Gestiona el almacenamiento con el software Element.

Element Software

NetApp
November 12, 2025

Tabla de contenidos

Gestiona el almacenamiento con el software Element.

Gestiona el almacenamiento con el software Element.

Utilice el software Element para configurar el almacenamiento SolidFire , supervisar la capacidad y el rendimiento del clúster y gestionar la actividad de almacenamiento en una infraestructura multiinquilino.

Element es el sistema operativo de almacenamiento que constituye el núcleo de un clúster SolidFire . El software Element se ejecuta de forma independiente en todos los nodos del clúster y permite que los nodos del clúster combinen recursos y se presenten como un único sistema de almacenamiento a los clientes externos. El software Element es responsable de toda la coordinación del clúster, la escalabilidad y la gestión del sistema en su conjunto.

La interfaz de software está construida sobre la API de Element.

- "Acceda a la interfaz de usuario del software Element"
- "Configure las opciones del sistema SolidFire después de la implementación."
- "Actualizar los componentes del sistema de almacenamiento"
- "Utilice las opciones básicas de la interfaz de usuario del software Element."
- "Gestionar cuentas"
- "Administra tu sistema"
- "Gestionar volúmenes y volúmenes virtuales"
- "Proteja sus datos"
- "Soluciona los problemas de tu sistema"

Encuentra más información

- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Acceda a la interfaz de usuario del software Element

Puede acceder a la interfaz de usuario de Element utilizando la dirección IP virtual de administración (MVIP) del nodo principal del clúster.

Debes asegurarte de que los bloqueadores de ventanas emergentes y la configuración de NoScript estén desactivados en tu navegador.

Puede acceder a la interfaz de usuario utilizando direcciones IPv4 o IPv6, según la configuración realizada durante la creación del clúster.

1. Elija una de las siguientes opciones:
    - IPv6: Introduzca https://[dirección IPv6 MVIP]. Por ejemplo:

```
https://[fd20:8b1e:b256:45a::1234]/
```

- IPv4: Introduzca https://[dirección IPv4 MVIP]. Por ejemplo:

```
https://10.123.456.789/
```

2. Para DNS, introduzca el nombre del host.
3. Ignore cualquier mensaje de certificado de autenticación.

Encuentra más información

- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Configure las opciones del sistema SolidFire después de la implementación.

Configure las opciones del sistema SolidFire después de la implementación.

Después de configurar su sistema SolidFire , es posible que desee realizar algunas tareas opcionales.

Si modifica las credenciales del sistema, es posible que desee conocer el impacto en otros componentes.

Además, puede configurar los ajustes para la autenticación multifactor, la gestión de claves externas y la seguridad de los Estándares Federales de Procesamiento de Información (FIPS). También deberías considerar actualizar tus contraseñas cuando sea necesario.

Encuentra más información

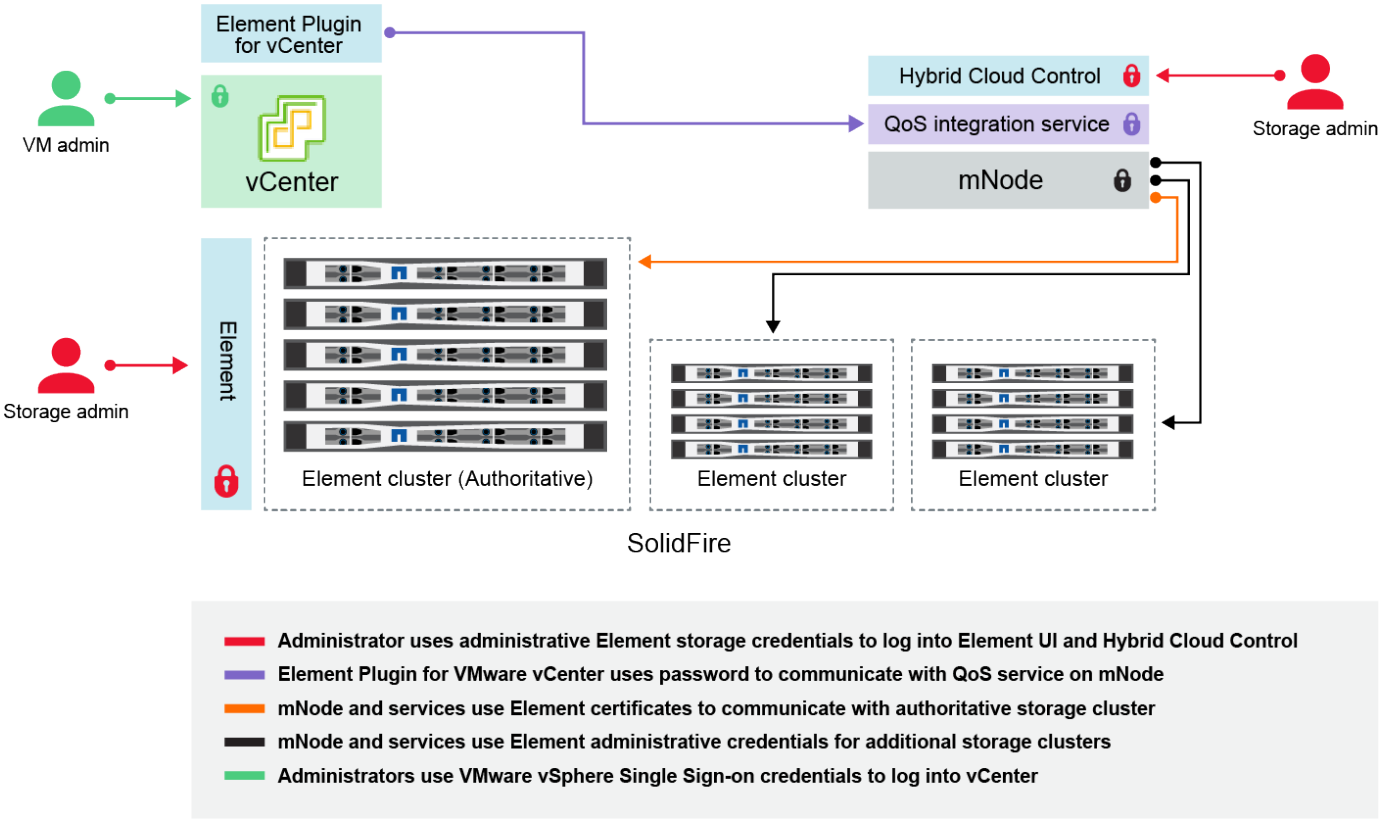
- "Cambiar credenciales en NetApp HCI y NetApp SolidFire"
- "Cambiar el certificado SSL predeterminado del software Element"
- "Cambiar la contraseña IPMI para los nodos"
- "Habilitar la autenticación multifactor"
- "Comience con la administración de claves externas"
- "Cree un clúster que admita unidades FIPS."

Cambiar credenciales en NetApp HCI y NetApp SolidFire

Dependiendo de las políticas de seguridad de la organización que implementó NetApp HCI o NetApp SolidFire, el cambio de credenciales o contraseñas suele formar parte de las prácticas de seguridad. Antes de cambiar las contraseñas, debe tener en cuenta el impacto que esto tendrá en otros componentes de software de la implementación.

Si cambia las credenciales de un componente de una implementación de NetApp HCI o NetApp SolidFire , la siguiente tabla proporciona orientación sobre el impacto en otros componentes.

Interacciones de componentes de NetApp SolidFire
:



Tipo de credencial e icono	Uso por parte del administrador	Consulte estas instrucciones
Credenciales de elemento 	**Aplica a**: NetApp HCI y SolidFire Los administradores utilizan estas credenciales para iniciar sesión en: • Interfaz de usuario de Element en el clúster de almacenamiento de Element • Control de nube híbrida en el nodo de administración (mnode) Cuando Hybrid Cloud Control administra varios clústeres de almacenamiento, solo acepta las credenciales de administrador para los clústeres de almacenamiento, conocidos como el *clúster autorizado* para el cual se configuró inicialmente el mnode. Para los clústeres de almacenamiento que se agreguen posteriormente a Hybrid Cloud Control, el nodo M almacena de forma segura las credenciales de administrador. Si se modifican las credenciales de los clústeres de almacenamiento añadidos posteriormente, también deben actualizarse las credenciales en el mnode utilizando la API de mnode.	• "Actualice las contraseñas de administrador del clúster de almacenamiento." • Actualice las credenciales de administrador del clúster de almacenamiento en el nodo M mediante el siguiente método:"API de modificación de administración de clústeres" .
Credenciales de inicio de sesión único de vSphere 	**Aplica a**: Solo NetApp HCI Los administradores utilizan estas credenciales para iniciar sesión en el cliente VMware vSphere. Cuando vCenter forma parte de la instalación de NetApp HCI , las credenciales se configuran en el motor de implementación de NetApp de la siguiente manera: • nombredeusuario@vsphere.local con la contraseña especificada, y • administrador@vsphere.local con la contraseña especificada. Cuando se utiliza un vCenter existente para implementar NetApp HCI, las credenciales de inicio de sesión único de vSphere son gestionadas por los administradores de TI de VMware.	"Actualizar las credenciales de vCenter y ESXi".

Tipo de credencial e icono	Uso por parte del administrador	Consulte estas instrucciones
Credenciales del controlador de gestión de la placa base (BMC) 	**Aplica a**: Solo NetApp HCI Los administradores utilizan estas credenciales para iniciar sesión en el BMC de los nodos de cómputo de NetApp en una implementación de NetApp HCI . El BMC proporciona funciones básicas de monitorización de hardware y de consola virtual. Las credenciales BMC (a veces denominadas *IPMI*) para cada nodo de cómputo de NetApp se almacenan de forma segura en el mnode en las implementaciones de NetApp HCI . NetApp Hybrid Cloud Control utiliza las credenciales de BMC en una cuenta de servicio para comunicarse con el BMC en los nodos de cómputo durante las actualizaciones de firmware de los nodos de cómputo. Cuando se cambian las credenciales de BMC , también deben actualizarse las credenciales de los nodos de cómputo respectivos en el mnode para conservar todas las funcionalidades de Hybrid Cloud Control.	• "Configure IPMI para cada nodo en NetApp HCI.". • Para los nodos H410C, H610C y H615C,"cambiar la contraseña predeterminada de IPMI" . • Para los nodos H410S y H610S,"cambiar la contraseña predeterminada de IPM" . • "Cambiar las credenciales de BMC en el nodo de administración".
credenciales de ESXi 	**Aplica a**: Solo NetApp HCI Los administradores pueden iniciar sesión en los hosts ESXi utilizando SSH o la DCUI local con una cuenta de root local. En las implementaciones de NetApp HCI , el nombre de usuario es 'root' y la contraseña se especificó durante la instalación inicial de ese nodo de cómputo en NetApp Deployment Engine. Las credenciales raíz de ESXi para cada nodo de cómputo de NetApp se almacenan de forma segura en el mnode en las implementaciones de NetApp HCI . NetApp Hybrid Cloud Control utiliza las credenciales en una cuenta de servicio para comunicarse directamente con los hosts ESXi durante las actualizaciones de firmware de los nodos de cómputo y las comprobaciones de estado. Cuando un administrador de VMware cambia las credenciales raíz de ESXi, las credenciales de los nodos de cómputo respectivos deben actualizarse en el mnode para conservar la funcionalidad de Hybrid Cloud Control.	"Actualizar las credenciales para los hosts de vCenter y ESXi".

Tipo de credencial e icono	Uso por parte del administrador	Consulte estas instrucciones
contraseña de integración de QoS 	**Se aplica a**: NetApp HCI y opcional en SolidFire No se utiliza para inicios de sesión interactivos por parte de los administradores. La integración de QoS entre VMware vSphere y Element Software se habilita mediante: • Complemento Element para vCenter Server, y • Servicio QoS en el nodo M. Para la autenticación, el servicio QoS utiliza una contraseña que se usa exclusivamente en este contexto. La contraseña de QoS se especifica durante la instalación inicial del complemento Element para vCenter Server, o se genera automáticamente durante la implementación de NetApp HCI . Sin impacto en otros componentes.	"Actualizar las credenciales de QoSSIOC en el complemento NetApp Element para vCenter Server". La contraseña SIOC del complemento NetApp Element para vCenter Server también se conoce como la contraseña *QoSSIOC*. Revise el artículo de la base de conocimientos Element Plug-in para vCenter Server.
Credenciales del dispositivo de servicio de vCenter 	**Aplica a**: NetApp HCI solo si se configura mediante NetApp Deployment Engine Los administradores pueden iniciar sesión en las máquinas virtuales del dispositivo vCenter Server. En las implementaciones de NetApp HCI , el nombre de usuario es 'root' y la contraseña se especificó durante la instalación inicial de ese nodo de cómputo en el motor de implementación de NetApp . Dependiendo de la versión de VMware vSphere implementada, ciertos administradores del dominio de inicio de sesión único de vSphere también pueden iniciar sesión en el dispositivo. Sin impacto en otros componentes.	No se necesitan cambios.
Credenciales de administrador del nodo de administración de NetApp 	**Se aplica a**: NetApp HCI y opcional en SolidFire Los administradores pueden iniciar sesión en las máquinas virtuales del nodo de administración de NetApp para realizar configuraciones avanzadas y solucionar problemas. Dependiendo de la versión del nodo de gestión implementada, el inicio de sesión mediante SSH no está habilitado de forma predeterminada. En las implementaciones de NetApp HCI , el nombre de usuario y la contraseña fueron especificados por el usuario durante la instalación inicial de ese nodo de cómputo en NetApp Deployment Engine. Sin impacto en otros componentes.	No se necesitan cambios.

Encuentra más información

- "Cambiar el certificado SSL predeterminado del software Element"
- "Cambiar la contraseña IPMI para los nodos"
- "Habilitar la autenticación multifactor"
- "Comience con la administración de claves externas"
- "Cree un clúster que admita unidades FIPS."

Cambiar el certificado SSL predeterminado del software Element

Puede cambiar el certificado SSL y la clave privada predeterminados del nodo de almacenamiento en el clúster mediante la API de NetApp Element .

Cuando se crea un clúster de software NetApp Element , el clúster crea un certificado Secure Sockets Layer (SSL) autofirmado único y una clave privada que se utiliza para toda la comunicación HTTPS a través de la interfaz de usuario de Element, la interfaz de usuario por nodo o las API. El software Element admite certificados autofirmados, así como certificados emitidos y verificados por una Autoridad de Certificación (CA) de confianza.

Puede utilizar los siguientes métodos de la API para obtener más información sobre el certificado SSL predeterminado y realizar cambios.

- **Obtener certificado SSL**

  Puedes usar el"Método GetSSLCertificate" Para recuperar información sobre el certificado SSL actualmente instalado, incluyendo todos los detalles del certificado.

- **Establecer certificado SSL**

  Puedes usar el"Método SetSSLCertificate" para configurar los certificados SSL del clúster y por nodo con el certificado y la clave privada que usted proporcione. El sistema valida el certificado y la clave privada para evitar que se aplique un certificado no válido.

- **Eliminar certificado SSL**

  El"Método RemoveSSLCertificate" Elimina el certificado SSL y la clave privada actualmente instalados. A continuación, el clúster genera un nuevo certificado autofirmado y una clave privada.

> El certificado SSL del clúster se aplica automáticamente a todos los nodos nuevos que se agreguen al clúster. Cualquier nodo eliminado del clúster vuelve a utilizar un certificado autofirmado y toda la información de certificado y clave definida por el usuario se elimina del nodo.

Encuentra más información

- "Cambiar el certificado SSL predeterminado del nodo de administración"
- "¿Cuáles son los requisitos para configurar certificados SSL personalizados en Element Software?"
- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Cambiar la contraseña IPMI predeterminada para los nodos

Puede cambiar la contraseña de administrador predeterminada de la interfaz de administración de plataforma inteligente (IPMI) tan pronto como tenga acceso IPMI remoto al nodo. Es posible que desee hacer esto si hubiera alguna actualización de instalación.

Para obtener detalles sobre la configuración del acceso IPM para los nodos, consulte"Configure IPMI para cada nodo" .

Puedes cambiar la contraseña de IPM para estos nodos:

- nodos H410S
- nodos H610S

Cambiar la contraseña IPMI predeterminada para los nodos H410S

Debe cambiar la contraseña predeterminada de la cuenta de administrador de IPMI en cada nodo de almacenamiento tan pronto como configure el puerto de red IPMI.

Lo que necesitarás

Deberías haber configurado la dirección IP IPMI para cada nodo de almacenamiento.

Pasos

1. Abra un navegador web en un ordenador que pueda acceder a la red IPMI y navegue hasta la dirección IP IPMI del nodo.
2. Introduzca el nombre de usuario `ADMIN` y contraseña `ADMIN` en la pantalla de inicio de sesión.
3. Tras iniciar sesión, haga clic en la pestaña **Configuración**.
4. Haz clic en **Usuarios**.
5. Seleccione el `ADMIN` usuario y haga clic en **Modificar usuario**.
6. Seleccione la casilla de verificación **Cambiar contraseña**.
7. Introduzca una nueva contraseña en los campos **Contraseña** y **Confirmar contraseña**.
8. Haz clic en **Modificar** y luego en **Aceptar**.
9. Repita este procedimiento para cualquier otro nodo H410S con contraseñas IPMI predeterminadas.

Cambiar la contraseña IPMI predeterminada para los nodos H610S

Debe cambiar la contraseña predeterminada de la cuenta de administrador de IPMI en cada nodo de almacenamiento tan pronto como configure el puerto de red IPMI.

Lo que necesitarás

Deberías haber configurado la dirección IP IPMI para cada nodo de almacenamiento.

Pasos

1. Abra un navegador web en un ordenador que pueda acceder a la red IPMI y navegue hasta la dirección IP IPMI del nodo.
2. Introduzca el nombre de usuario `root` y contraseña `calvin` en la pantalla de inicio de sesión.

3. Tras iniciar sesión, haga clic en el icono de navegación del menú situado en la parte superior izquierda de la página para abrir el panel lateral.
4. Haz clic en **Configuración**.
5. Haz clic en **Gestión de usuarios**.
6. Seleccione el usuario **Administrador** de la lista.
7. Habilite la casilla de verificación **Cambiar contraseña**.
8. Introduzca una contraseña nueva y segura en los campos **Contraseña** y **Confirmar contraseña**.
9. Haz clic en **Guardar** en la parte inferior de la página.
10. Repita este procedimiento para cualquier otro nodo H610S con contraseñas IPMI predeterminadas.

Encuentra más información

- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Utilice las opciones básicas de la interfaz de usuario del software Element.

Utilice las opciones básicas de la interfaz de usuario del software Element.

La interfaz web de usuario del software NetApp Element (Element UI) le permite supervisar y realizar tareas comunes en su sistema SolidFire .

Las opciones básicas incluyen visualizar los comandos de la API activados por la actividad de la interfaz de usuario y proporcionar comentarios.

- "Ver actividad de la API"
- "Iconos en la interfaz de Elemento"
- "Enviar comentarios"

Para más información

- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

actividad de la API

Ver actividad de la API

El sistema Element utiliza la API de NetApp Element como base para sus características y funcionalidades. La interfaz de usuario de Element le permite ver varios tipos de actividad de la API en tiempo real en el sistema mientras utiliza la interfaz. Con el registro de la API, puede ver la actividad de la API del sistema iniciada por el usuario y en segundo plano, así como las llamadas a la API realizadas en la página que está viendo actualmente.

Puedes usar el registro de la API para identificar qué métodos de la API se utilizan para determinadas tareas y ver cómo usar los métodos y objetos de la API para crear aplicaciones personalizadas.

Para obtener información sobre cada método, consulte "Referencia de la API de Element Software".

1. Desde la barra de navegación de la interfaz de usuario de Element, haga clic en **Registro de API**.
2. Para modificar el tipo de actividad de la API que se muestra en la ventana de registro de la API, siga los siguientes pasos:
   a. Seleccione **Solicitudes** para mostrar el tráfico de solicitudes de la API.
   b. Seleccione **Respuestas** para mostrar el tráfico de respuesta de la API.
   c. Filtre los tipos de tráfico de API seleccionando una de las siguientes opciones:
      - **Iniciado por el usuario**: Tráfico de API generado por sus actividades durante esta sesión de interfaz de usuario web.
      - **Consulta en segundo plano**: Tráfico de API generado por la actividad del sistema en segundo plano.
      - **Página actual**: Tráfico de la API generado por las tareas en la página que está viendo actualmente.

Encuentra más información

- "Gestionar el almacenamiento con la API de Element"
- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

La frecuencia de actualización de la interfaz se ve afectada por la carga del clúster.

Dependiendo de los tiempos de respuesta de la API, el clúster podría ajustar automáticamente el intervalo de actualización de datos para ciertas partes de la página del software NetApp Element que está visualizando.

El intervalo de actualización se restablece al valor predeterminado cuando recargas la página en tu navegador. Puedes ver el intervalo de actualización actual haciendo clic en el nombre del clúster en la parte superior derecha de la página. Tenga en cuenta que el intervalo controla la frecuencia con la que se realizan las solicitudes a la API, no la rapidez con la que los datos regresan del servidor.

Cuando un clúster está bajo una carga elevada, puede poner en cola las solicitudes de API desde la interfaz de usuario de Element. En raras ocasiones, cuando la respuesta del sistema se retrasa significativamente, como por ejemplo una conexión de red lenta combinada con un clúster ocupado, es posible que se cierre su sesión en la interfaz de usuario de Element si el sistema no responde con la suficiente rapidez a las solicitudes de API en cola. Si se le redirige a la pantalla de cierre de sesión, puede volver a iniciar sesión después de descartar cualquier solicitud de autenticación inicial del navegador. Al regresar a la página de resumen, es posible que se le soliciten las credenciales del clúster si su navegador no las ha guardado.

Iconos en la interfaz de Elemento

La interfaz del software NetApp Element muestra iconos que representan las acciones que puede realizar sobre los recursos del sistema.

La siguiente tabla proporciona una referencia rápida:

Icono	Descripción
	Comportamiento
	Copia de seguridad a
	Clonar o copiar
	Eliminar o purgar
	Editar
	Filtrar
	Par
	Refrescar
	Restaurar
	Restaurar desde
	Reversión
	Snapshot

Enviar comentarios

Puedes ayudar a mejorar la interfaz de usuario web del software Element y solucionar cualquier problema de la interfaz utilizando el formulario de comentarios que está accesible en toda la interfaz.

1. Desde cualquier página de la interfaz de usuario de Element, haga clic en el botón **Comentarios**.
2. Introduzca la información pertinente en los campos Resumen y Descripción.

3. Adjunta cualquier captura de pantalla que pueda ser útil.
4. Introduzca un nombre y una dirección de correo electrónico.
5. Seleccione la casilla de verificación para incluir datos sobre su entorno actual.
6. Haga clic en **Enviar**.

Encuentra más información

- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Gestionar cuentas

Gestionar cuentas

En los sistemas de almacenamiento SolidFire , los inquilinos pueden usar cuentas para permitir que los clientes se conecten a volúmenes en un clúster. Cuando se crea un volumen, este se asigna a una cuenta específica. También puede administrar las cuentas de administrador de clúster para un sistema de almacenamiento SolidFire .

- "Trabajar con cuentas que utilizan CHAP"
- "Administrar cuentas de usuario de administrador de clúster"

Para más información

- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Trabajar con cuentas que utilizan CHAP

En los sistemas de almacenamiento SolidFire , los inquilinos pueden usar cuentas para permitir que los clientes se conecten a volúmenes en un clúster. Una cuenta contiene el protocolo de autenticación Challenge-Handshake Authentication Protocol (CHAP) necesario para acceder a los volúmenes que le han sido asignados. Cuando se crea un volumen, este se asigna a una cuenta específica.

Una cuenta puede tener asignados hasta dos mil volúmenes, pero un volumen solo puede pertenecer a una cuenta.

algoritmos CHAP

A partir del Elemento 12.7, se admiten los algoritmos CHAP seguros compatibles con FIPS SHA1, SHA-256 y SHA3-256. Cuando un iniciador iSCSI de host crea una sesión iSCSI con un destino iSCSI de Element, solicita una lista de algoritmos CHAP para usar. El destino iSCSI de Element elige el primer algoritmo que admite de la lista solicitada por el iniciador iSCSI del host. Para confirmar que el destino iSCSI de Element elige el algoritmo más seguro, debe configurar el iniciador iSCSI del host para que envíe una lista de algoritmos ordenados desde el más seguro, por ejemplo, SHA3-256, hasta el menos seguro, por ejemplo, SHA1 o MD5. Cuando el iniciador iSCSI del host no solicita algoritmos SHA, el destino iSCSI de Element elige MD5, suponiendo que la lista de algoritmos propuestos por el host contiene MD5. Es posible que deba

actualizar la configuración del iniciador iSCSI del host para habilitar la compatibilidad con los algoritmos de seguridad.

Durante una actualización a Element 12.7 o posterior, si ya ha actualizado la configuración del iniciador iSCSI del host para enviar una solicitud de sesión con una lista que incluye algoritmos SHA, a medida que se reinician los nodos de almacenamiento, se activan los nuevos algoritmos seguros y se establecen sesiones iSCSI nuevas o reconectadas utilizando el protocolo más seguro. Todas las sesiones iSCSI existentes pasarán de MD5 a SHA durante la actualización. Si no actualiza la configuración del iniciador iSCSI del host para solicitar SHA, las sesiones iSCSI existentes seguirán utilizando MD5. Posteriormente, después de actualizar los algoritmos CHAP del iniciador iSCSI del host, las sesiones iSCSI deberían pasar gradualmente de MD5 a SHA con el tiempo, en función de las actividades de mantenimiento que resulten en reconexiones de sesiones iSCSI.

Por ejemplo, el iniciador iSCSI de host predeterminado en Red Hat Enterprise Linux (RHEL) 8.3 tiene el `node.session.auth.chap_algs = SHA3-256,SHA256,SHA1,MD5` Se ha comentado la configuración, lo que provoca que el iniciador iSCSI solo utilice MD5. Descomentar esta configuración en el host y reiniciar el iniciador iSCSI activa las sesiones iSCSI desde ese host para que comiencen a usar SHA3-256.

Si es necesario, puede utilizar el "Lista de sesiones ISCSIS" Método API para ver los algoritmos CHAP que se utilizan en cada sesión.

Crea una cuenta

Es posible crear una cuenta para permitir el acceso a los volúmenes.

Cada nombre de cuenta en el sistema debe ser único.

1. Seleccione **Administración** > **Cuentas**.
2. Haz clic en **Crear cuenta**.
3. Introduce un **Nombre de usuario**.
4. En la sección **Configuración CHAP**, introduzca la siguiente información:

   Deje los campos de credenciales en blanco para generar automáticamente cualquiera de las contraseñas.

   - **Secreto del iniciador** para la autenticación de sesión de nodo CHAP.
   - **Secreto de destino** para la autenticación de sesión de nodo CHAP.
5. Haz clic en **Crear cuenta**.

Ver detalles de la cuenta

Puede visualizar la actividad de rendimiento de cuentas individuales en formato gráfico.

La información del gráfico proporciona información sobre las operaciones de entrada/salida y el rendimiento de la cuenta. Los niveles de actividad promedio y máximo se muestran en incrementos de períodos de reporte de 10 segundos. Estas estadísticas incluyen la actividad de todos los volúmenes asignados a la cuenta.

1. Seleccione **Administración** > **Cuentas**.
2. Haz clic en el icono de Acciones para una cuenta.
3. Haga clic en **Ver detalles**.

Aquí tenéis algunos detalles:

- **Estado**: El estado de la cuenta. Valores posibles:
  - activa: Una cuenta activa.
  - bloqueado: Una cuenta bloqueada.
  - Eliminada: Una cuenta que ha sido borrada y purgada.
- **Volúmenes activos**: El número de volúmenes activos asignados a la cuenta.
- **Compresión**: La puntuación de eficiencia de compresión para los volúmenes asignados a la cuenta.
- **Desduplicación**: La puntuación de eficiencia de deduplicación para los volúmenes asignados a la cuenta.
- **Aprovisionamiento ligero**: La puntuación de eficiencia del aprovisionamiento ligero para los volúmenes asignados a la cuenta.
- **Eficiencia general**: La puntuación de eficiencia general para los volúmenes asignados a la cuenta.

Editar una cuenta

Puedes editar una cuenta para cambiar el estado, cambiar las claves CHAP o modificar el nombre de la cuenta.

Modificar la configuración CHAP en una cuenta o eliminar iniciadores o volúmenes de un grupo de acceso puede provocar que los iniciadores pierdan el acceso a los volúmenes de forma inesperada. Para verificar que el acceso al volumen no se pierda inesperadamente, cierre siempre las sesiones iSCSI que se verán afectadas por un cambio de cuenta o de grupo de acceso, y verifique que los iniciadores puedan volver a conectarse a los volúmenes después de que se hayan completado los cambios en la configuración del iniciador y la configuración del clúster.

> Los volúmenes persistentes asociados a los servicios de administración se asignan a una nueva cuenta que se crea durante la instalación o actualización. Si utiliza volúmenes persistentes, no modifique ni elimine la cuenta asociada.

1. Seleccione **Administración** > **Cuentas**.
2. Haz clic en el icono de Acciones para una cuenta.
3. En el menú que aparece, seleccione **Editar**.
4. **Opcional:** Edita el **Nombre de usuario**.
5. **Opcional:** Haga clic en la lista desplegable **Estado** y seleccione un estado diferente.

   > Al cambiar el estado a **bloqueado**, se terminan todas las conexiones iSCSI a la cuenta y esta deja de ser accesible. Los volúmenes asociados a la cuenta se mantienen; sin embargo, no son detectables mediante iSCSI.

6. **Opcional:** En **Configuración CHAP**, edite las credenciales **Secreto del iniciador** y **Secreto del destino** utilizadas para la autenticación de la sesión del nodo.

   > Si no modifica las credenciales de **Configuración CHAP**, estas permanecerán sin cambios. Si dejas en blanco los campos de credenciales, el sistema generará nuevas contraseñas.

7. Haz clic en **Guardar cambios**.

Eliminar una cuenta

Puedes eliminar una cuenta cuando ya no sea necesaria.

Elimine y purgue cualquier volumen asociado con la cuenta antes de eliminar la cuenta.

> Los volúmenes persistentes asociados a los servicios de administración se asignan a una nueva cuenta que se crea durante la instalación o actualización. Si utiliza volúmenes persistentes, no modifique ni elimine la cuenta asociada.

1. Seleccione **Administración** > **Cuentas**.
2. Haz clic en el icono de Acciones de la cuenta que deseas eliminar.
3. En el menú que aparece, seleccione **Eliminar**.
4. Confirma la acción.

