Crear y solucionar problemas en las relaciones de protección

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/es-es/active-iq-unified-manager-918/data-protection/concept_types_of_snapmirror_protection.html on November 13, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

Crear y solucionar problemas en las relaciones de protección . . . 1
Tipos de protección de SnapMirror en Active IQ Unified Manager . . . 1
Relaciones de protección asíncronas tradicionales de SnapMirror . . . 1
SnapMirror Protección asíncrona con replicación flexible en cuanto a versiones . . . 1
SnapMirror Protección asíncrona con replicación flexible entre versiones y opción de backup . . . 1
SnapMirror replicación unificada (espejo y almacén) . . . 2
SnapMirror protección síncrona con sincronización estricta . . . 2
SnapMirror Protección síncrona con sincronización periódica . . . 2
SnapMirror active sync . . . 2
Configura relaciones de protección en Unified Manager . . . 3
Configura relaciones de protección en Active IQ Unified Manager . . . 3
Configura una conexión entre Workflow Automation y Active IQ Unified Manager . . . 3
Comprobar el almacenamiento en caché de la fuente de datos de Active IQ Unified Manager en Workflow Automation . . . 4
Cómo la reinstalación o actualización de OnCommand Workflow Automation afecta a Active IQ Unified Manager . . . 5
Elimina la configuración de OnCommand Workflow Automation de Active IQ Unified Manager . . . 5
Realiza la conmutación por error y la conmutación de retorno de una relación de protección . . . 5
Realiza una conmutación por error y una conmutación de retorno de una relación de protección en Active IQ Unified Manager . . . 5
Rompe una relación de protección de SnapMirror desde la página Volumen/Estado de Active IQ Unified Manager . . . 7
Invierte las relaciones de protección desde la página de detalles de Volumen/Estado en Active IQ Unified Manager . . . 7
Eliminar una relación de protección desde la página de detalles de Volumen/Estado en Active IQ Unified Manager . . . 8
Resincroniza las relaciones de protección desde la página de detalles de Volumen/Estado en Active IQ Unified Manager . . . 9
Solucionar un fallo en una tarea de protección . . . 10
Soluciona un error en una tarea de protección en Active IQ Unified Manager . . . 10
Identifica el problema y realiza acciones correctivas para un fallo en una tarea de protección en Active IQ Unified Manager . . . 10
Soluciona los problemas de retraso en Active IQ Unified Manager . . . 13

Crear y solucionar problemas en las relaciones de protección

Tipos de protección de SnapMirror en Active IQ Unified Manager

En función de la implementación de tu topología de almacenamiento de datos, Unified Manager te permite configurar varios tipos de relaciones de protección SnapMirror. Todas las variantes de protección SnapMirror ofrecen protección de conmutación por error y recuperación ante desastres, pero tienen distintas capacidades en cuanto a rendimiento, flexibilidad de versiones y protección de varias copias de backup.

Relaciones de protección asíncronas tradicionales de SnapMirror

La protección asíncrona tradicional de SnapMirror proporciona protección de reflejo mediante replicación de bloques entre los volúmenes de origen y de destino.

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

SnapMirror Protección asíncrona con replicación flexible en cuanto a versiones

SnapMirror La protección asíncrona con replicación flexible entre versiones proporciona protección de reflejo con replicación lógica entre los volúmenes de origen y destino, incluso si esos volúmenes se ejecutan con distintas versiones del software ONTAP 8.3 o posterior (por ejemplo, de la versión 8.3 a la 8.3.1, de la 8.3 a la 9.1 o de la 9.2.2 a la 9.2).

En las relaciones de SnapMirror con replicación de versión flexible, las operaciones de reflejo no se ejecutan tan rápido como lo harían en las relaciones tradicionales de SnapMirror.

Debido a la menor velocidad de ejecución, SnapMirror con protección de replicación flexible en cuanto a versiones no es adecuado para implementarlo en cualquiera de las siguientes circunstancias:

- El objeto de origen contiene más de 10 millones de archivos que hay que proteger.
- El objetivo de punto de recuperación de los datos protegidos es de dos horas o menos. (Es decir, el destino debe contener siempre datos reflejados y recuperables que no tengan más de dos horas de antigüedad respecto a los datos del origen.)

