



# **Crear y solucionar problemas de relaciones de protección**

**Active IQ Unified Manager 9.13**

NetApp  
December 18, 2023

# Tabla de contenidos

- Creación, supervisión y solución de problemas de relaciones de protección ..... 1
  - Tipos de protección SnapMirror ..... 1
  - Configuración de las relaciones de protección en Unified Manager ..... 3
  - Recuperación tras fallos y recuperación de una relación de protección ..... 5
  - Solucionar un error de un trabajo de protección ..... 10
  - Resolución de problemas de desfase ..... 13

# Creación, supervisión y solución de problemas de relaciones de protección

Unified Manager permite crear relaciones de protección, supervisar y solucionar problemas de protección de reflejos y protección de almacén de backup de los datos almacenados en clústeres gestionados, así como restaurar datos cuando se sobrescriben o se pierden.

## Tipos de protección SnapMirror

Según la puesta en marcha de la topología de almacenamiento de datos, Unified Manager permite configurar varios tipos de relaciones de protección de SnapMirror. Todas las variaciones de la protección de SnapMirror ofrecen protección de recuperación tras fallos, pero ofrecen distintas funcionalidades en cuanto a rendimiento, flexibilidad de versiones y protección de backups múltiples.

### Relaciones de protección asíncrona de SnapMirror tradicionales

La protección asíncrona de SnapMirror tradicional proporciona protección con mirroring de replicación en bloques entre los volúmenes de origen y de destino.

En las relaciones de SnapMirror tradicionales, las operaciones de mirroring se ejecutan más rápido de lo que tendrían en relaciones de SnapMirror alternativas, ya que la operación de mirroring se basa en la replicación por bloques. Sin embargo, la protección SnapMirror tradicional requiere que el volumen de destino se ejecute con la misma versión secundaria o posterior del software ONTAP que el volumen de origen en la misma versión principal (por ejemplo, la versión 8.x a la 8.x o de 9.x a 9.x). No se admite la replicación de un origen 9.1 a un destino 9.0 porque el destino ejecuta una versión principal anterior.

### Protección asíncrona de SnapMirror con replicación de versión flexible

La protección asíncrona de SnapMirror con la replicación flexible de versiones proporciona protección de reflejos de replicación lógica entre volúmenes de origen y de destino, incluso si dichos volúmenes se ejecutan en versiones diferentes de ONTAP 8.3 o posteriores (por ejemplo, de la versión 8.3 a la 8.3.1, o de 8.3 a 9.1, o de 9.2.2 a 9.2).

En las relaciones de SnapMirror con una replicación de versión flexible, las operaciones de mirroring no se ejecutan con la misma rapidez que en las relaciones tradicionales de SnapMirror.

Debido a una ejecución más lenta, SnapMirror con protección de replicación flexible de versión no es adecuado de ninguna de las siguientes circunstancias:

- El objeto de origen contiene más de 10 millones de archivos que proteger.
- El objetivo de punto de recuperación de los datos protegidos es de dos horas o menos. (Es decir, el destino siempre debe contener datos duplicados y recuperables, que tengan una antigüedad superior a dos horas respecto a los datos de origen).

En una de las circunstancias indicadas, se requiere la ejecución más rápida basada en replicación por bloques de la protección SnapMirror predeterminada.

## Protección asíncrona de SnapMirror con la replicación con versión flexible y la opción de backup

La protección asíncrona de SnapMirror con la opción de backup y replicación flexible con versión proporciona protección mediante mirroring entre volúmenes de origen y de destino, y la posibilidad de almacenar varias copias de los datos reflejados en el destino.

El administrador de almacenamiento puede especificar qué copias Snapshot se reflejan de un origen a un destino y también puede especificar el tiempo que debe retener esas copias en el destino, incluso si se eliminan en el origen.

En las relaciones de SnapMirror con una opción de backup y replicación de versión flexible, las operaciones de mirroring no se ejecutan con la misma rapidez que en las relaciones tradicionales de SnapMirror.