Encuentra más información

- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Administrar cuentas de usuario de administrador de clúster

Puede administrar las cuentas de administrador de clúster para un sistema de almacenamiento SolidFire creando, eliminando y editando cuentas de administrador de clúster, cambiando la contraseña de administrador de clúster y configurando los ajustes de LDAP para administrar el acceso al sistema para los usuarios.

tipos de cuentas de administrador de clúster de almacenamiento

En un clúster de almacenamiento que ejecuta el software NetApp Element , pueden existir dos tipos de cuentas de administrador: la cuenta de administrador principal del clúster y una cuenta de administrador del clúster.

- **Cuenta de administrador principal del clúster**

  Esta cuenta de administrador se crea cuando se crea el clúster. Esta cuenta es la cuenta administrativa principal con el nivel más alto de acceso al clúster. Esta cuenta es análoga a un usuario root en un sistema Linux. Puedes cambiar la contraseña de esta cuenta de administrador.

- **Cuenta de administrador del clúster**

  Puede otorgar a una cuenta de administrador de clúster un rango limitado de acceso administrativo para realizar tareas específicas dentro de un clúster. Las credenciales asignadas a cada cuenta de administrador del clúster se utilizan para autenticar las solicitudes de API y de la interfaz de usuario de Element dentro del sistema de almacenamiento.

> Se requiere una cuenta de administrador de clúster local (no LDAP) para acceder a los nodos activos de un clúster a través de la interfaz de usuario por nodo. No se requieren credenciales de cuenta para acceder a un nodo que aún no forma parte de un clúster.

Ver detalles de administración del clúster

1. Para crear una cuenta de administrador de clúster (no LDAP) para todo el clúster, realice las siguientes acciones:
   a. Haz clic en **Usuarios** > **Administradores del clúster**.
2. En la página Administradores del clúster de la pestaña Usuarios, puede ver la siguiente información.

   - **ID**: Número secuencial asignado a la cuenta del administrador del clúster.
   - **Nombre de usuario**: El nombre asignado a la cuenta de administrador del clúster cuando se creó.
   - **Acceso**: Los permisos de usuario asignados a la cuenta de usuario. Valores posibles:
     - leer
     - informes
     - nodos
     - unidades
     - volúmenes
     - cuentas
     - administradores de clúster
     - administrador
     - Administrador de soporte

     > Todos los permisos están disponibles para el tipo de acceso de administrador.
     >
     > Existen tipos de acceso disponibles a través de la API que no están disponibles en la interfaz de usuario de Element.

   +

   - **Tipo**: El tipo de administrador del clúster. Valores posibles:
     - Grupo
     - LDAP
   - **Atributos**: Si la cuenta de administrador del clúster se creó utilizando la API de Element, esta columna muestra cualquier par nombre-valor que se haya establecido utilizando ese método.

     Ver"Referencia de la API de NetApp Element Software" .

Crea una cuenta de administrador de clúster

Puede crear nuevas cuentas de administrador de clúster con permisos para permitir o restringir el acceso a áreas específicas del sistema de almacenamiento. Cuando configuras los permisos de la cuenta de administrador del clúster, el sistema otorga derechos de solo lectura para cualquier permiso que no asignes al administrador del clúster.

Si desea crear una cuenta de administrador de clúster LDAP, asegúrese de que LDAP esté configurado en el clúster antes de comenzar.

"Habilite la autenticación LDAP con la interfaz de usuario de Element."

Posteriormente, puede cambiar los privilegios de la cuenta de administrador del clúster para la generación de informes, nodos, unidades, volúmenes, cuentas y acceso a nivel de clúster. Cuando habilitas un permiso, el sistema asigna acceso de escritura para ese nivel. El sistema otorga al usuario administrador acceso de solo lectura para los niveles que usted no seleccione.

Posteriormente también podrá eliminar cualquier cuenta de usuario administrador del clúster creada por un administrador del sistema. No se puede eliminar la cuenta de administrador principal del clúster que se creó cuando se creó el clúster.

1. Para crear una cuenta de administrador de clúster (no LDAP) para todo el clúster, realice las siguientes acciones:
   a. Haz clic en **Usuarios** > **Administradores del clúster**.
   b. Haga clic en **Crear administrador de clúster**.
   c. Seleccione el tipo de usuario **Cluster**.
   d. Introduce un nombre de usuario y una contraseña para la cuenta y confirma la contraseña.
   e. Seleccione los permisos de usuario que se aplicarán a la cuenta.
   f. Seleccione la casilla de verificación para aceptar el Acuerdo de Licencia de Usuario Final.
   g. Haga clic en **Crear administrador de clúster**.
2. Para crear una cuenta de administrador de clúster en el directorio LDAP, realice las siguientes acciones:
   a. Haga clic en **Clúster** > **LDAP**.
   b. Asegúrese de que la autenticación LDAP esté habilitada.
   c. Haz clic en **Probar autenticación de usuario** y copia el nombre distintivo que aparece para el usuario o uno de los grupos a los que pertenece el usuario para que puedas pegarlo más tarde.
   d. Haz clic en **Usuarios** > **Administradores del clúster**.
   e. Haga clic en **Crear administrador de clúster**.
   f. Seleccione el tipo de usuario LDAP.
   g. En el campo Nombre distintivo, siga el ejemplo del cuadro de texto para introducir un nombre distintivo completo para el usuario o grupo. Como alternativa, péguelo del nombre distinguido que copió anteriormente.

      Si el nombre distinguido forma parte de un grupo, cualquier usuario que sea miembro de ese grupo en el servidor LDAP tendrá los permisos de esta cuenta de administrador.

   Para agregar usuarios o grupos de administradores de clúster LDAP, el formato general del nombre de usuario es “LDAP:<Nombre distinguido completo>”.

   a. Seleccione los permisos de usuario que se aplicarán a la cuenta.
   b. Seleccione la casilla de verificación para aceptar el Acuerdo de Licencia de Usuario Final.
   c. Haga clic en **Crear administrador de clúster**.

Editar permisos de administrador del clúster

Puede cambiar los privilegios de la cuenta de administrador del clúster para la generación de informes, nodos, unidades, volúmenes, cuentas y acceso a nivel de clúster. Cuando habilitas un permiso, el sistema asigna acceso de escritura para ese nivel. El sistema otorga al usuario administrador acceso de solo lectura para los niveles que usted no seleccione.

1. Haz clic en **Usuarios** > **Administradores del clúster**.
2. Haga clic en el icono Acciones del administrador del clúster que desea editar.
3. Haga clic en **Editar**.
4. Seleccione los permisos de usuario que se aplicarán a la cuenta.
5. Haz clic en **Guardar cambios**.

Cambiar las contraseñas de las cuentas de administrador del clúster

Puede utilizar la interfaz de usuario de Element para cambiar las contraseñas de administrador del clúster.

1. Haz clic en **Usuarios** > **Administradores del clúster**.
2. Haga clic en el icono Acciones del administrador del clúster que desea editar.
3. Haga clic en **Editar**.
4. En el campo Cambiar contraseña, introduzca una nueva contraseña y confírmela.
5. Haz clic en **Guardar cambios**.

Información relacionada

- "Obtenga información sobre los tipos de acceso disponibles para las API de Element."
- "Habilite la autenticación LDAP con la interfaz de usuario de Element."
- "Deshabilitar LDAP"
- "Plugin de NetApp Element para vCenter Server"

Administrar LDAP

Puede configurar el Protocolo Ligero de Acceso a Directorios (LDAP) para habilitar la funcionalidad de inicio de sesión segura basada en directorios para el almacenamiento SolidFire . Puede configurar LDAP a nivel de clúster y autorizar usuarios y grupos LDAP.

La gestión de LDAP implica configurar la autenticación LDAP en un clúster SolidFire utilizando un entorno de Microsoft Active Directory existente y probar la configuración.

Puedes utilizar direcciones IPv4 e IPv6.

Habilitar LDAP implica los siguientes pasos generales, descritos en detalle:

1. **Complete los pasos de preconfiguración para la compatibilidad con LDAP**. Compruebe que dispone de todos los datos necesarios para configurar la autenticación LDAP.
2. **Habilitar la autenticación LDAP**. Utilice la interfaz de usuario de Element o la API de Element.
3. **Validar la configuración LDAP**. Opcionalmente, verifique que el clúster esté configurado con los valores correctos ejecutando el método de la API GetLdapConfiguration o revisando la configuración de LCAP mediante la interfaz de usuario de Element.
4. **Prueba la autenticación LDAP** (con el `readonly` usuario). Compruebe que la configuración LDAP es correcta ejecutando el método API TestLdapAuthentication o utilizando la interfaz de usuario de Element. Para esta prueba inicial, utilice el nombre de usuario “sAMAccountName” de `readonly` usuario. Esto validará que su clúster esté configurado correctamente para la autenticación LDAP y también validará que el `readonly` Las credenciales y el acceso son correctos. Si este paso falla, repita los pasos del 1 al 3.

5. **Prueba la autenticación LDAP** (con una cuenta de usuario que quieras agregar). Repita el paso 4 con una cuenta de usuario que desee agregar como administrador del clúster de Element. Copia el `distinguished` nombre (DN) o el usuario (o el grupo). Este DN se utilizará en el paso 6.
6. **Agregue el administrador del clúster LDAP** (copie y pegue el DN del paso de prueba de autenticación LDAP). Utilizando la interfaz de usuario de Element o el método de la API AddLdapClusterAdmin, cree un nuevo usuario administrador de clúster con el nivel de acceso adecuado. Para el nombre de usuario, pegue el DN completo que copió en el paso 5. Esto garantiza que el DN esté formateado correctamente.
7. **Prueba el acceso de administrador del clúster**. Inicie sesión en el clúster utilizando el usuario administrador del clúster LDAP recién creado. Si has añadido un grupo LDAP, puedes iniciar sesión como cualquier usuario de ese grupo.

Complete los pasos de preconfiguración para la compatibilidad con LDAP.

Antes de habilitar la compatibilidad con LDAP en Element, debe configurar un servidor de Active Directory de Windows y realizar otras tareas de preconfiguración.

Pasos

1. Configurar un servidor de directorio activo de Windows.
2. **Opcional:** Habilitar la compatibilidad con LDAPS.
3. Crear usuarios y grupos.
4. Cree una cuenta de servicio de solo lectura (como “sfreadonly”) para usarla para buscar en el directorio LDAP.

Habilite la autenticación LDAP con la interfaz de usuario de Element.

Puede configurar la integración del sistema de almacenamiento con un servidor LDAP existente. Esto permite a los administradores de LDAP gestionar de forma centralizada el acceso de los usuarios al sistema de almacenamiento.

Puede configurar LDAP mediante la interfaz de usuario de Element o la API de Element. Este procedimiento describe cómo configurar LDAP utilizando la interfaz de usuario de Element.

Este ejemplo muestra cómo configurar la autenticación LDAP en SolidFire y utiliza `SearchAndBind` como tipo de autenticación. El ejemplo utiliza un único servidor Active Directory de Windows Server 2012 R2.

Pasos

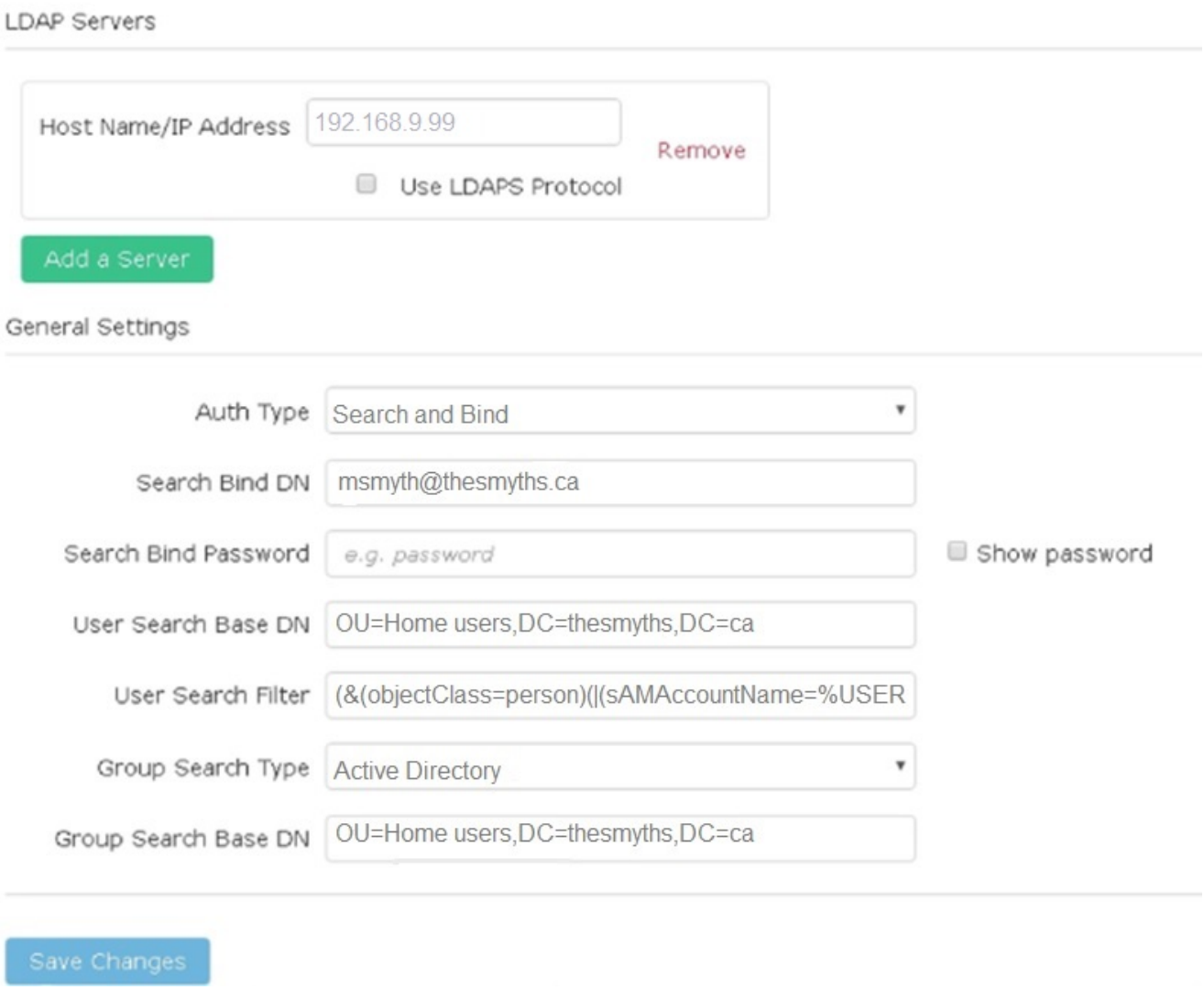
1. Haga clic en **Clúster** > **LDAP**.
2. Haga clic en **Sí** para habilitar la autenticación LDAP.
3. Haz clic en **Añadir un servidor**.
4. Introduzca el **Nombre de host/Dirección IP**.

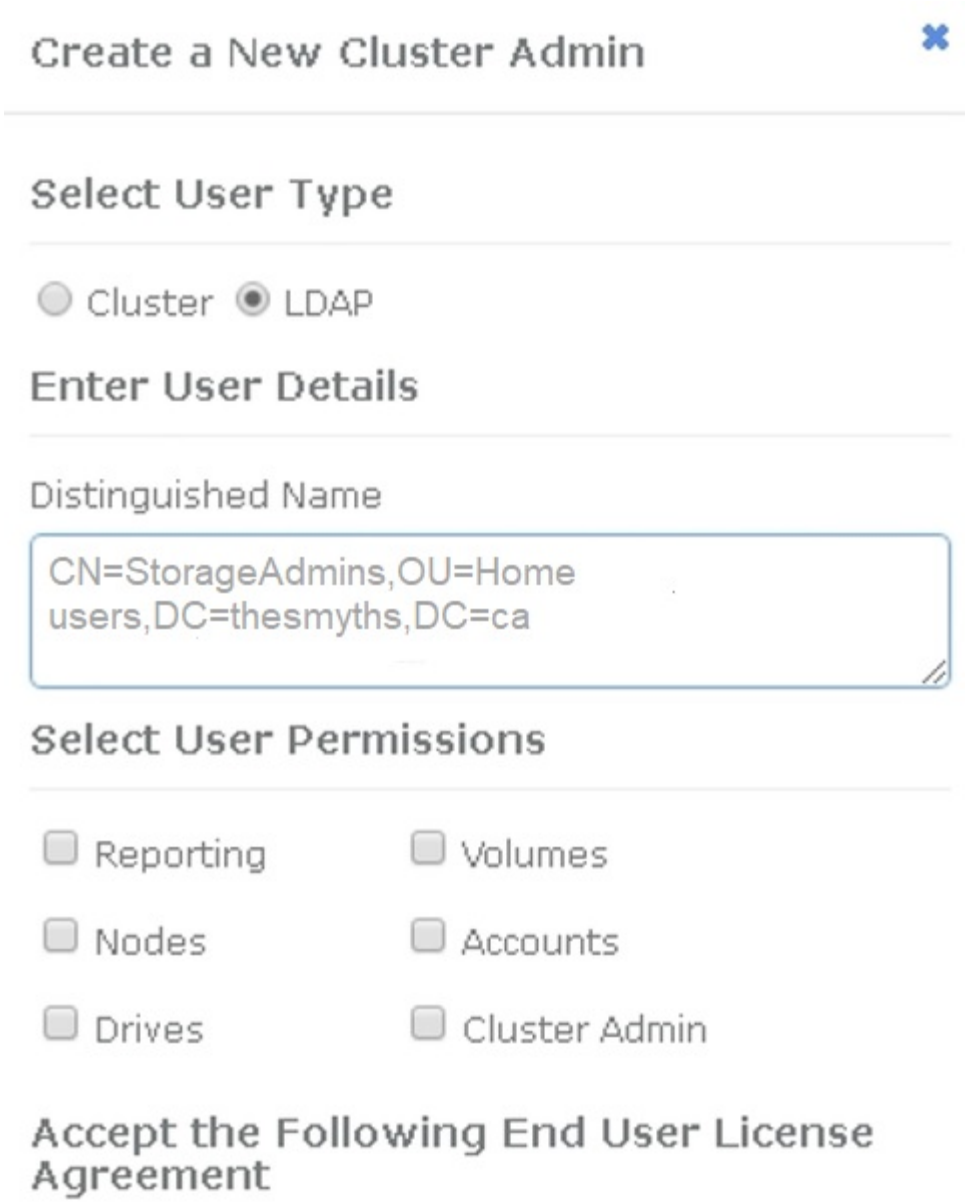
   También se puede introducir un número de puerto personalizado opcional.

   Por ejemplo, para agregar un número de puerto personalizado, ingrese <nombre de host o dirección IP>:<número de puerto>

5. **Opcional:** Seleccione **Usar protocolo LDAPS**.
6. Introduzca la información requerida en **Ajustes generales**.



7. Haga clic en **Habilitar LDAP**.
8. Haz clic en **Probar autenticación de usuario** si quieres probar el acceso al servidor de un usuario.
9. Copie el nombre distintivo y la información del grupo de usuarios que aparece para utilizarlos posteriormente al crear administradores de clúster.
10. Haz clic en **Guardar cambios** para guardar la nueva configuración.
11. Para crear un usuario en este grupo para que cualquiera pueda iniciar sesión, complete lo siguiente:
    a. Haz clic en **Usuario** > **Ver**.



b. Para el nuevo usuario, haga clic en **LDAP** para Tipo de usuario y pegue el grupo que copió en el campo Nombre distintivo.
c. Seleccione los permisos, normalmente todos los permisos.
d. Desplácese hacia abajo hasta el Acuerdo de Licencia de Usuario Final y haga clic en **Acepto**.
e. Haga clic en **Crear administrador de clúster**.

   Ahora tienes un usuario con el valor de un grupo de Active Directory.

Para probar esto, cierre sesión en la interfaz de usuario de Element y vuelva a iniciar sesión como usuario de ese grupo.

Habilite la autenticación LDAP con la API de Element.

Puede configurar la integración del sistema de almacenamiento con un servidor LDAP existente. Esto permite a los administradores de LDAP gestionar de forma centralizada el acceso de los usuarios al sistema de almacenamiento.

Puede configurar LDAP mediante la interfaz de usuario de Element o la API de Element. Este procedimiento describe cómo configurar LDAP utilizando la API de Element.

Para aprovechar la autenticación LDAP en un clúster de SolidFire , primero debe habilitar la autenticación LDAP en el clúster mediante el siguiente método: `EnableLdapAuthentication` Método API.

Pasos

1. Habilite primero la autenticación LDAP en el clúster utilizando `EnableLdapAuthentication` Método API.
2. Ingrese la información requerida.

```
{
     "method":"EnableLdapAuthentication",
     "params":{
          "authType": "SearchAndBind",
          "groupSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
          "groupSearchType": "ActiveDirectory",
          "searchBindDN": "SFReadOnly@prodtest.solidfire.net",
          "searchBindPassword": "ReadOnlyPW",
          "userSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net ",
          "userSearchFilter":
"(&(objectClass=person)(sAMAccountName=%USERNAME%))"
          "serverURIs": [
               "ldap://172.27.1.189",
          [
     },
  "id":"1"
}
```

3. Cambie los valores de los siguientes parámetros:

Parámetros utilizados	Descripción
Tipo de autenticación: Buscar y vincular	Indica que el clúster utilizará la cuenta de servicio de solo lectura para buscar primero al usuario que se está autenticando y, posteriormente, vincularlo si se encuentra y se autentica.
groupSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	Especifica la ubicación en el árbol LDAP donde comenzar la búsqueda de grupos. Para este ejemplo, hemos utilizado la raíz de nuestro árbol. Si su árbol LDAP es muy grande, es posible que desee configurarlo en un subárbol más granular para disminuir los tiempos de búsqueda.

Parámetros utilizados	Descripción
userSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	Especifica la ubicación en el árbol LDAP donde comenzar la búsqueda de usuarios. Para este ejemplo, hemos utilizado la raíz de nuestro árbol. Si su árbol LDAP es muy grande, es posible que desee configurarlo en un subárbol más granular para disminuir los tiempos de búsqueda.
groupSearchType: ActiveDirectory	Utiliza el servidor Active Directory de Windows como servidor LDAP.

`userSearchFilter: "(&(objectClass=person)(sAMAccountName=%USERNAME%))"`
 	
Para usar el nombre principal de usuario (dirección de correo electrónico para iniciar sesión), puede cambiar el filtro de búsqueda de usuario a:
 	
`"(&(objectClass=person)(userPrincipalName=%USERNAME%))"`
 	
O bien, para buscar tanto userPrincipalName como sAMAccountName, puede utilizar el siguiente userSearchFilter:
 	
`"(&(objectClass=person)(`
	(sAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%)))" ----

Utilizamos sAMAccountName como nombre de usuario para iniciar sesión en el clúster SolidFire . Estos ajustes le indican a LDAP que busque el nombre de usuario especificado durante el inicio de sesión en el atributo sAMAccountName y también que limite la búsqueda a las entradas que tengan "person" como valor en el atributo objectClass.	searchBindDN
Este es el nombre distintivo del usuario de solo lectura que se utilizará para buscar en el directorio LDAP. Para Active Directory, lo más sencillo suele ser utilizar el nombre principal de usuario (formato de dirección de correo electrónico) para el usuario.	buscarContraseñaVinculada

Para probar esto, cierre sesión en la interfaz de usuario de Element y vuelva a iniciar sesión como usuario de ese grupo.

Ver detalles de LDAP

Consulte la información LDAP en la página LDAP de la pestaña Clúster.

Debe habilitar LDAP para ver esta configuración de LDAP.

1. Para ver los detalles de LDAP con la interfaz de usuario de Element, haga clic en **Clúster** > **LDAP**.
   - **Nombre de host/Dirección IP**: Dirección de un servidor de directorio LDAP o LDAPS.
   - **Tipo de autenticación**: El método de autenticación del usuario. Valores posibles:
     - Enlace directo
     - Buscar y enlazar
   - **DN de enlace de búsqueda**: Un DN completo para iniciar sesión y realizar una búsqueda LDAP del usuario (necesita acceso de nivel de enlace al directorio LDAP).
   - **Contraseña de enlace de búsqueda**: Contraseña utilizada para autenticar el acceso al servidor LDAP.
   - **DN base de búsqueda de usuarios**: El DN base del árbol utilizado para iniciar la búsqueda de usuarios. El sistema busca en el subárbol desde la ubicación especificada.
   - **Filtro de búsqueda de usuario**: Introduzca lo siguiente utilizando su nombre de dominio:

     ```
     (&(objectClass=person)(|(sAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%)))
     ```

   - **Tipo de búsqueda de grupo**: Tipo de búsqueda que controla el filtro de búsqueda de grupo predeterminado utilizado. Valores posibles:
     - Active Directory: Membresía anidada de todos los grupos LDAP de un usuario.
     - Sin grupos: No hay soporte para grupos.
     - DN de miembro: Grupos de estilo DN de miembro (de un solo nivel).
   - **DN base de búsqueda de grupo**: El DN base del árbol utilizado para iniciar la búsqueda de grupo. El sistema busca en el subárbol desde la ubicación especificada.
   - **Prueba de autenticación de usuario**: Después de configurar LDAP, utilice esto para probar la autenticación de nombre de usuario y contraseña para el servidor LDAP. Introduce una cuenta que ya exista para probar esto. Aparece el nombre distintivo y la información del grupo de usuarios, que puede copiar para su uso posterior al crear administradores de clúster.

Prueba la configuración LDAP

Tras configurar LDAP, debe probarlo utilizando la interfaz de usuario de Element o la API de Element. `TestLdapAuthentication` método.

Pasos

1. Para probar la configuración LDAP con la interfaz de usuario de Element, haga lo siguiente:
   a. Haga clic en **Clúster** > **LDAP**.
   b. Haga clic en **Probar autenticación LDAP**.
   c. Resuelva cualquier problema utilizando la información de la siguiente tabla:

Mensaje de error	Descripción
`xLDAPUserNotFound`	• No se encontró al usuario que se estaba probando en la configuración. `userSearchBaseDN` subárbol. • El `userSearchFilter` está configurado incorrectamente.
`xLDAPBindFailed (Error: Invalid credentials)`	• El nombre de usuario que se está probando es un usuario LDAP válido, pero la contraseña proporcionada es incorrecta. • El nombre de usuario que se está probando es un usuario LDAP válido, pero la cuenta está actualmente deshabilitada.
`xLDAPSearchBindFailed (Error: Can't contact LDAP server)`	La URI del servidor LDAP es incorrecta.
`xLDAPSearchBindFailed (Error: Invalid credentials)`	El nombre de usuario o la contraseña de solo lectura están configurados incorrectamente.
`xLDAPSearchFailed (Error: No such object)`	El `userSearchBaseDN` no es una ubicación válida dentro del árbol LDAP.
`xLDAPSearchFailed (Error: Referral)`	• El `userSearchBaseDN` no es una ubicación válida dentro del árbol LDAP. • El `userSearchBaseDN` y `groupSearchBaseDN` están en una unidad organizativa anidada. Esto puede causar problemas de permisos. La solución alternativa consiste en incluir la OU en las entradas DN base de usuario y grupo, (por ejemplo: `ou=storage, cn=company, cn=com`)

2. Para probar la configuración LDAP con la API de Element, haga lo siguiente:
   a. Llama al método TestLdapAuthentication.

```
{
  "method":"TestLdapAuthentication",
     "params":{
        "username":"admin1",
        "password":"admin1PASS
      },
      "id": 1
}
```

b. Revisa los resultados. Si la llamada a la API se realiza correctamente, los resultados incluyen el nombre distintivo del usuario especificado y una lista de los grupos a los que pertenece el usuario.

```
{
"id": 1
     "result": {
         "groups": [

"CN=StorageMgmt,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
         ],
         "userDN": "CN=Admin1
Jones,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
     }
}
```

Deshabilitar LDAP

Puede deshabilitar la integración LDAP mediante la interfaz de usuario de Element.

Antes de comenzar, debe anotar todas las opciones de configuración, ya que deshabilitar LDAP borra todas las configuraciones.

Pasos

1. Haga clic en **Clúster** > **LDAP**.
2. Haga clic en **No**.
3. Haga clic en **Deshabilitar LDAP**.

Encuentra más información

- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Administra tu sistema

Administra tu sistema

Puedes gestionar tu sistema en la interfaz de usuario de Element. Esto incluye habilitar la autenticación multifactor, administrar la configuración del clúster, admitir los estándares federales de procesamiento de información (FIPS) y utilizar la administración de claves externas.

- "Habilitar la autenticación multifactor"
- "Configurar los ajustes del clúster"
- "Cree un clúster que admita unidades FIPS."
- "Comience con la administración de claves externas"

Para más información

- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Habilitar la autenticación multifactor

Configurar la autenticación multifactor

La autenticación multifactor (MFA) utiliza un proveedor de identidad (IdP) de terceros a través del lenguaje de marcado de aserción de seguridad (SAML) para gestionar las sesiones de usuario. La autenticación multifactor (MFA) permite a los administradores configurar factores de autenticación adicionales según sea necesario, como contraseña y mensaje de texto, y contraseña y mensaje de correo electrónico.

Puedes utilizar estos pasos básicos a través de la API de Element para configurar tu clúster para que utilice la autenticación multifactor.

Los detalles de cada método de la API se pueden encontrar en el "Referencia de la API de elementos".

1. Cree una nueva configuración de proveedor de identidad (IdP) de terceros para el clúster llamando al siguiente método de la API y pasando los metadatos del IdP en formato JSON: `CreateIdpConfiguration`

   Los metadatos del IdP, en formato de texto plano, se recuperan del IdP de terceros. Es necesario validar estos metadatos para asegurar que estén formateados correctamente en JSON. Existen numerosas aplicaciones de formato JSON disponibles que puedes utilizar, por ejemplo: https://freeformatter.com/json-escape.html.

2. Recupere los metadatos del clúster, a través de spMetadataUrl, para copiarlos al IdP de terceros llamando al siguiente método de API: `ListIdpConfigurations`

   spMetadataUrl es una URL utilizada para recuperar metadatos del proveedor de servicios del clúster para el IdP con el fin de establecer una relación de confianza.

3. Configure las aserciones SAML en el IdP de terceros para incluir el atributo “NameID” para identificar de forma única a un usuario para el registro de auditoría y para que el cierre de sesión único funcione correctamente.