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

SnapMirror Protección asíncrona con replicación flexible entre versiones y opción de backup

SnapMirror La protección asíncrona, con replicación flexible en cuanto a versiones y opción de backup, ofrece

protección mediante duplicación entre los volúmenes de origen y destino, así como la posibilidad de almacenar varias copias de los datos reflejados en el destino.

El administrador de almacenamiento puede especificar qué copias de Snapshot se reflejan desde el origen al destino y también puede indicar durante cuánto tiempo conservar esas copias en el destino, incluso si se eliminan en el origen.

En las relaciones de SnapMirror con replicación flexible por versión y opción de backup, las operaciones de reflejo no se ejecutan tan rápido como lo harían en las relaciones tradicionales de SnapMirror.

SnapMirror replicación unificada (espejo y almacén)

La replicación unificada de SnapMirror te permite configurar la recuperación ante desastres y el archivado en el mismo volumen de destino. Al igual que con SnapMirror, la protección de datos unificada realiza una transferencia completa la primera vez que la invocas. Una transferencia completa con la política de protección de datos unificada predeterminada “MirrorAndVault” crea una copia de Snapshot del volumen de origen y luego transfiere esa 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 de Snapshot antiguas en la referencia.

SnapMirror protección síncrona con sincronización estricta

SnapMirror La protección síncrona con sincronización «`strict`» garantiza que los volúmenes primario y secundario sean siempre una copia exacta el uno del otro. Si se produce un fallo de replicación al intentar escribir datos en el volumen secundario, se interrumpe la E/S del cliente hacia el volumen primario.

SnapMirror Protección síncrona con sincronización periódica

SnapMirror La protección síncrona con sincronización «`regular`» no requiere que el volumen primario y el secundario sean siempre una copia exacta el uno 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 dejan de estar sincronizados y la E/S del cliente continuará en el volumen primario.

> El botón «Restaurar» y los botones de operación de relaciones no están disponibles al supervisar las relaciones de protección síncrona desde la vista «Estado: todos los volúmenes» o desde la página de detalles «Volumen / Estado».

SnapMirror active sync

La función de sincronización activa de SnapMirror está disponible con ONTAP 9.8 y versiones posteriores, y puedes usarla para proteger aplicaciones con LUN, lo que permite que las aplicaciones hagan una conmutación por error de forma transparente y garantiza la continuidad del negocio en caso de desastre.

Te permite detectar y supervisar las relaciones síncronas de SnapMirror para grupos de consistencia (CG) disponibles en clústeres y máquinas virtuales de almacenamiento desde Unified Manager. SnapMirror active sync es compatible con clústeres AFF o clústeres All SAN Array (ASA), donde los clústeres primario y secundario pueden ser AFF o ASA. SnapMirror active sync protege las aplicaciones con LUN de iSCSI o FCP.

Al consultar los volúmenes y los LUN protegidos por la relación de sincronización activa SnapMirror, podrás obtener una vista unificada de las relaciones de protección, los grupos de consistencia en el inventario de volúmenes, ver la topología de protección de las relaciones de grupos de consistencia y ver los datos históricos de las relaciones de grupos de consistencia de hasta un año. También puedes descargar el informe. También puedes ver el resumen de las relaciones de grupos de consistencia, la compatibilidad de búsqueda

para las relaciones de grupos de consistencia y obtener información sobre los volúmenes protegidos por el grupo de consistencia.

En la página «Relaciones», también puedes ordenar, filtrar y ampliar la protección de los objetos de almacenamiento de origen y destino y de su relación, que están protegidos por el grupo de consistencia.

Para obtener más información sobre SnapMirror active sync, consulta "Documentación de ONTAP 9 para Snapmirror active sync (formerly SM-BC)".

Configura relaciones de protección en Unified Manager

Configura relaciones de protección en Active IQ Unified Manager

Hay varios pasos que debes seguir para usar Unified Manager y OnCommand Workflow Automation para configurar relaciones de SnapMirror y SnapVault para proteger tus datos.

Antes de empezar

- Debes tener el rol de Application Administrator o Storage Administrator.
- Debes haber establecido relaciones entre iguales entre dos clústeres o dos máquinas virtuales de almacenamiento (SVM).
- OnCommand Workflow Automation debe integrarse con Unified Manager:
  - "Configura OnCommand Workflow Automation".
  - "Comprobación del almacenamiento en caché del origen de datos de Unified Manager en Workflow Automation".

