros (también llamada aplicación de administración de datos o DMA).
- Es un administrador de clúster.
- Se instalan dispositivos de cinta y un servidor multimedia opcional.
- Los dispositivos de cinta están conectados al clúster a través de un switch Fibre Channel (FC) y no están conectados directamente.
- Al menos un dispositivo de cinta tiene un número de unidad lógica (LUN) de 0.

Flujo de trabajo de configuración de NDMP

La configuración del backup en cinta mediante NDMP implica preparar la configuración NDMP, verificar las conexiones del dispositivo de cinta, habilitar las reservas en cinta, configurar NDMP en el nivel de SVM o nodo, habilitar NDMP en el clúster, configurar un usuario de backup, configurar LIF y configurar la aplicación de backup.



Prepárese para la configuración de NDMP

Antes de configurar el acceso al backup a cinta mediante el protocolo de gestión de datos de red (NDMP), debe comprobar que la configuración planificada es compatible y comprobar que las unidades de cinta aparecen como unidades adecuadas en cada nodo, verificar que todos los nodos tienen LIF de interconexión de clústeres. E identifique si la aplicación de backup es compatible con la extensión Cluster Aware Backup (CAB).

Pasos

1. Consulte la matriz de compatibilidad del proveedor de aplicaciones de backup para obtener información sobre la compatibilidad con ONTAP (NetApp no reúne los requisitos de aplicaciones de backup de terceros con ONTAP o NDMP).

   Debe verificar que los siguientes componentes de NetApp sean compatibles:

   - La versión de ONTAP 9 que se ejecuta en el clúster.
   - El proveedor de aplicaciones de backup y la versión: Por ejemplo, Veritas NetBackup 8.2 o

CommVault.

- Los detalles de los dispositivos de cinta, como el fabricante, el modelo y la interfaz de las unidades de cinta: Por ejemplo, IBM Ultrium 8 o HPE StoreEver Ultrium 30750 LTO-8.
- Las plataformas de los nodos del clúster: Por ejemplo, FAS8700 o A400.

> Puede encontrar matrices de compatibilidad con ONTAP heredadas para aplicaciones de backup en la "Herramienta de matriz de interoperabilidad de NetApp".

2. Compruebe que las unidades de cinta aparecen como unidades cualificadas en el archivo de configuración de cinta incorporado de cada nodo:

   a. En la interfaz de línea de comandos, consulte el archivo de configuración de cinta incorporado mediante la `storage tape show-supported-status` comando.

```
cluster1::> storage tape show-supported-status

Node: cluster1-1
                                  Is
Tape Drives                       Supported  Support Status
-------------------------------  ---------
--------------------------------
Certance Ultrium 2                true       Dynamically Qualified
Certance Ultrium 3                true       Dynamically Qualified
Digital DLT2000                   true       Qualified
```

   b. Compare las unidades de cinta con la lista de unidades cualificadas de la salida.

> Los nombres de los dispositivos de cinta de la salida pueden variar ligeramente con respecto a los nombres de la etiqueta del dispositivo o de la matriz de interoperabilidad. Por ejemplo, Digital DLT2000 también se conoce como DLT2k. Puede ignorar estas pequeñas diferencias de nomenclatura.

   c. Si un dispositivo no aparece como cualificado en el resultado a pesar de que el dispositivo está cualificado según la matriz de interoperabilidad, descargue e instale un archivo de configuración actualizado para el dispositivo con las instrucciones en el sitio de soporte de NetApp.

      "Descargas de NetApp: Archivos de configuración de dispositivo de cinta"

   Es posible que un dispositivo cualificado no aparezca en el archivo de configuración de cinta integrado si el dispositivo de cinta fue cualificado después de enviar el nodo.

3. Compruebe que todos los nodos del clúster tienen una LIF de interconexión de clústeres:

   a. Consulte las LIF de interconexión de clústeres de los nodos mediante el `network interface show -role intercluster` comando.

```
cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
```

b. Si no hay ninguna LIF de interconexión de clústeres en ningún nodo, cree una LIF de interconexión de clústeres mediante la `network interface create` comando.

```
cluster1::> network interface create -vserver cluster1 -lif IC2 -role
intercluster
-home-node cluster1-2 -home-port e0b -address 192.0.2.68 -netmask
255.255.255.0
-status-admin up -failover-policy local-only -firewall-policy
intercluster

cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2        up/up      192.0.2.68/24      cluster1-2
e0b     true
```

"Gestión de redes"

4. Identifique si la aplicación de backup es compatible con Cluster Aware Backup (CAB) mediante la documentación proporcionada con la aplicación de backup.

   El soporte CAB es un factor clave a la hora de determinar el tipo de backup que se puede realizar.

Compruebe las conexiones del dispositivo de cinta

Debe asegurarse de que todas las unidades e intercambiadores de medios sean visibles en ONTAP como dispositivos.

Pasos

1. Ver información acerca de todas las unidades e intercambiadores de medios utilizando `storage tape show` comando.

```
cluster1::> storage tape show

Node: cluster1-01
Device ID                Device Type     Description
Status
----------------------  --------------  ------------------------------
--------
sw4:10.11                tape drive      HP LTO-3
normal
0b.125L1                 media changer   HP MSL G3 Series
normal
0d.4                     tape drive      IBM LTO 5 ULT3580
normal
0d.4L1                   media changer   IBM 3573-TL
normal
...
```

2. Si no se muestra una unidad de cinta, solucione el problema.
3. Si no se muestra un cambiador de materiales, consulte la información sobre los intercambiadores de material utilizando `storage tape show-media-changer` y, a continuación, solucione el problema.

```
cluster1::> storage tape show-media-changer

Media Changer: sw4:10.11L1
  Description: PX70-TL
         WWNN: 2:00a:000e11:10b919
         WWPN: 2:00b:000e11:10b919
Serial Number: 00FRU7800000_LL1

       Errors: -

Paths:
Node                      Initiator  Alias    Device State
Status
------------------------  ---------  -------  ------------------------
--------
cluster1-01               2b         mc0      in-use
normal
...
```

Activar reservas de cinta

Debe asegurarse de que las unidades de cinta estén reservadas para que las aplicaciones de backup las operaciones de backup de NDMP.

Acerca de esta tarea

La configuración de las reservas varía en diferentes aplicaciones de backup, y esta configuración debe coincidir con la aplicación de backup y los nodos o servidores que utilizan las mismas unidades. Consulte la documentación del proveedor de la aplicación de backup para obtener los ajustes de reserva correctos.

Pasos

1. Habilite las reservas mediante el `options -option-name tape.reservations -option-value persistent` comando.

   El siguiente comando habilita las reservas con `persistent` valor:

   ```
   cluster1::> options -option-name tape.reservations -option-value
   persistent
   2 entries were modified.
   ```

2. Compruebe que las reservas estén habilitadas en todos los nodos mediante el `options tape.reservations` y, a continuación, revise el resultado.

   ```
   cluster1::> options tape.reservations

   cluster1-1
       tape.reservations                persistent

   cluster1-2
       tape.reservations                persistent
   2 entries were displayed.
   ```

Configure NDMP con ámbito SVM

Habilite NDMP con ámbito de SVM en el clúster

Si el DMA admite la extensión Cluster Aware Backup (CAB), puede realizar un backup de todos los volúmenes alojados en diferentes nodos de un clúster mediante la habilitación de NDMP de ámbito SVM, la habilitación del servicio NDMP en el clúster (SVM de administrador) y la configuración de LIF para la conexión de datos y control.

Lo que necesitará

La extensión DE LA CABINA debe ser compatible con el DMA.

Acerca de esta tarea

Al desactivar el modo de NDMP con ámbito del nodo, es posible habilitar el modo NDMP con ámbito SVM en

el clúster.

Pasos

1. Habilitar modo NDMP en ámbito de SVM:

```
cluster1::> system services ndmp node-scope-mode off
```

   El modo NDMP en el ámbito de SVM está habilitado.