4. Cree una o más cuentas de usuario de administrador de clúster autenticadas por un IdP de terceros para la autorización llamando al siguiente método de API:`AddIdpClusterAdmin`

   > El nombre de usuario del administrador del clúster IdP debe coincidir con la asignación de nombre/valor del atributo SAML para lograr el efecto deseado, como se muestra en los siguientes ejemplos:

   - email=bob@company.com — donde el IdP está configurado para liberar una dirección de correo electrónico en los atributos SAML.
   - grupo=administrador-de-clúster - donde el IdP está configurado para liberar una propiedad de grupo a la que todos los usuarios deberían tener acceso. Tenga en cuenta que, por motivos de seguridad, el emparejamiento de nombre/valor del atributo SAML distingue entre mayúsculas y minúsculas.
5. Habilite la autenticación multifactor (MFA) para el clúster llamando al siguiente método de la API: `EnableIdpAuthentication`

Encuentra más información

- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Información adicional sobre la autenticación multifactor

Debes tener en cuenta las siguientes advertencias en relación con la autenticación multifactor.

- Para actualizar los certificados IdP que ya no son válidos, deberá utilizar un usuario administrador que no sea IdP para llamar al siguiente método de la API: `UpdateIdpConfiguration`
- La autenticación multifactor (MFA) es incompatible con certificados de menos de 2048 bits de longitud. Por defecto, se crea un certificado SSL de 2048 bits en el clúster. Debe evitar establecer un certificado de tamaño reducido al llamar al método de la API: `SetSSLCertificate`

  > Si el clúster utiliza un certificado de menos de 2048 bits antes de la actualización, el certificado del clúster debe actualizarse con un certificado de 2048 bits o superior después de la actualización a Element 12.0 o posterior.

- Los usuarios administradores de IdP no pueden utilizarse para realizar llamadas a la API directamente (por ejemplo, a través de SDK o Postman) ni para otras integraciones (por ejemplo, OpenStack Cinder o el complemento de vCenter). Si necesita crear usuarios con estas capacidades, agregue usuarios administradores de clúster LDAP o usuarios administradores de clúster locales.

Encuentra más información

- "Gestionar el almacenamiento con la API de Element"
- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Configurar los ajustes del clúster

Habilitar y deshabilitar el cifrado en reposo para un clúster

Con los clústeres SolidFire , puede cifrar todos los datos en reposo almacenados en las unidades del clúster. Puede habilitar la protección de unidades de autocifrado (SED) en todo el clúster mediante cualquiera de los siguientes métodos:"Cifrado en reposo basado en hardware o software" .

Puede habilitar el cifrado de hardware en reposo mediante la interfaz de usuario o la API de Element. Habilitar la función de cifrado de hardware en reposo no afecta al rendimiento ni a la eficiencia del clúster. Solo puede habilitar el cifrado de software en reposo utilizando la API de Element.

El cifrado de datos en reposo basado en hardware no está habilitado de forma predeterminada durante la creación del clúster y se puede habilitar y deshabilitar desde la interfaz de usuario de Element.

> Para los clústeres de almacenamiento all-flash SolidFire , el cifrado de software en reposo debe habilitarse durante la creación del clúster y no puede deshabilitarse después de que se haya creado el clúster.

Lo que necesitarás

- Usted tiene privilegios de administrador de clúster para habilitar o cambiar la configuración de cifrado.
- Para el cifrado en reposo basado en hardware, debe asegurarse de que el clúster se encuentre en buen estado antes de cambiar la configuración de cifrado.
- Si va a deshabilitar el cifrado, dos nodos deben participar en un clúster para acceder a la clave para deshabilitar el cifrado en una unidad.

Comprobar el estado del cifrado en reposo

Para ver el estado actual del cifrado en reposo y/o del cifrado de software en reposo en el clúster, utilice la siguiente información:"Obtener información del clúster" método. Puedes usar el"Obtener información de cifrado de software en reposo" Método para obtener información sobre el clúster que utiliza para cifrar los datos en reposo.

> El panel de control de la interfaz de usuario del software Element en `https://<MVIP>/` Actualmente solo se muestra el estado de cifrado en reposo para el cifrado basado en hardware.

Opciones

- Habilitar el cifrado basado en hardware en reposo
- Habilitar el cifrado basado en software en reposo
- Deshabilitar el cifrado basado en hardware en reposo

Habilitar el cifrado basado en hardware en reposo

> Para habilitar el cifrado en reposo mediante una configuración de administración de claves externa, debe habilitar el cifrado en reposo a través de"API" . Habilitar esta función mediante el botón de la interfaz de usuario de Element existente hará que se vuelva a utilizar la generación interna de claves.

1. Desde la interfaz de usuario de Element, seleccione **Cluster** > **Settings**.

2. Seleccione **Habilitar cifrado en reposo**.

Habilitar el cifrado basado en software en reposo

> El cifrado de software en reposo no se puede deshabilitar después de que se haya habilitado en el clúster.

1. Durante la creación del clúster, ejecute el"método de creación de clúster" con `enableSoftwareEncryptionAtRest` empezar a `true` .

Deshabilitar el cifrado basado en hardware en reposo

1. Desde la interfaz de usuario de Element, seleccione **Cluster** > **Settings**.
2. Seleccione **Deshabilitar el cifrado en reposo**.

Encuentra más información

- "Documentación del software SolidFire y Element"
- "Documentación para versiones anteriores de los productos NetApp SolidFire y Element"

Establezca el umbral completo del clúster

Puedes cambiar el nivel en el que el sistema genera una advertencia de llenado del clúster de bloques siguiendo los pasos que se indican a continuación. Además, puede utilizar el método de la API ModifyClusterFullThreshold para cambiar el nivel en el que el sistema genera una advertencia de bloqueo o de metadatos.

Lo que necesitarás

Debe tener privilegios de administrador de clúster.

Pasos

1. Haz clic en **Clúster** > **Configuración**.
2. En la sección Configuración completa del clúster, ingrese un porcentaje en **Generar una alerta de advertencia cuando quede un _% de capacidad antes de que Helix no pueda recuperarse de una falla de nodo**.
3. Haz clic en **Guardar cambios**.

Encuentra más información

"¿Cómo se calculan los umbrales de blockSpace para Element?"

Habilitar y deshabilitar el balanceo de carga de volumen

A partir de Element 12.8, puede usar el balanceo de carga de volumen para equilibrar los volúmenes entre nodos según las IOPS reales de cada volumen en lugar de las IOPS mínimas configuradas en la política de QoS. Puede activar y desactivar el balanceo de carga de volumen, que está desactivado de forma predeterminada, mediante la interfaz de usuario o la API de Element.

Pasos

1. Seleccione **Clúster** > **Configuración**.
2. En la sección Específica del clúster, cambie el estado de Balanceo de carga de volumen:

   Habilitar el equilibrio de carga de volumen

   Seleccione **Habilitar balanceo de carga en IOPS reales** y confirme su selección.

   Deshabilitar el equilibrio de carga de volumen:

   Seleccione **Deshabilitar el balanceo de carga en IOPS reales** y confirme su selección.

3. Opcionalmente, seleccione **Informes** > **Resumen** para confirmar el cambio de estado de Balance en IOPS reales. Es posible que tengas que desplazarte hacia abajo en la información de estado del clúster para ver el estado.

Encuentra más información

- "Habilite el balanceo de carga de volumen mediante la API"
- "Deshabilitar el balanceo de carga de volumen mediante la API"
- "Crear y gestionar políticas de QoS de volumen"

Habilitar y deshabilitar el acceso de soporte

Puede habilitar el acceso de soporte para permitir temporalmente que el personal de soporte de NetApp acceda a los nodos de almacenamiento a través de SSH para la resolución de problemas.

Debe tener privilegios de administrador de clúster para cambiar el acceso de soporte.

1. Haz clic en **Clúster** > **Configuración**.
2. En la sección Habilitar/Deshabilitar acceso de soporte, ingrese la duración (en horas) durante la cual desea permitir que el soporte tenga acceso.
3. Haga clic en **Habilitar acceso de soporte**.
4. **Opcional:** Para deshabilitar el acceso al soporte, haga clic en **Deshabilitar acceso al soporte**.

Gestionar el banner de Condiciones de uso

Puedes habilitar, editar o configurar un banner que contenga un mensaje para el usuario.

Opciones

Habilita el banner de Condiciones de uso Edita el banner de Condiciones de uso Desactivar el banner de Condiciones de uso

Habilita el banner de Condiciones de uso

Puedes habilitar un banner de Condiciones de uso que aparezca cuando un usuario inicie sesión en la interfaz de usuario de Element. Cuando el usuario haga clic en el banner, aparecerá un cuadro de diálogo de texto con el mensaje que ha configurado para el clúster. El banner puede eliminarse en cualquier momento.

Debe tener privilegios de administrador de clúster para habilitar la funcionalidad de Términos de uso.

1. Haz clic en **Usuarios** > **Condiciones de uso**.
2. En el formulario **Condiciones de uso**, introduzca el texto que se mostrará en el cuadro de diálogo de Condiciones de uso.

   No exceda los 4096 caracteres.

3. Haga clic en **Habilitar**.

Edita el banner de Condiciones de uso

Puedes editar el texto que ve un usuario cuando selecciona el banner de inicio de sesión de los Términos de uso.

Lo que necesitarás

- Para configurar las Condiciones de uso, debe tener privilegios de administrador de clúster.
- Asegúrese de que la función de Condiciones de uso esté habilitada.

Pasos

1. Haz clic en **Usuarios** > **Condiciones de uso**.
2. En el cuadro de diálogo **Condiciones de uso**, edite el texto que desea que aparezca.

   No exceda los 4096 caracteres.

3. Haz clic en **Guardar cambios**.

Desactivar el banner de Condiciones de uso

Puedes desactivar el banner de Condiciones de uso. Con el banner desactivado, ya no se le solicita al usuario que acepte los términos de uso al utilizar la interfaz de usuario de Element.

Lo que necesitarás

- Para configurar las Condiciones de uso, debe tener privilegios de administrador de clúster.
- Asegúrese de que las Condiciones de uso estén habilitadas.

Pasos

1. Haz clic en **Usuarios** > **Condiciones de uso**.
2. Haga clic en **Desactivar**.

Configurar el protocolo de tiempo de red

Configure los servidores del Protocolo de Tiempo de Red (NTP) para que el clúster los consulte.

Puede instruir a cada nodo de un clúster para que consulte a un servidor de Protocolo de Tiempo de Red (NTP) para obtener actualizaciones. El clúster solo contacta con los servidores configurados y les solicita información NTP.

El protocolo NTP se utiliza para sincronizar los relojes a través de una red. La conexión a un servidor NTP interno o externo debe formar parte de la configuración inicial del clúster.

Configure NTP en el clúster para que apunte a un servidor NTP local. Puede utilizar la dirección IP o el

nombre de host FQDN. El servidor NTP predeterminado al momento de la creación del clúster se establece en us.pool.ntp.org; sin embargo, no siempre se puede establecer una conexión con este sitio dependiendo de la ubicación física del clúster SolidFire .

El uso del FQDN depende de si la configuración DNS del nodo de almacenamiento individual está implementada y operativa. Para ello, configure los servidores DNS en cada nodo de almacenamiento y asegúrese de que los puertos estén abiertos consultando la página de Requisitos de puertos de red.

Puedes introducir hasta cinco servidores NTP diferentes.

Puedes utilizar direcciones IPv4 e IPv6.

Lo que necesitarás

Para configurar este ajuste, debe tener privilegios de administrador de clúster.

Pasos

1. Configure una lista de direcciones IP y/o nombres de dominio completos (FQDN) en la configuración del servidor.
2. Asegúrese de que el DNS esté configurado correctamente en los nodos.
3. Haz clic en **Clúster** > **Configuración**.
4. En Configuración del protocolo de tiempo de red, seleccione **No**, que utiliza la configuración NTP estándar.
5. Haz clic en **Guardar cambios**.

Encuentra más información

- "Configure el clúster para que escuche las transmisiones NTP."
- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Configure el clúster para que escuche las transmisiones NTP.

Al utilizar el modo de difusión, puede indicar a cada nodo de un clúster que escuche en la red los mensajes de difusión del Protocolo de tiempo de red (NTP) procedentes de un servidor determinado.

El protocolo NTP se utiliza para sincronizar los relojes a través de una red. La conexión a un servidor NTP interno o externo debe formar parte de la configuración inicial del clúster.

Lo que necesitarás

- Para configurar este ajuste, debe tener privilegios de administrador de clúster.
- Debe configurar un servidor NTP en su red como servidor de difusión.

Pasos

1. Haz clic en **Clúster** > **Configuración**.
2. Introduzca en la lista de servidores el servidor o servidores NTP que utilizan el modo de difusión.
3. En Configuración del protocolo de tiempo de red, seleccione **Sí** para usar un cliente de difusión.
4. Para configurar el cliente de difusión, en el campo **Servidor**, introduzca el servidor NTP que configuró en modo de difusión.

5. Haz clic en **Guardar cambios**.

Encuentra más información

- "Configure los servidores del Protocolo de Tiempo de Red (NTP) para que el clúster los consulte."
- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Administrar SNMP

Obtenga más información sobre SNMP

Puede configurar el Protocolo Simple de Administración de Red (SNMP) en su clúster.

Puede seleccionar un solicitante SNMP, seleccionar qué versión de SNMP utilizar, identificar el usuario del modelo de seguridad basado en usuario (USM) de SNMP y configurar traps para monitorear el clúster SolidFire . También puede ver y acceder a los archivos de la base de datos de información de gestión.

Puedes utilizar direcciones IPv4 e IPv6.

Detalles SNMP

En la página SNMP de la pestaña Clúster, puede ver la siguiente información.

- **MIB SNMP**

  Los archivos MIB que puede ver o descargar.

- **Configuración general de SNMP**

  Puede habilitar o deshabilitar SNMP. Una vez habilitado SNMP, puede elegir qué versión utilizar. Si utiliza la versión 2, puede agregar solicitantes, y si utiliza la versión 3, puede configurar usuarios USM.

- **Configuración de trampas SNMP**

  Puedes identificar qué trampas quieres capturar. Puede configurar el host, el puerto y la cadena de comunidad para cada destinatario de la trampa.

Configurar un solicitante SNMP

Cuando SNMP versión 2 está habilitada, puede habilitar o deshabilitar un solicitante y configurar los solicitantes para que reciban solicitudes SNMP autorizadas.

1. Menú de clic: Clúster[SNMP].
2. En **Configuración general de SNMP**, haga clic en **Sí** para habilitar SNMP.
3. De la lista **Versión**, seleccione **Versión 2**.
4. En la sección **Solicitantes**, ingrese la **Cadena de comunidad** y la información de **Red**.

Por defecto, la cadena de comunidad es pública y la red es localhost. Puedes cambiar esta configuración predeterminada.

5. **Opcional:** Para agregar otro solicitante, haga clic en **Agregar un solicitante** e ingrese la **Cadena de comunidad** y la información de **Red**.
6. Haz clic en **Guardar cambios**.

Encuentra más información

- Configurar traps SNMP
- Visualización de datos de objetos gestionados mediante archivos de la base de información de gestión.

Configurar un usuario SNMP USM

Cuando habilite SNMP versión 3, deberá configurar un usuario USM para que reciba las solicitudes SNMP autorizadas.

1. Haga clic en **Clúster** > **SNMP**.
2. En **Configuración general de SNMP**, haga clic en **Sí** para habilitar SNMP.
3. De la lista **Versión**, seleccione **Versión 3**.
4. En la sección **Usuarios de USM**, ingrese el nombre, la contraseña y la frase de contraseña.
5. **Opcional:** Para agregar otro usuario de USM, haga clic en **Agregar un usuario de USM** e ingrese el nombre, la contraseña y la frase de contraseña.
6. Haz clic en **Guardar cambios**.

Configurar traps SNMP

Los administradores de sistemas pueden usar traps SNMP, también conocidas como notificaciones, para monitorear el estado del clúster SolidFire .

Cuando las alertas SNMP están habilitadas, el clúster SolidFire genera alertas asociadas con entradas del registro de eventos y alertas del sistema. Para recibir notificaciones SNMP, debe elegir las trampas que se deben generar e identificar los destinatarios de la información de la trampa. Por defecto, no se generan trampas.

1. Haga clic en **Clúster** > **SNMP**.
2. Seleccione uno o más tipos de traps en la sección **Configuración de traps SNMP** que el sistema debería generar:
   - Trampas de fallos de clúster
   - Trampas de fallos resueltas en clúster
   - Trampas de eventos de clúster
3. En la sección **Destinatarios de la trampa**, ingrese la información del host, el puerto y la cadena de comunidad para un destinatario.
4. **Opcional**: Para agregar otro destinatario de trampa, haga clic en **Agregar un destinatario de trampa** e ingrese la información de host, puerto y cadena de comunidad.
5. Haz clic en **Guardar cambios**.

Visualización de datos de objetos gestionados mediante archivos de la base de información de gestión.

Puede ver y descargar los archivos de la base de información de gestión (MIB) utilizados

para definir cada uno de los objetos gestionados. La función SNMP admite el acceso de solo lectura a los objetos definidos en SolidFire-StorageCluster-MIB.

Los datos estadísticos proporcionados en la MIB muestran la actividad del sistema para lo siguiente:

- Estadísticas de clúster
- Estadísticas de volumen
- Estadísticas de volúmenes por cuenta
- Estadísticas de nodos
- Otros datos como informes, errores y eventos del sistema

El sistema también admite el acceso al archivo MIB que contiene los puntos de acceso de nivel superior (OIDS) a los productos de la serie SF.

Pasos

1. Haga clic en **Clúster** > **SNMP**.
2. En **SNMP MIBs**, haga clic en el archivo MIB que desea descargar.
3. En la ventana de descarga resultante, abra o guarde el archivo MIB.

Administrar unidades

Cada nodo contiene una o más unidades físicas que se utilizan para almacenar una parte de los datos del clúster. El clúster utiliza la capacidad y el rendimiento de la unidad después de que esta se haya agregado correctamente al clúster. Puedes utilizar la interfaz de usuario de Element para administrar las unidades.

Detalles de las unidades

La página Unidades en la pestaña Clúster proporciona una lista de las unidades activas en el clúster. Puede filtrar la página seleccionando entre las pestañas Activos, Disponibles, Eliminando, Borrando y Fallidos.

Cuando se inicializa un clúster por primera vez, la lista de unidades activas está vacía. Puede agregar unidades que no estén asignadas a un clúster y que aparezcan en la pestaña Disponible después de crear un nuevo clúster SolidFire .

Los siguientes elementos aparecen en la lista de unidades activas.

- **Identificador de unidad**

  El número secuencial asignado a la unidad.

- **ID del nodo**

  El número de nodo asignado cuando el nodo se agrega al clúster.

- **Nombre del nodo**

  El nombre del nodo que aloja la unidad.

- **Ranura**

El número de ranura donde se encuentra físicamente la unidad.

- **Capacidad**

  Tamaño de la unidad, en GB.

- **De serie**

  El número de serie de la unidad.

- **Desgaste restante**

  El indicador del nivel de desgaste.

  El sistema de almacenamiento informa la cantidad aproximada de desgaste disponible en cada unidad de estado sólido (SSD) para la escritura y el borrado de datos. Una unidad que ha consumido el 5 por ciento de sus ciclos de escritura y borrado diseñados reporta un desgaste restante del 95 por ciento. El sistema no actualiza automáticamente la información sobre el desgaste de la unidad; puede actualizar la página o cerrarla y volver a cargarla para actualizar la información.

- **Tipo**

  El tipo de transmisión. El tipo puede ser bloque o metadatos.

Para más información

- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Gestionar nodos

Gestionar nodos

Puede administrar el almacenamiento SolidFire y los nodos Fibre Channel desde la página Nodos de la pestaña Clúster.

Si un nodo recién agregado representa más del 50 por ciento de la capacidad total del clúster, parte de la capacidad de este nodo se vuelve inutilizable ("varada"), de modo que cumpla con la regla de capacidad. Esto seguirá siendo así hasta que se añada más capacidad de almacenamiento. Si se añade un nodo muy grande que también incumple la regla de capacidad, el nodo que antes estaba aislado dejará de estarlo, mientras que el nodo recién añadido quedará aislado. La capacidad siempre debe añadirse por pares para evitar que esto ocurra. Cuando un nodo queda aislado, se genera un fallo de clúster apropiado.

Encuentra más información

Agregar un nodo a un clúster

Agregar un nodo a un clúster

Puedes agregar nodos a un clúster cuando se necesite más almacenamiento o después de la creación del clúster. Los nodos requieren una configuración inicial cuando se encienden por primera vez. Una vez configurado el nodo, aparece en la lista de nodos pendientes y se puede agregar a un clúster.

La versión del software en cada nodo de un clúster debe ser compatible. Cuando se agrega un nodo a un clúster, este instala la versión del software NetApp Element correspondiente en el nuevo nodo, según sea necesario.

Puedes agregar nodos de menor o mayor capacidad a un clúster existente. Puede agregar capacidades de nodo mayores a un clúster para permitir el crecimiento de la capacidad. Los nodos más grandes que se agreguen a un clúster con nodos más pequeños deben agregarse por pares. Esto proporciona espacio suficiente para que Double Helix pueda mover los datos en caso de que falle uno de los nodos más grandes. Puedes agregar nodos de menor capacidad a un clúster de nodos más grande para mejorar el rendimiento.

> Si un nodo recién agregado representa más del 50 por ciento de la capacidad total del clúster, parte de la capacidad de este nodo se vuelve inutilizable ("varada"), de modo que cumpla con la regla de capacidad. Esto seguirá siendo así hasta que se añada más capacidad de almacenamiento. Si se añade un nodo muy grande que también incumple la regla de capacidad, el nodo que antes estaba aislado dejará de estarlo, mientras que el nodo recién añadido quedará aislado. La capacidad siempre debe añadirse por pares para evitar que esto ocurra. Cuando un nodo queda aislado, se produce un fallo de clúster strandedCapacity.

"Vídeo de NetApp : Escala a tu manera: Ampliación de un clúster SolidFire"

Puedes agregar nodos a los dispositivos NetApp HCI .

Pasos

1. Seleccione **Clúster** > **Nodos**.
2. Haz clic en **Pendientes** para ver la lista de nodos pendientes.

   Cuando finaliza el proceso de adición de nodos, estos aparecen en la lista de nodos activos. Hasta entonces, los nodos pendientes aparecerán en la lista de Nodos Activos Pendientes.

   SolidFire instala la versión del software Element del clúster en los nodos pendientes cuando los agrega a un clúster. Esto podría tardar unos minutos.

3. Debe realizar una de las siguientes acciones:
   - Para agregar nodos individuales, haga clic en el icono **Acciones** del nodo que desea agregar.
   - Para agregar varios nodos, seleccione la casilla de verificación de los nodos que desea agregar y luego **Acciones en lote**. **Nota:** Si el nodo que está agregando tiene una versión del software Element diferente a la versión que se ejecuta en el clúster, el clúster actualiza de forma asíncrona el nodo a la versión del software Element que se ejecuta en el maestro del clúster. Después de que se actualiza el nodo, se agrega automáticamente al clúster. Durante este proceso asíncrono, el nodo estará en estado pendingActive.
4. Haga clic en **Agregar**.

   El nodo aparece en la lista de nodos activos.

Encuentra más información

Control de versiones y compatibilidad de nodos

Control de versiones y compatibilidad de nodos

La compatibilidad de los nodos se basa en la versión del software Element instalada en

un nodo. Los clústeres de almacenamiento basados en software de Element crean automáticamente una imagen de un nodo a la versión del software de Element en el clúster si el nodo y el clúster no tienen versiones compatibles.

La siguiente lista describe los niveles de importancia de las versiones de software que componen el número de versión del software Element:

- **Importante**

  El primer número designa una versión del software. No se puede agregar un nodo con un número de componente principal a un clúster que contenga nodos con un número de parche principal diferente, ni se puede crear un clúster con nodos de versiones principales mixtas.

- **Menor**

  El segundo número designa características de software menores o mejoras a características de software existentes que se han añadido a una versión principal. Este componente se incrementa dentro de un componente de versión principal para indicar que esta versión incremental no es compatible con ninguna otra versión incremental del software Element que tenga un componente secundario diferente. Por ejemplo, la versión 11.0 no es compatible con la 11.1, y la versión 11.1 no es compatible con la 11.2.

- **Micro**

  El tercer número designa un parche compatible (versión incremental) para la versión del software Element representada por los componentes mayor.menor. Por ejemplo, la versión 11.0.1 es compatible con la versión 11.0.2, y la versión 11.0.2 es compatible con la versión 11.0.3.

Para garantizar la compatibilidad, los números de versión principal y secundaria deben coincidir. Los números micro no tienen que coincidir para ser compatibles.

Capacidad del clúster en un entorno de nodos mixtos

Puedes mezclar diferentes tipos de nodos en un clúster. Las series SF 2405, 3010, 4805, 6010, 9605, 9010, 19210, 38410 y la serie H pueden coexistir en un clúster.

La serie H consta de los nodos H610S-1, H610S-2, H610S-4 y H410S. Estos nodos son compatibles tanto con 10GbE como con 25GbE.

Lo mejor es no mezclar nodos no cifrados con nodos cifrados. En un clúster de nodos mixtos, ningún nodo puede ser mayor que el 33 por ciento de la capacidad total del clúster. Por ejemplo, en un clúster con cuatro nodos SF-Series 4805, el nodo más grande que se puede agregar individualmente es un SF-Series 9605. El umbral de capacidad del clúster se calcula en función de la pérdida potencial del nodo más grande en esta situación.

Dependiendo de la versión del software Element, los siguientes nodos de almacenamiento de la serie SF no son compatibles:

A partir de…	Nodo de almacenamiento no compatible…
Elemento 12.8	• SF4805 • SF9605 • SF19210 • SF38410
Elemento 12.7	• SF2405 • SF9608
Elemento 12.0	• SF3010 • SF6010 • SF9010

Si intenta actualizar uno de estos nodos a una versión de Element no compatible, verá un error que indica que el nodo no es compatible con Element 12.x.

Ver detalles del nodo

Puede ver detalles de nodos individuales, como etiquetas de servicio, detalles de la unidad y gráficos de utilización y estadísticas de la unidad. La página Nodos de la pestaña Clúster proporciona la columna Versión, donde puede ver la versión de software de cada nodo.

Pasos

1. Haz clic en **Clúster** > **Nodos**.
2. Para ver los detalles de un nodo específico, haga clic en el icono **Acciones** del nodo.
3. Haga clic en **Ver detalles**.
4. Revisa los detalles del nodo:
   - **ID de nodo**: El ID generado por el sistema para el nodo.
   - **Nombre del nodo**: El nombre de host del nodo.
   - **Rol del nodo**: El rol que el nodo tiene en el clúster. Valores posibles:
     - Maestro del clúster: El nodo que realiza tareas administrativas en todo el clúster y contiene el MVIP y el SVIP.
     - Nodo de conjunto: Un nodo que participa en el clúster. Hay 3 o 5 nodos de conjunto dependiendo del tamaño del clúster.
     - Canal de fibra: Un nodo en el clúster.
   - **Tipo de nodo**: El tipo de modelo del nodo.
   - **Unidades activas**: El número de unidades activas en el nodo.
   - **Utilización del nodo**: Porcentaje de utilización del nodo basado en nodeHeat. El valor mostrado es recentPrimaryTotalHeat como porcentaje. Disponible a partir del Elemento 12.8.
   - **IP de gestión**: La dirección IP de gestión (MIP) asignada al nodo para tareas de administración de red de 1GbE o 10GbE.

- **IP del clúster**: La dirección IP del clúster (CIP) asignada al nodo y utilizada para la comunicación entre nodos del mismo clúster.
- **IP de almacenamiento**: La dirección IP de almacenamiento (SIP) asignada al nodo utilizada para el descubrimiento de la red iSCSI y todo el tráfico de datos de la red.
- **ID de VLAN de administración**: El ID virtual para la red de área local de administración.
- **ID de VLAN de almacenamiento**: El ID virtual para la red de área local de almacenamiento.
- **Versión**: La versión del software que se ejecuta en cada nodo.
- **Puerto de replicación**: El puerto utilizado en los nodos para la replicación remota.
- **Etiqueta de servicio**: El número de etiqueta de servicio único asignado al nodo.
- **Dominio de protección personalizado**: El dominio de protección personalizado asignado al nodo.

Ver detalles de los puertos Fibre Channel

En la página de puertos FC puede consultar los detalles de los puertos Fibre Channel, como su estado, nombre y dirección.

Consulte la información sobre los puertos Fibre Channel conectados al clúster.

Pasos

1. Haga clic en **Clúster** > **Puertos FC**.
2. Para filtrar la información de esta página, haga clic en **Filtrar**.
3. Revisa los detalles:
   - **ID de nodo**: El nodo que aloja la sesión para la conexión.
   - **Nombre del nodo**: Nombre del nodo generado por el sistema.
   - **Ranura**: Número de ranura donde se encuentra el puerto Fibre Channel.
   - **Puerto HBA**: Puerto físico en el adaptador de bus de host de Fibre Channel (HBA).
   - **WWNN**: Nombre del nodo mundial.
   - **WWPN**: Nombre del puerto mundial de destino.
   - **WWN del switch**: Nombre mundial del switch Fibre Channel.
   - **Estado del puerto**: Estado actual del puerto.
   - **nPort ID**: El ID del puerto del nodo en la estructura Fibre Channel.
   - **Velocidad**: La velocidad negociada del canal de fibra. Los valores posibles son los siguientes:
     - 4Gbps
     - 8Gbps
     - 16Gbps

Encuentra más información

- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Gestionar redes virtuales

Gestionar redes virtuales

La virtualización de redes en el almacenamiento SolidFire permite que el tráfico entre múltiples clientes que se encuentran en redes lógicas separadas se conecte a un solo clúster. Las conexiones al clúster se segregan en la pila de red mediante el uso de etiquetado VLAN.

Encuentra más información

- Agregar una red virtual
- Habilitar el enrutamiento y reenvío virtual
- Editar una red virtual
- Editar VLAN VRF
- Eliminar una red virtual

Agregar una red virtual

Puede agregar una nueva red virtual a una configuración de clúster para habilitar una conexión de entorno multiinquilino a un clúster que ejecuta el software Element.

Lo que necesitarás

- Identifique el bloque de direcciones IP que se asignarán a las redes virtuales en los nodos del clúster.
- Identifique una dirección IP de red de almacenamiento (SVIP) que se utilizará como punto final para todo el tráfico de almacenamiento de NetApp Element .

Para esta configuración, debe tener en cuenta los siguientes criterios:

- Las VLAN que no tienen habilitado VRF requieren que los iniciadores estén en la misma subred que la SVIP.
- Las VLAN que tienen habilitado VRF no requieren que los iniciadores estén en la misma subred que la SVIP, y se admite el enrutamiento.
- La SVIP predeterminada no requiere que los iniciadores estén en la misma subred que la SVIP, y admite el enrutamiento.