Pasos

1. Dependiendo del tipo de relación de protección que quieras crear, realiza una de las siguientes acciones:
   - "Crear una relación de protección de SnapMirror".
   - "Crear una relación de protección de SnapVault".
2. Si deseas crear una política para la relación, dependiendo del tipo de relación que estés creando, realiza una de las siguientes acciones:
   - "Crear una política de SnapVault".
   - "Crear una política de SnapMirror".
3. "Crea una programación de SnapMirror o SnapVault".

Configura una conexión entre Workflow Automation y Active IQ Unified Manager

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

Antes de empezar

- La versión instalada de Workflow Automation debe ser la 5.1.1P6 o una versión posterior.

El “WFA pack for managing Clustered Data ONTAP” está incluido en WFA 5.1.1P6, así que no necesitas descargar este pack de la NetAppStorage Automation Store ni instalarlo por separado en tu servidor WFA como se requería antes. "Descarga de WFA"

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

  A este usuario de la base de datos se le debe haber asignado el rol de usuario Integration Schema.

- Debes tener asignado el rol Administrator o el rol Architect en Workflow Automation.
- Para configurar Workflow Automation, debes disponer de la dirección del host, el número de puerto 443, el nombre de usuario y la contraseña.
- Debes tener el rol de Application Administrator o Storage Administrator.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **Workflow Automation**.
2. En el área **Database User** de la **Workflow Automation page**, selecciona el nombre e introduce la contraseña del usuario de la base de datos que has creado para admitir las conexiones de Unified Manager y Workflow Automation.
3. En el apartado **Workflow Automation Credentials** de la página, introduce el nombre de host o la dirección IP (IPv4 o IPv6), así como el nombre de usuario y la contraseña para la configuración de Workflow Automation.

   Debes utilizar el puerto del servidor de Unified Manager (puerto 443).

4. Haz clic en **Guardar**.
5. Si utilizas un certificado autofirmado, haz clic en **Sí** para autorizar el certificado de seguridad.

   Aparece la página Workflow Automation.

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

Información relacionada

"NetApp Documentación: OnCommand Workflow Automation (versiones actuales)"

Comprobar el almacenamiento en caché de la fuente de datos de Active IQ Unified Manager en Workflow Automation

Puedes determinar si el almacenamiento en caché de las fuentes de datos de Unified Manager funciona correctamente comprobando si la adquisición de fuentes de datos se realiza correctamente en Workflow Automation. Puede que quieras hacerlo al integrar Workflow Automation con Unified Manager para asegurarte de que la funcionalidad de Workflow Automation esté disponible después de la integración.

Antes de empezar

Para realizar esta tarea, debes tener asignado el rol Administrator o el rol Architect en Workflow Automation.

Pasos

1. En la UI de Workflow Automation, selecciona **Execution** > **Data Sources**.
2. Haz clic con el botón derecho en el nombre de la fuente de datos de Unified Manager y, a continuación, selecciona **Acquire Now**.
3. Comprueba que la adquisición se complete sin errores.

   Para que la integración de Workflow Automation con Unified Manager se lleve a cabo con éxito, es necesario resolver los errores de adquisición.

Cómo la reinstalación o actualización de OnCommand Workflow Automation afecta a Active IQ Unified Manager

Antes de reinstalar o actualizar OnCommand Workflow Automation, primero debes eliminar la conexión entre OnCommand Workflow Automation y Unified Manager, y asegurarte de detener todas las tareas de OnCommand Workflow Automation que se estén ejecutando o que estén programadas.

También debes eliminar manualmente Unified Manager de OnCommand Workflow Automation.

Después de reinstalar o actualizar OnCommand Workflow Automation, debes volver a configurar la conexión con Unified Manager.

Elimina la configuración de OnCommand Workflow Automation de Active IQ Unified Manager

Puedes eliminar la configuración de OnCommand Workflow Automation de Unified Manager cuando ya no quieras usar Workflow Automation.

Antes de empezar

Debes tener el rol de Application Administrator o Storage Administrator.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **Workflow Automation** en el menú **Setup** de la izquierda.
2. En la página **Workflow Automation**, haz clic en **Remove Setup**.