2. Habilite el servicio NDMP en la SVM de administrador:

```
cluster1::> vserver services ndmp on -vserver cluster1
```

   El tipo de autenticación se establece en `challenge` de forma predeterminada, la autenticación de texto sin formato está deshabilitada.

   > Para una comunicación segura, debe mantener la autenticación de texto sin formato deshabilitada.

3. Compruebe que el servicio NDMP está activado:

```
cluster1::> vserver services ndmp show
```

```
Vserver       Enabled   Authentication type
------------- --------- -------------------
cluster1      true      challenge
vs1           false     challenge
```

Habilitar un usuario de backup para la autenticación NDMP

Para autenticar NDMP de ámbito SVM desde la aplicación de backup, debe haber un usuario administrativo con suficientes privilegios y una contraseña NDMP.

Acerca de esta tarea

Debe generar una contraseña de NDMP para los usuarios administradores de backup. Puede habilitar los usuarios administradores de backup en el nivel del clúster o la SVM; si fuera necesario, puede crear un usuario nuevo. De forma predeterminada, los usuarios con los siguientes roles pueden autenticar para el backup NDMP:

- En todo el clúster: `admin` o. `backup`
- SVM individuales: `vsadmin` o. `vsadmin-backup`

Si utiliza un usuario NIS o LDAP, el usuario debe existir en el servidor correspondiente. No puede utilizar un usuario de Active Directory.

Pasos

1. Mostrar los usuarios y permisos de administrador actuales:

   ```
   security login show
   ```

2. Si es necesario, cree un nuevo usuario de backup NDMP con el `security login create` Y el rol apropiado para privilegios de SVM individuales o en todo el clúster.

   Puede especificar un nombre de usuario de backup local o un nombre de usuario NIS o LDAP para el `-user-or-group-name` parámetro.

   El siguiente comando crea el usuario de backup `backup_admin1` con la `backup` rol para todo el clúster:

   ```
   cluster1::> security login create -user-or-group-name backup_admin1
   -application ssh -authmethod password -role backup
   ```

   El siguiente comando crea el usuario de backup `vsbackup_admin1` con la `vsadmin-backup` Rol para una SVM individual:

   ```
   cluster1::> security login create -user-or-group-name vsbackup_admin1
   -application ssh -authmethod password -role vsadmin-backup
   ```

   Introduzca una contraseña para el nuevo usuario y confirme.

3. Genere una contraseña para la SVM de administrador con el `vserver services ndmp generate password` comando.

   La contraseña generada debe utilizarse para autenticar la conexión NDMP por parte de la aplicación de copia de seguridad.

   ```
   cluster1::> vserver services ndmp generate-password -vserver cluster1
   -user backup_admin1

    Vserver: cluster1
       User: backup_admin1
   Password: qG5CqQHYxw7tE57g
   ```

Configure las LIF

Debe identificar las LIF que se usarán para establecer una conexión de datos entre los recursos de cinta y los de datos, y para controlar la conexión entre la SVM de administrador y la aplicación de backup. Tras identificar las LIF, debe verificar que las políticas de conmutación por error y firewall están establecidas para las LIF y especificar el rol de interfaz preferido.

A partir de ONTAP 9.10.1, las políticas de firewall están obsoletas y sustituidas por completo por políticas de servicios LIF. Para obtener más información, consulte "LIF y políticas de servicio en ONTAP 9.6 y posteriores".

Pasos

1. Identifique los LIF de interconexión de clústeres, gestión de clústeres y gestión de nodos mediante el `network interface show` con el `-role` parámetro.

   El siguiente comando muestra las LIF de interconexión de clústeres:

```
cluster1::> network interface show -role intercluster

            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------        ---------- ------------------
------------- ------- ----
cluster1    IC1               up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2               up/up      192.0.2.68/24      cluster1-2
e0b     true
```

   El siguiente comando muestra la LIF de gestión del clúster:

```
cluster1::> network interface show -role cluster-mgmt

            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------        ---------- ------------------
------------- ------- ----
cluster1    cluster_mgmt      up/up      192.0.2.60/24      cluster1-2
e0M     true
```

   El siguiente comando muestra las LIF de gestión de nodos:

```
cluster1::> network interface show -role node-mgmt

            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------        ---------- ------------------ ------------
------  ------
cluster1    cluster1-1_mgmt1  up/up      192.0.2.69/24      cluster1-1
e0M     true
            cluster1-2_mgmt1  up/up      192.0.2.70/24      cluster1-2
e0M     true
```

2. Compruebe que la política de firewall está habilitada para NDMP en las LIF de interconexión de clústeres, gestión de clústeres (gestión de clústeres) y gestión de nodos (gestión de nodos):

   a. Compruebe que la directiva de firewall está activada para NDMP mediante el `system services firewall policy show` comando.

      El siguiente comando muestra la política de firewall para la LIF de administración de clústeres:

```
cluster1::> system services firewall policy show -policy cluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -----------------
cluster     cluster      dns        0.0.0.0/0
                         http       0.0.0.0/0
                         https      0.0.0.0/0
                        ** ndmp       0.0.0.0/0**
                         ndmps      0.0.0.0/0
                         ntp        0.0.0.0/0
                         rsh        0.0.0.0/0
                         snmp       0.0.0.0/0
                         ssh        0.0.0.0/0
                         telnet     0.0.0.0/0
10 entries were displayed.
```

      El siguiente comando muestra la política de firewall para la LIF de interconexión de clústeres:

```
cluster1::> system services firewall policy show -policy intercluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
                         **ndmp       0.0.0.0/0, ::/0**
                         ndmps      -
                         ntp        -
                         rsh        -
                         ssh        -
                         telnet     -
9 entries were displayed.
```

El siguiente comando muestra la política de firewall de la LIF de gestión de nodos:

```
cluster1::> system services firewall policy show -policy mgmt

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1-1  mgmt         dns        0.0.0.0/0, ::/0
                         http       0.0.0.0/0, ::/0
                         https      0.0.0.0/0, ::/0
                         **ndmp       0.0.0.0/0, ::/0**
                         ndmps      0.0.0.0/0, ::/0
                         ntp        0.0.0.0/0, ::/0
                         rsh        -
                         snmp       0.0.0.0/0, ::/0
                         ssh        0.0.0.0/0, ::/0
                         telnet     -
10 entries were displayed.
```

b. Si la directiva de firewall no está activada, active la directiva de firewall mediante el `system services firewall policy modify` con el `-service` parámetro.

   El siguiente comando habilita la política de firewall para la LIF de interconexión de clústeres:

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. Asegurarse de que la política de conmutación por error esté establecida de forma adecuada para todos los LIF:

a. Compruebe que la política de conmutación por error para la LIF de administración del clúster está establecida en `broadcast-domain-wide`Y la directiva para las LIF de interconexión de clústeres y de gestión de nodos se establece en `local-only` mediante el uso de `network interface show -failover` comando.

   El siguiente comando muestra la política de conmutación por error para las LIF de gestión de clústeres, interconexión de clústeres y nodos:

```
cluster1::> network interface show -failover

           Logical            Home               Failover
Failover
Vserver    Interface          Node:Port          Policy
Group
---------- -----------------  ----------------- --------------------
--------
cluster    cluster1_clus1     cluster1-1:e0a    local-only
cluster
                                                     Failover Targets:
                                                     .......

**cluster1   cluster_mgmt       cluster1-1:e0m    broadcast-domain-wide
Default**
                                                     Failover Targets:
                                                     .......
           **IC1                 cluster1-1:e0a    local-only
Default**
                                                     Failover Targets:
           **IC2                 cluster1-1:e0b    local-only
Default**
                                                     Failover Targets:
                                                     .......
**cluster1-1 cluster1-1_mgmt1   cluster1-1:e0m    local-only
Default**
                                                     Failover Targets:
                                                     ......
**cluster1-2 cluster1-2_mgmt1   cluster1-2:e0m    local-only
Default**
                                                     Failover Targets:
                                                     ......
```

a. Si las políticas de conmutación por error no están definidas de forma adecuada, modifique la política de conmutación por error mediante el `network interface modify` con el `-failover-policy` parámetro.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

4. Especifique las LIF necesarias para la conexión de datos mediante el `vserver services ndmp modify` con el `preferred-interface-role` parámetro.

```
cluster1::> vserver services ndmp modify -vserver cluster1 -preferred
-interface-role intercluster,cluster-mgmt,node-mgmt
```

5. Compruebe que el rol de interfaz preferida esté establecido para el clúster mediante el `vserver services ndmp show` comando.

```
cluster1::> vserver services ndmp show -vserver cluster1

                            Vserver: cluster1
                       NDMP Version: 4
                       .......
                       .......
            Preferred Interface Role: intercluster, cluster-mgmt, node-
mgmt
```

Configure el NDMP de ámbito del nodo

Habilite NDMP de ámbito del nodo en el clúster

Puede realizar backups de volúmenes alojados en un único nodo. Para ello, active el NDMP de ámbito del nodo, lo que habilita el servicio NDMP y configura una LIF para la conexión de datos y control. Esto puede hacerse para todos los nodos del clúster.