Cuando se agrega una red virtual, se crea una interfaz para cada nodo y cada una requiere una dirección IP de red virtual. El número de direcciones IP que especifique al crear una nueva red virtual debe ser igual o mayor que el número de nodos del clúster. Las direcciones de red virtuales se aprovisionan de forma masiva y se asignan a nodos individuales automáticamente. No es necesario asignar manualmente direcciones de red virtuales a los nodos del clúster.

Pasos

1. Haga clic en **Clúster** > **Red**.
2. Haga clic en **Crear VLAN**.
3. En el cuadro de diálogo **Crear una nueva VLAN**, introduzca los valores en los siguientes campos:
    - **Nombre de VLAN**

- **Etiqueta VLAN**
- **SVIP**
- **Máscara de red**
- (Opcional) **Descripción**

4. Ingrese la dirección **IP inicial** para el rango de direcciones IP en **Bloques de direcciones IP**.
5. Ingrese el **Tamaño** del rango de IP como el número de direcciones IP que se incluirán en el bloque.
6. Haz clic en **Agregar un bloque** para añadir un bloque no contiguo de direcciones IP para esta VLAN.
7. Haga clic en **Crear VLAN**.

Ver detalles de la red virtual

Pasos

1. Haga clic en **Clúster** > **Red**.
2. Revise los detalles.
   - **ID**: Identificador único de la red VLAN, asignado por el sistema.
   - **Nombre**: Nombre único asignado por el usuario para la red VLAN.
   - **Etiqueta VLAN**: Etiqueta VLAN asignada cuando se creó la red virtual.
   - **SVIP**: Dirección IP virtual de almacenamiento asignada a la red virtual.
   - **Máscara de red**: Máscara de red para esta red virtual.
   - **Puerta de enlace**: Dirección IP única de una puerta de enlace de red virtual. VRF debe estar habilitado.
   - **VRF habilitado**: Indicación de si el enrutamiento y reenvío virtual está habilitado o no.
   - **Direcciones IP utilizadas**: El rango de direcciones IP de red virtual utilizadas para la red virtual.

Habilitar el enrutamiento y reenvío virtual

Puede habilitar el enrutamiento y reenvío virtual (VRF), lo que permite que existan varias instancias de una tabla de enrutamiento en un enrutador y funcionen simultáneamente. Esta funcionalidad solo está disponible para redes de almacenamiento.

Solo puedes habilitar VRF al momento de crear una VLAN. Si desea volver a un modo no VRF, deberá eliminar y volver a crear la VLAN.

1. Haga clic en **Clúster** > **Red**.
2. Para habilitar VRF en una nueva VLAN, seleccione **Crear VLAN**.
   a. Introduzca la información pertinente para la nueva VRF/VLAN. Consulte la sección "Agregar una red virtual".
   b. Seleccione la casilla de verificación **Habilitar VRF**.
   c. **Opcional**: Introduzca una puerta de enlace.
3. Haga clic en **Crear VLAN**.

Encuentra más información

Agregar una red virtual

Editar una red virtual

Puedes cambiar los atributos de la VLAN, como el nombre de la VLAN, la máscara de red y el tamaño de los bloques de direcciones IP. La etiqueta VLAN y la SVIP no se pueden modificar para una VLAN. El atributo de puerta de enlace no es un parámetro válido para VLAN que no sean VRF.

Si existen sesiones iSCSI, de replicación remota u otras sesiones de red, la modificación podría fallar.

Al administrar el tamaño de los rangos de direcciones IP de VLAN, debe tener en cuenta las siguientes limitaciones:

- Solo puedes eliminar direcciones IP del rango de direcciones IP inicial asignado en el momento de la creación de la VLAN.
- Puedes eliminar un bloque de direcciones IP que se agregó después del rango de direcciones IP inicial, pero no puedes cambiar el tamaño de un bloque de IP eliminando direcciones IP.
- Cuando intentas eliminar direcciones IP, ya sea del rango de direcciones IP inicial o de un bloque IP, que están en uso por nodos del clúster, la operación podría fallar.
- No se pueden reasignar direcciones IP específicas en uso a otros nodos del clúster.

Puede agregar un bloque de direcciones IP siguiendo el siguiente procedimiento:

1. Seleccione **Clúster** > **Red**.
2. Seleccione el icono Acciones para la VLAN que desea editar.
3. Seleccione **Editar**.
4. En el cuadro de diálogo **Editar VLAN**, introduzca los nuevos atributos para la VLAN.
5. Seleccione **Agregar un bloque** para agregar un bloque no contiguo de direcciones IP para la red virtual.
6. Seleccione **Guardar cambios**.

Enlace a artículos de la base de conocimientos para la resolución de problemas

Enlace a los artículos de la Base de conocimientos para obtener ayuda con la resolución de problemas relacionados con la administración de sus rangos de direcciones IP de VLAN.

- "Advertencia de IP duplicada tras agregar un nodo de almacenamiento en la VLAN del clúster Element"
- "Cómo determinar qué direcciones IP de VLAN están en uso y a qué nodos están asignadas esas direcciones IP en Element"

Editar VLAN VRF

Puede cambiar los atributos de VLAN de VRF, como el nombre de VLAN, la máscara de red, la puerta de enlace y los bloques de direcciones IP.

1. Haga clic en **Clúster** > **Red**.
2. Haz clic en el icono Acciones de la VLAN que deseas editar.

3. Haga clic en **Editar**.
4. Introduzca los nuevos atributos para la VLAN VRF en el cuadro de diálogo **Editar VLAN**.
5. Haz clic en **Guardar cambios**.

Eliminar una red virtual

Puedes eliminar un objeto de red virtual. Debes agregar los bloques de direcciones a otra red virtual antes de eliminar una red virtual.

1. Haga clic en **Clúster** > **Red**.
2. Haz clic en el icono de Acciones de la VLAN que deseas eliminar.
3. Haga clic en **Eliminar**.
4. Confirma el mensaje.

Encuentra más información

Editar una red virtual

Cree un clúster que admita unidades FIPS.

Preparar el clúster Element para la función de unidades FIPS

La seguridad se está convirtiendo en un aspecto cada vez más crítico para el despliegue de soluciones en muchos entornos de clientes. Las Normas Federales de Procesamiento de Información (FIPS) son normas para la seguridad informática y la interoperabilidad. El cifrado certificado FIPS 140-2 para datos en reposo es un componente de la solución de seguridad general.

Para preparar la activación de la función de unidades FIPS, debe evitar mezclar nodos en los que algunos sean compatibles con unidades FIPS y otros no.

Un clúster se considera compatible con las unidades FIPS según las siguientes condiciones:

- Todas las unidades están certificadas como unidades FIPS.
- Todos los nodos son nodos de unidades FIPS.
- El cifrado en reposo (EAR) está habilitado.
- La función de controladores FIPS está habilitada. Todas las unidades y nodos deben ser compatibles con FIPS y el cifrado en reposo debe estar habilitado para poder habilitar la función de unidad FIPS.

Habilitar el cifrado en reposo

Puede habilitar y deshabilitar el cifrado en reposo para todo el clúster. Esta función no está habilitada de forma predeterminada. Para admitir unidades FIPS, debe habilitar el cifrado en reposo.

1. En la interfaz de usuario del software NetApp Element , haga clic en **Clúster** > **Configuración**.
2. Haga clic en **Habilitar cifrado en reposo**.

Encuentra más información

- Habilitar y deshabilitar el cifrado para un clúster
- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Identificar si los nodos están listos para la función de controladores FIPS

Debe comprobar si todos los nodos del clúster de almacenamiento están preparados para admitir unidades FIPS utilizando el método de la API GetFipsReport del software NetApp Element .

El informe resultante muestra uno de los siguientes estados:

- Ninguno: El nodo no es compatible con la función de unidades FIPS.
- Parcial: El nodo es compatible con FIPS, pero no todas las unidades son compatibles con FIPS.
- Listo: El nodo es compatible con FIPS y todas las unidades son unidades FIPS o no hay unidades presentes.

Pasos

1. Utilizando la API de Element, compruebe si los nodos y las unidades del clúster de almacenamiento son compatibles con unidades FIPS introduciendo el siguiente comando:

   ```
   GetFipsReport
   ```

2. Revise los resultados y observe si algún nodo no mostró el estado "Listo".
3. Para cualquier nodo que no muestre el estado Listo, compruebe si la unidad es compatible con la función de unidades FIPS:
   - Utilizando la API de Element, ingrese: `GetHardwareList`
   - Tenga en cuenta el valor de **DriveEncryptionCapabilityType**. Si es "fips", el hardware puede admitir la función de controladores FIPS.

     Ver detalles sobre `GetFipsReport` o `ListDriveHardware` en el "Referencia de la API de elementos".

4. Si la unidad no admite la función de unidades FIPS, reemplace el hardware con hardware FIPS (ya sea el nodo o las unidades).

Encuentra más información

- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Habilitar la función de controladores FIPS

Puede habilitar la función de unidades FIPS mediante el software NetApp Element . `EnableFeature` Método API.

El cifrado en reposo debe estar habilitado en el clúster y todos los nodos y unidades deben ser compatibles con FIPS, como se indica cuando GetFipsReport muestra un estado Listo para todos los nodos.

Paso

1. Utilizando la API de Element, habilite FIPS en todas las unidades introduciendo:

   ```
   EnableFeature params: FipsDrives
   ```

Encuentra más información

- "Gestiona el almacenamiento con la API de Element"
- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Compruebe el estado de la unidad FIPS

Puede comprobar si la función de unidades FIPS está habilitada en el clúster mediante el software NetApp Element . `GetFeatureStatus` Método API que muestra si el estado de activación de las unidades FIPS es verdadero o falso.

1. Utilizando la API de Element, compruebe la función de unidades FIPS en el clúster introduciendo:

   ```
   GetFeatureStatus
   ```

2. Revisar los resultados de `GetFeatureStatus` Llamada a la API. Si el valor de FIPS Drives enabled es True, la función FIPS drives está habilitada.

   ```
   {"enabled": true,
   "feature": "FipsDrives"
   }
   ```

Encuentra más información

- "Gestiona el almacenamiento con la API de Element"
- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Solucionar problemas de la función de la unidad FIPS

Mediante la interfaz de usuario del software NetApp Element , puede ver alertas con información sobre fallos del clúster o errores del sistema relacionados con la función de unidades FIPS.

1. Utilizando la interfaz de usuario de Element, seleccione **Informes** > **Alertas**.
2. Busque fallos en el clúster, incluidos los siguientes:
   - Las unidades FIPS no coinciden
   - FIPS genera incumplimiento
3. Para obtener sugerencias de resolución, consulte la información sobre el código de error del clúster.

Encuentra más información

- Códigos de falla del clúster
- "Gestiona el almacenamiento con la API de Element"
- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Establecer una comunicación segura

Habilite FIPS 140-2 para HTTPS en su clúster.

Puede utilizar el método API EnableFeature para habilitar el modo de funcionamiento FIPS 140-2 para comunicaciones HTTPS.

Con el software NetApp Element , puede optar por habilitar el modo de funcionamiento de los Estándares Federales de Procesamiento de Información (FIPS) 140-2 en su clúster. Habilitar este modo activa el Módulo de Seguridad Criptográfica de NetApp (NCSM) y aprovecha el cifrado certificado FIPS 140-2 Nivel 1 para todas las comunicaciones a través de HTTPS con la interfaz de usuario y la API de NetApp Element .

> Una vez habilitado el modo FIPS 140-2, no se puede deshabilitar. Cuando se habilita el modo FIPS 140-2, cada nodo del clúster se reinicia y ejecuta una autocomprobación para garantizar que el NCSM esté correctamente habilitado y funcionando en el modo certificado FIPS 140-2. Esto provoca una interrupción tanto en las conexiones de gestión como en las de almacenamiento del clúster. Debe planificar cuidadosamente y habilitar este modo solo si su entorno necesita el mecanismo de cifrado que ofrece.

Para obtener más información, consulte la información de la API de Element.

El siguiente es un ejemplo de la solicitud a la API para habilitar FIPS:

```
{
  "method": "EnableFeature",
    "params": {
        "feature" : "fips"
    },
    "id": 1
}
```

Una vez habilitado este modo de funcionamiento, todas las comunicaciones HTTPS utilizan los cifrados aprobados por FIPS 140-2.

Encuentra más información

- cifrados SSL
- "Gestiona el almacenamiento con la API de Element"
- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

cifrados SSL

Los cifrados SSL son algoritmos de cifrado utilizados por los hosts para establecer una comunicación segura. Existen cifrados estándar que admite el software Element y cifrados no estándar cuando está habilitado el modo FIPS 140-2.

Las siguientes listas proporcionan los cifrados SSL (Secure Socket Layer) estándar compatibles con el software Element y los cifrados SSL compatibles cuando el modo FIPS 140-2 está habilitado:

- **FIPS 140-2 desactivado**

  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 2048) - A

  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A

  TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 2048) - A

  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A

  TLS_ECDHE_RSA_CON_AES_128_CBC_SHA256 (secp256r1) - A

  TLS_ECDHE_RSA_CON_AES_128_GCM_SHA256 (secp256r1) - A

  TLS_ECDHE_RSA_CON_AES_256_CBC_SHA384 (secp256r1) - A

  TLS_ECDHE_RSA_CON_AES_256_GCM_SHA384 (secp256r1) - A

  TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C

  TLS_RSA_CON_AES_128_CBC_SHA (rsa 2048) - A

  TLS_RSA_CON_AES_128_CBC_SHA256 (rsa 2048) - A

  TLS_RSA_CON_AES_128_GCM_SHA256 (rsa 2048) - A

  TLS_RSA_CON_AES_256_CBC_SHA (rsa 2048) - A

  TLS_RSA_CON_AES_256_CBC_SHA256 (rsa 2048) - A

  TLS_RSA_CON_AES_256_GCM_SHA384 (rsa 2048) - A

  TLS_RSA_CON_CAMELLIA_128_CBC_SHA (rsa 2048) - A

  TLS_RSA_CON_CAMELLIA_256_CBC_SHA (rsa 2048) - A

  TLS_RSA_WITH_IDEA_CBC_SHA (rsa 2048) - A

  TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C

  TLS_RSA_CON_RC4_128_SHA (rsa 2048) - C

  TLS_RSA_WITH_SEED_CBC_SHA (rsa 2048) - A

- **FIPS 140-2 habilitado**

  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 2048) - A

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 2048) - A

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A

TLS_ECDHE_RSA_CON_AES_128_CBC_SHA256 (sección 571r1) - A

TLS_ECDHE_RSA_CON_AES_128_CBC_SHA256 (secp256r1) - A

TLS_ECDHE_RSA_CON_AES_128_GCM_SHA256 (secp256r1) - A

TLS_ECDHE_RSA_CON_AES_128_GCM_SHA256 (sect571r1) - A

TLS_ECDHE_RSA_CON_AES_256_CBC_SHA384 (sección 571r1) - A

TLS_ECDHE_RSA_CON_AES_256_CBC_SHA384 (secp256r1) - A

TLS_ECDHE_RSA_CON_AES_256_GCM_SHA384 (secp256r1) - A

TLS_ECDHE_RSA_CON_AES_256_GCM_SHA384 (sección 571r1) - A

TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C

TLS_RSA_CON_AES_128_CBC_SHA (rsa 2048) - A

TLS_RSA_CON_AES_128_CBC_SHA256 (rsa 2048) - A

TLS_RSA_CON_AES_128_GCM_SHA256 (rsa 2048) - A

TLS_RSA_CON_AES_256_CBC_SHA (rsa 2048) - A

TLS_RSA_CON_AES_256_CBC_SHA256 (rsa 2048) - A

TLS_RSA_CON_AES_256_GCM_SHA384 (rsa 2048) - A

Encuentra más información

Habilite FIPS 140-2 para HTTPS en su clúster.

Comience con la administración de claves externas

Comience con la administración de claves externas

La gestión de claves externas (EKM) proporciona una gestión segura de claves de autenticación (AK) junto con un servidor de claves externas fuera del clúster (EKS). Las AK se utilizan para bloquear y desbloquear unidades de autocifrado (SED) cuando"cifrado en reposo" está habilitado en el clúster. El EKS proporciona generación y almacenamiento seguros de los AK. El clúster utiliza el protocolo de interoperabilidad de gestión de claves (KMIP), un protocolo estándar definido por OASIS, para comunicarse con el EKS.

- "Establecer la gestión externa"

- "Rekey cifrado de software en reposo clave maestra"
- "Recuperar claves de autenticación inaccesibles o no válidas"
- "Comandos de la API de administración de claves externas"

Encuentra más información

- "API CreateCluster que se puede usar para habilitar el cifrado de software en reposo"
- "Documentación del software SolidFire y Element"
- "Documentación para versiones anteriores de los productos NetApp SolidFire y Element"

Configurar la gestión de claves externas

Puedes seguir estos pasos y usar los métodos de la API de Element que se enumeran para configurar tu función de administración de claves externas.

Lo que necesitarás

- Si está configurando la administración de claves externas en combinación con el cifrado de software en reposo, habrá habilitado el cifrado de software en reposo mediante el uso de"CrearClúster" método en un nuevo clúster que no contiene volúmenes.

Pasos

1. Establecer una relación de confianza con el servidor de claves externo (EKS).
   a. Cree un par de claves pública/privada para el clúster de Element que se utiliza para establecer una relación de confianza con el servidor de claves llamando al siguiente método de la API:"Crear par de claves públicas y privadas"
   b. Obtenga la solicitud de firma de certificado (CSR) que la Autoridad de Certificación necesita firmar. La CSR permite al servidor de claves verificar que el clúster de Element que accederá a las claves esté autenticado como tal. Llama al siguiente método de la API:"Solicitud de firma de certificado de cliente"
   c. Utilice la EKS/Autoridad de Certificación para firmar la CSR recuperada. Consulte la documentación de terceros para obtener más información.
2. Cree un servidor y un proveedor en el clúster para comunicarse con EKS. Un proveedor de claves define dónde se debe obtener una clave, y un servidor define los atributos específicos del EKS con el que se comunicará.
   a. Cree un proveedor de claves donde residirán los detalles del servidor de claves llamando al siguiente método de la API:"CrearKeyProviderKmip"
   b. Cree un servidor de claves que proporcione el certificado firmado y el certificado de clave pública de la Autoridad de Certificación llamando a los siguientes métodos de la API:"CrearKeyServerKmip" "Servidor de claves de prueba Kmip"

      Si la prueba falla, verifique la conectividad y la configuración de su servidor. Luego, repita la prueba.

   c. Agregue el servidor de claves al contenedor del proveedor de claves llamando a los siguientes métodos de la API:"Agregar servidor de claves al proveedor Kmip" "TestKeyProviderKmip"

      Si la prueba falla, verifique la conectividad y la configuración de su servidor. Luego, repita la prueba.
3. Como siguiente paso para el cifrado en reposo, realice una de las siguientes acciones:
   a. (Para cifrado de hardware en reposo) Habilitar"Cifrado de hardware en reposo" proporcionando el ID del proveedor de claves que contiene el servidor de claves utilizado para almacenar las claves

mediante una llamada a"Habilitar cifrado en reposo" Método API.

> Debe habilitar el cifrado en reposo a través de"API" . Habilitar el cifrado en reposo mediante el botón existente de la interfaz de usuario de Element hará que la función vuelva a utilizar claves generadas internamente.

b. (Para el cifrado de software en reposo) Para"Cifrado de software en reposo" Para utilizar el proveedor de claves recién creado, pase el ID del proveedor de claves al"Clave maestra de cifrado de software en reposo" Método API.

Encuentra más información

- "Habilitar y deshabilitar el cifrado para un clúster"
- "Documentación del software SolidFire y Element"
- "Documentación para versiones anteriores de los productos NetApp SolidFire y Element"

Rekey cifrado de software en reposo clave maestra

Puedes usar la API de Element para volver a generar una clave existente. Este proceso crea una nueva clave maestra de reemplazo para su servidor de administración de claves externo. Las claves maestras siempre se reemplazan por nuevas claves maestras y nunca se duplican ni se sobrescriben.

Es posible que necesite volver a introducir las teclas como parte de uno de los siguientes procedimientos:

- Cree una nueva clave como parte de un cambio de gestión de claves interna a gestión de claves externa.
- Cree una nueva clave como reacción a un evento relacionado con la seguridad o como protección contra el mismo.

> Este proceso es asíncrono y devuelve una respuesta antes de que se complete la operación de reenvío de claves. Puedes usar el"ObtenerResultadoAsíncrono" Método para consultar al sistema y comprobar cuándo ha finalizado el proceso.

Lo que necesitarás

- Has habilitado el cifrado de software en reposo mediante"CrearClúster" método en un nuevo clúster que no contiene volúmenes y no tiene E/S. Utilice el siguiente enlace: ../api/reference_element_api_getsoftwareencryptionatrestinfo.html[`GetSoftwareEncryptionatRestInfo`] para confirmar que el estado es `enabled` antes de continuar.
- Tienes"Se estableció una relación de confianza" entre el clúster SolidFire y un servidor de claves externo (EKS). Ejecutar el"TestKeyProviderKmip" Método para verificar que se ha establecido una conexión con el proveedor de claves.

Pasos

1. Ejecutar el"Proveedores de claves de lista Kmip" comando y copia del ID del proveedor de claves(`keyProviderID`).
2. Ejecutar el"Clave maestra de cifrado de software en reposo" con el `keyManagementType` parámetro como `external` y `keyProviderID` como el número de identificación del proveedor de claves del paso anterior:

```
{
 "method": "rekeysoftwareencryptionatrestmasterkey",
 "params": {
   "keyManagementType": "external",
   "keyProviderID": "<ID number>"
 }
}
```

3. Copia el `asyncHandle` valor de la `RekeySoftwareEncryptionAtRestMasterKey` Respuesta al comando.
4. Ejecutar el"ObtenerResultadoAsíncrono" comando con el `asyncHandle` Valor del paso anterior para confirmar el cambio de configuración. En la respuesta del comando, debería ver que la configuración de la clave maestra anterior se ha actualizado con la nueva información de la clave. Copie el nuevo ID del proveedor de claves para usarlo en un paso posterior.

```
{
   "id": null,
   "result": {
     "createTime": "2021-01-01T22:29:18Z",
     "lastUpdateTime": "2021-01-01T22:45:51Z",
     "result": {
       "keyToDecommission": {
         "keyID": "<value>",
         "keyManagementType": "internal"
     },
     "newKey": {
       "keyID": "<value>",
       "keyManagementType": "external",
       "keyProviderID": <value>
     },
     "operation": "Rekeying Master Key. Master Key management being
transferred from Internal Key Management to External Key Management with
keyProviderID=<value>",
     "state": "Ready"
   },
   "resultType": "RekeySoftwareEncryptionAtRestMasterKey",
   "status": "complete"
}
```

5. Ejecutar el `GetSoftwareEncryptionatRestInfo` orden para confirmar que los nuevos detalles clave, incluyendo el `keyProviderID` , han sido actualizados.

```
{
   "id": null,
   "result": {
     "masterKeyInfo": {
       "keyCreatedTime": "2021-01-01T22:29:18Z",
       "keyID": "<updated value>",
       "keyManagementType": "external",
       "keyProviderID": <value>
     },
     "rekeyMasterKeyAsyncResultID": <value>
     "status": "enabled",
     "version": 1
   },
}
```

Encuentra más información

- "Gestiona el almacenamiento con la API de Element"
- "Documentación del software SolidFire y Element"
- "Documentación para versiones anteriores de los productos NetApp SolidFire y Element"

Recuperar claves de autenticación inaccesibles o no válidas

Ocasionalmente, puede producirse un error que requiere la intervención del usuario. En caso de error, se generará un fallo de clúster (denominado código de fallo de clúster). Aquí se describen los dos casos más probables.

El clúster no puede desbloquear las unidades debido a un fallo de clúster KmipServerFault.

Esto puede ocurrir cuando el clúster se inicia por primera vez y el servidor de claves es inaccesible o la clave requerida no está disponible.

1. Siga los pasos de recuperación indicados en los códigos de error del clúster (si los hay).

Es posible que se establezca un fallo sliceServiceUnhealthy porque las unidades de metadatos se han marcado como fallidas y se han colocado en el estado "Disponible".

Pasos para despejar:

1. Vuelva a agregar las unidades.
2. Después de 3 a 4 minutos, compruebe que el `sliceServiceUnhealthy` La avería se ha solucionado.

Ver"códigos de falla del clúster" Para más información.

Comandos de la API de administración de claves externas

Lista de todas las API disponibles para gestionar y configurar EKM.

Se utiliza para establecer una relación de confianza entre el clúster y los servidores externos propiedad del cliente:

- Crear par de claves públicas y privadas
- Solicitud de firma de certificado de cliente

Se utiliza para definir los detalles específicos de los servidores externos propiedad del cliente:

- CrearKeyServerKmip
- ModificarKeyServerKmip
- EliminarKeyServerKmip
- ObtenerKeyServerKmip
- Lista de servidores clave Kmip
- Servidor de claves de prueba Kmip

Se utiliza para crear y mantener proveedores de claves que gestionan servidores de claves externos:

- CrearKeyProviderKmip
- EliminarKeyProviderKmip
- Agregar servidor de claves al proveedor Kmip
- Eliminar servidor de claves del proveedor Kmip
- ObtenerProveedorDeClavesKmip
- Proveedores de claves de lista Kmip
- Clave maestra de cifrado de software en reposo
- TestKeyProviderKmip

Para obtener información sobre los métodos de la API, consulte "Información de referencia de la API".

Gestionar volúmenes y volúmenes virtuales

Aprenda sobre la gestión de volúmenes y volúmenes virtuales.

Puede administrar los datos en un clúster que ejecuta el software Element desde la pestaña Administración en la interfaz de usuario de Element. Las funciones de gestión de clústeres disponibles incluyen la creación y gestión de volúmenes de datos, grupos de acceso a volúmenes, iniciadores y políticas de calidad de servicio (QoS).

Trabajar con volúmenes

El sistema SolidFire aprovisiona almacenamiento mediante volúmenes. Los volúmenes son dispositivos de bloque a los que acceden a través de la red los clientes iSCSI o Fibre Channel. Desde la página Volúmenes en la pestaña Administración, puede crear, modificar, clonar y eliminar volúmenes en un nodo. También puede consultar estadísticas sobre el ancho de banda del volumen y el uso de E/S.

"Aprenda a trabajar con volúmenes"

Trabajar con volúmenes virtuales

Puede ver información y realizar tareas para volúmenes virtuales y sus contenedores de almacenamiento asociados, puntos finales de protocolo, enlaces y hosts utilizando la interfaz de usuario de Element.

El sistema de almacenamiento de software NetApp Element se suministra con la función de volúmenes virtuales (VVols) desactivada. Debe realizar una tarea única de habilitar manualmente la funcionalidad de vSphere VVol a través de la interfaz de usuario de Element.

Después de habilitar la funcionalidad VVol, aparece una pestaña VVols en la interfaz de usuario que ofrece opciones de monitoreo y administración limitadas relacionadas con VVols. Además, un componente de software del lado del almacenamiento conocido como Proveedor VASA actúa como un servicio de reconocimiento de almacenamiento para vSphere. La mayoría de los comandos de VVols, como la creación, clonación y edición de VVols, son iniciados por un servidor vCenter o un host ESXi y traducidos por el proveedor VASA a las API de Element para el sistema de almacenamiento de software Element. Los comandos para crear, eliminar y administrar contenedores de almacenamiento y eliminar volúmenes virtuales se pueden iniciar mediante la interfaz de usuario de Element.

La mayoría de las configuraciones necesarias para utilizar la funcionalidad de Volúmenes Virtuales con los sistemas de almacenamiento de software Element se realizan en vSphere. Consulte la _Guía de configuración de volúmenes virtuales de VMware vSphere para almacenamiento SolidFire para registrar el proveedor VASA en vCenter, crear y administrar almacenes de datos VVol y administrar el almacenamiento según las políticas.

> Para Element 12.5 y versiones anteriores, no registre más de un proveedor NetApp Element VASA en una sola instancia de vCenter. Cuando se agrega un segundo proveedor NetApp Element VASA, todos los almacenes de datos VVOL quedan inaccesibles.

> La compatibilidad con VASA para múltiples vCenters está disponible como un parche de actualización si ya ha registrado un proveedor de VASA con su vCenter. Para instalar, descargue el archivo VASA39 .tar.gz desde el "Descargas de software de NetApp" Visite el sitio y siga las instrucciones del manifiesto. El proveedor NetApp Element VASA utiliza un certificado NetApp . Con este parche, vCenter utiliza el certificado sin modificaciones para admitir múltiples vCenters para el uso de VASA y VVols. No modifique el certificado. VASA no admite certificados SSL personalizados.

"Aprenda a trabajar con volúmenes virtuales"

Trabajar con grupos de acceso por volumen e iniciadores

Puede utilizar iniciadores iSCSI o iniciadores Fibre Channel para acceder a los volúmenes definidos dentro de los grupos de acceso a volúmenes.

Puede crear grupos de acceso asignando IQN de iniciador iSCSI o WWPN de Fibre Channel en una colección de volúmenes. Cada IQN que agregue a un grupo de acceso puede acceder a cada volumen del grupo sin necesidad de autenticación CHAP.

Existen dos tipos de métodos de autenticación CHAP:

- Autenticación CHAP a nivel de cuenta: Puede asignar la autenticación CHAP a la cuenta.
- Autenticación CHAP a nivel de iniciador: Puede asignar un destino CHAP y secretos únicos para iniciadores específicos sin estar limitado a un único CHAP en una sola cuenta. Esta autenticación CHAP a nivel de iniciador reemplaza las credenciales a nivel de cuenta.

Opcionalmente, con CHAP por iniciador, puede exigir la autorización del iniciador y la autenticación CHAP por

iniciador. Estas opciones pueden definirse para cada iniciador y un grupo de acceso puede contener una combinación de iniciadores con diferentes opciones.

Cada WWPN que agregue a un grupo de acceso habilita el acceso a la red Fibre Channel a los volúmenes del grupo de acceso.

Los grupos de acceso por volumen tienen los siguientes límites:

- Se permite un máximo de 64 IQN o WWPN en un grupo de acceso.
- Un grupo de acceso puede estar compuesto por un máximo de 2000 volúmenes.
- Un IQN o WWPN solo puede pertenecer a un grupo de acceso.
- Un único volumen puede pertenecer a un máximo de cuatro grupos de acceso.

"Aprenda a trabajar con grupos de acceso por volumen e iniciadores."