## Replicación unificada de SnapMirror (mirroring y almacén)

La replicación unificada de SnapMirror le permite configurar la recuperación ante desastres y el archivado en el mismo volumen de destino. Al igual que sucede con SnapMirror, la protección de datos unificada realiza una transferencia de referencia la primera vez que se invoca. Una transferencia básica con la política de protección de datos unificada predeterminada «MirrorAndVault» hace una copia Snapshot del volumen de origen y, a continuación, transfiere dicha copia y los bloques de datos a los que hace referencia al volumen de destino. Al igual que SnapVault, la protección de datos unificada no incluye copias Snapshot anteriores en la referencia.

## Protección de SnapMirror Synchronous con una sincronización estricta

La protección SnapMirror Synchronous con sincronización «esencial» garantiza que los volúmenes primario y secundario siempre sean una copia real del otro. Si se produce un fallo de replicación al intentar escribir datos en el volumen secundario, las operaciones de I/O del cliente en el volumen primario se interrumpen.

## Protección de SnapMirror Synchronous con sincronización normal

La protección de SnapMirror Synchronous con sincronización «relativamente» no requiere que el volumen primario y el secundario siempre sean una copia real del otro, lo que garantiza la disponibilidad del volumen primario. Si se produce un fallo de replicación al intentar escribir datos en el volumen secundario, los volúmenes primario y secundario quedan sin sincronizar y la I/O del cliente continuará en el volumen primario.



El botón Restaurar y los botones de operación de relación no están disponibles al supervisar las relaciones de protección síncrona en la vista Estado: Todos los volúmenes o la página de detalles volumen / Estado.

## Continuidad del negocio de SnapMirror Synchronous

La función de continuidad del negocio de SnapMirror (SM-BC) está disponible con ONTAP 9.8 y versiones posteriores, y puede usarla para proteger las aplicaciones con LUN, lo que permite que las aplicaciones se conmute de forma transparente y garantiza la continuidad del negocio en caso de desastre.

Permite detectar y supervisar las relaciones síncronas de SnapMirror para los grupos de consistencia (CG) disponibles en los clústeres y las máquinas virtuales de almacenamiento de Unified Manager. SM-BC es compatible en clústeres AFF o clústeres de cabina All SAN (ASA), donde los clústeres principal y secundario pueden ser AFF o ASA. SM-BC protege las aplicaciones con LUN iSCSI o FCP.

Cuando se ven los volúmenes y las LUN protegidos por la relación SM-BC, puede obtener una vista unificada

de las relaciones de protección, los grupos de coherencia en el inventario de volúmenes, ver la topología de la protección para las relaciones de grupos de coherencia, ver datos históricos de las relaciones de grupos de coherencia de hasta un año. También puede descargar el informe. También se puede ver el resumen de las relaciones del grupo de coherencia, buscar el soporte de las relaciones del grupo de coherencia y obtener información sobre los volúmenes que está protegido por el grupo de coherencia.

En la página Relationships, también se puede ordenar, filtrar y extender la protección en los objetos de almacenamiento de origen y destino, y su relación que está protegida por el grupo de coherencia.

Si quiere más información sobre la continuidad del negocio de SnapMirror síncrono, consulte ["Documentación de ONTAP 9 para SM-BC"](#).

## Configuración de las relaciones de protección en Unified Manager

Hay varios pasos que debe realizar para usar Unified Manager y OnCommand Workflow Automation a fin de configurar las relaciones de SnapMirror y SnapVault para proteger sus datos.

### Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber establecido relaciones entre iguales entre dos clústeres o dos máquinas virtuales de almacenamiento (SVM).
- OnCommand Workflow Automation debe integrarse con Unified Manager:
  - ["Configure OnCommand Workflow Automation"](#).
  - ["Verificación del almacenamiento en caché de origen de datos de Unified Manager en Workflow Automation"](#).

### Pasos

1. Según el tipo de relación de protección que desee crear, realice una de las siguientes acciones:
  - ["Cree una relación de protección de SnapMirror"](#).
  - ["Cree una relación de protección SnapVault"](#).
2. Si desea crear una directiva para la relación, en función del tipo de relación que esté creando, realice una de las siguientes acciones:
  - ["Cree una política de SnapVault"](#).
  - ["Cree una política de SnapMirror"](#).
3. ["Cree una programación de SnapMirror o SnapVault"](#).

## Configuración de una conexión entre Workflow Automation y Unified Manager

Puede configurar una conexión segura entre OnCommand Workflow Automation (WFA) y Unified Manager. La conexión a Workflow Automation le permite usar funciones de protección como flujos de trabajo de configuración de SnapMirror y SnapVault, así como comandos para gestionar las relaciones de SnapMirror.