> NDMP de ámbito del nodo está obsoleto en ONTAP 9.

Acerca de esta tarea

Cuando se utiliza NDMP en el modo de alcance del nodo, la autenticación debe configurarse por nodo. Para obtener más información, consulte "El artículo de la base de conocimientos "Cómo configurar la autenticación NDMP en el modo de alcance de nodo"".

Pasos

1. Habilitar modo NDMP de ámbito de nodo:

```
cluster1::> system services ndmp node-scope-mode on
```

NDMP node-scope-mode está activado.

2. Habilite el servicio NDMP en todos los nodos del clúster:

   Si utiliza el comodín "'*'", se habilita el servicio NDMP en todos los nodos al mismo tiempo.

   Debe especificar una contraseña para la autenticación de la conexión NDMP mediante la aplicación de backup.

```
cluster1::> system services ndmp on -node *
```

```
Please enter password:
Confirm password:
2 entries were modified.
```

3. Deshabilite el `-clear-text` Opción de comunicación segura de la contraseña NDMP:

   Usando el comodín "'*" `disables the` `-clear-text` opción en todos los nodos al mismo tiempo.

```
cluster1::> system services ndmp modify -node * -clear-text false
```

4. Compruebe que el servicio NDMP esté habilitado y el `-clear-text` la opción está desactivada:

```
cluster1::> system services ndmp show
```

```
Node                  Enabled   Clear text  User Id
--------------------- --------- ----------- ---------
cluster1-1            true      false        root
cluster1-2            true      false        root
2 entries were displayed.
```

Configure una LIF

Debe identificar una LIF que se utilizará para establecer una conexión de datos y controlar la conexión entre el nodo y la aplicación de backup. Tras identificar la LIF, debe verificar que las políticas de firewall y recuperación tras fallos están establecidas para la LIF.

> A partir de ONTAP 9.10.1, las políticas de firewall están obsoletas y sustituidas por completo por políticas de servicios LIF. Para obtener más información, consulte "Configurar políticas de firewall para LIF".

Pasos

1. Identifique la LIF de interconexión de clústeres alojada en los nodos mediante el `network interface`

`show` con el `-role` parámetro.

```
cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1    e0a
true
cluster1    IC2        up/up      192.0.2.68/24      cluster1-2    e0b
true
```

2. Compruebe que la política de firewall está activada para NDMP en las LIF de interconexión de clústeres:

   a. Compruebe que la directiva de firewall está activada para NDMP mediante el `system services firewall policy show` comando.

      El siguiente comando muestra la política de firewall para la LIF de interconexión de clústeres:

```
cluster1::> system services firewall policy show -policy intercluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
                         **ndmp       0.0.0.0/0, ::/0**
                         ndmps      -
                         ntp        -
                         rsh        -
                         ssh        -
                         telnet     -
9 entries were displayed.
```

   b. Si la directiva de firewall no está activada, active la directiva de firewall mediante el `system services firewall policy modify` con el `-service` parámetro.

      El siguiente comando habilita la política de firewall para la LIF de interconexión de clústeres:

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. Asegúrese de que la normativa de recuperación tras fallos esté establecida de forma adecuada para las LIF de interconexión de clústeres:
   a. Compruebe que la política de recuperación tras fallos de las LIF de interconexión de clústeres está establecida en `local-only` mediante el uso de `network interface show -failover` comando.

```
cluster1::> network interface show -failover
            Logical          Home               Failover     Failover
Vserver     Interface        Node:Port          Policy       Group
--------    ---------------  ----------------- ------------ --------
cluster1    **IC1               cluster1-1:e0a    local-only
Default**
                                                    Failover Targets:
                                                    .......
            **IC2               cluster1-2:e0b    local-only
Default**
                                                    Failover Targets:
                                                    .......
cluster1-1  cluster1-1_mgmt1 cluster1-1:e0m    local-only    Default
                                                    Failover Targets:
                                                    .......
```

   b. Si la política de conmutación por error no está definida de forma adecuada, modifique la política de conmutación por error mediante el `network interface modify` con el `-failover-policy` parámetro.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

Configure la aplicación de backup

Una vez que se configura el clúster para el acceso NDMP, debe recopilar información de la configuración del clúster y, a continuación, configurar el resto del proceso de backup en la aplicación de backup.

Pasos

1. Recopile la siguiente información configurada anteriormente en ONTAP:
   - El nombre de usuario y la contraseña que la aplicación de backup necesita para crear la conexión NDMP
   - Las direcciones IP de las LIF de interconexión de clústeres que necesita la aplicación de backup para conectarse al clúster
2. En ONTAP, muestre los alias que ONTAP asignó a cada dispositivo utilizando `storage tape alias show` comando.

   Los alias suelen ser útiles para configurar la aplicación de copia de seguridad.

```
cluster1::> storage tape show -alias

  Device ID: 2a.0
Device Type: tape drive
Description: Hewlett-Packard LTO-5

Node                        Alias     Mapping
--------------------------- --------- ------------------------------
stsw-3220-4a-4b-02          st2       SN[HU19497WVR]
...
```

3. En la aplicación de copia de seguridad, configure el resto del proceso de copia de seguridad utilizando la documentación de la aplicación de copia de seguridad.

Después de terminar

Si se produce un evento de movilidad de datos, como un movimiento de volúmenes o una migración LIF, debe estar preparado para reiniciar todas las operaciones de backup interrumpidas.

Replicación entre software de NetApp Element y ONTAP

Replicación entre software de NetApp Element y información general de ONTAP

Puede garantizar la continuidad empresarial en un sistema Element mediante SnapMirror para replicar copias de Snapshot de un volumen de Element en un destino de ONTAP. En caso de desastre en el sitio de Element, podrá seguir prestando servicio a los clientes desde el sistema ONTAP y, a continuación, reactivar el sistema Element cuando el servicio se restaure.

A partir de ONTAP 9.4, puede replicar copias Snapshot de una LUN creada en un nodo ONTAP de nuevo en un sistema Element. Puede haber creado una LUN durante una interrupción del servicio en el sitio de Element, o bien podría utilizar una LUN para migrar datos desde ONTAP al software Element.

Debe trabajar con Element en el backup de ONTAP si se aplica lo siguiente:

- Quiere utilizar las prácticas recomendadas, no explorar todas las opciones disponibles.
- Desea usar la interfaz de línea de comandos (CLI) de ONTAP, no System Manager ni una herramienta de secuencias de comandos automatizada.
- Usted utiliza iSCSI para servir datos a los clientes.

Si se necesita información conceptual o de configuración adicional, consulte la siguiente documentación:

- Configuración de Element

  "Documentación sobre el software NetApp Element"

- Conceptos y configuración de SnapMirror

  "Información general sobre la protección de datos"

Acerca de la replicación entre Element y ONTAP

A partir de ONTAP 9.3, se puede usar SnapMirror para replicar copias de Snapshot de un volumen de Element en un destino de ONTAP. En caso de desastre en el sitio de Element, puede seguir prestando servicio a los clientes desde el sistema ONTAP y, a continuación, reactivar el volumen de origen de Element cuando el servicio se restaure.