Realiza la conmutación por error y la conmutación de retorno de una relación de protección

Realiza una conmutación por error y una conmutación de retorno de una relación de protección en Active IQ Unified Manager

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

Antes de empezar

- Debes tener el rol de Application Administrator o Storage Administrator.
- Para realizar esta operación, debes haber configurado OnCommand Workflow Automation.

Pasos

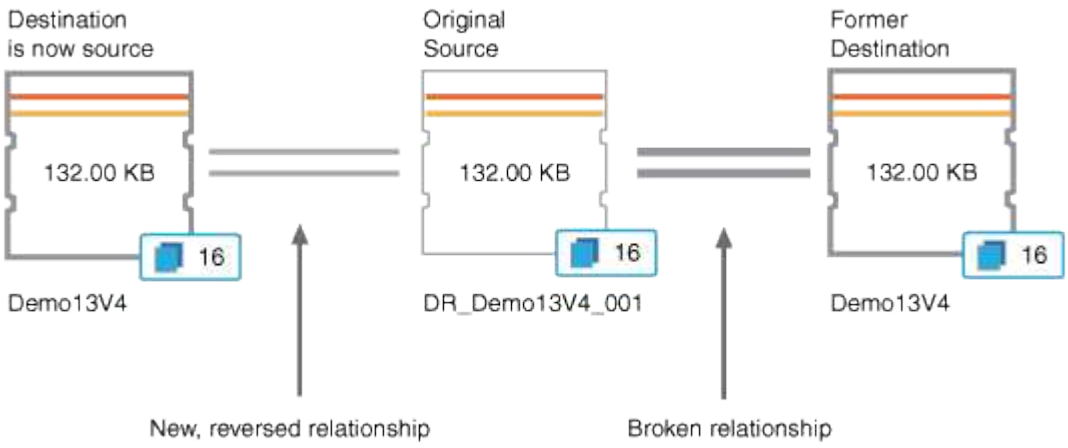
1. "Romper la relación de SnapMirror".

   Debes romper la relación antes de poder convertir el destino de un volumen de protección de datos en un volumen de lectura/escritura y antes de poder invertir la relación.

2. "Invertir la relación de protección".

   Cuando el volumen de origen original vuelva a estar disponible, es posible que decidas restablecer la relación de protección original restaurando el volumen de origen. Antes de poder restaurar el volumen de origen, debes sincronizarlo con los datos escritos en el destino anterior. Usas la operación de resincronización inversa para crear una nueva relación de protección invirtiendo los roles de la relación original y sincronizando el volumen de origen con el destino anterior. Se crea una nueva copia de Snapshot básica para la nueva relación.

   La relación inversa se parece a una relación en cascada:



3. "Rompe la relación invertida de SnapMirror".

   Cuando el volumen de origen original se haya resincronizado y pueda volver a proporcionar datos, utiliza la operación «break» para romper la relación inversa.

4. "Eliminar la relación".

   Cuando la relación invertida ya no sea necesaria, debes eliminar esa relación antes de restablecer la relación original.

5. "Resincronizar la relación".

   Utiliza la operación de resincronización para sincronizar los datos del origen con el destino y restablecer la relación original.

Rompe una relación de protección de SnapMirror desde la página Volumen/Estado de Active IQ Unified Manager

Puedes romper una relación de protección desde la página de detalles de Volume / Health y detener las transferencias de datos entre un volumen de origen y un volumen de destino en una relación SnapMirror. Puede que quieras romper una relación cuando quieras migrar datos, para la recuperación ante desastres o para probar aplicaciones. El volumen de destino se convierte en un volumen de lectura y escritura. No puedes romper una relación SnapVault.

Antes de empezar

- Debes tener el rol de Application Administrator o Storage Administrator.
- Debes haber configurado Workflow Automation.

Pasos

1. En la pestaña **Protección** de la página de detalles **Volumen / Estado**, selecciona en la topología la relación «SnapMirror» que deseas interrumpir.
2. Haz clic con el botón derecho del ratón en el destino y selecciona **Break** del menú.

   Aparece el cuadro de diálogo «Romper relación».

3. Haz clic en **Continue** para romper la relación.
4. En la topología, comprueba que la relación esté interrumpida.

Invierte las relaciones de protección desde la página de detalles de Volumen/Estado en Active IQ Unified Manager

Cuando un desastre inutiliza el volumen de origen en tu relación de protección, puedes usar el volumen de destino para servir datos convirtiéndolo en lectura/escritura mientras reparas o sustituyes el origen. Cuando el origen vuelva a estar disponible para recibir datos, puedes usar la operación de resincronización inversa para establecer la relación en sentido inverso y sincronizar los datos del origen con los del volumen de destino de lectura/escritura.