### Lo que necesitará

- La versión instalada de Workflow Automation debe ser 5.1 o superior.



El «paquete WFA para gestionar Clustered Data ONTAP» se incluye en WFA 5.1, por lo que no es necesario descargar este paquete del almacén de automatización del almacenamiento de NetApp e instalarlo por separado en su servidor WFA, tal y como se requería en el pasado. ["PAQUETE WFA para gestionar ONTAP"](#)

- Debe tener el nombre del usuario de la base de datos que ha creado en Unified Manager para admitir conexiones de WFA y Unified Manager.

Este usuario de la base de datos debe haber sido asignado el rol de usuario del Esquema de integración.

- Debe tener asignado la función de administrador o de arquitecto en Workflow Automation.
- Debe tener la dirección de host, el número de puerto 443, el nombre de usuario y la contraseña para la configuración de Workflow Automation.
- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

## Pasos

1. En el panel de navegación izquierdo, haga clic en **General > Workflow Automation**.
2. En el área **Usuario de base de datos** de la página **Automatización de flujos de trabajo**, seleccione el nombre e introduzca la contraseña del usuario de base de datos que creó para admitir conexiones de Unified Manager y Workflow Automation.
3. En el área **Workflow Automation Credentials** de la página, introduzca el nombre de host o la dirección IP (IPv4 o IPv6) y el nombre de usuario y la contraseña para la configuración de Workflow Automation.

Debe usar el puerto del servidor de Unified Manager (puerto 443).

4. Haga clic en **Guardar**.
5. Si utiliza un certificado autofirmado, haga clic en **Sí** para autorizar el certificado de seguridad.

Se mostrará la página Workflow Automation.

6. Haga clic en **Sí** para volver a cargar la interfaz de usuario web y agregar las funciones de Workflow Automation.

## Información relacionada

["Documentación de NetApp: OnCommand Workflow Automation \(versiones actuales\)"](#)

## Verificación del almacenamiento en caché de origen de datos de Unified Manager en Workflow Automation

Puede determinar si el almacenamiento en caché de origen de datos de Unified Manager funciona correctamente comprobando si la adquisición del origen de datos se ha realizado correctamente en Workflow Automation. Puede hacerlo cuando se integre Workflow Automation con Unified Manager para garantizar que la funcionalidad Workflow Automation esté disponible después de la integración.

## Lo que necesitará

Para realizar esta tarea, debe tener asignado la función Administrador o la función Arquitecto de Workflow

Automation.

### **Pasos**

1. En la interfaz de usuario de Workflow Automation, seleccione **ejecución > orígenes de datos**.
2. Haga clic con el botón derecho del ratón en el nombre del origen de datos de Unified Manager y, a continuación, seleccione **adquirir ahora**.
3. Compruebe que la adquisición se realiza correctamente sin errores.

Para que la integración de Workflow Automation en Unified Manager se tenga éxito, es necesario resolver los errores de adquisición.

## **Qué ocurre cuando se vuelve a instalar o actualizar OnCommand Workflow Automation**

Antes de reinstalar o actualizar OnCommand Workflow Automation, primero debe quitar la conexión entre OnCommand Workflow Automation y Unified Manager y asegurarse de que se hayan detenido todos los trabajos programados o en ejecución actualmente de OnCommand Workflow Automation.

También debe eliminar manualmente Unified Manager de OnCommand Workflow Automation.

Después de reinstalar o actualizar OnCommand Workflow Automation, debe configurar de nuevo la conexión con Unified Manager.

## **Se elimina la configuración de OnCommand Workflow Automation de Unified Manager**

Puede eliminar la configuración de OnCommand Workflow Automation de Unified Manager cuando ya no desee usar Workflow Automation.

### **Lo que necesitará**

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

### **Pasos**

1. En el panel de navegación izquierdo, haga clic en **General > Workflow Automation** en el menú de configuración izquierdo.
2. En la página **Workflow Automation**, haga clic en **Eliminar configuración**.