A partir de ONTAP 9.4, puede replicar copias Snapshot de una LUN creada en un nodo ONTAP de nuevo en un sistema Element. Puede haber creado una LUN durante una interrupción del servicio en el sitio de Element, o bien podría utilizar una LUN para migrar datos desde ONTAP al software Element.

Los tipos de relaciones de protección de datos

SnapMirror ofrece dos tipos de relación de protección de datos. Para cada tipo, SnapMirror crea una copia Snapshot del volumen de origen de Element antes de inicializar o actualizar la relación:

- En una relación de protección de datos *recuperación ante desastres (DR)*, el volumen de destino solo contiene la copia Snapshot creada por SnapMirror, desde la cual puede continuar sirviendo datos en el caso de una catástrofe en el sitio principal.
- En una relación de protección de datos *de retención a largo plazo*, el volumen de destino contiene copias Snapshot puntuales creadas por el software Element, así como la copia de Snapshot creada por SnapMirror. Podría querer conservar copias Snapshot mensuales creadas en un plazo de 20 años, por ejemplo.

Políticas predeterminadas

La primera vez que se invoca SnapMirror, se realiza una transferencia *baseline* del volumen de origen al volumen de destino. La *política de SnapMirror* define el contenido de la línea de base y cualquier actualización.

Se puede usar una política predeterminada o personalizada al crear una relación de protección de datos. El *policy type* determina qué copias Snapshot se incluirán y cuántas copias se retendrán.

La siguiente tabla muestra las directivas predeterminadas. Utilice la `MirrorLatest` Política para crear una relación de recuperación ante desastres tradicional. Utilice la `MirrorAndVault` o. `Unified7year` Política para crear una relación de replicación unificada, en la que la recuperación ante desastres y la retención a largo plazo se configuran en el mismo volumen de destino.

Política	Tipo de directiva	Comportamiento de actualización
MirrorÚltimas	reflejo asíncrono	Transfiera la copia snapshot creada por SnapMirror.
Reflejo de AndVault	mirror-vault	Transferir la copia snapshot creada por SnapMirror y cualquier otra copia snapshot menos reciente realizada desde la última actualización, siempre y cuando tengan etiquetas de SnapMirror «día» o «semanal».
Unified7 año	mirror-vault	Transferir la copia snapshot creada por SnapMirror y cualquier otra copia snapshot menos reciente realizada desde la última actualización, siempre y cuando tengan etiquetas de SnapMirror «día», «semanal» o «mensual».

Para obtener información de referencia completa sobre las políticas de SnapMirror, incluidas las directrices sobre qué política usar, consulte "Protección de datos".

Etiquetas de SnapMirror

Todas las normas que tengan el tipo de política «espejo» deben tener una regla que especifique las copias snapshot que desea replicar. La regla «diaria», por ejemplo, indica que solo deben replicarse las copias Snapshot asignadas a la etiqueta «diaria» de SnapMirror. La etiqueta de SnapMirror se asigna al configurar copias de Snapshot de Element.

Replicación desde un clúster de origen de Element a un clúster de destino de ONTAP

SnapMirror se puede usar para replicar copias de Snapshot de un volumen de Element en un sistema de destino de ONTAP. En caso de desastre en el sitio de Element, puede seguir prestando servicio a los clientes desde el sistema ONTAP y, a continuación, reactivar el volumen de origen de Element cuando el servicio se restaure.

Un volumen de Element es aproximadamente equivalente a una LUN de ONTAP. SnapMirror crea un LUN con el nombre del volumen de Element cuando se inicializa una relación de protección de datos entre el software Element y ONTAP. SnapMirror replica datos a una LUN existente si la LUN cumple con los requisitos para la replicación de Element en ONTAP.

Las reglas de replicación son las siguientes:

- Un volumen de ONTAP puede contener datos solo de un volumen de Element.
- No es posible replicar datos desde un volumen de ONTAP en varios volúmenes de Element.

Replicación desde un clúster de origen de ONTAP a un clúster de destino de Element

A partir de ONTAP 9.4, puede replicar copias Snapshot de una LUN creada en un sistema ONTAP de vuelta a un volumen de Element:

- Si ya existe una relación de SnapMirror entre un origen de elemento y un destino de ONTAP, una LUN creada mientras ofrece datos desde el destino se replica automáticamente cuando el origen se vuelve a activar.
- De lo contrario, debe crear e inicializar una relación de SnapMirror entre el clúster de origen de ONTAP y el clúster de destino de Element.

Las reglas de replicación son las siguientes:

- La relación de replicación debe tener una política de tipo «"duplicación asíncrona"».

  No se admiten las políticas de tipo «espejo».

- Solo se admiten LUN iSCSI.
- No es posible replicar más de un LUN desde un volumen de ONTAP a un volumen de Element.
- No es posible replicar un LUN desde un volumen de ONTAP a varios volúmenes de Element.

Requisitos previos

Debe haber completado las siguientes tareas antes de configurar una relación de protección de datos entre Element y ONTAP:

- El clúster de Element debe ejecutar la versión 10.1 o posterior del software NetApp Element.
- El clúster de ONTAP debe ejecutar ONTAP 9.3 o una versión posterior.
- Debe haber obtenido la licencia de SnapMirror en el clúster de ONTAP.
- Debe haber configurado volúmenes en los clústeres de Element y ONTAP que sean lo suficientemente grandes como para manejar las transferencias de datos anticipadas.
- Si utiliza el tipo de política «mirror-vault», debe haber configurado una etiqueta de SnapMirror para que se repliquen las copias Snapshot de Element.

> Es posible realizar esta tarea únicamente en la interfaz de usuario web del software Element. Para obtener más información, consulte "Documentación sobre el software NetApp Element"

- Debe haberse asegurado de que el puerto 5010 está disponible.
- Si prevé que podría necesitar mover un volumen de destino, debe asegurarse de que existe una conectividad de malla completa entre el origen y el destino. Cada nodo del clúster de origen de Element debe poder comunicarse con cada nodo del clúster de destino de ONTAP.

Detalles de soporte

En la siguiente tabla se muestran detalles de compatibilidad de elemento en un backup de ONTAP.