Para más información

- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Trabajar con volúmenes

Políticas de gestión de la calidad del servicio

Una política de Calidad de Servicio (QoS) le permite crear y guardar una configuración de calidad de servicio estandarizada que se puede aplicar a muchos volúmenes. Puede crear, editar y eliminar políticas de QoS desde la página Políticas de QoS en la pestaña Administración.

Si está utilizando políticas de QoS, no utilice QoS personalizada en un volumen. La QoS personalizada anulará y ajustará los valores de la política de QoS para la configuración de QoS de volumen.

"Vídeo de NetApp : Políticas de calidad de servicio de SolidFire"

Ver"Rendimiento y calidad del servicio" .

- Crea una política de QoS
- Editar una política de QoS
- Eliminar una política de QoS

Crea una política de QoS

Puede crear políticas de QoS y aplicarlas al crear volúmenes.

1. Seleccione **Administración** > **Políticas de QoS**.
2. Haga clic en **Crear política QoS**.
3. Ingrese el **Nombre de la póliza**.

4. Ingrese los valores de **IOPS mínimos**, **IOPS máximos** e **IOPS de ráfaga**.
5. Haga clic en **Crear política QoS**.

Editar una política de QoS

Puede cambiar el nombre de una política QoS existente o editar los valores asociados a la política. Modificar una política de QoS afecta a todos los volúmenes asociados a dicha política.

1. Seleccione **Administración** > **Políticas de QoS**.
2. Haz clic en el icono Acciones de la política QoS que quieras editar.
3. En el menú resultante, seleccione **Editar**.
4. En el cuadro de diálogo **Editar política de QoS**, modifique las siguientes propiedades según sea necesario:
   - Nombre de la póliza
   - IOPS mínimas
   - IOPS máximas
   - Burst IOPS
5. Haz clic en **Guardar cambios**.

Eliminar una política de QoS

Puede eliminar una política QoS si ya no es necesaria. Cuando se elimina una política de QoS, todos los volúmenes asociados a la política mantienen la configuración de QoS pero dejan de estar asociados a la política.

> Si en cambio intenta desvincular un volumen de una política QoS, puede cambiar la configuración QoS de ese volumen a personalizada.

1. Seleccione **Administración** > **Políticas de QoS**.
2. Haz clic en el icono Acciones de la política QoS que deseas eliminar.
3. En el menú que aparece, seleccione **Eliminar**.
4. Confirma la acción.

Encuentra más información

- "Eliminar la asociación de política QoS de un volumen"
- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Administrar volúmenes

El sistema SolidFire aprovisiona almacenamiento mediante volúmenes. Los volúmenes son dispositivos de bloque a los que acceden a través de la red los clientes iSCSI o Fibre Channel.

Desde la página Volúmenes en la pestaña Administración, puede crear, modificar, clonar y eliminar volúmenes en un nodo.

Crear un volumen

Puede crear un volumen y asociar ese volumen a una cuenta determinada. Cada volumen debe estar asociado a una cuenta. Esta asociación otorga a la cuenta acceso al volumen a través de los iniciadores iSCSI utilizando las credenciales CHAP.

Puede especificar la configuración de QoS para un volumen durante su creación.

1. Seleccione **Administración** > **Volúmenes**.
2. Haz clic en **Crear volumen**.
3. En el cuadro de diálogo **Crear un nuevo volumen**, introduzca el **Nombre del volumen**.
4. Introduzca el tamaño total del volumen.

   La selección de tamaño de volumen predeterminada está en GB. Puede crear volúmenes utilizando tamaños medidos en GB o GiB:

   - 1 GB = 1 000 000 000 bytes
   - 1 GiB = 1 073 741 824 bytes
5. Seleccione un **Tamaño de bloque** para el volumen.
6. Haz clic en la lista desplegable **Cuenta** y selecciona la cuenta que debería tener acceso al volumen.

   Si no existe una cuenta, haga clic en el enlace **Crear cuenta**, ingrese un nuevo nombre de cuenta y haga clic en **Crear**. La cuenta se crea y se asocia con el nuevo volumen.

   Si hay más de 50 cuentas, la lista no aparece. Empieza a escribir y la función de autocompletar te mostrará los valores posibles para que elijas.
7. Para configurar la **Calidad del Servicio**, realice una de las siguientes acciones:
   a. En **Política**, puede seleccionar una política QoS existente, si está disponible.
   b. En **Configuración personalizada**, establezca valores mínimos, máximos y de ráfaga personalizados para IOPS o utilice los valores QoS predeterminados.

      Los volúmenes que tienen un valor de IOPS máximo o de ráfaga superior a 20 000 IOPS podrían requerir una gran profundidad de cola o varias sesiones para alcanzar este nivel de IOPS en un solo volumen.
8. Haz clic en **Crear volumen**.

Ver detalles del volumen

1. Seleccione **Administración** > **Volúmenes**.
2. Revise los detalles.
   - **ID**: El ID generado por el sistema para el volumen.
   - **Nombre**: El nombre que se le dio al volumen cuando fue creado.
   - **Cuenta**: El nombre de la cuenta asignada al volumen.
   - **Grupos de acceso**: El nombre del grupo o grupos de acceso al volumen al que pertenece el volumen.
   - **Acceso**: El tipo de acceso asignado al volumen cuando se creó. Valores posibles:

        - Lectura/Escritura: Se aceptan todas las lecturas y escrituras.
        - Solo lectura: Se permite toda la actividad de lectura; no se permiten escrituras.
        - Bloqueado: Solo se permite el acceso de administrador.
        - ReplicationTarget: Designado como volumen de destino en un par de volúmenes replicados.
    - **Usado**: El porcentaje de espacio utilizado en el volumen.
    - **Tamaño**: El tamaño total (en GB) del volumen.
    - **ID del nodo primario**: El nodo primario para este volumen.
    - **ID de nodo secundario**: La lista de nodos secundarios para este volumen. Puede tener múltiples valores durante estados transitorios, como el cambio de nodos secundarios, pero normalmente tendrá un solo valor.
    - **Limitación de QoS**: Identifica si el volumen está siendo limitado debido a una alta carga en el nodo de almacenamiento primario.
    - **Política de QoS**: El nombre y el enlace a la política de QoS definida por el usuario.
    - **IOPS mínimas**: El número mínimo de IOPS garantizado para el volumen.
    - **IOPS máx.**: El número máximo de IOPS permitido para el volumen.
    - **IOPS de ráfaga**: El número máximo de IOPS permitidos durante un corto período de tiempo para el volumen. Valor predeterminado = 15.000.
    - **Instantáneas**: Número de instantáneas creadas para el volumen.
    - **Atributos**: Atributos que se han asignado al volumen como un par clave/valor a través de un método de API.
    - **512e**: Indicación de si 512e está habilitado en un volumen. Valores posibles:
        - Sí
        - No
    - **Fecha de creación**: La fecha y hora en que se creó el volumen.

Ver detalles de cada volumen

Puedes consultar las estadísticas de rendimiento de volúmenes individuales.

1. Seleccione **Informes** > **Rendimiento del volumen**.
2. En la lista de volúmenes, haga clic en el icono Acciones de un volumen.
3. Haga clic en **Ver detalles**.

   En la parte inferior de la página aparece una bandeja con información general sobre el volumen.

4. Para ver información más detallada sobre el volumen, haga clic en **Ver más detalles**.

   El sistema muestra información detallada, así como gráficos de rendimiento del volumen.

Editar volúmenes activos

Puede modificar atributos de volumen como los valores QoS, el tamaño del volumen y la unidad de medida en la que se calculan los valores de bytes. También puede modificar el acceso a la cuenta para el uso de replicación o para restringir el acceso al volumen.

Puede cambiar el tamaño de un volumen cuando haya suficiente espacio en el clúster bajo las siguientes condiciones:

- Condiciones normales de funcionamiento.
- Se están reportando errores o fallos de volumen.
- Se está clonando el volumen.
- El volumen se está resincronizando.

Pasos

1. Seleccione **Administración** > **Volúmenes**.
2. En la ventana **Activa**, haga clic en el icono Acciones del volumen que desea editar.
3. Haga clic en **Editar**.
4. **Opcional:** Cambie el tamaño total del volumen.
   - Puedes aumentar, pero no disminuir, el tamaño del volumen. Solo se puede cambiar el tamaño de un volumen en una sola operación de cambio de tamaño. Las operaciones de recolección de basura y las actualizaciones de software no interrumpen la operación de cambio de tamaño.
   - Si está ajustando el tamaño del volumen para la replicación, primero debe aumentar el tamaño del volumen asignado como destino de la replicación. Luego puedes cambiar el tamaño del volumen de origen. El volumen objetivo puede ser mayor o igual en tamaño que el volumen de origen, pero no puede ser menor.

     La selección de tamaño de volumen predeterminada está en GB. Puede crear volúmenes utilizando tamaños medidos en GB o GiB:

   - 1 GB = 1 000 000 000 bytes
   - 1 GiB = 1 073 741 824 bytes
5. **Opcional:** Seleccione un nivel de acceso a la cuenta diferente de entre los siguientes:
   - Solo lectura
   - Leer/Escribir
   - Bloqueado
   - Destino de replicación
6. **Opcional:** Seleccione la cuenta que debería tener acceso al volumen.

   Si la cuenta no existe, haga clic en el enlace **Crear cuenta**, ingrese un nuevo nombre de cuenta y haga clic en **Crear**. La cuenta se crea y se asocia al volumen.

   > Si hay más de 50 cuentas, la lista no aparece. Empieza a escribir y la función de autocompletar te mostrará los valores posibles para que elijas.

7. **Opcional:** Para cambiar la selección en **Calidad del servicio**, realice una de las siguientes acciones:
   a. En **Política**, puede seleccionar una política QoS existente, si está disponible.
   b. En **Configuración personalizada**, establezca valores mínimos, máximos y de ráfaga personalizados para IOPS o utilice los valores QoS predeterminados.

Si está utilizando políticas de QoS en un volumen, puede configurar una QoS personalizada para eliminar la asociación de la política de QoS con el volumen. La QoS personalizada anulará y ajustará los valores de la política de QoS para la configuración de QoS de volumen.

Cuando cambie los valores de IOPS, debe incrementarlos en decenas o centenas. Los valores de entrada deben ser números enteros válidos.

Configure volúmenes con un valor de ráfaga extremadamente alto. Esto permite que el sistema procese cargas de trabajo secuenciales de bloques grandes ocasionales más rápidamente, al tiempo que limita las IOPS sostenidas para un volumen.

8. Haz clic en **Guardar cambios**.

Eliminar un volumen

Puede eliminar uno o más volúmenes de un clúster de almacenamiento Element.

El sistema no elimina inmediatamente un volumen borrado; el volumen permanece disponible durante aproximadamente ocho horas. Si restaura un volumen antes de que el sistema lo elimine, el volumen vuelve a estar en línea y se restablecen las conexiones iSCSI.

Si se elimina un volumen utilizado para crear una instantánea, sus instantáneas asociadas quedan inactivas. Cuando se eliminan los volúmenes de origen borrados, las instantáneas inactivas asociadas también se eliminan del sistema.

Los volúmenes persistentes asociados a los servicios de gestión se crean y se asignan a una nueva cuenta durante la instalación o actualización. Si utiliza volúmenes persistentes, no modifique ni elimine los volúmenes ni la cuenta asociada.

Pasos

1. Seleccione **Administración** > **Volúmenes**.
2. Para eliminar un solo volumen, siga los siguientes pasos:
   a. Haz clic en el icono Acciones del volumen que deseas eliminar.
   b. En el menú que aparece, haga clic en **Eliminar**.
   c. Confirma la acción.

   El sistema mueve el volumen al área **Eliminados** en la página **Volúmenes**.
3. Para eliminar varios volúmenes, siga los siguientes pasos:
   a. En la lista de volúmenes, marque la casilla junto a los volúmenes que desee eliminar.
   b. Haz clic en **Acciones en lote**.
   c. En el menú que aparece, haga clic en **Eliminar**.
   d. Confirma la acción.

   El sistema mueve los volúmenes al área **Eliminados** en la página **Volúmenes**.

Restaurar un volumen eliminado

Puedes restaurar un volumen en el sistema si ha sido eliminado pero aún no se ha purgado. El sistema elimina automáticamente un volumen aproximadamente ocho horas después de haber sido borrado. Si el sistema ha borrado el volumen, no podrá recuperarlo.

1. Seleccione **Administración** > **Volúmenes**.
2. Haz clic en la pestaña **Eliminados** para ver la lista de volúmenes eliminados.
3. Haz clic en el icono Acciones del volumen que deseas restaurar.
4. En el menú que aparece, haga clic en **Restaurar**.
5. Confirma la acción.

   El volumen se coloca en la lista de volúmenes **activos** y se restablecen las conexiones iSCSI al volumen.

Purgar un volumen

Cuando se purga un volumen, se elimina permanentemente del sistema. Se pierden todos los datos del volumen.

El sistema elimina automáticamente los volúmenes borrados ocho horas después de su eliminación. Sin embargo, si desea purgar un volumen antes de la hora programada, puede hacerlo.

1. Seleccione **Administración** > **Volúmenes**.
2. Haz clic en el botón **Eliminado**.
3. Realice los pasos para purgar un solo volumen o varios volúmenes.

Opción	Pasos
Purgar un solo volumen	a. Haz clic en el icono Acciones del volumen que deseas purgar. b. Haga clic en **Purgar**. c. Confirma la acción.
Purgar varios volúmenes	a. Seleccione los volúmenes que desea purgar. b. Haz clic en **Acciones en lote**. c. En el menú que aparece, seleccione **Purgar**. d. Confirma la acción.

Clonar un volumen

Puede crear un clon de un solo volumen o de varios volúmenes para realizar una copia de los datos en un momento dado. Cuando se clona un volumen, el sistema crea una instantánea del volumen y luego crea una copia de los datos a los que hace referencia la instantánea. Este es un proceso asíncrono, y el tiempo que requiere depende del tamaño del volumen que se está clonando y de la carga actual del clúster.

El clúster admite hasta dos solicitudes de clonación en ejecución por volumen a la vez y hasta ocho operaciones de clonación de volumen activas a la vez. Las solicitudes que superen estos límites se pondrán en cola para su posterior procesamiento.

Los sistemas operativos difieren en la forma en que tratan los volúmenes clonados. VMware ESXi tratará un volumen clonado como una copia de volumen o un volumen de instantánea. El volumen será un dispositivo disponible que se podrá utilizar para crear un nuevo almacén de datos. Para obtener más información sobre el montaje de volúmenes clonados y la gestión de LUN de instantáneas, consulte la documentación de VMware sobre "Montando una copia del almacén de datos VMFS" y "gestión de almacenes de datos VMFS duplicados" .

Antes de truncar un volumen clonado clonándolo a un tamaño menor, asegúrese de preparar las particiones para que quepan en el volumen más pequeño.

Pasos

1. Seleccione **Administración** > **Volúmenes**.
2. Para clonar un solo volumen, siga los siguientes pasos:
   a. En la lista de volúmenes de la página **Activos**, haga clic en el icono Acciones del volumen que desea clonar.
   b. En el menú que aparece, haga clic en **Clonar**.
   c. En la ventana **Clonar volumen**, introduzca un nombre para el volumen recién clonado.
   d. Seleccione un tamaño y una medida para el volumen utilizando el cuadro de selección y la lista **Tamaño del volumen**.

      La selección de tamaño de volumen predeterminada está en GB. Puede crear volúmenes utilizando tamaños medidos en GB o GiB:

      - 1 GB = 1 000 000 000 bytes
      - 1 GiB = 1 073 741 824 bytes

   e. Seleccione el tipo de acceso para el volumen recién clonado.
   f. Seleccione una cuenta para asociarla con el volumen recién clonado de la lista **Cuenta**.

      Puedes crear una cuenta durante este paso si haces clic en el enlace **Crear cuenta**, introduces un nombre de cuenta y haces clic en **Crear**. El sistema añade automáticamente la cuenta a la lista **Cuentas** después de crearla.

3. Para clonar varios volúmenes, siga los siguientes pasos:
   a. En la lista de volúmenes de la página **Activos**, marque la casilla junto a los volúmenes que desee clonar.
   b. Haz clic en **Acciones en lote**.
   c. En el menú resultante, seleccione **Clonar**.
   d. En el cuadro de diálogo **Clonar varios volúmenes**, introduzca un prefijo para los volúmenes clonados en el campo **Prefijo de nombre de volumen nuevo**.
   e. Seleccione una cuenta para asociar con los volúmenes clonados de la lista **Cuenta**.
   f. Seleccione el tipo de acceso para los volúmenes clonados.
4. Haz clic en **Iniciar clonación**.

Al aumentar el tamaño del volumen de un clon, se obtiene un nuevo volumen con espacio libre adicional al final del volumen. Dependiendo del uso que le des al volumen, es posible que necesites extender particiones o crear nuevas particiones en el espacio libre para poder utilizarlo.

Para más información

- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Asignar LUN a volúmenes Fibre Channel

Puede cambiar la asignación de LUN para un volumen Fibre Channel en un grupo de acceso a volúmenes. También puede realizar asignaciones de LUN de volumen Fibre Channel al crear un grupo de acceso a volúmenes.

La asignación de nuevas LUN de Fibre Channel es una función avanzada y podría tener consecuencias desconocidas en el host conectado. Por ejemplo, es posible que el nuevo ID de LUN no se detecte automáticamente en el host, y que el host requiera un nuevo escaneo para detectar el nuevo ID de LUN.

1. Seleccione **Administración** > **Grupos de acceso**.
2. Haz clic en el icono Acciones del grupo de acceso que deseas editar.
3. En el menú resultante, seleccione **Editar**.
4. En el cuadro de diálogo **Editar grupo de acceso a volumen**, bajo **Asignar ID de LUN**, haga clic en la flecha de la lista **Asignaciones de LUN**.
5. Para cada volumen de la lista al que desee asignar un LUN, introduzca un nuevo valor en el campo **LUN** correspondiente.
6. Haz clic en **Guardar cambios**.

Aplicar una política de QoS a los volúmenes

Puede aplicar de forma masiva una política QoS existente a uno o más volúmenes.

La política de QoS que desea aplicar de forma masiva debe existir.

1. Seleccione **Administración** > **Volúmenes**.
2. En la lista de volúmenes, marque la casilla junto a los volúmenes a los que desee aplicar la política de QoS.
3. Haz clic en **Acciones en lote**.
4. En el menú que aparece, haga clic en **Aplicar política de QoS**.
5. Seleccione la política de QoS de la lista desplegable.
6. Haga clic en **Aplicar**.

Encuentra más información

Políticas de calidad del servicio

Eliminar la asociación de política QoS de un volumen

Puede eliminar una asociación de política QoS de un volumen seleccionando una configuración QoS personalizada.

El volumen que desea modificar debe estar asociado a una política de QoS.

1. Seleccione **Administración** > **Volúmenes**.
2. Haga clic en el icono Acciones del volumen que contiene la política QoS que desea modificar.
3. Haga clic en **Editar**.
4. En el menú que aparece en **Calidad de servicio**, haga clic en **Configuración personalizada**.
5. Modifique **IOPS mínimas**, **IOPS máximas** e **IOPS de ráfaga**, o mantenga la configuración predeterminada.
6. Haz clic en **Guardar cambios**.

Encuentra más información

Eliminar una política de QoS

Trabajar con volúmenes virtuales

Habilitar volúmenes virtuales

Debe habilitar manualmente la funcionalidad de vSphere Virtual Volumes (VVols) a través del software NetApp Element . El sistema de software Element viene con la funcionalidad VVols desactivada por defecto, y no se activa automáticamente como parte de una nueva instalación o actualización. Habilitar la función VVols es una tarea de configuración que se realiza una sola vez.

Lo que necesitarás

- El clúster debe estar ejecutando Element 9.0 o posterior.
- El clúster debe estar conectado a un entorno ESXi 6.0 o posterior que sea compatible con VVols.
- Si está utilizando Element 11.3 o posterior, el clúster debe estar conectado a un entorno ESXi 6.0 actualización 3 o posterior.

> Habilitar la funcionalidad de volúmenes virtuales de vSphere modifica permanentemente la configuración del software Element. Solo debe habilitar la funcionalidad VVols si su clúster está conectado a un entorno compatible con VMware ESXi VVols. Solo se puede desactivar la función VVols y restaurar la configuración predeterminada devolviendo el clúster a la imagen de fábrica, lo que elimina todos los datos del sistema.

Pasos

1. Seleccione **Clústeres** > **Configuración**.
2. Encuentre la configuración específica del clúster para volúmenes virtuales.
3. Haga clic en **Habilitar volúmenes virtuales**.
4. Haga clic en **Sí** para confirmar el cambio de configuración de volúmenes virtuales.

La pestaña **VVols** aparece en la interfaz de usuario de Element.

> Cuando se habilita la funcionalidad VVols, el clúster SolidFire inicia el proveedor VASA, abre el puerto 8444 para el tráfico VASA y crea puntos de conexión de protocolo que pueden ser detectados por vCenter y todos los hosts ESXi.

5. Copie la URL del proveedor VASA de la configuración de Volúmenes Virtuales (VVols) en **Clústeres** > **Configuración**. Utilizará esta URL para registrar el proveedor VASA en vCenter.
6. Cree un contenedor de almacenamiento en **VVols** > **Contenedores de almacenamiento**.

> Debe crear al menos un contenedor de almacenamiento para que las máquinas virtuales puedan aprovisionarse en un almacén de datos VVol.

7. Seleccione **VVols** > **Puntos finales del protocolo**.
8. Verifique que se haya creado un punto final de protocolo para cada nodo del clúster.

> En vSphere se requieren tareas de configuración adicionales. Consulte la _Guía de configuración de volúmenes virtuales de VMware vSphere para almacenamiento SolidFire para registrar el proveedor VASA en vCenter, crear y administrar almacenes de datos VVol y administrar el almacenamiento según las políticas.

Encuentra más información

"Guía de configuración de VMware vSphere Virtual Volumes para SolidFire Storage"

Ver detalles del volumen virtual

En la interfaz de usuario de Element puede consultar la información de volumen virtual para todos los volúmenes virtuales activos en el clúster. También puede ver la actividad de rendimiento de cada volumen virtual, incluyendo entrada, salida, rendimiento, latencia, profundidad de cola e información del volumen.

Lo que necesitarás

- Deberías haber habilitado la funcionalidad VVols en la interfaz de usuario de Element para el clúster.
- Deberías haber creado un contenedor de almacenamiento asociado.
- Deberías haber configurado tu clúster vSphere para usar la funcionalidad VVols del software Element.
- Deberías haber creado al menos una máquina virtual en vSphere.

Pasos

1. Haga clic en **VVols** > **Volúmenes virtuales**.

   Se muestra la información de todos los volúmenes virtuales activos.

2. Haga clic en el icono **Acciones** del volumen virtual que desea revisar.
3. En el menú que aparece, seleccione **Ver detalles**.

Detalles

La página Volúmenes virtuales de la pestaña VVols proporciona información sobre cada volumen virtual activo en el clúster, como el ID del volumen, el ID de la instantánea, el ID del volumen virtual principal y el ID del volumen virtual.

- **ID de volumen**: El ID del volumen subyacente.
- **ID de instantánea**: El ID de la instantánea de volumen subyacente. El valor es 0 si el volumen virtual no representa una instantánea de SolidFire .
- **ID de volumen virtual principal**: El ID de volumen virtual del volumen virtual principal. Si el ID está compuesto únicamente por ceros, el volumen virtual es independiente y no tiene vínculo con un elemento principal.
- **ID de volumen virtual**: El UUID del volumen virtual.
- **Nombre**: El nombre asignado al volumen virtual.
- **Contenedor de almacenamiento**: El contenedor de almacenamiento que posee el volumen virtual.
- **Tipo de SO invitado**: Sistema operativo asociado al volumen virtual.
- **Tipo de volumen virtual**: El tipo de volumen virtual: Configuración, Datos, Memoria, Intercambio u Otro.
- **Acceso**: Los permisos de lectura y escritura asignados al volumen virtual.
- **Tamaño**: El tamaño del volumen virtual en GB o GiB.
- **Instantáneas**: El número de instantáneas asociadas. Haz clic en el número para acceder a los detalles de la captura de pantalla.
- **IOPS mínimas**: La configuración QoS de IOPS mínima del volumen virtual.
- **IOPS máx.**: La configuración QoS de IOPS máxima del volumen virtual.
- **IOPS de ráfaga**: La configuración QoS de ráfaga máxima del volumen virtual.
- **VMW_VmID**: La información en los campos precedidos por "VMW_" está definida por VMware.
- **Hora de creación**: Hora en que se completó la tarea de creación del volumen virtual.

Detalles de volumen virtual individual

La página Volúmenes virtuales en la pestaña VVols proporciona la siguiente información sobre el volumen virtual cuando selecciona un volumen virtual individual y ve sus detalles.

- **VMW_XXX**: La información en los campos precedidos por "VMW_" está definida por VMware.
- **ID de volumen virtual principal**: El ID de volumen virtual del volumen virtual principal. Si el ID está compuesto únicamente por ceros, el volumen virtual es independiente y no tiene vínculo con un elemento principal.
- **ID de volumen virtual**: El UUID del volumen virtual.
- **Tipo de volumen virtual**: El tipo de volumen virtual: Configuración, Datos, Memoria, Intercambio u Otro.
- **ID de volumen**: El ID del volumen subyacente.
- **Acceso**: Los permisos de lectura y escritura asignados al volumen virtual.
- **Nombre de la cuenta**: Nombre de la cuenta que contiene el volumen.
- **Grupos de acceso**: Grupos de acceso a volúmenes asociados.
- **Tamaño total del volumen**: Capacidad total aprovisionada en bytes.
- **Bloques distintos de cero**: Número total de bloques de 4 KiB con datos después de que se haya

completado la última operación de recolección de basura.

- **Bloques Cero**: Número total de bloques de 4 KiB sin datos después de que se haya completado la última ronda de operación de recolección de basura.
- **Instantáneas**: El número de instantáneas asociadas. Haz clic en el número para acceder a los detalles de la captura de pantalla.
- **IOPS mínimas**: La configuración QoS de IOPS mínima del volumen virtual.
- **IOPS máx.**: La configuración QoS de IOPS máxima del volumen virtual.
- **IOPS de ráfaga**: La configuración QoS de ráfaga máxima del volumen virtual.
- **Habilitar 512**: Debido a que los volúmenes virtuales siempre usan la emulación de tamaño de bloque de 512 bytes, el valor siempre es sí.
- **Volúmenes emparejados**: Indica si un volumen está emparejado.
- **Hora de creación**: Hora en que se completó la tarea de creación del volumen virtual.
- **Tamaño de los bloques**: Tamaño de los bloques en el volumen.
- **Escrituras no alineadas**: Para volúmenes 512e, el número de operaciones de escritura que no estaban en un límite de sector de 4k. Un número elevado de escrituras no alineadas podría indicar una alineación de particiones incorrecta.
- **Lecturas no alineadas**: Para volúmenes 512e, el número de operaciones de lectura que no estaban en un límite de sector de 4k. Un elevado número de lecturas no alineadas podría indicar una alineación de particiones incorrecta.
- **scsiEUIDeviceID**: Identificador de dispositivo SCSI único global para el volumen en formato de 16 bytes basado en EUI-64.
- **scsiNAADeviceID**: Identificador de dispositivo SCSI único a nivel mundial para el volumen en formato NAA IEEE Registered Extended.
- **Atributos**: Lista de pares nombre-valor en formato de objeto JSON.

Eliminar un volumen virtual

Aunque los volúmenes virtuales siempre deben eliminarse desde la capa de administración de VMware, la funcionalidad para eliminar volúmenes virtuales está habilitada desde la interfaz de usuario de Element. Solo debes eliminar un volumen virtual desde la interfaz de usuario de Element cuando sea absolutamente necesario, por ejemplo, cuando vSphere no pueda limpiar los volúmenes virtuales en el almacenamiento SolidFire .

1. Seleccione **VVols** > **Volúmenes virtuales**.
2. Haz clic en el icono Acciones del volumen virtual que deseas eliminar.
3. En el menú que aparece, seleccione **Eliminar**.

> Debe eliminar un volumen virtual de la capa de administración de VMware para asegurarse de que el volumen virtual se desvincule correctamente antes de su eliminación. Solo debes eliminar un volumen virtual desde la interfaz de usuario de Element cuando sea absolutamente necesario, por ejemplo, cuando vSphere no pueda limpiar los volúmenes virtuales en el almacenamiento SolidFire . Si elimina un volumen virtual desde la interfaz de usuario de Element, el volumen se eliminará inmediatamente.

4. Confirma la acción.
5. Actualice la lista de volúmenes virtuales para confirmar que el volumen virtual se ha eliminado.
6. **Opcional**: Seleccione **Informes** > **Registro de eventos** para confirmar que la purga se ha realizado correctamente.

Gestionar contenedores de almacenamiento

Un contenedor de almacenamiento es una representación de un almacén de datos de vSphere creado en un clúster que ejecuta el software Element.

Los contenedores de almacenamiento se crean y se vinculan a las cuentas de NetApp Element . Un contenedor de almacenamiento creado en Element Storage aparece como un almacén de datos de vSphere en vCenter y ESXi. Los contenedores de almacenamiento no asignan ningún espacio en el almacenamiento de Element. Simplemente se utilizan para asociar lógicamente volúmenes virtuales.

Se admite un máximo de cuatro contenedores de almacenamiento por clúster. Se requiere un mínimo de un contenedor de almacenamiento para habilitar la funcionalidad VVols.

Crea un contenedor de almacenamiento

Puede crear contenedores de almacenamiento en la interfaz de usuario de Element y descubrirlos en vCenter. Debe crear al menos un contenedor de almacenamiento para comenzar a aprovisionar máquinas virtuales respaldadas por VVol.

Antes de comenzar, habilite la funcionalidad VVols en la interfaz de usuario de Element para el clúster.

Pasos

1. Seleccione **VVols** > **Contenedores de almacenamiento**.
2. Haz clic en el botón **Crear contenedores de almacenamiento**.
3. Introduzca la información del contenedor de almacenamiento en el cuadro de diálogo **Crear un nuevo contenedor de almacenamiento**:
   a. Introduzca un nombre para el contenedor de almacenamiento.
   b. Configure los secretos de iniciador y destino para CHAP.

      Deje en blanco los campos de Configuración CHAP para generar secretos automáticamente.

   c. Haz clic en el botón **Crear contenedor de almacenamiento**.
4. Verifique que el nuevo contenedor de almacenamiento aparezca en la lista de la subpestaña **Contenedores de almacenamiento**.

   Dado que se crea automáticamente un ID de cuenta de NetApp Element y se asigna al contenedor de almacenamiento, no es necesario crear una cuenta manualmente.

Ver detalles del contenedor de almacenamiento

En la página Contenedores de almacenamiento de la pestaña VVols, puede ver información sobre todos los contenedores de almacenamiento activos en el clúster.