## **Recuperación tras fallos y recuperación de una relación de protección**

Cuando se deshabilita un volumen de origen en la relación de protección debido a un error de hardware o un desastre, se pueden usar las funciones de relaciones de protección en Unified Manager para que el destino de la protección sea accesible de lectura/escritura y se pueda conmutar por error a ese volumen hasta que el origen vuelva a estar en línea; a continuación, puede volver a la fuente original cuando esté disponible para servir datos.

## Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado OnCommand Workflow Automation para realizar esta operación.

## Pasos

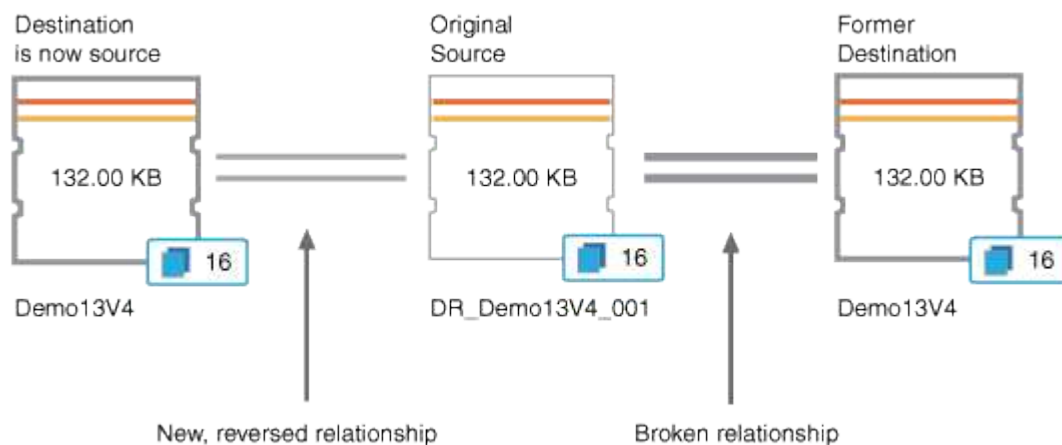
### 1. "Rompa la relación de SnapMirror".

Se debe romper la relación antes de convertir el destino de un volumen de protección de datos a un volumen de lectura/escritura, y antes de poder revertir la relación.

### 2. "Invierta la relación de protección".

Cuando el volumen de origen original vuelva a estar disponible, se puede decidir restablecer la relación de protección original mediante la restauración del volumen de origen. Para poder restaurar el origen, debe sincronizarlo con los datos escritos en el destino anterior. Utiliza la operación de resincronización inversa para crear una nueva relación de protección mediante la reversión de los roles de la relación original y la sincronización del volumen de origen con el destino anterior. Se crea una nueva copia Snapshot de referencia para la nueva relación.

La relación inversa tiene un aspecto similar a una relación en cascada:



### 3. "Rompa la relación de SnapMirror invertida".

Cuando se resincronizaba el volumen de origen original y se pueden volver a servir datos, use la operación de interrupción para romper la relación inversa.

### 4. "Eliminar la relación".

Cuando la relación inversa ya no sea necesaria, debe eliminar dicha relación antes de volver a establecer la relación original.

### 5. "Resincronice la relación".

Utilice la operación Resynchronize para sincronizar los datos del origen con el destino y restablecer la relación original.



## Romper una relación de SnapMirror en la página de detalles Volume/Health

Es posible interrumpir una relación de protección en la página de detalles Volume/Health y detener las transferencias de datos entre un volumen de origen y un volumen de destino en una relación de SnapMirror. Puede romper una relación cuando desea migrar datos, para la recuperación ante desastres o para la prueba de aplicaciones. El volumen de destino se cambia a un volumen de lectura/escritura. No es posible interrumpir una relación de SnapVault.

### Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation.

### Pasos

1. En la pestaña **Protección** de la página de detalles **volumen / Salud**, seleccione en la topología la relación de SnapMirror que desea romper.
2. Haga clic con el botón derecho del ratón en el destino y seleccione **romper** en el menú.

Se muestra el cuadro de diálogo romper relación.

3. Haga clic en **continuar** para romper la relación.
4. En la topología, compruebe que la relación está rota.

## Inversión de las relaciones de protección desde la página de detalles volumen / Estado

Cuando un desastre deshabilita el volumen de origen en la relación de protección, es posible usar el volumen de destino para suministrar datos mediante la conversión a lectura/escritura mientras se repara o se reemplaza el origen. Cuando el origen vuelve a estar disponible para recibir datos, puede utilizar la operación de resincronización inversa para establecer la relación en la dirección inversa y sincronizar los datos del origen con los datos en el destino de lectura/escritura.

### Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation.
- La relación no debe ser una relación de SnapVault.
- Debe haber una relación de protección.
- La relación de protección debe romperse.
- El origen y el destino deben estar en línea.
- El origen no debe ser el destino de otro volumen de protección de datos.
- Cuando realiza esta tarea, se eliminan los datos en el origen más nuevos que los de la copia Snapshot común.
- Las políticas y las programaciones creadas en la relación de resincronización inversa son las mismas que

en la relación de protección original.

Si no existen las políticas y las programaciones, se crean.

### Pasos

1. En la ficha **Protección** de la página de detalles **volumen / Salud**, busque en la topología la relación de SnapMirror en la que desea invertir el origen y el destino y haga clic con el botón derecho del ratón en él.
2. Seleccione **Reverse Resync** en el menú.

Se muestra el cuadro de diálogo Reverse Resync.

3. Compruebe que la relación mostrada en el cuadro de diálogo **Resync. Inversa** es la que desea realizar la operación de resincronización inversa y, a continuación, haga clic en **Enviar**.

Se cierra el cuadro de diálogo Reverse Resync y se muestra un enlace del trabajo en la parte superior de la página de detalles Volume/Health.

4. **Opcional:** haga clic en **Ver trabajos** en la página de detalles **volumen / Salud** para realizar un seguimiento del estado de cada trabajo de resincronización inversa.

Se muestra una lista filtrada de trabajos.

5. **Opcional:** haga clic en la flecha **Atrás** de su navegador para volver a la página de detalles **volumen / Salud**.

La operación de resincronización inversa se finaliza cuando todas las tareas de trabajo se completaron correctamente.

## Eliminación de una relación de protección de la página de detalles Volume / Health

Puede quitar una relación de protección para eliminar de forma permanente una relación existente entre el origen y el destino seleccionados: Por ejemplo, cuando desea crear una relación con otro destino. Esta operación elimina todos los metadatos y no puede deshacerse.

### Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation.

### Pasos

1. En la ficha **Protección** de la página de detalles **volumen / Estado**, seleccione en la topología la relación de SnapMirror que desee eliminar.
2. Haga clic con el botón derecho del ratón en el nombre del destino y seleccione **Quitar** en el menú.

Se muestra el cuadro de diálogo Eliminar relación.

3. Haga clic en **continuar** para eliminar la relación.

La relación se elimina de la página de detalles Volume/Health.

## Resincronizando las relaciones de protección desde la página de detalles Volume / Health

Puede volver a sincronizar los datos de una relación de SnapMirror o SnapVault que se rompió y, a continuación, el destino se hizo de lectura/escritura para que los datos del origen coincidan con los del destino. También es posible resincronizar cuando se elimina una copia Snapshot común requerida en el volumen de origen, y esto provoca errores en las actualizaciones de SnapMirror o SnapVault.

### Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado OnCommand Workflow Automation.

### Pasos

1. En la ficha **Protección** de la página de detalles **volumen / Salud**, busque en la topología la relación de protección que desea volver a sincronizar y haga clic con el botón derecho del ratón en ella.
2. Seleccione **Resynchronize** en el menú.

Como alternativa, en el menú **acciones**, seleccione **relación > Resincronizar** para volver a sincronizar la relación para la que está viendo los detalles.

Aparecerá el cuadro de diálogo Resynchronize.

3. En la pestaña **Opciones de resincronización**, seleccione una prioridad de transferencia y la tasa de transferencia máxima.
4. Haga clic en **copias Snapshot de origen**; a continuación, en la columna **copia Snapshot**, haga clic en **predeterminado**.

Se muestra el cuadro de diálogo Seleccionar copia Snapshot de origen.

5. Si desea especificar una copia Snapshot existente en lugar de transferir la copia Snapshot predeterminada, haga clic en **copia Snapshot existente** y seleccione una copia Snapshot de la lista.
6. Haga clic en **Enviar**.

Volverá al cuadro de diálogo Resynchronize.