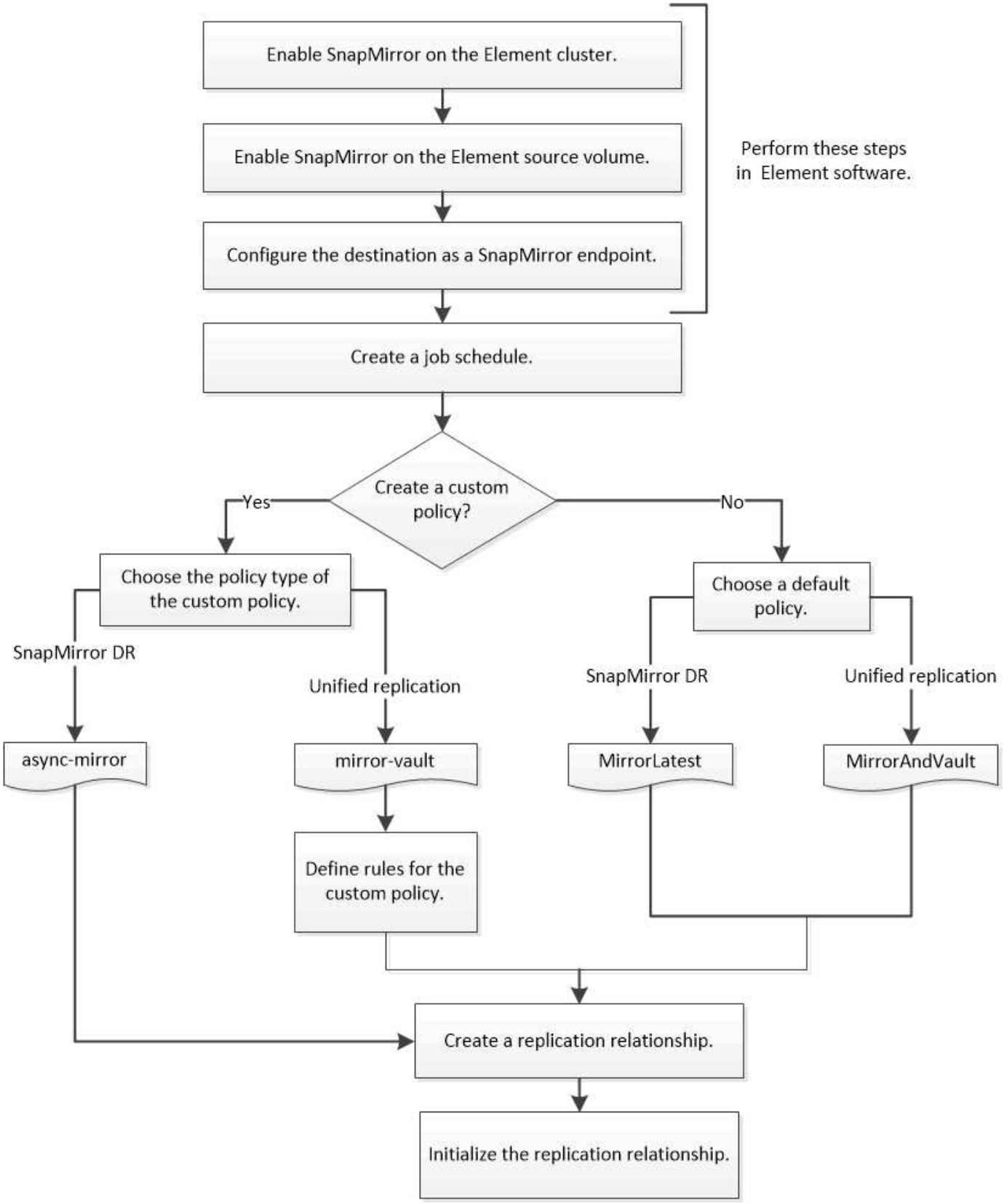
Recurso o característica	Detalles de soporte
SnapMirror	• No se admite la función SnapMirror restore. • La `MirrorAllSnapshots` y.. `XDPDefault` no se admiten políticas. • No se admite el tipo de política «'vault»». • No se admite la regla definida por el sistema "'all_source_snapshots'". • El tipo de política «mirror-vault» solo se admite para la replicación del software Element a ONTAP. Utilice «duplicación asíncrona» para la replicación de ONTAP al software Element. • La `-schedule` y.. `-prefix` opciones para `snapmirror policy add-rule` no son compatibles. • La `-preserve` y.. `-quick-resync` opciones para `snapmirror resync` no son compatibles. • No se mantiene la eficiencia del almacenamiento. • No se admiten las puestas en marcha de protección de datos en cascada ni en distribución ramificada.
ONTAP	• ONTAP Select es compatible a partir de ONTAP 9.4 y Element 10.3. • Cloud Volumes ONTAP es compatible a partir de ONTAP 9.5 y Element 11.0.

Elemento	• El límite de tamaño del volumen es de 8 TIB. • El tamaño de bloque del volumen debe ser 512 bytes. No se admite un tamaño de bloque de 4 KB. • El tamaño del volumen debe ser múltiplo de 1 MIB. • Los atributos del volumen no se conservan. • El número máximo de copias de Snapshot que se deben replicar es 30.
Red	• Se permite una sola conexión TCP por transferencia. • El nodo de Element se debe especificar como dirección IP. No se admite la búsqueda de nombre de host DNS. • No se admiten los espacios IP.
SnapLock	No se admiten los volúmenes de SnapLock.
FlexGroup	No se admiten los volúmenes de FlexGroup.
DR DE SVM	No se admiten los volúmenes de ONTAP en una configuración de recuperación ante desastres de SVM.
MetroCluster	No se admiten los volúmenes de ONTAP en una configuración de MetroCluster.

Flujo de trabajo de replicación entre Element y ONTAP

Si va a replicar datos de Element en ONTAP o de ONTAP a Element, debe configurar una programación de trabajo, especificar una política y crear e inicializar la relación. Puede usar una directiva predeterminada o personalizada.

En el flujo de trabajo se supone que ha completado las tareas de requisitos previos que se enumeran en Requisitos previos. Para obtener información de referencia completa sobre las políticas de SnapMirror, incluidas las directrices sobre qué política usar, consulte "Protección de datos".



Habilite SnapMirror en el software Element

Habilite SnapMirror en el clúster de Element

Es necesario habilitar SnapMirror en el clúster de Element para poder crear una relación

de replicación. Es posible realizar esta tarea únicamente en la interfaz de usuario web del software Element.

Antes de empezar

- El clúster de Element debe ejecutar la versión 10.1 o posterior del software NetApp Element.
- Solo se puede habilitar SnapMirror en clústeres de Element que se usan con los volúmenes de ONTAP de NetApp.

Acerca de esta tarea

El sistema Element viene con SnapMirror deshabilitado de forma predeterminada. SnapMirror no se habilita automáticamente como parte de una nueva instalación o actualización.

> Una vez que está habilitada, SnapMirror no se puede deshabilitar. Solo puede deshabilitar la función SnapMirror y restaurar la configuración predeterminada si devuelve el clúster a la imagen de fábrica.

Pasos

1. Haga clic en **Clusters** > **Configuración**.
2. Busque la configuración específica del clúster para SnapMirror.
3. Haga clic en **Activar SnapMirror**.

Habilite SnapMirror en el volumen de origen de Element

Es necesario habilitar SnapMirror en el volumen de origen de Element para poder crear una relación de replicación. Es posible realizar esta tarea únicamente en la interfaz de usuario web del software Element.

Antes de empezar

- Debe haber habilitado SnapMirror en el clúster de Element.
- El tamaño de bloque del volumen debe ser 512 bytes.
- El volumen no debe participar en la replicación remota de Element.
- El tipo de acceso al volumen no debe ser «'destino de replicación»».

Acerca de esta tarea

En el siguiente procedimiento se asume que el volumen ya existe. SnapMirror también es posible habilitar cuando se crea o se clona un volumen.

Pasos

1. Seleccione **Gestión** > **volúmenes**.
2. Seleccione la botón para el volumen.
3. En el menú desplegable, seleccione **Editar**.
4. En el cuadro de diálogo **Editar volumen**, seleccione **Activar SnapMirror**.
5. Seleccione **Guardar cambios**.

Cree un extremo de SnapMirror

Debe crear un extremo de SnapMirror para poder crear una relación de replicación. Es

posible realizar esta tarea únicamente en la interfaz de usuario web del software Element.

Antes de empezar

Debe haber habilitado SnapMirror en el clúster de Element.

Pasos

1. Haga clic en **Protección de datos** > **terminales de SnapMirror**.
2. Haga clic en **Crear extremo**.
3. En el cuadro de diálogo **Crear un nuevo extremo**, introduzca la dirección IP de administración del clúster ONTAP.
4. Introduzca el ID de usuario y la contraseña del administrador del clúster de ONTAP.
5. Haga clic en **Crear extremo**.

Configurar una relación de replicación

Cree una programación de trabajo de replicación

Si va a replicar datos de Element en ONTAP o de ONTAP a Element, debe configurar una programación de trabajo, especificar una política y crear e inicializar la relación. Puede usar una directiva predeterminada o personalizada.

Puede utilizar el `job schedule cron create` comando para crear una programación de trabajo de replicación. La programación de tareas determina el momento en que SnapMirror actualiza automáticamente la relación de protección de datos a la que se asigna la programación.

Acerca de esta tarea

Debe asignar una programación de tareas cuando crea una relación de protección de datos. Si no asigna una programación de trabajo, debe actualizar la relación manualmente.