Antes de empezar

- Debes tener el rol de Application Administrator o Storage Administrator.
- Debes haber configurado Workflow Automation.
- La relación no debe ser una relación de SnapVault.
- Ya debe existir una relación de protección.
- Hay que romper la relación de protección.
- Tanto el origen como el destino deben estar en línea.
- El origen no debe ser el destino de otro volumen de protección de datos.
- Al realizar esta tarea, se eliminan los datos del origen que sean más recientes que los de la copia Snapshot común.
- Las políticas y las programaciones creadas en la relación de resincronización inversa son las mismas que las de la relación de protección original.

Si no existen políticas ni programaciones, se crean.

Pasos

1. En la pestaña **Protección** de la página de detalles **Volumen / Estado**, localiza en la topología la relación SnapMirror en la que quieres invertir el origen y el destino, y haz clic con el botón derecho sobre ella.
2. Selecciona **Resincronización inversa** en el menú.

   Aparece el cuadro de diálogo «Resincronización inversa».

3. Comprueba que la relación que aparece en el cuadro de diálogo **Resincronización inversa** sea aquella para la que deseas realizar la operación de resincronización inversa y, a continuación, haz clic en **Enviar**.

   Se cierra el cuadro de diálogo Resincronización inversa y se muestra un enlace al trabajo en la parte superior de la página de detalles de Volumen/Estado.

4. **Opcional:** haz clic en **Ver tareas** en la página de detalles de **Volumen / Estado** para realizar un seguimiento del estado de cada tarea de resincronización inversa.

   Se muestra una lista filtrada de trabajos.

5. **Opcional:** haz clic en la flecha **Back** de tu navegador para volver a la página de detalles de **Volume / Health**.

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

Eliminar una relación de protección desde la página de detalles de Volumen/Estado en Active IQ Unified Manager

Puedes eliminar una relación de protección para borrar de forma permanente una relación existente entre la fuente y el destino seleccionados: por ejemplo, cuando quieras crear una relación utilizando un destino diferente. Esta operación elimina todos los metadatos y no puedes deshacerla.

Antes de empezar

- Debes tener el rol de Application Administrator o Storage Administrator.
- Debes haber configurado Workflow Automation.

Pasos

1. En la pestaña **Protección** de la página de detalles **Volumen / Estado**, selecciona en la topología la relación SnapMirror que deseas eliminar.
2. Haz clic con el botón derecho del ratón sobre el nombre del destino y selecciona **Eliminar** del menú.

   Aparece el cuadro de diálogo «Eliminar relación».

3. Haz clic en **Continuar** para eliminar la relación.

   La relación se elimina de la página de detalles de Volumen / Estado.

Resincroniza las relaciones de protección desde la página de detalles de Volumen/Estado en Active IQ Unified Manager

Puedes resincronizar los datos de una relación de SnapMirror o SnapVault que se interrumpió y luego se configuró el destino como lectura/escritura para que los datos del origen coincidan con los del destino. También puedes resincronizar cuando se elimina una copia Snapshot común necesaria en el volumen de origen, lo que hace que fallen las actualizaciones de SnapMirror o SnapVault.

Antes de empezar

- Debes tener el rol de Application Administrator o Storage Administrator.
- Debes haber configurado OnCommand Workflow Automation.

Pasos

1. En la pestaña **Protección** de la página de detalles **Volumen / Estado**, localiza en la topología la relación de protección que deseas resincronizar y haz clic con el botón derecho del ratón sobre ella.
2. Selecciona **Resynchronize** en el menú.

   También puedes, desde el menú **Acciones**, seleccionar **Relación** > **Resincronizar** para resincronizar la relación cuyos detalles estás viendo en ese momento.

   Aparece el cuadro de diálogo «Resynchronize».

3. En la pestaña **Opciones de resincronización**, selecciona una prioridad de transferencia y la tasa de transferencia máxima.
4. Haz clic en **Copias de instantáneas de origen**; a continuación, en la columna **Copia de instantánea**, haz clic en **Predeterminada**.

   Aparece el cuadro de diálogo «Seleccionar copia de Snapshot de origen».