7. Si ha seleccionado más de un origen para volver a sincronizar, haga clic en **predeterminado** para el siguiente origen para el que desea especificar una copia Snapshot existente.
8. Haga clic en **Enviar** para iniciar el trabajo de resincronización.

El trabajo de resincronización se inició, regresará a la página de detalles Volume / Health y se mostrará un enlace de trabajos en la parte superior de la página.

9. **Opcional:** haga clic en **Ver trabajos** en la página **volumen / Detalles de la salud** para realizar un seguimiento del estado de cada trabajo de resincronización.

Se muestra una lista filtrada de trabajos.

10. **Opcional:** haga clic en la flecha **Atrás** de su navegador para volver a la página de detalles **volumen / Salud**.

El trabajo de resincronización finaliza cuando se completan correctamente todas las tareas de trabajo.

## Solucionar un error de un trabajo de protección

Este flujo de trabajo proporciona un ejemplo de cómo se puede identificar y resolver un error de trabajo de protección en la consola de Unified Manager.

### Lo que necesitará

Debido a que algunas tareas de este flujo de trabajo requieren que inicie sesión utilizando la función Administrador, debe estar familiarizado con las funciones necesarias para utilizar varias funciones.

En este caso, debe acceder a la página Dashboard para ver si hay algún problema con los trabajos de protección. En el área incidente de protección, se observa que hay un incidente de trabajo terminado, mostrando un error de trabajo de protección en un volumen. Investiga este error para determinar la causa posible y la resolución potencial.

### Pasos

1. En el panel Protection Incidents del área Dashboard Unresolved Incidents and Risks, haga clic en el evento **Protection job failed**.



El texto vinculado para el evento se escribe en el formulario

```
object_name:/object_name - Error Name, por ejemplo  
cluster2_src_svm:/cluster2_src_vol2 - Protection Job Failed.
```

Se muestra la página de detalles Event del trabajo de protección con errores.

2. Revise el mensaje de error en el campo causa del área **Resumen** para determinar el problema y evaluar las posibles acciones correctivas.

Consulte "[Identificar el problema y realizar acciones correctivas para un trabajo de protección con errores](#)".

## Identificar el problema y realizar acciones correctivas para un trabajo de protección con errores

Revisa el mensaje de error de error de trabajo en el campo CAUSE de la página de detalles Event y determina que el trabajo ha fallado debido a un error de copia de Snapshot. Luego continúa a la página de detalles Volume / Health para recopilar más información.

### Lo que necesitará

Debe tener la función Administrador de aplicaciones.

El mensaje de error proporcionado en el campo causa de la página de detalles Event contiene el siguiente texto sobre el trabajo con errores:

```
Protection Job Failed. Reason: (Transfer operation for
relationship 'cluster2_src_svm:cluster2_src_vol2->cluster3_dst_svm:
managed_svc2_vol3' ended unsuccessfully. Last error reported by
Data ONTAP: Failed to create Snapshot copy 0426cluster2_src_vol2snap
on volume cluster2_src_svm:cluster2_src_vol2. (CSM: An operation
failed due to an ONC RPC failure.)
Job Details
```

Este mensaje proporciona la siguiente información:

- Un trabajo de backup o reflejo no se completó correctamente.

El trabajo implicaba una relación de protección entre el volumen de origen `cluster2_src_vol2` en el servidor virtual `cluster2_src_svm` y el volumen de destino `managed_svc2_vol3` en el servidor virtual llamado `cluster3_dst_svm`.

- Error de un trabajo de copia Snapshot para `0426cluster2_src_vol2snap` en el volumen de origen `cluster2_src_svm:/cluster2_src_vol2`.

En este caso, puede identificar la causa y las posibles acciones correctivas del error del trabajo. Sin embargo, para resolver el fallo es necesario acceder a la interfaz de usuario web de System Manager o a los comandos de la CLI de ONTAP.

## Pasos

1. Revisa el mensaje de error y determina que ha producido un error en un trabajo de copia Snapshot en el volumen de origen, lo que indica que probablemente haya un problema con el volumen de origen.

Si lo desea, puede hacer clic en el enlace **Detalles del trabajo** al final del mensaje de error, pero a efectos de este escenario, elige no hacerlo.