Paso

1. Crear un programa de trabajo:

   ```
   job schedule cron create -name job_name -month month -dayofweek day_of_week
   -day day_of_month -hour hour -minute minute
   ```

   Para `-month`, `-dayofweek`, y. `-hour`, puede especificar `all` para ejecutar el trabajo cada mes, día de la semana y hora, respectivamente.

   A partir de ONTAP 9.10.1, puede incluir Vserver para su programación de trabajo:

   ```
   job schedule cron create -name job_name -vserver Vserver_name -month month
   -dayofweek day_of_week -day day_of_month -hour hour -minute minute
   ```

   En el ejemplo siguiente se crea una programación de trabajo denominada `my_weekly` Es decir, los sábados a las 3:00 horas:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

Personalizar una política de replicación

Cree una política de replicación personalizada

Puede usar una directiva predeterminada o personalizada al crear una relación de replicación. Para una política de replicación unificada personalizada, debe definir una o más *rules* que determinen las copias snapshot que se transfieren durante la inicialización y actualización.

Puede crear una directiva de replicación personalizada si la directiva predeterminada para una relación no es adecuada. Puede que desee comprimir datos en una transferencia de red, por ejemplo, o modificar el número de intentos que realiza SnapMirror para transferir copias Snapshot.

Acerca de esta tarea

El *policy type* de la directiva de replicación determina el tipo de relación que admite. En la siguiente tabla se muestran los tipos de directivas disponibles.

Tipo de política	Tipo de relación
reflejo asíncrono	Recuperación ante desastres de SnapMirror
mirror-vault	Replicación unificada

Paso

1. Cree una política de replicación personalizada:

   ```
   snapmirror policy create -vserver SVM -policy policy -type async-
   mirror|mirror-vault -comment comment -tries transfer_tries -transfer-priority
   low|normal -is-network-compression-enabled true|false
   ```

   Para obtener una sintaxis de comando completa, consulte la página man.

   A partir de ONTAP 9.5, puede especificar la programación para crear una programación de copia Snapshot común para relaciones de SnapMirror síncrono mediante la `-common-snapshot-schedule` parámetro. De forma predeterminada, la programación común de copias de Snapshot para relaciones de SnapMirror síncrono es una hora. Puede especificar un valor de 30 minutos a dos horas para la programación de la copia de Snapshot para las relaciones de SnapMirror Synchronous.

   En el ejemplo siguiente se crea una política de replicación personalizada para la recuperación ante desastres de SnapMirror que permite la compresión de red para las transferencias de datos:

   ```
   cluster_dst::> snapmirror policy create -vserver svm1 -policy
   DR_compressed -type async-mirror -comment “DR with network compression
   enabled” -is-network-compression-enabled true
   ```

En el ejemplo siguiente se crea una política de replicación personalizada para la replicación unificada:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy my_unified
-type mirror-vault
```

Después de terminar

En el caso de los tipos de políticas «mirror-vault», debe definir las reglas que determinen las copias snapshot que se transfieren durante la inicialización y la actualización.

Utilice la `snapmirror policy show` Comando para comprobar que la política de SnapMirror se ha creado. Para obtener una sintaxis de comando completa, consulte la página man.

Defina una regla para una política

En el caso de las directivas personalizadas con el tipo de política «mirror-vault», debe definir al menos una regla que determine las copias snapshot que se transfieren durante la inicialización y la actualización. También puede definir reglas para las políticas predeterminadas con el tipo de política «mirror-vault».

Acerca de esta tarea

Todas las normas que tengan el tipo de política «espejo» deben tener una regla que especifique las copias snapshot que desea replicar. La regla «'bimensual'», por ejemplo, indica que sólo deben replicarse las copias snapshot asignadas a la etiqueta «'bimensual'» de SnapMirror. La etiqueta de SnapMirror se asigna al configurar copias de Snapshot de Element.

Cada tipo de política está asociado a una o más reglas definidas por el sistema. Estas reglas se asignan automáticamente a una directiva cuando se especifica su tipo de directiva. La siguiente tabla muestra las reglas definidas por el sistema.

Regla definida por el sistema	Se utiliza en tipos de políticas	Resultado
sm_creado	reflejo asíncrono, reflejo de almacenes	Una copia Snapshot creada por SnapMirror se transfiere tras la inicialización y la actualización.
todos los días	mirror-vault	Las nuevas copias snapshot del origen con la etiqueta de SnapMirror «día» se transfieren durante la inicialización y actualización.
semanal	mirror-vault	Al inicializar y actualizar, se transfieren las nuevas copias snapshot del origen con la etiqueta de SnapMirror «'Weekly».

mensual	mirror-vault	Las nuevas copias snapshot en el origen con la etiqueta de SnapMirror «mensual» se transfieren durante la inicialización y actualización.

Puede especificar reglas adicionales según sea necesario, para directivas predeterminadas o personalizadas. Por ejemplo:

- Para el valor predeterminado `MirrorAndVault` Política puede crear una regla llamada «bimensual» para hacer coincidir las copias Snapshot de la fuente con la etiqueta «bimensual» de SnapMirror.
- En el caso de una política personalizada con el tipo de política «mercado de productos vault», puede crear una regla llamada «bisemanal» para hacer coincidir las copias Snapshot del origen con la etiqueta de SnapMirror «bisemanales».

Paso

1. Definir una regla para una directiva:

   `snapmirror policy add-rule -vserver` *`SVM`* `-policy` *`policy_for_rule`* `-snapmirror -label` *`snapmirror-label`* `-keep` *`retention_count`*

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el siguiente ejemplo, se añade una regla con la etiqueta de SnapMirror `bi-monthly` al valor predeterminado `MirrorAndVault` política:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   MirrorAndVault -snapmirror-label bi-monthly -keep 6
   ```

   En el siguiente ejemplo, se añade una regla con la etiqueta de SnapMirror `bi-weekly` al personalizado `my_snapvault` política:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   my_snapvault -snapmirror-label bi-weekly -keep 26
   ```

   En el siguiente ejemplo, se añade una regla con la etiqueta de SnapMirror `app_consistent` al personalizado `Sync` política:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy Sync
   -snapmirror-label app_consistent -keep 1
   ```

   Luego, puede replicar las copias Snapshot del clúster de origen que coincidan con esta etiqueta de SnapMirror:

```
cluster_src::> snapshot create -vserver vs1 -volume vol1 -snapshot
snapshot1 -snapmirror-label app_consistent
```

Cree una relación de replicación

Crear una relación desde un origen de elemento a un destino de ONTAP

La relación entre el volumen de origen del almacenamiento primario y el volumen de destino del almacenamiento secundario se denomina *relación de protección de datos*. Puede utilizar el `snapmirror create` Comando para crear una relación de protección de datos desde un origen de elemento a un destino de ONTAP, o desde un origen de ONTAP a un destino de Element.

SnapMirror se puede usar para replicar copias de Snapshot de un volumen de Element en un sistema de destino de ONTAP. En caso de desastre en el sitio de Element, puede seguir prestando servicio a los clientes desde el sistema ONTAP y, a continuación, reactivar el volumen de origen de Element cuando el servicio se restaure.

Antes de empezar

- ONTAP debe haber accesible desde el nodo Element que contiene el volumen que se va a replicar.
- El volumen de Element debe estar habilitado para la replicación de SnapMirror.
- Si utiliza el tipo de política «mirror-vault», debe haber configurado una etiqueta de SnapMirror para que se repliquen las copias Snapshot de Element.

> Es posible realizar esta tarea únicamente en la interfaz de usuario web del software Element. Para obtener más información, consulte "Documentación de Element".

Acerca de esta tarea

Debe especificar la ruta de origen del elemento en el formulario `hostip:/lun/name`, donde «'lun'» es la cadena real «'lun'» y. `name` Es el nombre del volumen de Element.

Un volumen de Element es aproximadamente equivalente a una LUN de ONTAP. SnapMirror crea un LUN con el nombre del volumen de Element cuando se inicializa una relación de protección de datos entre el software Element y ONTAP. SnapMirror replica datos a una LUN existente si la LUN cumple con los requisitos para replicar del software Element en ONTAP.