- **ID de cuenta**: El ID de la cuenta de NetApp Element asociada con el contenedor de almacenamiento.
- **Nombre**: El nombre del contenedor de almacenamiento.
- **Estado**: El estado del contenedor de almacenamiento. Valores posibles:
  - Activo: El contenedor de almacenamiento está en uso.
  - Bloqueado: El contenedor de almacenamiento está bloqueado.
- **Tipo de PE**: El tipo de punto final del protocolo (SCSI es el único protocolo disponible para el software Element).
- **ID del contenedor de almacenamiento**: El UUID del contenedor de almacenamiento del volumen virtual.
- **Volúmenes virtuales activos**: El número de volúmenes virtuales activos asociados al contenedor de almacenamiento.

Ver detalles de cada contenedor de almacenamiento

Puede ver la información del contenedor de almacenamiento para un contenedor de almacenamiento individual seleccionándolo en la página Contenedores de almacenamiento de la pestaña VVols.

- **ID de cuenta**: El ID de la cuenta de NetApp Element asociada con el contenedor de almacenamiento.
- **Nombre**: El nombre del contenedor de almacenamiento.
- **Estado**: El estado del contenedor de almacenamiento. Valores posibles:
  - Activo: El contenedor de almacenamiento está en uso.
  - Bloqueado: El contenedor de almacenamiento está bloqueado.
- **Secreto del Iniciador del Capítulo**: El secreto único del Capítulo para el iniciador.
- **Secreto del Objetivo CHAP**: El secreto CHAP único para el objetivo.
- **ID del contenedor de almacenamiento**: El UUID del contenedor de almacenamiento del volumen virtual.
- **Tipo de punto final de protocolo**: Indica el tipo de punto final de protocolo (SCSI es el único protocolo disponible).

Editar un contenedor de almacenamiento

Puede modificar la autenticación CHAP del contenedor de almacenamiento en la interfaz de usuario de Element.

1. Seleccione **VVols** > **Contenedores de almacenamiento**.
2. Haz clic en el icono **Acciones** del contenedor de almacenamiento que deseas editar.
3. En el menú que aparece, seleccione **Editar**.
4. En la configuración de CHAP, edite las credenciales de Secreto de Iniciador y Secreto de Destino utilizadas para la autenticación.

   Si no modifica las credenciales de configuración CHAP, estas permanecerán sin cambios. Si dejas en blanco los campos de credenciales, el sistema generará automáticamente nuevos secretos.

5. Haz clic en **Guardar cambios**.

Eliminar un contenedor de almacenamiento

Puedes eliminar contenedores de almacenamiento desde la interfaz de usuario de Element.

Lo que necesitarás

Asegúrese de que todas las máquinas virtuales se hayan eliminado del almacén de datos VVol.

Pasos

1. Seleccione **VVols** > **Contenedores de almacenamiento**.
2. Haz clic en el icono **Acciones** del contenedor de almacenamiento que deseas eliminar.
3. En el menú que aparece, seleccione **Eliminar**.
4. Confirma la acción.
5. Actualice la lista de contenedores de almacenamiento en la subpestaña **Contenedores de almacenamiento** para confirmar que el contenedor de almacenamiento se ha eliminado.

puntos finales del protocolo

Aprenda sobre los puntos finales del protocolo

Los puntos de conexión del protocolo son puntos de acceso utilizados por un host para direccionar el almacenamiento en un clúster que ejecuta el software NetApp Element . Los puntos de conexión del protocolo no pueden ser eliminados ni modificados por un usuario, no están asociados a una cuenta y no pueden agregarse a un grupo de acceso por volumen.

Un clúster que ejecuta el software Element crea automáticamente un punto final de protocolo por cada nodo de almacenamiento en el clúster. Por ejemplo, un clúster de almacenamiento de seis nodos tiene seis puntos finales de protocolo que están asignados a cada host ESXi. Los puntos finales del protocolo son gestionados dinámicamente por el software Element y se crean, mueven o eliminan según sea necesario sin ninguna intervención. Los puntos finales del protocolo son el destino del enrutamiento múltiple y actúan como un proxy de E/S para las LUN subsidiarias. Cada extremo del protocolo consume una dirección SCSI disponible, al igual que un destino iSCSI estándar. Los puntos finales del protocolo aparecen como un dispositivo de almacenamiento de un solo bloque (512 bytes) en el cliente vSphere, pero este dispositivo de almacenamiento no está disponible para formatearse ni utilizarse como almacenamiento.

iSCSI es el único protocolo compatible. El protocolo Fibre Channel no es compatible.

Detalles de los puntos de conexión del protocolo

La página Puntos de conexión del protocolo en la pestaña VVols proporciona información sobre los puntos de conexión del protocolo.

- **ID del proveedor principal**

  El ID del proveedor del punto final del protocolo principal.

- **ID del proveedor secundario**

  El ID del proveedor del punto final del protocolo secundario.

- **ID del punto final del protocolo**

El UUID del punto final del protocolo.

- **Estado del punto final del protocolo**

  Estado del punto final del protocolo. Los valores posibles son los siguientes:

  - Activo: El punto final del protocolo está en uso.
  - Inicio: El punto final del protocolo se está iniciando.
  - Conmutación por error: El extremo del protocolo ha conmutado por error.
  - Reservado: El punto final del protocolo está reservado.
- **Tipo de proveedor**

  El tipo de proveedor del punto final del protocolo. Los valores posibles son los siguientes:

  - Primario
  - Secundario
- **ID de dispositivo SCSI NAA**

  El identificador de dispositivo SCSI único a nivel mundial para el punto final del protocolo en formato extendido registrado IEEE NAA.

Fijaciones

Aprende sobre encuadernaciones

Para realizar operaciones de E/S con un volumen virtual, un host ESXi primero debe enlazar el volumen virtual.

El clúster SolidFire elige un punto final de protocolo óptimo, crea un enlace que asocia el host ESXi y el volumen virtual con el punto final de protocolo y devuelve el enlace al host ESXi. Una vez enlazado, el host ESXi puede realizar operaciones de E/S con el volumen virtual enlazado.

Detalles de encuadernación

La página de enlaces en la pestaña VVols proporciona información de enlace sobre cada volumen virtual.

Se muestra la siguiente información:

- **ID del host**

  El UUID del host ESXi que aloja volúmenes virtuales y que es conocido por el clúster.
- **ID del punto final del protocolo**

  Identificadores de punto final del protocolo que corresponden a cada nodo en el clúster SolidFire .
- **Punto final del protocolo en la ID de banda**

  El ID de dispositivo SCSI de NAA del extremo del protocolo.

- **Tipo de punto final del protocolo**

  El tipo de punto final del protocolo.

- **ID de enlace VVol**

  El UUID de enlace del volumen virtual.

- **ID de VVol**

  El identificador único universal (UUID) del volumen virtual.

- **ID secundaria de VVol**

  El ID secundario del volumen virtual que es un ID de LUN SCSI de segundo nivel.

Detalles del anfitrión

La página Hosts de la pestaña VVols proporciona información sobre los hosts VMware ESXi que alojan volúmenes virtuales.

Se muestra la siguiente información:

- **ID del host**

  El UUID del host ESXi que aloja volúmenes virtuales y que es conocido por el clúster.

- **Dirección del host**

  La dirección IP o el nombre DNS del host ESXi.

- **Encuadernaciones**

  Identificadores de enlace para todos los volúmenes virtuales enlazados por el host ESXi.

- **ID de clúster ESX**

  El ID del clúster de host de vSphere o el GUID de vCenter.

- **Números de identificación de iniciador**

  IQN de iniciador para el host de volumen virtual.

- * Identificadores de punto final del protocolo SolidFire *

  Los puntos finales del protocolo que actualmente son visibles para el host ESXi.

Trabajar con grupos de acceso por volumen e iniciadores

Crear un grupo de acceso por volumen

Puede crear grupos de acceso a volúmenes asignando iniciadores a una colección de volúmenes para un acceso seguro. Luego puede otorgar acceso a los volúmenes del

grupo con un secreto de iniciador CHAP de cuenta y un secreto de destino.

Si utiliza CHAP basado en iniciador, puede agregar credenciales CHAP para un único iniciador en un grupo de acceso por volumen, lo que proporciona mayor seguridad. Esto le permite aplicar esta opción a los grupos de acceso por volumen que ya existen.

Pasos

1. Haz clic en **Administración** > **Grupos de acceso**.
2. Haga clic en **Crear grupo de acceso**.
3. Introduzca un nombre para el grupo de acceso al volumen en el campo **Nombre**.
4. Agregue un iniciador al grupo de acceso al volumen de una de las siguientes maneras:

Opción	Descripción
Agregar un iniciador de canal de fibra	a. En Agregar iniciadores, seleccione un iniciador de canal de fibra existente de la lista Iniciadores de canal de fibra no enlazados. b. Haga clic en **Agregar iniciador FC**. Puedes crear un iniciador durante este paso si haces clic en el enlace **Crear iniciador**, introduces un nombre para el iniciador y haces clic en **Crear**. El sistema añade automáticamente el iniciador a la lista de Iniciadores después de crearlo. Un ejemplo del formato es el siguiente: `5f:47:ac:c0:5c:74:d4:02`

Opción	Descripción
Agregar un iniciador iSCSI	En Agregar iniciadores, seleccione un iniciador existente de la lista de Iniciadores. **Nota:** Puede crear un iniciador durante este paso si hace clic en el enlace **Crear iniciador**, introduce un nombre de iniciador y hace clic en **Crear**. El sistema añade automáticamente el iniciador a la lista de Iniciadores después de crearlo. Un ejemplo del formato es el siguiente: `iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b` Puede encontrar el IQN del iniciador para cada volumen seleccionando **Ver detalles** en el menú Acciones del volumen en la lista **Administración** > **Volúmenes** > **Activos**. Al modificar un iniciador, puede cambiar el atributo requiredCHAP a True, lo que le permite establecer el secreto del iniciador de destino. Para obtener más detalles, consulte la información de la API sobre el método de la API ModifyInitiator. "Gestiona el almacenamiento con la API de Element"

5. **Opcional:** Agregue más iniciadores según sea necesario.
6. En Agregar volúmenes, seleccione un volumen de la lista **Volúmenes**.

   El volumen aparece en la lista de **Volúmenes adjuntos**.
7. **Opcional:** Añada más volúmenes según sea necesario.
8. Haga clic en **Crear grupo de acceso**.

Encuentra más información

Agregar volúmenes a un grupo de acceso

Ver detalles del grupo de acceso individual

Puede ver los detalles de un grupo de acceso individual, como los volúmenes conectados y los iniciadores, en formato gráfico.

1. Haz clic en **Administración** > **Grupos de acceso**.
2. Haz clic en el icono de Acciones para un grupo de acceso.
3. Haga clic en **Ver detalles**.

Detalles del grupo de acceso por volumen

La página Grupos de acceso en la pestaña Administración proporciona información sobre los grupos de acceso a volúmenes.

Se muestra la siguiente información:

- **ID**: El ID generado por el sistema para el grupo de acceso.
- **Nombre**: El nombre asignado al grupo de acceso cuando se creó.
- **Volúmenes activos**: El número de volúmenes activos en el grupo de acceso.
- **Compresión**: Puntuación de eficiencia de compresión para el grupo de acceso.
- **Desduplicación**: La puntuación de eficiencia de deduplicación para el grupo de acceso.
- **Aprovisionamiento ligero**: La puntuación de eficiencia del aprovisionamiento ligero para el grupo de acceso.
- **Eficiencia general**: La puntuación de eficiencia general para el grupo de acceso.
- **Iniciadores**: El número de iniciadores conectados al grupo de acceso.

Agregar volúmenes a un grupo de acceso

Puede agregar volúmenes a un grupo de acceso a volúmenes. Cada volumen puede pertenecer a más de un grupo de acceso a volúmenes; puede ver los grupos a los que pertenece cada volumen en la página de volúmenes **activos**.

También puede utilizar este procedimiento para agregar volúmenes a un grupo de acceso a volúmenes de Fibre Channel.

1. Haz clic en **Administración** > **Grupos de acceso**.
2. Haga clic en el icono Acciones del grupo de acceso al que desea agregar volúmenes.
3. Haz clic en el botón **Editar**.
4. En Agregar volúmenes, seleccione un volumen de la lista **Volúmenes**.

   Puedes añadir más volúmenes repitiendo este paso.

5. Haz clic en **Guardar cambios**.

Eliminar volúmenes de un grupo de acceso

Cuando se elimina un volumen de un grupo de acceso, el grupo ya no tiene acceso a ese volumen.

Modificar la configuración CHAP en una cuenta o eliminar iniciadores o volúmenes de un grupo de acceso puede provocar que los iniciadores pierdan el acceso a los volúmenes de forma inesperada. Para verificar que el acceso al volumen no se pierda inesperadamente, cierre siempre las sesiones iSCSI que se verán afectadas por un cambio de cuenta o de grupo de acceso, y verifique que los iniciadores puedan volver a conectarse a los volúmenes después de que se hayan completado los cambios en la configuración del iniciador y la configuración del clúster.

1. Haz clic en **Administración** > **Grupos de acceso**.
2. Haga clic en el icono Acciones del grupo de acceso del que desea eliminar volúmenes.
3. Haga clic en **Editar**.
4. En Agregar volúmenes del cuadro de diálogo **Editar grupo de acceso a volúmenes**, haga clic en la flecha de la lista **Volúmenes conectados**.

5. Seleccione el volumen que desea eliminar de la lista y haga clic en el icono **x** para eliminar el volumen de la lista.

   Puedes eliminar más volúmenes repitiendo este paso.

6. Haz clic en **Guardar cambios**.

Crear un iniciador

Puede crear iniciadores iSCSI o Fibre Channel y, opcionalmente, asignarles alias.

También puede asignar atributos CHAP basados en el iniciador mediante una llamada a la API. Para agregar un nombre de cuenta CHAP y credenciales por iniciador, debe usar el `CreateInitiator` Llamada a la API para eliminar y agregar acceso y atributos CHAP. El acceso del iniciador se puede restringir a una o más VLAN especificando uno o más ID de red virtual a través de `CreateInitiators` y `ModifyInitiators` Llamadas a la API. Si no se especifican redes virtuales, el iniciador puede acceder a todas las redes.

Para obtener más detalles, consulte la información de referencia de la API. "Gestiona el almacenamiento con la API de Element"

Pasos

1. Haz clic en **Administración** > **Iniciadores**.
2. Haz clic en **Crear iniciador**.
3. Siga los pasos para crear un único iniciador o varios iniciadores:

Opción	Pasos
Crea un único iniciador	a. Haga clic en **Crear un único iniciador**. b. Introduzca el IQN o WWPN del iniciador en el campo **IQN/WWPN**. c. Introduzca un nombre amigable para el iniciador en el campo **Alias**. d. Haz clic en **Crear iniciador**.
Crear múltiples iniciadores	a. Haga clic en **Crear iniciadores en masa**. b. Introduzca una lista de IQN o WWPN en el cuadro de texto. c. Haz clic en **Añadir iniciadores**. d. Elija un iniciador de la lista resultante y haga clic en el icono Agregar correspondiente en la columna **Alias** para agregar un alias al iniciador. e. Haz clic en la marca de verificación para confirmar el nuevo alias. f. Haz clic en **Crear iniciadores**.

Editar un iniciador

Puedes cambiar el alias de un iniciador existente o agregar un alias si aún no existe.

Para agregar un nombre de cuenta CHAP y credenciales por iniciador, debe usar el `ModifyInitiator` Llamada a la API para eliminar y agregar acceso y atributos CHAP.

Ver"Gestiona el almacenamiento con la API de Element" .

Pasos

1. Haz clic en **Administración** > **Iniciadores**.
2. Haz clic en el icono de Acciones del iniciador que deseas editar.
3. Haga clic en **Editar**.
4. Introduzca un nuevo alias para el iniciador en el campo **Alias**.
5. Haz clic en **Guardar cambios**.

Agregar un único iniciador a un grupo de acceso a volumen

Puede agregar un iniciador a un grupo de acceso a volúmenes existente.

Cuando se agrega un iniciador a un grupo de acceso a volúmenes, dicho iniciador tiene acceso a todos los volúmenes de ese grupo de acceso a volúmenes.

Puede encontrar el iniciador de cada volumen haciendo clic en el icono Acciones y luego seleccionando **Ver detalles** para el volumen en la lista de volúmenes activos.

Si utiliza CHAP basado en iniciador, puede agregar credenciales CHAP para un único iniciador en un grupo de acceso por volumen, lo que proporciona mayor seguridad. Esto le permite aplicar esta opción a los grupos de acceso por volumen que ya existen.

Pasos

1. Haz clic en **Administración** > **Grupos de acceso**.
2. Haga clic en el icono **Acciones** del grupo de acceso que desea editar.
3. Haga clic en **Editar**.
4. Para agregar un iniciador Fibre Channel al grupo de acceso a volúmenes, siga los siguientes pasos:
   a. En Agregar iniciadores, seleccione un iniciador de canal de fibra existente de la lista **Iniciadores de canal de fibra no enlazados**.
   b. Haga clic en **Agregar iniciador FC**.

   Puedes crear un iniciador durante este paso si haces clic en el enlace **Crear iniciador**, introduces un nombre para el iniciador y haces clic en **Crear**. El sistema añade automáticamente al iniciador a la lista de **Iniciadores** después de crearlo.

   Un ejemplo del formato es el siguiente:

```
5f:47:ac:c0:5c:74:d4:02
```

5. Para agregar un iniciador iSCSI al grupo de acceso al volumen, en Agregar iniciadores, seleccione un iniciador existente de la lista **Iniciadores**.

   Puedes crear un iniciador durante este paso si haces clic en el enlace **Crear iniciador**, introduces un nombre para el iniciador y haces clic en **Crear**. El sistema añade automáticamente al iniciador a la lista de **Iniciadores** después de crearlo.

   El formato aceptado de un IQN iniciador es el siguiente: iqn.yyyy-mm, donde y y m son dígitos, seguido de

texto que solo debe contener dígitos, caracteres alfabéticos en minúscula, un punto (.), dos puntos (:) o un guion (-).

Un ejemplo del formato es el siguiente:

```
iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b
```

Puede encontrar el IQN del iniciador para cada volumen en la página **Administración** > **Volúmenes** Volúmenes activos haciendo clic en el icono Acciones y luego seleccionando **Ver detalles** para el volumen.

6. Haz clic en **Guardar cambios**.

Agregue varios iniciadores a un grupo de acceso por volumen.

Puede agregar varios iniciadores a un grupo de acceso a volúmenes existente para permitir el acceso a los volúmenes del grupo de acceso a volúmenes con o sin necesidad de autenticación CHAP.

Cuando se agregan iniciadores a un grupo de acceso a volúmenes, los iniciadores tienen acceso a todos los volúmenes de ese grupo de acceso a volúmenes.

Puede encontrar el iniciador de cada volumen haciendo clic en el icono Acciones y luego en **Ver detalles** para el volumen en la lista de volúmenes activos.

Puede agregar varios iniciadores a un grupo de acceso a volúmenes existente para habilitar el acceso a los volúmenes y asignar credenciales CHAP únicas para cada iniciador dentro de ese grupo de acceso a volúmenes. Esto le permite aplicar esta opción a los grupos de acceso por volumen que ya existen.

Puede asignar atributos CHAP basados en el iniciador mediante una llamada a la API. Para agregar un nombre de cuenta CHAP y credenciales por iniciador, debe usar la llamada a la API ModifyInitiator para eliminar y agregar el acceso y los atributos CHAP.

Para más detalles, consulte"Gestiona el almacenamiento con la API de Element" .

Pasos

1. Haz clic en **Administración** > **Iniciadores**.
2. Seleccione los iniciadores que desea agregar a un grupo de acceso.
3. Haz clic en el botón **Acciones en lote**.
4. Haga clic en **Agregar al grupo de acceso por volumen**.
5. En el cuadro de diálogo Agregar a grupo de acceso por volumen, seleccione un grupo de acceso de la lista **Grupo de acceso por volumen**.
6. Haga clic en **Agregar**.

Eliminar iniciadores de un grupo de acceso

Cuando se elimina un iniciador de un grupo de acceso, este ya no puede acceder a los volúmenes de ese grupo de acceso a volúmenes. El acceso normal de la cuenta al

volumen no se ve interrumpido.

Modificar la configuración CHAP en una cuenta o eliminar iniciadores o volúmenes de un grupo de acceso puede provocar que los iniciadores pierdan el acceso a los volúmenes de forma inesperada. Para verificar que el acceso al volumen no se pierda inesperadamente, cierre siempre las sesiones iSCSI que se verán afectadas por un cambio de cuenta o de grupo de acceso, y verifique que los iniciadores puedan volver a conectarse a los volúmenes después de que se hayan completado los cambios en la configuración del iniciador y la configuración del clúster.

Pasos

1. Haz clic en **Administración** > **Grupos de acceso**.
2. Haz clic en el icono **Acciones** del grupo de acceso que deseas eliminar.
3. En el menú que aparece, seleccione **Editar**.
4. En Agregar iniciadores en el cuadro de diálogo **Editar grupo de acceso a volumen**, haga clic en la flecha de la lista **Iniciadores**.
5. Seleccione el icono x para cada iniciador que desee eliminar del grupo de acceso.
6. Haz clic en **Guardar cambios**.

Eliminar un grupo de acceso

Puede eliminar un grupo de acceso cuando ya no sea necesario. No es necesario eliminar los ID de iniciador ni los ID de volumen del grupo de acceso a volúmenes antes de eliminar el grupo. Una vez eliminado el grupo de acceso, se interrumpe el acceso del grupo a los volúmenes.

1. Haz clic en **Administración** > **Grupos de acceso**.
2. Haz clic en el icono **Acciones** del grupo de acceso que deseas eliminar.
3. En el menú que aparece, haga clic en **Eliminar**.
4. Para eliminar también los iniciadores asociados a este grupo de acceso, seleccione la casilla de verificación **Eliminar iniciadores en este grupo de acceso**.
5. Confirma la acción.

Eliminar un iniciador

Puedes eliminar un iniciador cuando ya no sea necesario. Cuando se elimina un iniciador, el sistema lo quita de cualquier grupo de acceso a volúmenes asociado. Las conexiones que utilizan el iniciador permanecen válidas hasta que se restablece la conexión.

Pasos

1. Haz clic en **Administración** > **Iniciadores**.
2. Siga los pasos para eliminar un único iniciador o varios iniciadores:

Opción	Pasos
Eliminar iniciador único	a. Haz clic en el icono **Acciones** del iniciador que deseas eliminar. b. Haga clic en **Eliminar**. c. Confirma la acción.
Eliminar varios iniciadores	a. Seleccione las casillas de verificación junto a los iniciadores que desea eliminar. b. Haz clic en el botón **Acciones en lote**. c. En el menú que aparece, seleccione **Eliminar**. d. Confirma la acción.

Proteja sus datos

Proteja sus datos

El software NetApp Element le permite proteger sus datos de diversas maneras con funcionalidades como instantáneas para volúmenes individuales o grupos de volúmenes, replicación entre clústeres y volúmenes que se ejecutan en Element y replicación a sistemas ONTAP .

- **Instantáneas**

  La protección de datos de solo instantáneas replica los datos modificados en momentos específicos en un clúster remoto. Solo se replican las instantáneas creadas en el clúster de origen. Las escrituras activas desde el volumen de origen no lo son.

  Utilice instantáneas de volumen para la protección de datos.

- **Replicación remota entre clústeres y volúmenes que se ejecutan en Element**

  Puede replicar datos de volumen de forma síncrona o asíncrona desde cualquiera de los clústeres de un par de clústeres que se ejecutan en Element para escenarios de conmutación por error y recuperación ante fallos.

  Realizar replicación remota entre clústeres que ejecutan el software NetApp Element .

- *Replicación entre clústeres Element y ONTAP mediante la tecnología SnapMirror *

  Con la tecnología NetApp SnapMirror , puede replicar instantáneas tomadas con Element en ONTAP para fines de recuperación ante desastres. En una relación SnapMirror , Element es un punto final y ONTAP es el otro.

  Utilice la replicación SnapMirror entre los clústeres Element y ONTAP.

- **Realizar copias de seguridad y restaurar volúmenes desde SolidFire, S3 o almacenes de objetos Swift**

  Puede realizar copias de seguridad y restaurar volúmenes en otros almacenamientos SolidFire , así como

en almacenes de objetos secundarios compatibles con Amazon S3 u OpenStack Swift.

Realice copias de seguridad y restaure volúmenes en almacenes de objetos SolidFire, S3 o Swift.

Para más información

- "Documentación del software SolidFire y Element"
- "Plugin de NetApp Element para vCenter Server"

Utilice instantáneas de volumen para la protección de datos.

Utilice instantáneas de volumen para la protección de datos.

Una instantánea de volumen es una copia de un volumen en un momento dado. Puedes tomar una instantánea de un volumen y usarla más tarde si necesitas restaurar un volumen al estado en el que se encontraba en el momento en que se creó la instantánea.

Las instantáneas son similares a los clones de volumen. Sin embargo, las instantáneas son simplemente réplicas de los metadatos del volumen, por lo que no se pueden montar ni escribir en ellas. La creación de una instantánea de volumen también requiere una cantidad mínima de recursos del sistema y espacio, lo que hace que la creación de instantáneas sea más rápida que la clonación.

Puede tomar una instantánea de un volumen individual o de un conjunto de volúmenes.

Opcionalmente, replique las instantáneas en un clúster remoto y utilícelas como copia de seguridad del volumen. Esto le permite revertir un volumen a un punto específico en el tiempo mediante el uso de la instantánea replicada. Como alternativa, puede crear un clon de un volumen a partir de una instantánea replicada.

Encuentra más información

- Utilice instantáneas de volumen individuales para la protección de datos.
- Utilizar instantáneas de grupo para la tarea de protección de datos
- Programar una instantánea

Utilice instantáneas de volumen individuales para la protección de datos.

Utilice instantáneas de volumen individuales para la protección de datos.

Una instantánea de volumen es una copia de un volumen en un momento dado. Puede utilizar un volumen individual en lugar de un grupo de volúmenes para la instantánea.

Encuentra más información

- Cree una instantánea de volumen
- Editar retención de instantáneas
- Eliminar una instantánea
- Clonar un volumen a partir de una instantánea

- Revertir un volumen a una instantánea
- Realizar una copia de seguridad de una instantánea de volumen en un almacenamiento de objetos de Amazon S3
- Realizar una copia de seguridad de una instantánea de volumen en un almacén de objetos Swift de OpenStack
- Realizar una copia de seguridad de una instantánea de volumen en un clúster SolidFire

Cree una instantánea de volumen

Puede crear una instantánea de un volumen activo para conservar la imagen del volumen en cualquier momento. Puedes crear hasta 32 instantáneas para un solo volumen.

1. Haz clic en **Administración** > **Volúmenes**.
2. Haga clic en el icono **Acciones** del volumen que desea utilizar para la instantánea.
3. En el menú que aparece, seleccione **Instantánea**.
4. En el cuadro de diálogo **Crear instantánea del volumen**, introduzca el nombre de la nueva instantánea.
5. **Opcional:** Seleccione la casilla de verificación **Incluir instantánea en la replicación cuando se empareje** para garantizar que la instantánea se capture en la replicación cuando se empareje el volumen principal.
6. Para configurar el período de retención de la instantánea, seleccione una de las siguientes opciones:
   - Haz clic en **Conservar para siempre** para guardar la instantánea en el sistema indefinidamente.
   - Haz clic en **Establecer período de retención** y usa los controles de fecha para elegir el tiempo durante el cual el sistema conservará la instantánea.
7. Para tomar una instantánea única e inmediata, siga los siguientes pasos:
   a. Haz clic en **Tomar instantánea ahora**.
   b. Haz clic en **Crear instantánea**.
8. Para programar la ejecución de la instantánea en un momento futuro, siga los siguientes pasos:
   a. Haga clic en **Crear programación de instantáneas**.
   b. Ingrese un **Nuevo Nombre de Horario**.
   c. Elige un **Tipo de horario** de la lista.
   d. **Opcional:** Seleccione la casilla de verificación **Programación recurrente** para repetir la instantánea programada periódicamente.
   e. Haz clic en **Crear horario**.

Encuentra más información

Programa una instantánea

Editar retención de instantáneas

Puedes cambiar el período de retención de una instantánea para controlar cuándo o si el sistema elimina las instantáneas. El período de retención que especifique comienza cuando ingrese el nuevo intervalo. Al establecer un período de retención, puede

seleccionar un período que comience en el momento actual (la retención no se calcula a partir del momento de creación de la instantánea). Puedes especificar intervalos en minutos, horas y días.

Pasos

1. Haz clic en **Protección de datos** > **Instantáneas**.
2. Haz clic en el icono **Acciones** de la instantánea que quieras editar.
3. En el menú que aparece, haga clic en **Editar**.
4. **Opcional:** Seleccione la casilla de verificación **Incluir instantánea en la replicación cuando se empareje** para garantizar que la instantánea se capture en la replicación cuando se empareje el volumen principal.
5. **Opcional:** Seleccione una opción de retención para la instantánea:
   - Haz clic en **Conservar para siempre** para guardar la instantánea en el sistema indefinidamente.
   - Haga clic en **Establecer período de retención** y utilice los controles numéricos de fecha para seleccionar el período de tiempo durante el cual el sistema conservará la instantánea.
6. Haz clic en **Guardar cambios**.

Eliminar una instantánea

Puede eliminar una instantánea de volumen de un clúster de almacenamiento que ejecuta el software Element. Cuando borras una instantánea, el sistema la elimina inmediatamente.

Puedes eliminar las instantáneas que se están replicando desde el clúster de origen. Si una instantánea se está sincronizando con el clúster de destino cuando la eliminas, la replicación de sincronización se completa y la instantánea se elimina del clúster de origen. La instantánea no se elimina del clúster de destino.

También puede eliminar instantáneas que se hayan replicado en el destino desde el clúster de destino. La instantánea eliminada se mantiene en una lista de instantáneas eliminadas en el destino hasta que el sistema detecta que usted ha eliminado la instantánea en el clúster de origen. Cuando el destino detecta que has eliminado la instantánea de origen, detiene la replicación de la misma.

Cuando se elimina una instantánea del clúster de origen, la instantánea del clúster de destino no se ve afectada (y viceversa).

1. Haz clic en **Protección de datos** > **Instantáneas**.
2. Haz clic en el icono **Acciones** de la instantánea que deseas eliminar.
3. En el menú que aparece, seleccione **Eliminar**.
4. Confirma la acción.