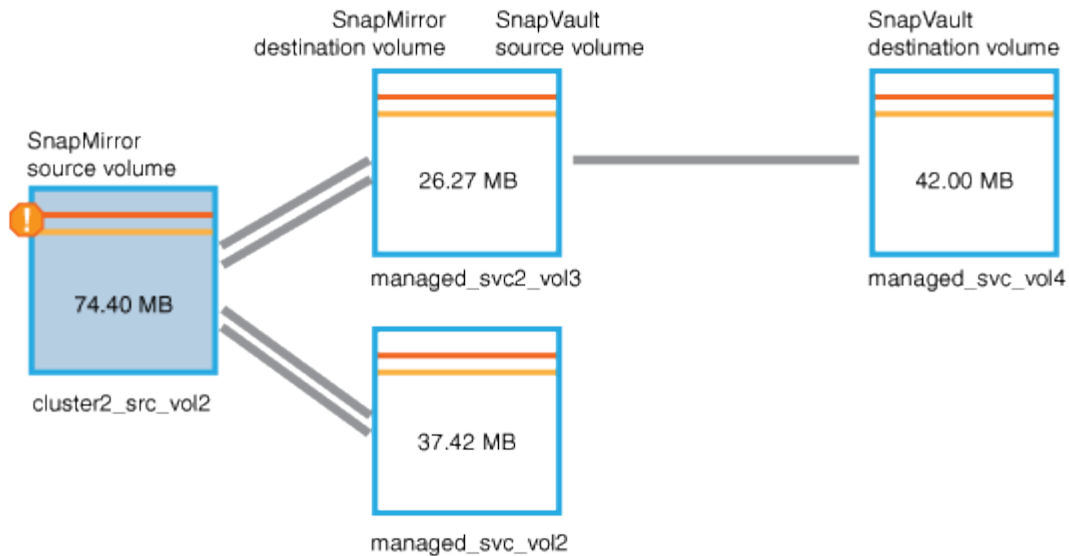
2. Decide que desea intentar resolver el evento, de modo que haga lo siguiente:
  - a. Haga clic en el botón **asignar a** y seleccione **Me** en el menú.
  - b. Haga clic en el botón **Confirmar** para que no siga recibiendo notificaciones de alerta de repetición, si se han configurado alertas para el evento.
  - c. Opcionalmente, también puede agregar notas sobre el evento.
3. Haga clic en el campo **Fuente** del panel **Resumen** para ver detalles sobre el volumen de origen.

El campo **origen** contiene el nombre del objeto de origen: En este caso, el volumen en el que se programó el trabajo de copia Snapshot.

Se muestra la página de detalles volumen / Estado para `cluster2_src_vol2`, que muestra el contenido de la ficha Protección .

4. Al ver el gráfico de topología de protección, se muestra un icono de error asociado con el primer volumen de la topología, que es el volumen de origen de la relación de SnapMirror.

También puede ver las barras horizontales en el icono de volumen de origen, que indican los umbrales de advertencia y error definidos para ese volumen.



5. Coloque el cursor sobre el icono de error para ver el cuadro de diálogo emergente que muestra la configuración del umbral y ver que el volumen ha superado el umbral de error, lo que indica un problema de capacidad.

6. Haga clic en la ficha **capacidad**.

Información de capacidad acerca de volumen `cluster2_src_vol2` pantallas.

7. En el panel **capacidad**, verá que hay un icono de error en el gráfico de barras, indicando de nuevo que la capacidad del volumen ha superado el nivel de umbral establecido para el volumen.

8. Debajo del gráfico de capacidad, puede ver que se deshabilitó el crecimiento automático del volumen y que se estableció una garantía de espacio de volumen.

Se puede decidir habilitar el crecimiento automático, pero para los fines de este escenario, se decide investigar más antes de tomar una decisión sobre cómo resolver el problema de capacidad.

9. Desplácese hacia abajo hasta la lista **Eventos** y vea que se generaron eventos error de trabajo de protección, volumen días hasta lleno y espacio de volumen lleno.

10. En la lista **Eventos**, usted hace clic en el evento **espacio de volumen lleno** para obtener más información, habiendo decidido que este evento parece más relevante para su problema de capacidad.

La página de detalles Event muestra el evento Volume Space Full para el volumen de origen.