Las reglas de replicación son las siguientes:

- Un volumen de ONTAP puede contener datos solo de un volumen de Element.
- No es posible replicar datos desde un volumen de ONTAP en varios volúmenes de Element.

En ONTAP 9.3 y versiones anteriores, los volúmenes de destino pueden contener hasta 251 copias Snapshot. A partir de la versión 9.4 de ONTAP, un volumen de destino puede contener hasta 1019 copias snapshot.

Paso

1. A partir del clúster de destino, cree una relación de replicación desde un origen de Element en un destino de ONTAP:

`snapmirror create -source-path hostip:/lun/name -destination-path SVM:volume |cluster://SVM/volume -type XDP -schedule schedule -policy policy`

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo se crea una relación de recuperación ante desastres de SnapMirror con los valores predeterminados `MirrorLatest` política:

```
cluster_dst::> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy MirrorLatest
```

En el ejemplo siguiente se crea una relación de replicación unificada con la opción predeterminada `MirrorAndVault` política:

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy MirrorAndVault
```

En el siguiente ejemplo se crea una relación de replicación unificada mediante `Unified7year` política:

```
cluster_dst::> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy Unified7year
```

En el siguiente ejemplo se crea una relación de replicación unificada mediante el método personalizado `my_unified` política:

```
cluster_dst::> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy my_unified
```

Después de terminar

Utilice la `snapmirror show` Comando para verificar que la relación de SnapMirror se ha creado. Para obtener una sintaxis de comando completa, consulte la página man.

Cree una relación desde un origen de ONTAP a un destino de elemento

A partir de ONTAP 9.4, puede usar SnapMirror para replicar copias Snapshot de una LUN creada en un origen de ONTAP de nuevo en un destino de Element. Es posible que utilice la LUN para migrar datos desde ONTAP al software Element.

Antes de empezar

- ONTAP debe haber accesible el nodo de destino de Element.

- El volumen de Element debe estar habilitado para la replicación de SnapMirror.

Acerca de esta tarea

Debe especificar la ruta de destino del elemento en el formulario `hostip:/lun/name`, donde «'lun'» es la cadena real «'lun'» y. `name` Es el nombre del volumen de Element.

Las reglas de replicación son las siguientes:

- La relación de replicación debe tener una política de tipo «"duplicación asíncrona"».

  Puede usar una directiva predeterminada o personalizada.

- Solo se admiten LUN iSCSI.
- No es posible replicar más de un LUN desde un volumen de ONTAP a un volumen de Element.
- No es posible replicar un LUN desde un volumen de ONTAP a varios volúmenes de Element.

Paso

1. Cree una relación de replicación desde un origen de ONTAP a un destino de Element:

   `snapmirror create -source-path SVM:volume|cluster://SVM/volume -destination -path hostip:/lun/name -type XDP -schedule schedule -policy policy`

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el siguiente ejemplo se crea una relación de recuperación ante desastres de SnapMirror con los valores predeterminados `MirrorLatest` política:

   ```
   cluster_dst::> snapmirror create -source-path svm_1:volA_dst
   -destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
   -policy MirrorLatest
   ```

   En el siguiente ejemplo se crea una relación de recuperación ante desastres de SnapMirror mediante el método personalizado `my_mirror` política:

   ```
   cluster_dst::> snapmirror create -source-path svm_1:volA_dst
   -destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
   -policy my_mirror
   ```

Después de terminar

Utilice la `snapmirror show` Comando para verificar que la relación de SnapMirror se ha creado. Para obtener una sintaxis de comando completa, consulte la página man.

Inicializar una relación de replicación

Para todos los tipos de relaciones, la inicialización realiza una *transferencia_de base*: Realiza una copia Snapshot del volumen de origen y, a continuación, transfiere esa copia y todos los bloques de datos a los que hace referencia al volumen de destino.

Antes de empezar

- ONTAP debe haber accesible desde el nodo Element que contiene el volumen que se va a replicar.
- El volumen de Element debe estar habilitado para la replicación de SnapMirror.
- Si utiliza el tipo de política «mirror-vault», debe haber configurado una etiqueta de SnapMirror para que se repliquen las copias Snapshot de Element.

Acerca de esta tarea

Debe especificar la ruta de origen del elemento en el formulario `hostip:/lun/name`, donde «'lun'» es la cadena real «'lun'» y. `name` Es el nombre del volumen de Element.

La inicialización puede requerir mucho tiempo. Puede ser conveniente ejecutar la transferencia básica en horas de menor actividad.

> Si la inicialización de una relación desde un origen de ONTAP a un destino de Element genera errores por cualquier motivo, seguirá presentando errores incluso después de haber corregido el problema (un nombre de LUN no válido, por ejemplo). La solución es la siguiente:
>
> 1. Eliminar la relación.
> 2. Elimine el volumen de destino de Element.
> 3. Cree un nuevo volumen de destino de Element.
> 4. Cree e inicialice una nueva relación desde el origen de ONTAP hasta el volumen de destino de Element.

Paso

1. Inicializar una relación de replicación:

   `snapmirror initialize -source-path hostip:/lun/name -destination-path SVM:volume|cluster://SVM/volume`

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el siguiente ejemplo, se inicializa la relación entre el volumen de origen `0005` En la dirección IP 10.0.0.11 y el volumen de destino `volA_dst` encendido `svm_backup`:

   ```
   cluster_dst::> snapmirror initialize -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

Proporcione datos desde un volumen de destino de recuperación ante desastres de SnapMirror

Haga que el volumen de destino sea modificable

Cuando el desastre deshabilita el sitio principal para una relación de recuperación ante desastres de SnapMirror, puede proporcionar datos del volumen de destino con una interrupción mínima. Se puede reactivar el volumen de origen cuando el servicio se restaura en el sitio primario.

Debe hacer que el volumen de destino sea editable, para poder proporcionar datos del volumen a los clientes. Puede utilizar el `snapmirror quiesce` comando para detener las transferencias programadas al destino, el `snapmirror abort` comando para detener las transferencias continuas y el `snapmirror break` comando para hacer que el destino sea editable.

Acerca de esta tarea

Debe especificar la ruta de origen del elemento en el formulario *`hostip:`*`/lun/`*`name`*, donde «'lun'» es la cadena real «'lun'» y. `name` Es el nombre del volumen de Element.

Pasos

1. Detenga las transferencias programadas al destino:

   `snapmirror quiesce -source-path` *`hostip:`*`/lun/`*`name`* `-destination-path` *`SVM:volume`* `|`*`cluster://SVM/volume`*

   Para obtener una sintaxis de comando completa, consulte la página man.

   El siguiente ejemplo detiene las transferencias programadas entre el volumen de origen `0005` En la dirección IP 10.0.0.11 y el volumen de destino `volA_dst` encendido `svm_backup`:

   ```
   cluster_dst::> snapmirror quiesce -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

2. Detenga las transferencias continuas al destino:

   `snapmirror abort -source-path` *`hostip:`*`/lun/`*`name`* `-destination-path` *`SVM:volume`* `|`*`cluster://SVM/volume`*

   Para obtener una sintaxis de comando completa, consulte la página man.

   El siguiente ejemplo detiene las transferencias continuas entre el volumen de origen `0005` En la dirección IP 10.0.0.11 y el volumen de destino `volA_dst` encendido `svm_backup`:

   ```
   cluster_dst::> snapmirror abort -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

3. Rompa la relación de recuperación ante desastres de SnapMirror:

   `snapmirror break -source-path` *`hostip:`*`/lun/`*`name`* `-destination-path` *`SVM:volume`* `|`*`cluster://SVM/volume`*

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el siguiente ejemplo, se rompe la relación entre el volumen de origen `0005` En la dirección IP 10.0.0.11 y el volumen de destino `volA_dst` encendido `svm_backup` y el volumen de destino `volA_dst` encendido `svm_backup`:

```
cluster_dst::> snapmirror break -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst
```

Configure el volumen de destino para acceder a los datos

Tras hacer que el volumen de destino sea editable, debe configurar el volumen para el acceso a los datos. Los hosts SAN pueden acceder a los datos desde el volumen de destino hasta que se reactive el volumen de origen.