Clonar un volumen a partir de una instantánea

Puedes crear un nuevo volumen a partir de una instantánea de un volumen. Al hacer esto, el sistema utiliza la información de la instantánea para clonar un nuevo volumen utilizando los datos que contenía el volumen en el momento en que se creó la instantánea. Este proceso almacena información sobre otras instantáneas del volumen en el volumen recién creado.

1. Haz clic en **Protección de datos** > **Instantáneas**.
2. Haga clic en el icono **Acciones** de la instantánea que desea utilizar para la clonación del volumen.
3. En el menú que aparece, haga clic en **Clonar volumen desde instantánea**.
4. Introduzca un **Nombre de volumen** en el cuadro de diálogo **Clonar volumen desde instantánea**.
5. Seleccione un **Tamaño total** y las unidades de tamaño para el nuevo volumen.
6. Seleccione un tipo de **Acceso** para el volumen.
7. Seleccione una **Cuenta** de la lista para asociarla con el nuevo volumen.
8. Haz clic en **Iniciar clonación**.

Revierte un volumen a una instantánea

Puedes restaurar un volumen a una instantánea anterior en cualquier momento. Esto revierte cualquier cambio realizado en el volumen desde que se creó la instantánea.

Pasos

1. Haz clic en **Protección de datos** > **Instantáneas**.
2. Haga clic en el icono **Acciones** de la instantánea que desea utilizar para la reversión de volumen.
3. En el menú resultante, seleccione **Revertir volumen a instantánea**.
4. **Opcional:** Para guardar el estado actual del volumen antes de volver a la instantánea:
   a. En el cuadro de diálogo **Revertir a instantánea**, seleccione **Guardar el estado actual del volumen como una instantánea**.
   b. Introduzca un nombre para la nueva instantánea.
5. Haga clic en **Revertir instantánea**.

Realizar una copia de seguridad de una instantánea de volumen

Realizar una copia de seguridad de una instantánea de volumen

Puede utilizar la función de copia de seguridad integrada para realizar una copia de seguridad de una instantánea de volumen. Puede realizar copias de seguridad de instantáneas desde un clúster SolidFire a un almacenamiento de objetos externo o a otro clúster SolidFire . Cuando se realiza una copia de seguridad de una instantánea en un almacenamiento de objetos externo, es necesario disponer de una conexión con dicho almacenamiento que permita operaciones de lectura/escritura.

- "Realizar una copia de seguridad de una instantánea de volumen en un almacenamiento de objetos de Amazon S3"
- "Realizar una copia de seguridad de una instantánea de volumen en un almacén de objetos Swift de OpenStack"
- "Realizar una copia de seguridad de una instantánea de volumen en un clúster SolidFire"

Realizar una copia de seguridad de una instantánea de volumen en un almacenamiento de objetos de Amazon S3

Puede realizar copias de seguridad de las instantáneas de SolidFire en almacenes de

objetos externos compatibles con Amazon S3.

1. Haga clic en **Protección de datos** > **Instantáneas**.
2. Haz clic en el icono **Acciones** de la instantánea que deseas respaldar.
3. En el menú resultante, haga clic en **Realizar copia de seguridad en**.
4. En el cuadro de diálogo **Copia de seguridad integrada**, en **Realizar copia de seguridad en**, seleccione **S3**.
5. Seleccione una opción en **Formato de datos**:
   - **Nativo**: Un formato comprimido legible únicamente por los sistemas de almacenamiento SolidFire .
   - **Sin comprimir**: Un formato sin comprimir compatible con otros sistemas.
6. Introduzca un nombre de host para acceder al almacén de objetos en el campo **Nombre de host**.
7. Introduzca un ID de clave de acceso para la cuenta en el campo **ID de clave de acceso**.
8. Introduzca la clave de acceso secreta de la cuenta en el campo **Clave de acceso secreta**.
9. Introduzca el bucket de S3 en el que se almacenará la copia de seguridad en el campo **Bucket de S3**.
10. **Opcional**: Introduzca una etiqueta de nombre para añadir al prefijo en el campo **Etiqueta de nombre**.
11. Haz clic en **Iniciar lectura**.

Realizar una copia de seguridad de una instantánea de volumen en un almacén de objetos Swift de OpenStack

Puede realizar copias de seguridad de las instantáneas de SolidFire en almacenes de objetos secundarios que sean compatibles con OpenStack Swift.

1. Haz clic en **Protección de datos** > **Instantáneas**.
2. Haz clic en el icono **Acciones** de la instantánea que deseas respaldar.
3. En el menú resultante, haga clic en **Realizar copia de seguridad en**.
4. En el cuadro de diálogo **Copia de seguridad integrada**, en **Realizar copia de seguridad en**, seleccione **Swift**.
5. Seleccione una opción en **Formato de datos**:
   - **Nativo**: Un formato comprimido legible únicamente por los sistemas de almacenamiento SolidFire .
   - **Sin comprimir**: Un formato sin comprimir compatible con otros sistemas.
6. Ingrese una **URL** para acceder al almacén de objetos.
7. Introduce un **Nombre de usuario** para la cuenta.
8. Introduzca la **Clave de autenticación** de la cuenta.
9. Introduzca el **Contenedor** en el que se almacenará la copia de seguridad.
10. **Opcional**: Introduzca una **etiqueta de nombre**.
11. Haz clic en **Iniciar lectura**.

Realizar una copia de seguridad de una instantánea de volumen en un clúster SolidFire

Puede realizar copias de seguridad de instantáneas de volumen que residen en un clúster SolidFire en un clúster SolidFire remoto.

Asegúrese de que los clústeres de origen y destino estén emparejados.

Al realizar copias de seguridad o restauraciones de un clúster a otro, el sistema genera una clave que se utilizará para la autenticación entre los clústeres. Esta clave de escritura de volumen masivo permite que el clúster de origen se autentique con el clúster de destino, proporcionando un nivel de seguridad al escribir en el volumen de destino. Como parte del proceso de copia de seguridad o restauración, debe generar una clave de escritura de volumen masivo desde el volumen de destino antes de iniciar la operación.

1. En el clúster de destino, haga clic en **Administración** > **Volúmenes**.
2. Haga clic en el icono **Acciones** del volumen de destino.
3. En el menú que aparece, haga clic en **Restaurar desde**.
4. En el cuadro de diálogo **Restauración integrada**, en **Restaurar desde**, seleccione * SolidFire*.
5. Seleccione un formato de datos en **Formato de datos**:
   - **Nativo**: Un formato comprimido legible únicamente por los sistemas de almacenamiento SolidFire .
   - **Sin comprimir**: Un formato sin comprimir compatible con otros sistemas.
6. Haz clic en **Generar clave**.
7. Copie la clave del cuadro **Clave de escritura de volumen masivo** al portapapeles.
8. En el clúster de origen, haga clic en **Protección de datos** > **Instantáneas**.
9. Haz clic en el icono Acciones de la instantánea que quieras usar para la copia de seguridad.
10. En el menú resultante, haga clic en **Realizar copia de seguridad en**.
11. En el cuadro de diálogo **Copia de seguridad integrada**, en **Realizar copia de seguridad en**, seleccione * SolidFire*.
12. Seleccione el mismo formato de datos que seleccionó anteriormente en el campo **Formato de datos**.
13. Introduzca la dirección IP virtual de gestión del clúster del volumen de destino en el campo **MVIP de clúster remoto**.
14. Introduzca el nombre de usuario del clúster remoto en el campo **Nombre de usuario del clúster remoto**.
15. Introduzca la contraseña del clúster remoto en el campo **Contraseña del clúster remoto**.
16. En el campo **Clave de escritura de volumen masivo**, pegue la clave que generó anteriormente en el clúster de destino.
17. Haz clic en **Iniciar lectura**.

Utilice instantáneas de grupo para la protección de datos.

Utilizar instantáneas de grupo para la tarea de protección de datos

Puede crear una instantánea de grupo de un conjunto de volúmenes relacionados para conservar una copia puntual de los metadatos de cada volumen. En el futuro, puede utilizar la instantánea del grupo como copia de seguridad o para revertir cambios y restaurar el estado del grupo de volúmenes a un estado anterior.

Encuentra más información

- Crea una instantánea de grupo
- Editar instantáneas de grupo

- Editar miembros de la instantánea del grupo
- Eliminar una instantánea de grupo
- Revertir volúmenes a una instantánea de grupo
- Clonar múltiples volúmenes
- Clonar varios volúmenes a partir de una instantánea de grupo

Detalles de la instantánea del grupo

La página Instantáneas de grupo en la pestaña Protección de datos proporciona información sobre las instantáneas de grupo.

- **IDENTIFICACIÓN**

  El ID generado por el sistema para la instantánea del grupo.

- **UUID**

  El identificador único de la instantánea del grupo.

- **Nombre**

  Nombre definido por el usuario para la instantánea del grupo.

- **Crear tiempo**

  La hora en la que se creó la instantánea del grupo.

- **Estado**

  Estado actual de la instantánea. Valores posibles:

  - Preparación: La instantánea se está preparando para su uso y aún no se puede escribir en ella.
  - Listo: Esta instantánea ha finalizado su preparación y ya se puede utilizar.
  - Activa: La instantánea corresponde a la rama activa.

- **# Volúmenes**

  El número de volúmenes en el grupo.

- **Conservar hasta**

  El día y la hora en que se eliminará la instantánea.

- **Replicación remota**

  Indicación de si la instantánea está habilitada o no para la replicación a un clúster SolidFire remoto. Valores posibles:

  - Habilitado: La instantánea está habilitada para la replicación remota.
  - Deshabilitado: La instantánea no está habilitada para la replicación remota.

Creación de una instantánea de grupo

Puede crear una instantánea de un grupo de volúmenes, y también puede crear una programación de instantáneas de grupo para automatizar las instantáneas de grupo. Una única instantánea de grupo puede capturar de forma consistente hasta 32 volúmenes a la vez.

Pasos

1. Haz clic en **Administración** > **Volúmenes**.
2. Utilice las casillas de verificación para seleccionar varios volúmenes para un grupo de volúmenes.
3. Haz clic en **Acciones en lote**.
4. Haga clic en **Instantánea de grupo**.
5. Introduzca un nuevo nombre para la instantánea de grupo en el cuadro de diálogo Crear instantánea de grupo de volúmenes.
6. **Opcional:** Seleccione la casilla de verificación **Incluir cada miembro de la instantánea del grupo en la replicación cuando se emparejen** para garantizar que cada instantánea se capture en la replicación cuando se empareje el volumen principal.
7. Seleccione una opción de retención para la instantánea del grupo:
   - Haz clic en **Conservar para siempre** para guardar la instantánea en el sistema indefinidamente.
   - Haz clic en **Establecer período de retención** y usa los controles de fecha para elegir el tiempo durante el cual el sistema conservará la instantánea.
8. Para tomar una instantánea única e inmediata, siga los siguientes pasos:
   a. Haz clic en **Tomar instantánea de grupo ahora**.
   b. Haz clic en **Crear instantánea de grupo**.
9. Para programar la ejecución de la instantánea en un momento futuro, siga los siguientes pasos:
   a. Haga clic en **Crear programación de instantáneas de grupo**.
   b. Ingrese un **Nuevo Nombre de Horario**.
   c. Seleccione un **Tipo de horario** de la lista.
   d. **Opcional:** Seleccione la casilla de verificación **Programación recurrente** para repetir la instantánea programada periódicamente.
   e. Haz clic en **Crear horario**.

Edición de instantáneas de grupo

Puede editar la configuración de replicación y retención para las instantáneas de grupo existentes.

1. Haz clic en **Protección de datos** > **Instantáneas de grupo**.
2. Haz clic en el icono Acciones de la instantánea de grupo que quieras editar.
3. En el menú que aparece, seleccione **Editar**.
4. **Opcional:** Para cambiar la configuración de replicación de la instantánea de grupo:
   a. Haga clic en **Editar** junto a **Replicación actual**.
   b. Seleccione la casilla de verificación **Incluir cada miembro de la instantánea del grupo en la**

replicación cuando se emparejen para garantizar que cada instantánea se capture en la replicación cuando se empareje el volumen principal.

5. **Opcional:** Para cambiar la configuración de retención de la instantánea de grupo, seleccione una de las siguientes opciones:
   a. Haga clic en **Editar** junto a **Retención actual**.
   b. Seleccione una opción de retención para la instantánea del grupo:
      - Haz clic en **Conservar para siempre** para guardar la instantánea en el sistema indefinidamente.
      - Haz clic en **Establecer período de retención** y usa los controles de fecha para elegir el tiempo durante el cual el sistema conservará la instantánea.
6. Haz clic en **Guardar cambios**.

Eliminar una instantánea de grupo

Puedes eliminar una instantánea de grupo del sistema. Al eliminar la instantánea del grupo, puede elegir si desea que se eliminen todas las instantáneas asociadas al grupo o que se conserven como instantáneas individuales.

Si elimina un volumen o una instantánea que sea miembro de una instantánea de grupo, ya no podrá revertir a la instantánea de grupo. Sin embargo, puede revertir cada volumen individualmente.

1. Haz clic en **Protección de datos** > **Instantáneas de grupo**.
2. Haz clic en el icono de Acciones de la instantánea que deseas eliminar.
3. En el menú que aparece, haga clic en **Eliminar**.
4. Seleccione una de las siguientes opciones en el cuadro de diálogo de confirmación:
   - Haga clic en **Eliminar instantánea de grupo Y todos los miembros de la instantánea de grupo** para eliminar la instantánea de grupo y todas las instantáneas de los miembros.
   - Haz clic en **Conservar miembros de instantáneas de grupo como instantáneas individuales** para eliminar la instantánea de grupo pero conservar todas las instantáneas de los miembros.
5. Confirma la acción.

Revertir volúmenes a una instantánea de grupo

Puede revertir un grupo de volúmenes en cualquier momento a una instantánea de grupo.

Cuando se revierte un grupo de volúmenes, todos los volúmenes del grupo se restauran al estado en el que se encontraban en el momento en que se creó la instantánea del grupo. La reversión también restaura los tamaños de volumen al tamaño registrado en la instantánea original. Si el sistema ha eliminado un volumen, todas las instantáneas de ese volumen también se eliminaron en el momento de la eliminación; el sistema no restaura ninguna instantánea de volumen eliminada.

1. Haz clic en **Protección de datos** > **Instantáneas de grupo**.
2. Haga clic en el icono Acciones de la instantánea de grupo que desea utilizar para la reversión de volumen.
3. En el menú resultante, seleccione **Revertir volúmenes a instantánea de grupo**.
4. **Opcional**: Para guardar el estado actual de los volúmenes antes de volver a la instantánea:
   a. En el cuadro de diálogo **Revertir a instantánea**, seleccione **Guardar el estado actual de los**

volúmenes como una instantánea de grupo.

b. Introduzca un nombre para la nueva instantánea.

5. Haga clic en **Revertir instantánea de grupo**.

Edición de la instantánea del grupo

Puedes editar la configuración de retención para los miembros de una instantánea de grupo existente.

1. Haz clic en **Protección de datos** > **Instantáneas**.
2. Haz clic en la pestaña **Miembros**.
3. Haz clic en el icono de Acciones del miembro de la instantánea del grupo que quieras editar.
4. En el menú que aparece, seleccione **Editar**.
5. Para cambiar la configuración de replicación de la instantánea, seleccione una de las siguientes opciones:
   - Haz clic en **Conservar para siempre** para guardar la instantánea en el sistema indefinidamente.
   - Haz clic en **Establecer período de retención** y usa los controles de fecha para elegir el tiempo durante el cual el sistema conservará la instantánea.
6. Haz clic en **Guardar cambios**.

Clonar múltiples volúmenes

Puede crear varios clones de volumen en una sola operación para crear una copia puntual de los datos en un grupo de volúmenes.

Cuando se clona un volumen, el sistema crea una instantánea del volumen y luego crea un nuevo volumen a partir de los datos de la instantánea. Puede montar y escribir en el nuevo clon de volumen. La clonación de múltiples volúmenes es un proceso asíncrono y requiere un tiempo variable dependiendo del tamaño y la cantidad de volúmenes que se clonan.

El tamaño del volumen y la carga actual del clúster afectan al tiempo necesario para completar una operación de clonación.

Pasos

1. Haz clic en **Administración** > **Volúmenes**.
2. Haz clic en la pestaña **Activa**.
3. Utilice las casillas de verificación para seleccionar varios volúmenes y crear un grupo de volúmenes.
4. Haz clic en **Acciones en lote**.
5. Haz clic en **Clonar** en el menú que aparece.
6. Introduzca un **Prefijo de nombre de volumen nuevo** en el cuadro de diálogo **Clonar varios volúmenes**.

   El prefijo se aplica a todos los volúmenes del grupo.

7. **Opcional:** Seleccione una cuenta diferente a la que pertenecerá el clon.

   Si no selecciona una cuenta, el sistema asigna los nuevos volúmenes a la cuenta de volumen actual.

8. **Opcional:** Seleccione un método de acceso diferente para los volúmenes en el clon.

Si no selecciona un método de acceso, el sistema utiliza el acceso al volumen actual.

9. Haz clic en **Iniciar clonación**.

Clonación de varios volúmenes a partir de una instantánea de grupo

Puede clonar un grupo de volúmenes a partir de una instantánea de grupo en un momento dado. Esta operación requiere que ya exista una instantánea de grupo de los volúmenes, ya que dicha instantánea se utiliza como base para crear los volúmenes. Una vez creados los volúmenes, podrá utilizarlos como cualquier otro volumen del sistema.

El tamaño del volumen y la carga actual del clúster afectan al tiempo necesario para completar una operación de clonación.

1. Haz clic en **Protección de datos** > **Instantáneas de grupo**.
2. Haga clic en el icono Acciones de la instantánea de grupo que desea utilizar para los clones de volumen.
3. En el menú resultante, seleccione **Clonar volúmenes desde instantánea de grupo**.
4. Introduzca un **Nuevo prefijo de nombre de volumen** en el cuadro de diálogo **Clonar volúmenes desde instantánea de grupo**.

   El prefijo se aplica a todos los volúmenes creados a partir de la instantánea del grupo.

5. **Opcional:** Seleccione una cuenta diferente a la que pertenecerá el clon.

   Si no selecciona una cuenta, el sistema asigna los nuevos volúmenes a la cuenta de volumen actual.

6. **Opcional:** Seleccione un método de acceso diferente para los volúmenes en el clon.

   Si no selecciona un método de acceso, el sistema utiliza el acceso al volumen actual.

7. Haz clic en **Iniciar clonación**.

Programa una instantánea

Programa una instantánea

Puede proteger los datos de un volumen o un grupo de volúmenes programando instantáneas de volumen para que se realicen a intervalos específicos. Puede programar la ejecución automática de instantáneas de un solo volumen o de instantáneas de grupo.

Al configurar una programación de instantáneas, puede elegir intervalos de tiempo basados en días de la semana o días del mes. También puedes especificar los días, horas y minutos antes de que se tome la siguiente instantánea. Puede almacenar las instantáneas resultantes en un sistema de almacenamiento remoto si el volumen se está replicando.

Encuentra más información

- Crea un cronograma de instantáneas
- Editar un cronograma de instantáneas
- Eliminar una programación de instantáneas

- Copiar un cronograma de instantánea

Detalles del cronograma de instantáneas

En la página Protección de datos > Programaciones, puede ver la siguiente información en la lista de programaciones de instantáneas.

- **IDENTIFICACIÓN**

  El ID generado por el sistema para la instantánea.

- **Tipo**

  El tipo de horario. Actualmente, solo se admite el tipo de instantánea.

- **Nombre**

  El nombre que se le dio al horario cuando se creó. Los nombres de programación de instantáneas pueden tener hasta 223 caracteres de longitud y contener caracteres az, 0-9 y guion (-).

- **Frecuencia**

  La frecuencia con la que se ejecuta la programación. La frecuencia se puede configurar en horas y minutos, semanas o meses.

- **Periódico**

  Indicación de si la programación debe ejecutarse solo una vez o a intervalos regulares.

- **Pausa manual**

  Indicación de si la programación se ha pausado manualmente o no.

- **Identificadores de volumen**

  El identificador del volumen que utilizará la programación cuando se ejecute.

- **Última carrera**

  La última vez que se ejecutó el horario.

- **Estado de la última ejecución**

  El resultado de la última ejecución programada. Valores posibles:

  - Éxito
  - Falla

Crea un cronograma de instantáneas

Puede programar la toma de instantáneas de uno o varios volúmenes para que se realicen automáticamente a intervalos específicos.

Al configurar una programación de instantáneas, puede elegir intervalos de tiempo basados en días de la semana o días del mes. También puedes crear una programación recurrente y especificar los días, horas y

minutos antes de que se produzca la siguiente instantánea.

Si programas una instantánea para que se ejecute en un período de tiempo que no sea divisible por 5 minutos, la instantánea se ejecutará en el siguiente período de tiempo que sea divisible por 5 minutos. Por ejemplo, si programa una instantánea para que se ejecute a las 12:42:00 UTC, se ejecutará a las 12:45:00 UTC. No se puede programar una instantánea para que se ejecute a intervalos inferiores a 5 minutos.

A partir de Element 12.5, puede habilitar la creación serial y seleccionar conservar las instantáneas en base a las primeras en entrar, primeras en salir (FIFO) desde la interfaz de usuario.

- La opción **Habilitar creación serial** especifica que solo se replica una instantánea a la vez. La creación de una nueva instantánea falla cuando la replicación de una instantánea anterior aún está en curso. Si la casilla de verificación no está seleccionada, se permite la creación de una instantánea cuando otra replicación de instantánea aún está en curso.
- La opción **FIFO** añade la capacidad de conservar un número constante de las últimas instantáneas. Cuando se selecciona la casilla de verificación, las instantáneas se conservan en orden FIFO (primero en entrar, primero en salir). Una vez que la cola de instantáneas FIFO alcanza su profundidad máxima, la instantánea FIFO más antigua se descarta cuando se inserta una nueva.

Pasos

1. Seleccione **Protección de datos** > **Programaciones**.
2. Seleccione **Crear horario**.
3. En el campo **CSV de ID de volumen**, introduzca un único ID de volumen o una lista de ID de volumen separados por comas para incluir en la operación de instantánea.
4. Introduzca un nuevo nombre para el horario.
5. Seleccione un tipo de horario y configúrelo a partir de las opciones proporcionadas.
6. **Opcional:** Seleccione **Programación recurrente** para repetir la programación de instantáneas indefinidamente.
7. **Opcional:** Introduzca un nombre para la nueva instantánea en el campo **Nombre de la nueva instantánea**.

   Si deja el campo en blanco, el sistema utilizará la fecha y hora de creación de la instantánea como nombre.

8. **Opcional:** Seleccione la casilla de verificación **Incluir instantáneas en la replicación cuando se emparejan** para garantizar que las instantáneas se capturen en la replicación cuando se empareje el volumen principal.
9. **Opcional:** Seleccione la casilla de verificación **Habilitar creación serial** para garantizar que solo se replique una instantánea a la vez.
10. Para configurar el período de retención de la instantánea, seleccione una de las siguientes opciones:
    - **Opcional:** Seleccione la casilla de verificación **FIFO (Primero en entrar, primero en salir)** para conservar un número constante de las instantáneas más recientes.
    - Seleccione **Conservar para siempre** para guardar la instantánea en el sistema indefinidamente.
    - Seleccione **Establecer período de retención** y utilice los controles numéricos de fecha para elegir el período de tiempo durante el cual el sistema conservará la instantánea.
11. Seleccione **Crear horario**.

Editar un cronograma de instantáneas

Puede modificar las programaciones de instantáneas existentes. Tras la modificación, la próxima vez que se ejecute la programación, utilizará los atributos actualizados. Las instantáneas creadas por la programación original permanecen en el sistema de almacenamiento.

Pasos

1. Haz clic en **Protección de datos** > **Programaciones**.
2. Haz clic en el icono **Acciones** del horario que quieras cambiar.
3. En el menú que aparece, haga clic en **Editar**.
4. En el campo **CSV de ID de volumen**, modifique el ID de volumen único o la lista de ID de volumen separados por comas que se incluyen actualmente en la operación de instantánea.
5. Para pausar o reanudar la programación, seleccione una de las siguientes opciones:
   - Para pausar una programación activa, seleccione **Sí** de la lista **Pausar programación manualmente**.
   - Para reanudar una programación pausada, seleccione **No** de la lista **Pausar programación manualmente**.
6. Si lo desea, introduzca un nombre diferente para el horario en el campo **Nombre del nuevo horario**.
7. Para cambiar la programación para que se ejecute en diferentes días de la semana o del mes, seleccione **Tipo de programación** y cambie la programación de las opciones proporcionadas.
8. **Opcional:** Seleccione **Programación recurrente** para repetir la programación de instantáneas indefinidamente.
9. **Opcional:** Introduzca o modifique el nombre de la nueva instantánea en el campo **Nombre de la nueva instantánea**.

   Si deja el campo en blanco, el sistema utilizará la fecha y hora de creación de la instantánea como nombre.

10. **Opcional:** Seleccione la casilla de verificación **Incluir instantáneas en la replicación cuando se emparejan** para garantizar que las instantáneas se capturen en la replicación cuando se empareje el volumen principal.
11. Para cambiar la configuración de retención, seleccione una de las siguientes opciones:
    - Haz clic en **Conservar para siempre** para guardar la instantánea en el sistema indefinidamente.
    - Haga clic en **Establecer período de retención** y utilice los controles numéricos de fecha para seleccionar el período de tiempo durante el cual el sistema conservará la instantánea.
12. Haz clic en **Guardar cambios**.

Copiar un cronograma de instantánea

Puede copiar una programación y mantener sus atributos actuales.

1. Haz clic en **Protección de datos** > **Programaciones**.
2. Haz clic en el icono de Acciones del horario que quieras copiar.
3. En el menú que aparece, haga clic en **Hacer una copia**.

   Aparece el cuadro de diálogo **Crear horario**, que se completa con los atributos actuales del horario.

4. **Opcional:** Introduzca un nombre y atributos actualizados para el nuevo horario.
5. Haz clic en **Crear horario**.

Eliminar una programación de instantáneas

Puedes eliminar una programación de instantáneas. Después de eliminar la programación, no se ejecutarán más instantáneas programadas. Las instantáneas creadas por la programación permanecen en el sistema de almacenamiento.

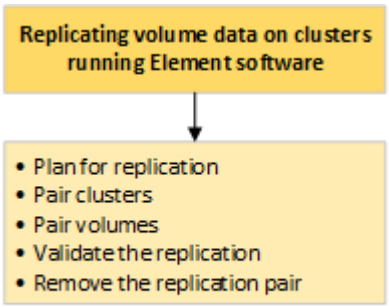
1. Haz clic en **Protección de datos** > **Programaciones**.
2. Haz clic en el icono **Acciones** del horario que deseas eliminar.
3. En el menú que aparece, haga clic en **Eliminar**.
4. Confirma la acción.

Realizar replicación remota entre clústeres que ejecutan el software NetApp Element .

Realizar replicación remota entre clústeres que ejecutan el software NetApp Element .

Para los clústeres que ejecutan el software Element, la replicación en tiempo real permite la creación rápida de copias remotas de datos de volumen. Puedes emparejar un clúster de almacenamiento con hasta cuatro clústeres de almacenamiento adicionales. Puede replicar datos de volumen de forma síncrona o asíncrona desde cualquiera de los clústeres de un par de clústeres para escenarios de conmutación por error y recuperación ante fallos.

El proceso de replicación incluye los siguientes pasos:



- "Planificar el emparejamiento de clústeres y volúmenes para la replicación en tiempo real."
- "Agrupaciones de pares para replicación"
- "Volúmenes de pares"
- "Validar la replicación de volumen"
- "Eliminar una relación de volumen después de la replicación"
- "Gestionar las relaciones de volumen"

Planificar el emparejamiento de clústeres y volúmenes para la replicación en tiempo real.

La replicación remota en tiempo real requiere que se emparejen dos clústeres de almacenamiento que ejecuten el software Element, se emparejen los volúmenes en cada clúster y se valide la replicación. Una vez finalizada la replicación, debe eliminar la relación de volumen.

Lo que necesitarás

- Debe tener privilegios de administrador de clúster en uno o ambos clústeres que se están emparejando.
- Todas las direcciones IP de los nodos en las redes de administración y almacenamiento para clústeres emparejados están enrutadas entre sí.
- La MTU de todos los nodos emparejados debe ser la misma y debe ser compatible de extremo a extremo entre los clústeres.
- Ambos clústeres de almacenamiento deben tener nombres de clúster únicos, MVIP, SVIP y direcciones IP de todos los nodos.
- La diferencia entre las versiones del software Element en los clústeres no es mayor que una versión principal. Si la diferencia es mayor, uno de los clústeres debe actualizarse para realizar la replicación de datos.

> NetApp no ha certificado los dispositivos WAN Accelerator para su uso en la replicación de datos. Estos dispositivos pueden interferir con la compresión y la deduplicación si se implementan entre dos clústeres que replican datos. Asegúrese de evaluar completamente los efectos de cualquier dispositivo WAN Accelerator antes de implementarlo en un entorno de producción.

Encuentra más información

- Agrupaciones de pares para replicación
- Volúmenes de pares
- Asignar una fuente y un destino de replicación a los volúmenes emparejados.

Agrupaciones de pares para replicación

Agrupaciones de pares para replicación

Como primer paso para utilizar la funcionalidad de replicación en tiempo real, debe emparejar dos clústeres. Después de emparejar y conectar dos clústeres, puede configurar los volúmenes activos de un clúster para que se repliquen continuamente en un segundo clúster, lo que proporciona protección continua de datos (CDP).

Lo que necesitarás

- Debe tener privilegios de administrador de clúster en uno o ambos clústeres que se están emparejando.
- Todas las MIP y SIP de los nodos están enrutadas entre sí.
- Debe haber menos de 2000 ms de latencia de ida y vuelta entre clústeres.
- Ambos clústeres de almacenamiento deben tener nombres de clúster únicos, MVIP, SVIP y direcciones IP de todos los nodos.
- La diferencia entre las versiones del software Element en los clústeres no es mayor que una versión

principal. Si la diferencia es mayor, uno de los clústeres debe actualizarse para realizar la replicación de datos.

> El emparejamiento de clústeres requiere conectividad completa entre los nodos de la red de gestión. La replicación requiere conectividad entre los nodos individuales de la red del clúster de almacenamiento.

Puedes emparejar un clúster con hasta cuatro clústeres más para replicar volúmenes. También puedes emparejar clústeres dentro del grupo de clústeres entre sí.