11. En el área **Resumen**, lee el campo causa del evento: The full threshold set at 90% is breached. 45.38 MB (95.54%) of 47.50 MB is used.

12. Debajo del área Resumen, verá acciones correctivas sugeridas.



Las acciones correctivas sugeridas se muestran solo para algunos eventos, de modo que no se ve esta área para todos los tipos de eventos.

Haga clic en la lista de acciones sugeridas que puede realizar para resolver el evento Volume Space Full:

- Habilite el crecimiento automático en este volumen.
- Cambie el tamaño del volumen.
- Habilite y ejecute la deduplicación en este volumen.

- Habilite y ejecute la compresión en este volumen.
13. Decida habilitar el crecimiento automático en el volumen, pero para hacerlo, debe determinar el espacio libre disponible en el agregado principal y la tasa de crecimiento del volumen actual:
- a. Observe el agregado principal, `cluster2_src_aggr1`, En el panel **dispositivos relacionados**.



Puede hacer clic en el nombre del agregado para obtener más detalles sobre él.

Se determina que el agregado tiene espacio suficiente para habilitar el crecimiento automático del volumen.

- b. En la parte superior de la página, observe el icono que indica una incidencia crítica y revise el texto debajo del icono.

Usted determina que "días a lleno: Menos de un día | tasa de crecimiento diario: 5.4%".

14. Vaya a System Manager o acceda a la CLI de ONTAP para habilitar el `volume autogrow` opción.



Anote los nombres del volumen y del agregado para que estén disponibles al habilitar el crecimiento automático.

15. Después de resolver el problema de capacidad, vuelva a la página de detalles de Unified Manager **evento** y marque el evento como solucionado.

## Resolución de problemas de desfase

Este flujo de trabajo proporciona un ejemplo de cómo puede resolver un problema de desfase. En esta situación, usted es administrador o operador que accede a la página Unified Manager Dashboard para ver si hay algún problema en las relaciones de protección y, si existen, para buscar soluciones.

### Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

En la página Dashboard, se puede ver el área Unresolved Incidents and Risks y se muestra un error de desfase de SnapMirror en el panel Protection Risks.

### Pasos

1. En el panel **Protection** de la página **Dashboard**, localice el error de retraso de la relación de SnapMirror y haga clic en él.

Se muestra la página de detalles Event para el evento de error de desfase.

2. En la página de detalles **evento** puede realizar una o más de las siguientes tareas:
  - Revise el mensaje de error en el campo causa del área Resumen para determinar si hay alguna acción correctiva sugerida.
  - Haga clic en el nombre del objeto, en este caso, un volumen, en el campo Source del área Summary para obtener detalles sobre el volumen.
  - Busque las notas que se podrían haber añadido acerca de este evento.

- Agregar una nota al evento.
  - Asignar el evento a un usuario específico.
  - Reconozca o resuelva el evento.
3. En este escenario, haga clic en el nombre del objeto (en este caso, un volumen) en el campo origen del área **Resumen** para obtener detalles sobre el volumen.

Se muestra la pestaña Protection de la página de detalles Volume / Health.

4. En la ficha **Protección**, verá el diagrama de topología.

Ha observado que el volumen con el error de desfase es el último volumen en una cascada de SnapMirror de tres volúmenes. El volumen seleccionado se resume en gris oscuro y una línea naranja doble del volumen de origen indica un error de relación de SnapMirror.



5. Haga clic en cada uno de los volúmenes en la cascada de SnapMirror.

Al seleccionar cada volumen, la información de protección en Summary, Topology, History, Events, Related Devices, Y las áreas Alertas relacionadas cambian para mostrar detalles relevantes para el volumen seleccionado.

6. Verá el área **Resumen** y coloque el cursor sobre el icono de información en el campo **Actualizar programa** de cada volumen.

En este caso, debe tener en cuenta que la política de SnapMirror es DPDefault, y la programación de SnapMirror se actualiza cada hora a los cinco minutos. Usted sabe que todos los volúmenes de la relación están intentando completar una transferencia de SnapMirror al mismo tiempo.

7. Para resolver el problema de desfase, se modifican los horarios de dos de los volúmenes en cascada de modo que cada destino inicie una transferencia de SnapMirror una vez que su origen haya completado una transferencia.



## Información de copyright

Copyright © 2023 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPTIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

## Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.