1. Asigne la LUN de Element al iGroup correspondiente.
2. Crear sesiones iSCSI desde los iniciadores de host SAN a los LIF DE SAN.
3. En el cliente SAN, realice una nueva exploración del almacenamiento para detectar la LUN conectada.

Vuelva a activar el volumen de origen original

Puede restablecer la relación de protección de datos original entre los volúmenes de origen y destino cuando ya no necesite servir datos desde el destino.

Acerca de esta tarea

En el siguiente procedimiento se asume que la línea base del volumen de origen original está intacta. Si la base de referencia no está intacta, debe crear e inicializar la relación entre el volumen desde el que se sirven datos y el volumen de origen original antes de realizar el procedimiento.

Debe especificar la ruta de origen del elemento en el formulario `hostip:/lun/name`, donde «'lun'» es la cadena real «'lun'» y. `name` Es el nombre del volumen de Element.

A partir de ONTAP 9.4, las copias Snapshot de una LUN creada mientras ofrece datos del destino de ONTAP se replican automáticamente cuando la fuente de Element se reactiva.

Las reglas de replicación son las siguientes:

- Solo se admiten LUN iSCSI.
- No es posible replicar más de un LUN desde un volumen de ONTAP a un volumen de Element.
- No es posible replicar un LUN desde un volumen de ONTAP a varios volúmenes de Element.

Pasos

1. Elimine la relación de protección de datos original:

   `snapmirror delete -source-path SVM:volume|cluster://SVM/volume -destination -path hostip:/lun/name -policy policy`

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el siguiente ejemplo, se elimina la relación entre el volumen de origen original, `0005` En la dirección IP 10.0.0.11 y el volumen desde el que se proporcionan datos, `volA_dst` encendido `svm_backup`:

```
cluster_dst::> snapmirror delete -source-path 10.0.0.11:/lun/0005
-policy MirrorLatest -destination-path svm_backup:volA_dst
```

2. Invierta la relación de protección de datos original:

   `snapmirror resync -source-path` *`SVM:volume|cluster://SVM/volume`* `-destination -path` *`hostip:`*`/lun/`*`name -policy policy`*

   Para obtener una sintaxis de comando completa, consulte la página man.

   Aunque la resincronización no requiere una transferencia básica, puede requerir mucho tiempo. Puede que desee ejecutar la resincronización en horas de menor actividad.

   En el siguiente ejemplo, se revierte la relación entre el volumen de origen original, `0005` En la dirección IP 10.0.0.11 y el volumen desde el que se proporcionan datos, `volA_dst` encendido `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
```

3. Actualice la relación de inversión:

   `snapmirror update -source-path` *`SVM:volume|cluster://SVM/volume`* `-destination -path` *`hostip:`*`/lun/`*`name`

   Para obtener una sintaxis de comando completa, consulte la página man.

   > El comando genera errores si no existe una copia Snapshot común en el origen y el destino. Uso `snapmirror initialize` para volver a inicializar la relación.

   En el siguiente ejemplo, se actualiza la relación entre el volumen desde el que se proporcionan datos, `volA_dst` encendido `svm_backup`, y el volumen de origen original, `0005` En la dirección IP 10.0.0.11:

```
cluster_dst::> snapmirror update -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

4. Detenga las transferencias programadas para la relación de inversión:

   `snapmirror quiesce -source-path` *`SVM:volume|cluster://SVM/volume`* `-destination -path` *`hostip:`*`/lun/`*`name`

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el siguiente ejemplo, se detienen las transferencias programadas entre el volumen desde el que se proporcionan datos: `volA_dst` encendido `svm_backup`, y el volumen de origen original, `0005` En la dirección IP 10.0.0.11:

```
cluster_dst::> snapmirror quiesce -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

5. Detenga las transferencias continuas para la relación de inversión:

   `snapmirror abort -source-path` *`SVM:volume|cluster://SVM/volume`* `-destination -path` *`hostip:`*`/lun/`*`name`*

   Para obtener una sintaxis de comando completa, consulte la página man.

   El ejemplo siguiente detiene las transferencias continuas entre el volumen desde el que ofrece datos, `volA_dst` encendido `svm_backup`, y el volumen de origen original, `0005` En la dirección IP 10.0.0.11:

```
cluster_dst::> snapmirror abort -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

6. Rompa la relación inversa:

   `snapmirror break -source-path` *`SVM:volume|cluster://SVM/volume`* `-destination -path` *`hostip:`*`/lun/`*`name`*

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el siguiente ejemplo, se rompe la relación entre el volumen desde el que se proporcionan datos, `volA_dst` encendido `svm_backup`, y el volumen de origen original, `0005` En la dirección IP 10.0.0.11:

```
cluster_dst::> snapmirror break -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

7. Elimine las relaciones de protección de datos revertidas:

   `snapmirror delete -source-path` *`SVM:volume|cluster://SVM/volume`* `-destination -path` *`hostip`*`:/lun/`*`name`* `-policy` *`policy`*

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el siguiente ejemplo, se elimina la relación inversa entre el volumen de origen original, `0005` En la dirección IP 10.0.0.11 y el volumen desde el que se proporcionan datos, `volA_dst` encendido `svm_backup`:

```
cluster_src::> snapmirror delete -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
```

8. Restablezca la relación de protección de datos original:

   `snapmirror resync -source-path` *`hostip`*`:/lun/`*`name`* `-destination-path`

SVM:volume|cluster://SVM/volume

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo, se restablece la relación entre el volumen de origen original, `0005` En la dirección IP 10.0.0.11, y el volumen de destino original, `volA_dst` encendido `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst
```

Después de terminar

Utilice la `snapmirror show` Comando para verificar que la relación de SnapMirror se ha creado. Para obtener una sintaxis de comando completa, consulte la página man.

Actualice manualmente una relación de replicación

Es posible que deba actualizar una relación de replicación manualmente si falla una actualización debido a un error de red.

Acerca de esta tarea

Debe especificar la ruta de origen del elemento en el formulario *hostip:*/lun/*name*, donde «'lun'» es la cadena real «'lun'» y. `name` Es el nombre del volumen de Element.

Pasos

1. Actualice manualmente una relación de replicación:

   snapmirror update -source-path *hostip:*/lun/*name* -destination-path *SVM:volume|cluster://SVM/volume*

   Para obtener una sintaxis de comando completa, consulte la página man.

   > El comando genera errores si no existe una copia Snapshot común en el origen y el destino. Uso `snapmirror initialize` para volver a inicializar la relación.

   En el ejemplo siguiente se actualiza la relación entre el volumen de origen `0005` En la dirección IP 10.0.0.11 y el volumen de destino `volA_dst` encendido `svm_backup`:

   ```
   cluster_src::> snapmirror update -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

Resincronice una relación de replicación

Es necesario volver a sincronizar una relación de replicación después de hacer que un volumen de destino sea modificable, después de un error en la actualización porque no existe una copia Snapshot común en los volúmenes de origen y destino o si desea cambiar la política de replicación de la relación.

Acerca de esta tarea

Aunque la resincronización no requiere una transferencia básica, puede requerir mucho tiempo. Puede que desee ejecutar la resincronización en horas de menor actividad.

Debe especificar la ruta de origen del elemento en el formulario `hostip:/lun/name`, donde «'lun'» es la cadena real «'lun'» y. `name` Es el nombre del volumen de Element.

Paso

1. Resincronización de los volúmenes de origen y destino:

   `snapmirror resync -source-path hostip:/lun/name -destination-path SVM:volume |cluster://SVM/volume -type XDP -policy policy`

   Para obtener una sintaxis de comando completa, consulte la página man.

   En el siguiente ejemplo, vuelva a establecer la relación entre el volumen de origen `0005` En la dirección IP 10.0.0.11 y el volumen de destino `volA_dst` encendido `svm_backup`:

   ```
   cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005
   -policy MirrorLatest -destination-path svm_backup:volA_dst
   ```