5. Si quieres especificar una copia Snapshot existente en lugar de transferir la copia Snapshot predeterminada, haz clic en **Existing Snapshot Copy** y selecciona una copia Snapshot de la lista.
6. Haz clic en **Enviar**.

   Volverás al cuadro de diálogo «Resynchronize».

7. Si has seleccionado más de una fuente para volver a sincronizar, haz clic en **Default** para la siguiente fuente para la que quieras especificar una copia Snapshot existente.
8. Haz clic en **Submit** para iniciar la tarea de resincronización.

   Se inicia la tarea de resincronización, vuelves a la página de detalles de Volumen / Estado y se muestra un enlace a las tareas en la parte superior de la página.

9. **Opcional:** haz clic en **View Jobs** en la página **Volume / Health details** para realizar un seguimiento del estado de cada tarea de resincronización.

   Se muestra una lista filtrada de trabajos.

10. **Opcional:** haz clic en la flecha **Back** de tu navegador para volver a la página de detalles de **Volume / Health**.

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

Solucionar un fallo en una tarea de protección

Soluciona un error en una tarea de protección en Active IQ Unified Manager

Este flujo de trabajo te ofrece un ejemplo de cómo puedes identificar y resolver un error en una tarea de protección desde el panel de Unified Manager.

Antes de empezar

Dado que algunas tareas de este flujo de trabajo requieren que inicies sesión con el rol Administrator, debes conocer los roles necesarios para usar las distintas funcionalidades.

En este escenario, accedes a la página Dashboard para ver si hay algún problema con tus trabajos de protección. En el área Protection Incident, observas que hay un incidente Job Terminated, que muestra un error Protection Job Failed en un volumen. Investigas este error para determinar la posible causa y la posible solución.

Pasos

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

   El texto del enlace del evento se escribe con el formato `object_name:/object_name - Error Name`, como `cluster2_src_svm:/cluster2_src_vol2 - Protection Job Failed`.

   Se muestra la página de detalles del evento correspondiente a la tarea de protección fallida.

2. Revisa el mensaje de error que aparece en el campo Cause del área **Summary** para identificar el problema y evaluar las posibles medidas correctivas.

   Consulta "Identificar el problema y aplicar medidas correctoras ante un fallo en una tarea de protección".

Identifica el problema y realiza acciones correctivas para un fallo en una tarea de protección en Active IQ Unified Manager

Revisas el mensaje de error de fallo del trabajo en el campo «Causa» de la página «Detalles del evento» y determinas que el trabajo falló debido a un error de copia Snapshot. Luego, vas a la página «Detalles de volumen / estado» para recopilar más información.

Antes de empezar

Debes tener el rol de Application Administrator.

El mensaje de error que aparece en el campo Causa de la página de detalles del evento contiene el siguiente texto sobre el trabajo fallido:

```
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:

- Una tarea de copia de seguridad o de duplicación no se completó correctamente.

  La tarea 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`.

- Falló una tarea de copia de Snapshot para `0426cluster2_src_vol2snap` en el volumen de origen `cluster2_src_svm:/cluster2_src_vol2`.

En este caso, puedes identificar la causa y las posibles medidas correctivas del fallo en la tarea. Sin embargo, para resolver el fallo, tienes que acceder a la interfaz de usuario web de System Manager o a los comandos de la CLI de ONTAP.

Pasos

1. Revisas el mensaje de error y concluyes que una tarea de copia de Snapshot falló en el volumen de origen, lo que indica que probablemente haya un problema con dicho volumen.

   Si lo deseas, puedes hacer clic en el enlace **Job Details** que aparece al final del mensaje de error, pero a efectos de este escenario, decides no hacerlo.

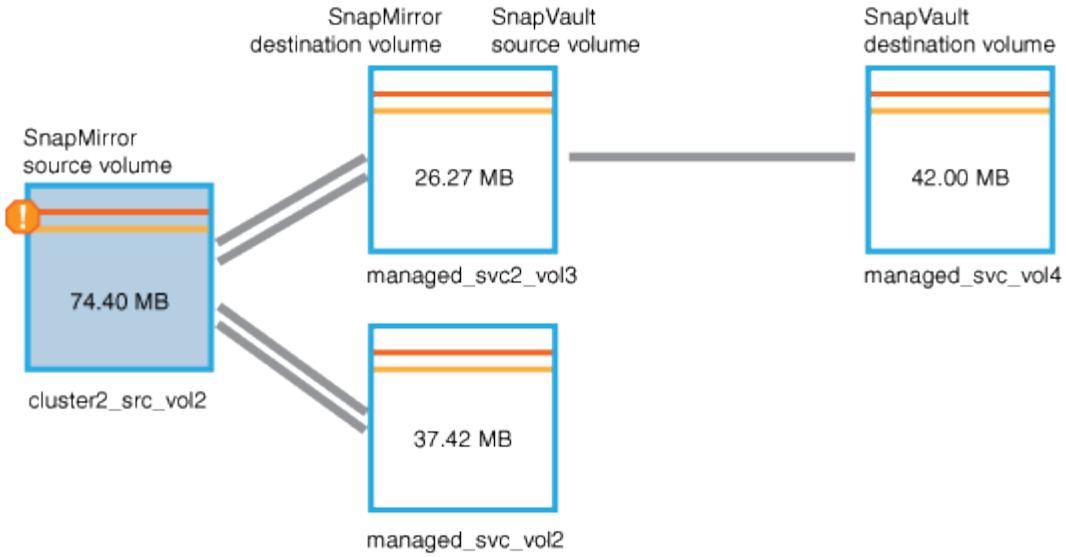
2. Decides que quieres intentar resolver el evento, así que haces lo siguiente:
   a. Haz clic en el botón **Assign To** y selecciona **Me** en el menú.
   b. Haz clic en el botón **Aceptar** para no seguir recibiendo notificaciones de alerta repetidas, si se configuraron alertas para el evento.
   c. Si lo deseas, también puedes añadir notas sobre el evento.
3. Haz clic en el campo **Origen** del panel **Resumen** para ver los detalles del volumen de origen.

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

   Se muestra la página de detalles de Volumen / Estado para `cluster2_src_vol2`, con el contenido de la pestaña Protección.

4. Al observar el gráfico de la topología de protección, verás un icono de error asociado al primer volumen de la topología, que es el volumen de origen de la relación de SnapMirror.

   También ves las barras horizontales en el icono del volumen de origen, que indican los umbrales de advertencia y error establecidos para ese volumen.



5. Coloca el cursor sobre el icono de error para ver el cuadro de diálogo emergente que muestra la configuración de umbral y comprobar que el volumen ha superado el umbral de error, lo que indica un problema de capacidad.
6. Haz clic en la pestaña **Capacidad**.

   Información sobre la capacidad de las pantallas `cluster2_src_vol2` de volumen.

7. En el panel **Capacidad**, ves que hay un icono de error en el gráfico de barras, lo que indica, una vez más, que la capacidad del volumen ha superado el nivel de umbral establecido para el volumen.
8. Debajo del gráfico de capacidad, verás que el crecimiento automático de volúmenes se ha desactivado y que se ha establecido una garantía de espacio en el volumen.

   Podrías optar por habilitar el crecimiento automático, pero para este escenario decides investigar más a fondo antes de tomar una decisión sobre cómo resolver el problema de capacidad.

9. Te desplazas hacia abajo hasta la lista **Events** y ves que se generaron los eventos «Protection Job Failed», «Volume Days Until Full» y «Volume Space Full».
10. En la lista **Eventos**, haces clic en el evento **Espacio del volumen lleno** para obtener más información, tras decidir que este evento parece el más relevante para tu problema de capacidad.

    La página de detalles del evento muestra el evento «Espacio del volumen lleno» correspondiente al volumen de origen.

11. En el área **Resumen**, lees el campo Cause 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, verás las acciones correctivas sugeridas.

    Las medidas correctivas sugeridas solo aparecen para algunos eventos, por lo que no verás esta sección en todos los tipos de eventos.

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

    - Activa el crecimiento automático de volúmenes en este volumen.
    - Cambia el tamaño del volumen.

- Activa y ejecuta la deduplicación en este volumen.
- Activa y ejecuta la compresión en este volumen.

13. Decides habilitar el crecimiento automático de volúmenes en el volumen, pero para ello debes determinar el espacio libre disponible en el agregado principal y la tasa de crecimiento actual del volumen:
    a. Fíjate en el agregado principal, `cluster2_src_aggr1` en el panel **Dispositivos relacionados**.

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

    Determinas que el agregado tiene suficiente espacio para habilitar el crecimiento automático de volúmenes.

    b. En la parte superior de la página, fíjate en el icono que indica un incidente crítico y lee el texto que aparece debajo del icono.

    Has determinado que «Días hasta llenarse por completo: menos de un día | Tasa de crecimiento diaria: 5,4 %».

14. Ve a System Manager o accede a la CLI de ONTAP para activar la opción `volume autogrow`.

    Anota los nombres del volumen y del agregado para tenerlos a mano cuando actives el crecimiento automático de volúmenes.

15. Una vez resuelto el problema de capacidad, vuelve a la página de detalles de **Event** de Unified Manager y marca el evento como resuelto.

Soluciona los problemas de retraso en Active IQ Unified Manager

Este flujo de trabajo ofrece un ejemplo de cómo puedes resolver un problema de retraso. En este escenario, eres un administrador u operador que accede a la página Unified ManagerDashboard para comprobar si hay algún problema con tus relaciones de protección y, si lo hay, encontrar soluciones.

Antes de empezar

Debes tener el rol de Application Administrator o Storage Administrator.

En la página Dashboard, ves en el área Incidentes y riesgos sin resolver un error de SnapMirror Lag en el panel Protección, dentro de Riesgos de protección.

Pasos

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

   Se muestra la página de detalles del evento correspondiente al error de retraso.

2. Desde la página de detalles de **Event** puedes realizar una o varias de las siguientes tareas:
   - Revisa el mensaje de error del campo Causa en el área Resumen para determinar si se sugiere alguna acción correctiva.

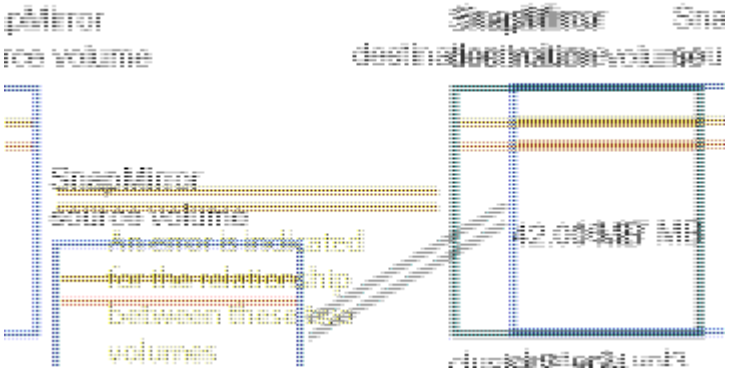
- Haz clic en el nombre del objeto, en este caso un volumen, en el campo Origen del área Resumen para obtener detalles sobre el volumen.
- Busca notas que se hayan podido añadir sobre este evento.
- Añade una nota al evento.
- Asigna el evento a un usuario concreto.
- Reconoce o resuelve el evento.

3. En este caso, haz clic en el nombre del objeto (en este caso, un volumen) en el campo «Origen» del área **Resumen** para obtener información detallada sobre el volumen.

   Se muestra la pestaña Protección de la página de detalles Volumen / Estado.

4. En la pestaña **Protección**, ves el diagrama de topología.

   Observas que el volumen con el error de desfase es el último volumen de una cascada de tres volúmenes SnapMirror. El volumen que seleccionaste está resaltado en gris oscuro, y una doble línea naranja desde el volumen de origen indica un error en la relación de SnapMirror.



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

   A medida que seleccionas cada volumen, la información de protección de las áreas Resumen, Topología, Historial, Eventos, Dispositivos relacionados y Alertas relacionadas cambia para mostrar los detalles relevantes del volumen seleccionado.

6. Fíjate en la sección **Resumen** y coloca el cursor sobre el icono de información del campo **Calendario de actualizaciones** de cada volumen.

   En este escenario, observas que la política SnapMirror es DPDefault y que la programación de SnapMirror se actualiza cada hora, cinco minutos después de la hora. Te das cuenta de que todos los volúmenes de la relación están intentando completar una transferencia de SnapMirror al mismo tiempo.

7. Para resolver el problema del retraso, modificas las programaciones de dos de los volúmenes en cascada para que cada destino inicie una transferencia de SnapMirror después de que su origen haya completado una transferencia.

Información de copyright

Copyright © 2026 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 INTERRUPCIÓN 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.