Emparejar clústeres usando MVIP o una clave de emparejamiento

Puede emparejar un clúster de origen y un clúster de destino utilizando el MVIP del clúster de destino si existe acceso de administrador de clúster a ambos clústeres. Si el acceso de administrador de clúster solo está disponible en uno de los clústeres de un par, se puede utilizar una clave de emparejamiento en el clúster de destino para completar el emparejamiento del clúster.

1. Seleccione uno de los siguientes métodos para emparejar clústeres:
   - "Agrupamiento de pares mediante MVIP"Utilice este método si existe acceso de administrador de clúster a ambos clústeres. Este método utiliza el MVIP del clúster remoto para emparejar dos clústeres.
   - "Agrupar grupos mediante una clave de emparejamiento"Utilice este método si solo uno de los clústeres tiene acceso de administrador. Este método genera una clave de emparejamiento que se puede utilizar en el clúster de destino para completar el emparejamiento del clúster.

Encuentra más información

Requisitos del puerto de red

Agrupamiento de pares mediante MVIP

Puede emparejar dos clústeres para la replicación en tiempo real utilizando el MVIP de un clúster para establecer una conexión con el otro clúster. Para utilizar este método se requiere acceso de administrador de clúster en ambos clústeres. El nombre de usuario y la contraseña del administrador del clúster se utilizan para autenticar el acceso al clúster antes de que los clústeres puedan emparejarse.

1. En el clúster local, seleccione **Protección de datos** > **Pares de clústeres**.
2. Haga clic en **Par de clústeres**.
3. Haga clic en **Iniciar emparejamiento** y haga clic en **Sí** para indicar que tiene acceso al clúster remoto.
4. Introduzca la dirección MVIP del clúster remoto.
5. Haga clic en **Completar el emparejamiento en el clúster remoto**.

   En la ventana **Autenticación requerida**, ingrese el nombre de usuario y la contraseña del administrador del clúster remoto.

6. En el clúster remoto, seleccione **Protección de datos** > **Pares de clústeres**.
7. Haga clic en **Par de clústeres**.
8. Haga clic en **Completar emparejamiento**.

9. Haz clic en el botón **Completar emparejamiento**.

Encuentra más información

- Agrupar grupos mediante una clave de emparejamiento
- "Emparejamiento de clústeres mediante MVIP (vídeo)"

Agrupar grupos mediante una clave de emparejamiento

Si tiene acceso de administrador de clúster a un clúster local pero no al clúster remoto, puede emparejar los clústeres utilizando una clave de emparejamiento. Se genera una clave de emparejamiento en un clúster local y luego se envía de forma segura a un administrador de clúster en un sitio remoto para establecer una conexión y completar el emparejamiento del clúster para la replicación en tiempo real.

1. En el clúster local, seleccione **Protección de datos** > **Pares de clústeres**.
2. Haga clic en **Par de clústeres**.
3. Haga clic en **Iniciar emparejamiento** y haga clic en **No** para indicar que no tiene acceso al clúster remoto.
4. Haz clic en **Generar clave**.

   Esta acción genera una clave de texto para el emparejamiento y crea un par de clúster no configurado en el clúster local. Si no completa el procedimiento, deberá eliminar manualmente el par de clústeres.

5. Copie la clave de emparejamiento del clúster al portapapeles.
6. Proporcione la clave de emparejamiento al administrador del clúster en el sitio remoto del clúster.

   La clave de emparejamiento del clúster contiene una versión de MVIP, nombre de usuario, contraseña e información de la base de datos para permitir conexiones de volumen para la replicación remota. Esta clave debe tratarse de forma segura y no almacenarse de manera que permita el acceso accidental o no seguro al nombre de usuario o la contraseña.

   No modifique ninguno de los caracteres de la clave de emparejamiento. La clave pierde validez si se modifica.

7. En el clúster remoto, seleccione **Protección de datos** > **Pares de clústeres**.
8. Haga clic en **Par de clústeres**.
9. Haga clic en **Completar emparejamiento** e ingrese la clave de emparejamiento en el campo **Clave de emparejamiento** (se recomienda pegar).
10. Haga clic en **Completar emparejamiento**.

Encuentra más información

- Agrupamiento de pares mediante MVIP
- "Emparejamiento de clústeres mediante una clave de emparejamiento de clústeres (vídeo)"

Validar la conexión del par de clústeres

Una vez completado el emparejamiento de clústeres, es posible que desee verificar la conexión del par de clústeres para garantizar el éxito de la replicación.

1. En el clúster local, seleccione **Protección de datos** > **Pares de clústeres**.
2. En la ventana **Pares de clústeres**, verifique que el par de clústeres esté conectado.
3. **Opcional:** Vuelva al clúster local y a la ventana **Pares de clústeres** y verifique que el par de clústeres esté conectado.

Volúmenes de pares

Volúmenes de pares

Una vez que haya establecido una conexión entre clústeres en un par de clústeres, puede emparejar un volumen de un clúster con un volumen del otro clúster del par. Cuando se establece una relación de emparejamiento de volúmenes, debe identificar cuál es el volumen de destino de la replicación.

Puede emparejar dos volúmenes para la replicación en tiempo real que estén almacenados en diferentes clústeres de almacenamiento en un par de clústeres conectados. Después de emparejar dos clústeres, puede configurar los volúmenes activos de un clúster para que se repliquen continuamente en un segundo clúster, lo que proporciona protección continua de datos (CDP). También puede asignar cualquiera de los volúmenes como origen o destino de la replicación.

Las relaciones de volumen son siempre uno a uno. Una vez que un volumen forma parte de un emparejamiento con un volumen en otro clúster, no se puede volver a emparejar con ningún otro volumen.

Lo que necesitarás

- Has establecido una conexión entre clústeres en un par de clústeres.
- Usted tiene privilegios de administrador de clúster en uno o ambos clústeres que están emparejados.

Pasos

1. Cree un volumen de destino con acceso de lectura o escritura.
2. Empareje los volúmenes utilizando un ID de volumen o una clave de emparejamiento.
3. Asignar una fuente y un destino de replicación a los volúmenes emparejados.

Cree un volumen de destino con acceso de lectura o escritura.

El proceso de replicación involucra dos puntos finales: el volumen de origen y el volumen de destino. Al crear el volumen de destino, este se configura automáticamente en modo de lectura/escritura para aceptar los datos durante la replicación.

1. Seleccione **Administración** > **Volúmenes**.
2. Haz clic en **Crear volumen**.
3. En el cuadro de diálogo Crear un nuevo volumen, introduzca el nombre del volumen.
4. Ingrese el tamaño total del volumen, seleccione un tamaño de bloque para el volumen y seleccione la cuenta que debe tener acceso al volumen.

5. Haz clic en **Crear volumen**.
6. En la ventana Activa, haga clic en el icono Acciones del volumen.
7. Haga clic en **Editar**.
8. Cambie el nivel de acceso de la cuenta a Destino de replicación.
9. Haz clic en **Guardar cambios**.

Empareje los volúmenes utilizando un ID de volumen o una clave de emparejamiento.

Emparejar volúmenes utilizando un ID de volumen

Puede emparejar un volumen con otro volumen en un clúster remoto si tiene acceso de administrador de clúster a ambos clústeres en los que se van a emparejar los volúmenes. Este método utiliza el ID del volumen en el clúster remoto para iniciar una conexión.

Lo que necesitarás

- Asegúrese de que los clústeres que contienen los volúmenes estén emparejados.
- Cree un nuevo volumen en el clúster remoto.

> Puede asignar un origen y un destino de replicación después del proceso de emparejamiento. Una fuente o destino de replicación puede ser cualquiera de los volúmenes de un par de volúmenes. Debe crear un volumen de destino que no contenga datos y tenga las características exactas del volumen de origen, como el tamaño, la configuración del tamaño de bloque para los volúmenes (ya sea 512e o 4k) y la configuración de QoS. Si asigna un volumen existente como destino de replicación, los datos de ese volumen se sobrescribirán. El volumen objetivo puede ser mayor o igual en tamaño que el volumen de origen, pero no puede ser menor.

- Conozca el ID del volumen de destino.

Pasos

1. Seleccione **Administración** > **Volúmenes**.
2. Haz clic en el icono **Acciones** del volumen que deseas emparejar.
3. Haga clic en **Emparejar**.
4. En el cuadro de diálogo **Emparejar volumen**, seleccione **Iniciar emparejamiento**.
5. Seleccione **Sí** para indicar que tiene acceso al clúster remoto.
6. Seleccione un **Modo de replicación** de la lista:
   - **Tiempo real (asíncrono)**: Las escrituras se confirman al cliente después de que se hayan confirmado en el clúster de origen.
   - **En tiempo real (síncrono)**: Las escrituras se confirman al cliente después de que se hayan confirmado tanto en el clúster de origen como en el de destino.
   - **Solo instantáneas**: Solo se replican las instantáneas creadas en el clúster de origen. Las escrituras activas desde el volumen de origen no se replican.
7. Seleccione un clúster remoto de la lista.
8. Seleccione un ID de volumen remoto.

9. Haga clic en **Iniciar emparejamiento**.

   El sistema abre una pestaña del navegador web que se conecta a la interfaz de usuario Element del clúster remoto. Es posible que se le solicite iniciar sesión en el clúster remoto con las credenciales de administrador del clúster.

10. En la interfaz de usuario de Element del clúster remoto, seleccione **Completar emparejamiento**.
11. Confirme los detalles en **Confirmar emparejamiento de volumen**.
12. Haga clic en **Completar emparejamiento**.

    Una vez confirmado el emparejamiento, los dos grupos inician el proceso de conexión de los volúmenes para el emparejamiento. Durante el proceso de emparejamiento, puede ver mensajes en la columna **Estado del volumen** de la ventana **Pares de volúmenes**. El par de pantallas de volumen `PausedMisconfigured` hasta que se asignen el origen y el destino del par de volúmenes.

    Una vez completado correctamente el emparejamiento, se recomienda actualizar la tabla Volúmenes para eliminar la opción **Emparejar** de la lista **Acciones** del volumen emparejado. Si no actualiza la tabla, la opción **Par** seguirá disponible para su selección. Si vuelve a seleccionar la opción **Emparejar**, se abrirá una nueva pestaña y, dado que el volumen ya está emparejado, el sistema informará de un `StartVolumePairing Failed: xVolumeAlreadyPaired` Mensaje de error en la ventana **Emparejar volumen** de la página de la interfaz de usuario de Element.

Encuentra más información

- Mensajes de emparejamiento de volumen
- Advertencias de emparejamiento de volumen
- Asignar una fuente y un destino de replicación a los volúmenes emparejados.

Emparejar volúmenes mediante una clave de emparejamiento

Si solo tiene acceso de administrador de clúster al clúster de origen (no tiene credenciales de administrador de clúster para un clúster remoto), puede emparejar un volumen con otro volumen en un clúster remoto mediante una clave de emparejamiento.

Lo que necesitarás

- Asegúrese de que los clústeres que contienen los volúmenes estén emparejados.
- Asegúrese de que exista un volumen en el clúster remoto para utilizarlo para el emparejamiento.

> Puede asignar un origen y un destino de replicación después del proceso de emparejamiento. Una fuente o destino de replicación puede ser cualquiera de los volúmenes de un par de volúmenes. Debe crear un volumen de destino que no contenga datos y tenga las características exactas del volumen de origen, como el tamaño, la configuración del tamaño de bloque para los volúmenes (ya sea 512e o 4k) y la configuración de QoS. Si asigna un volumen existente como destino de replicación, los datos de ese volumen se sobrescribirán. El volumen objetivo puede ser mayor o igual en tamaño que el volumen de origen, pero no puede ser menor.

Pasos

1. Seleccione **Administración** > **Volúmenes**.

2. Haz clic en el icono **Acciones** del volumen que quieras emparejar.
3. Haga clic en **Emparejar**.
4. En el cuadro de diálogo **Emparejar volumen**, seleccione **Iniciar emparejamiento**.
5. Seleccione **No tengo** para indicar que no tiene acceso al clúster remoto.
6. Seleccione un **Modo de replicación** de la lista:
   - **Tiempo real (asíncrono)**: Las escrituras se confirman al cliente después de que se hayan confirmado en el clúster de origen.
   - **En tiempo real (síncrono)**: Las escrituras se confirman al cliente después de que se hayan confirmado tanto en el clúster de origen como en el de destino.
   - **Solo instantáneas**: Solo se replican las instantáneas creadas en el clúster de origen. Las escrituras activas desde el volumen de origen no se replican.
7. Haz clic en **Generar clave**.

   Esta acción genera una clave de texto para el emparejamiento y crea un par de volúmenes no configurados en el clúster local. Si no completa el procedimiento, deberá eliminar manualmente el par de volúmenes.

8. Copia la clave de emparejamiento al portapapeles de tu ordenador.
9. Proporcione la clave de emparejamiento al administrador del clúster en el sitio del clúster remoto.

   La clave de emparejamiento de volumen debe tratarse de forma segura y no utilizarse de manera que permita un acceso accidental o no seguro.

   No modifique ninguno de los caracteres de la clave de emparejamiento. La clave pierde validez si se modifica.

10. En la interfaz de usuario de Element del clúster remoto, seleccione **Administración** > **Volúmenes**.
11. Haz clic en el icono de Acciones del volumen que deseas emparejar.
12. Haga clic en **Emparejar**.
13. En el cuadro de diálogo **Emparejar volumen**, seleccione **Completar emparejamiento**.
14. Pegue la clave de emparejamiento del otro grupo en el cuadro **Clave de emparejamiento**.
15. Haga clic en **Completar emparejamiento**.

    Una vez confirmado el emparejamiento, los dos grupos inician el proceso de conexión de los volúmenes para el emparejamiento. Durante el proceso de emparejamiento, puede ver mensajes en la columna **Estado del volumen** de la ventana **Pares de volúmenes**. El par de pantallas de volumen `PausedMisconfigured` hasta que se asignen el origen y el destino del par de volúmenes.

    Una vez completado correctamente el emparejamiento, se recomienda actualizar la tabla Volúmenes para eliminar la opción **Emparejar** de la lista **Acciones** del volumen emparejado. Si no actualiza la tabla, la opción **Par** seguirá disponible para su selección. Si vuelve a seleccionar la opción **Emparejar**, se abrirá una nueva pestaña y, dado que el volumen ya está emparejado, el sistema informará de un `StartVolumePairing Failed: xVolumeAlreadyPaired` Mensaje de error en la ventana **Emparejar volumen** de la página de la interfaz de usuario de Element.

Encuentra más información

- Mensajes de emparejamiento de volumen
- Advertencias de emparejamiento de volumen
- Asignar una fuente y un destino de replicación a los volúmenes emparejados.

Asignar una fuente y un destino de replicación a los volúmenes emparejados.

Una vez emparejados los volúmenes, debe asignar un volumen de origen y su volumen de destino de replicación. Una fuente o destino de replicación puede ser cualquiera de los volúmenes de un par de volúmenes. También puede utilizar este procedimiento para redirigir los datos enviados a un volumen de origen a un volumen de destino remoto en caso de que el volumen de origen deje de estar disponible.

Lo que necesitarás

Tienes acceso a los clústeres que contienen los volúmenes de origen y destino.

Pasos

1. Prepare el volumen fuente:
   a. Desde el clúster que contiene el volumen que desea asignar como origen, seleccione **Administración** > **Volúmenes**.
   b. Haz clic en el icono **Acciones** del volumen que deseas asignar como fuente y haz clic en **Editar**.
   c. En la lista desplegable **Acceso**, seleccione **Lectura/Escritura**.

   > Si está invirtiendo la asignación de origen y destino, esta acción hará que el par de volúmenes muestre el siguiente mensaje hasta que se asigne un nuevo destino de replicación: `PausedMisconfigured`

   Cambiar el acceso pausa la replicación del volumen y provoca que se detenga la transmisión de datos. Asegúrese de haber coordinado estos cambios en ambos sitios.

   a. Haz clic en **Guardar cambios**.
2. Prepare el volumen objetivo:
   a. Desde el clúster que contiene el volumen que desea asignar como destino, seleccione **Administración** > **Volúmenes**.
   b. Haz clic en el icono Acciones del volumen que deseas asignar como destino y haz clic en **Editar**.
   c. En la lista desplegable **Acceso**, seleccione **Destino de replicación**.

   > Si asigna un volumen existente como destino de replicación, los datos de ese volumen se sobrescribirán. Debe utilizar un nuevo volumen de destino que no contenga datos y tenga las características exactas del volumen de origen, como el tamaño, la configuración 512e y la configuración QoS. El volumen objetivo puede ser mayor o igual en tamaño que el volumen de origen, pero no puede ser menor.

   d. Haz clic en **Guardar cambios**.

Encuentra más información

- Emparejar volúmenes utilizando un ID de volumen
- Emparejar volúmenes mediante una clave de emparejamiento

Validar la replicación de volumen

Después de replicar un volumen, debe asegurarse de que los volúmenes de origen y destino estén activos. Cuando se encuentra en estado activo, los volúmenes están emparejados, los datos se envían desde el volumen de origen al volumen de destino y los datos están sincronizados.

1. Desde ambos clústeres, seleccione **Protección de datos** > **Pares de volúmenes**.
2. Verifique que el estado del volumen sea Activo.

Encuentra más información

Advertencias de emparejamiento de volumen

Eliminar una relación de volumen después de la replicación

Una vez completada la replicación y cuando ya no necesite la relación de pares de volúmenes, puede eliminar dicha relación.

1. Seleccione **Protección de datos** > **Pares de volúmenes**.
2. Haz clic en el icono **Acciones** del par de volúmenes que deseas eliminar.
3. Haga clic en **Eliminar**.
4. Confirma el mensaje.

Gestionar las relaciones de volumen

Pausar la replicación

Puede pausar manualmente la replicación si necesita detener el procesamiento de E/S durante un corto período de tiempo. Puede que desee pausar la replicación si hay un aumento repentino en el procesamiento de E/S y desea reducir la carga de procesamiento.

1. Seleccione **Protección de datos** > **Pares de volúmenes**.
2. Haz clic en el icono de Acciones para el par de volúmenes.
3. Haga clic en **Editar**.
4. En el panel **Editar par de volúmenes**, pause manualmente el proceso de replicación.

> Pausar o reanudar manualmente la replicación de volúmenes provoca que la transmisión de datos se detenga o se reanude. Asegúrese de haber coordinado estos cambios en ambos sitios.

5. Haz clic en **Guardar cambios**.

Cambiar el modo de replicación

Puede editar las propiedades del par de volúmenes para cambiar el modo de replicación de la relación del par de volúmenes.

1. Seleccione **Protección de datos** > **Pares de volúmenes**.
2. Haz clic en el icono de Acciones para el par de volúmenes.
3. Haga clic en **Editar**.
4. En el panel **Editar par de volúmenes**, seleccione un nuevo modo de replicación:
   - **Tiempo real (asíncrono)**: Las escrituras se confirman al cliente después de que se hayan confirmado en el clúster de origen.
   - **En tiempo real (síncrono)**: Las escrituras se confirman al cliente después de que se hayan confirmado tanto en el clúster de origen como en el de destino.
   - **Solo instantáneas**: Solo se replican las instantáneas creadas en el clúster de origen. Las escrituras activas desde el volumen de origen no se replican. **Atención:** Cambiar el modo de replicación cambia el modo inmediatamente. Asegúrese de haber coordinado estos cambios en ambos sitios.
5. Haz clic en **Guardar cambios**.

Eliminar pares de volúmenes

Puede eliminar un par de volúmenes si desea eliminar la asociación entre dos volúmenes.

1. Seleccione **Protección de datos** > **Pares de volúmenes**.
2. Haz clic en el icono Acciones del par de volúmenes que deseas eliminar.
3. Haga clic en **Eliminar**.
4. Confirma el mensaje.

Eliminar un par de clústeres

Puedes eliminar un par de clústeres desde la interfaz de usuario de Element de cualquiera de los clústeres del par.

1. Haz clic en **Protección de datos** > **Pares de clústeres**.
2. Haz clic en el icono de Acciones para un par de clústeres.
3. En el menú que aparece, haga clic en **Eliminar**.
4. Confirma la acción.
5. Repita los pasos desde el segundo clúster en el emparejamiento de clústeres.

Detalles del par de clústeres

La página Pares de clústeres en la pestaña Protección de datos proporciona información sobre los clústeres que se han emparejado o que están en proceso de emparejamiento. El sistema muestra mensajes de emparejamiento y progreso en la columna de Estado.

- **IDENTIFICACIÓN**

Se asigna un ID generado por el sistema a cada par de clústeres.

- **Nombre del clúster remoto**

  El nombre del otro grupo del par.

- **MVIP remoto**

  La dirección IP virtual de gestión del otro clúster del par.

- **Estado**

  Estado de replicación del clúster remoto

- **Replicación de volúmenes**

  El número de volúmenes contenidos en el clúster que están emparejados para la replicación.

- **UUID**

  Se asigna un identificador único a cada clúster del par.

pares de volumen

Detalles del par de volúmenes

La página "Pares de volúmenes" en la pestaña "Protección de datos" proporciona información sobre los volúmenes que se han emparejado o que están en proceso de emparejamiento. El sistema muestra mensajes de emparejamiento y progreso en la columna Estado del volumen.

- **IDENTIFICACIÓN**

  Identificador generado por el sistema para el volumen.

- **Nombre**

  El nombre que se le dio al volumen cuando fue creado. Los nombres de volumen pueden tener hasta 223 caracteres y contener az, 0-9 y guion (-).

- **Cuenta**

  Nombre de la cuenta asignada al volumen.

- **Estado del volumen**

  Estado de replicación del volumen

- **Estado de la instantánea**

  Estado del volumen de instantáneas.

- **Modo**

  Método de replicación de escritura del cliente. Los valores posibles son los siguientes:

- Asíncrono
- Solo instantánea
- Sincronizar

- **Dirección**

  La dirección de los datos de volumen:

  - Icono de volumen de origen (→) indica que se están escribiendo datos en un destino fuera del clúster.
  - Icono de volumen objetivo (←) indica que se están escribiendo datos en el volumen local desde una fuente externa.

- **Retardo asíncrono**

  Tiempo transcurrido desde la última sincronización del volumen con el clúster remoto. Si el volumen no está emparejado, el valor es nulo.

- **Clúster remoto**

  Nombre del clúster remoto en el que reside el volumen.

- **ID de volumen remoto**

  Identificador del volumen en el clúster remoto.

- **Nombre del volumen remoto**

  Nombre asignado al volumen remoto cuando se creó.

Mensajes de emparejamiento de volumen

Puede ver los mensajes de emparejamiento de volúmenes durante el proceso de emparejamiento inicial en la página "Pares de volúmenes" que se encuentra en la pestaña "Protección de datos". Estos mensajes pueden mostrarse tanto en el extremo de origen como en el de destino del par en la vista de lista de volúmenes replicados.

- **PausadoDesconectado**

  Se agotó el tiempo de espera de las RPC de replicación de origen o de sincronización. Se ha perdido la conexión con el clúster remoto. Compruebe las conexiones de red al clúster.

- **Reanudando conexión**

  La sincronización de replicación remota ya está activa. Iniciando el proceso de sincronización y esperando datos.

- **Reanudando RRSync**

  Se está realizando una copia helicoidal única de los metadatos del volumen en el clúster emparejado.

- **Reanudando LocalSync**

  Se está realizando una copia de doble hélice de los metadatos del volumen en el clúster emparejado.

- **Reanudando la transferencia de datos**

  Se ha reanudado la transferencia de datos.

- **Activo**

  Los volúmenes están emparejados y los datos se envían del volumen de origen al de destino; los datos están sincronizados.

- **Inactivo**

  No se está produciendo ninguna actividad de replicación.

Advertencias de emparejamiento de volumen

La página "Pares de volúmenes" en la pestaña "Protección de datos" muestra estos mensajes después de emparejar volúmenes. Estos mensajes pueden mostrarse tanto en el extremo de origen como en el de destino del par (a menos que se indique lo contrario) en la vista de lista de volúmenes replicados.

- **ClústerCompleto en Pausa**

  Debido a que el clúster de destino está lleno, la replicación de origen y la transferencia masiva de datos no pueden continuar. El mensaje se muestra únicamente en el extremo de origen del par.

- **Pausa superada el número máximo de instantáneas**

  El volumen de destino ya tiene el número máximo de instantáneas y no puede replicar instantáneas adicionales.

- **Pausa manual**

  El volumen local se ha pausado manualmente. Debe reanudarse antes de que se reanude la replicación.

- **Control remoto manual en pausa**

  El volumen remoto está en modo de pausa manual. Se requiere intervención manual para reanudar la replicación del volumen remoto.

- **PausadoDesconfigurado**

  Esperando una fuente y un objetivo activos. Se requiere intervención manual para reanudar la replicación.

- **QoS en pausa**

  La QoS objetivo no pudo soportar la E/S entrante. La replicación se reanuda automáticamente. El mensaje se muestra únicamente en el extremo de origen del par.

- **Enlace lento en pausa**

  Se detectó un enlace lento y se detuvo la replicación. La replicación se reanuda automáticamente. El mensaje se muestra únicamente en el extremo de origen del par.

- **Desajuste en el tamaño del volumen en pausa**

El volumen de destino no tiene el mismo tamaño que el volumen de origen.

- **PausadoXCopy**

  Se está enviando un comando SCSI XCOPY a un volumen de origen. El comando debe completarse antes de que se pueda reanudar la replicación. El mensaje se muestra únicamente en el extremo de origen del par.

- **Detenido por mala configuración**

  Se ha detectado un error de configuración permanente. El volumen remoto se ha borrado o desvinculado. No es posible ninguna acción correctiva; debe establecerse un nuevo emparejamiento.

Utilice la replicación SnapMirror entre los clústeres Element y ONTAP (interfaz de usuario de Element).

Utilice la replicación SnapMirror entre los clústeres Element y ONTAP (interfaz de usuario de Element).

Puede crear relaciones SnapMirror desde la pestaña Protección de datos en la interfaz de usuario de NetApp Element . Para ver esto en la interfaz de usuario, debe estar habilitada la funcionalidad SnapMirror .

IPv6 no es compatible con la replicación SnapMirror entre el software NetApp Element y los clústeres ONTAP .

"Vídeo de NetApp : SnapMirror para NetApp HCI y Element Software"

Los sistemas que ejecutan el software NetApp Element admiten la funcionalidad SnapMirror para copiar y restaurar copias de instantáneas con sistemas NetApp ONTAP . La razón principal para utilizar esta tecnología es la recuperación ante desastres de NetApp HCI a ONTAP. Los puntos de conexión incluyen ONTAP, ONTAP Select y Cloud Volumes ONTAP. Consulte TR-4641 Protección de datos NetApp HCI .

"Informe técnico 4641 de NetApp : Protección de datos NetApp HCI"

Encuentra más información

- "Creación de su estructura de datos con NetApp HCI, ONTAP e infraestructura convergente"
- "Replicación entre NetApp Element Software y ONTAP (CLI de ONTAP)"

Descripción general de SnapMirror

Los sistemas que ejecutan el software NetApp Element admiten la funcionalidad SnapMirror para copiar y restaurar instantáneas con sistemas NetApp ONTAP .

Los sistemas que ejecutan Element pueden comunicarse directamente con SnapMirror en sistemas ONTAP 9.3 o superiores. La API de NetApp Element proporciona métodos para habilitar la funcionalidad SnapMirror en clústeres, volúmenes e instantáneas. Además, la interfaz de usuario de Element incluye todas las funcionalidades necesarias para gestionar las relaciones SnapMirror entre el software Element y los sistemas ONTAP .

En casos de uso específicos, puede replicar volúmenes originados en ONTAP a volúmenes de Element con funcionalidad limitada. Para obtener más información, consulte "Replicación entre el software Element y ONTAP (ONTAP CLI)".

Habilite SnapMirror en el clúster.

Debe habilitar manualmente la funcionalidad SnapMirror a nivel de clúster a través de la interfaz de usuario de NetApp Element . El sistema viene con la funcionalidad SnapMirror desactivada por defecto, y no se activa automáticamente como parte de una nueva instalación o actualización. Habilitar la función SnapMirror es una tarea de configuración que se realiza una sola vez.

SnapMirror solo se puede habilitar para clústeres que ejecutan el software Element utilizado junto con volúmenes en un sistema NetApp ONTAP . Solo debe habilitar la funcionalidad SnapMirror si su clúster está conectado para su uso con volúmenes NetApp ONTAP .

Lo que necesitarás

El clúster de almacenamiento debe estar ejecutando el software NetApp Element .

Pasos

1. Haz clic en **Clústeres** > **Configuración**.
2. Encuentre la configuración específica del clúster para SnapMirror.
3. Haz clic en **Habilitar SnapMirror**.

> Habilitar la funcionalidad SnapMirror modifica permanentemente la configuración del software Element. Solo puede desactivar la función SnapMirror y restaurar la configuración predeterminada devolviendo el clúster a la imagen de fábrica.

4. Haga clic en **Sí** para confirmar el cambio de configuración de SnapMirror .

Habilita SnapMirror en el volumen

Debe habilitar SnapMirror en el volumen en la interfaz de usuario de Element. Esto permite la replicación de datos en volúmenes ONTAP específicos. Este es un permiso del administrador del clúster que ejecuta el software NetApp Element para que SnapMirror controle un volumen.

Lo que necesitarás

- Has habilitado SnapMirror en la interfaz de usuario de Element para el clúster.
- Hay disponible un punto de conexión SnapMirror .
- El volumen debe tener un tamaño de bloque de 512e.
- El volumen no participa en la replicación remota.
- El tipo de acceso al volumen no es Destino de replicación.

> También puede configurar esta propiedad al crear o clonar un volumen.

Pasos

1. Haz clic en **Administración** > **Volúmenes**.
2. Haz clic en el icono **Acciones** del volumen para el que quieras habilitar SnapMirror .
3. En el menú que aparece, seleccione **Editar**.

4. En el cuadro de diálogo **Editar volumen**, seleccione la casilla de verificación **Habilitar SnapMirror**.
5. Haz clic en **Guardar cambios**.

Crea un punto de conexión de SnapMirror

Debe crear un punto de conexión SnapMirror en la interfaz de usuario de NetApp Element antes de poder crear una relación.

Un punto de conexión SnapMirror es un clúster ONTAP que sirve como destino de replicación para un clúster que ejecuta el software Element. Antes de crear una relación SnapMirror , primero debe crear un punto de conexión SnapMirror .

Puede crear y administrar hasta cuatro puntos de conexión SnapMirror en un clúster de almacenamiento que ejecute el software Element.

> Si un punto de conexión existente se creó originalmente utilizando la API y no se guardaron las credenciales, puede ver el punto de conexión en la interfaz de usuario de Element y verificar su existencia, pero no se puede administrar mediante la interfaz de usuario de Element. Este punto de conexión solo se puede gestionar mediante la API de Element.

Para obtener más detalles sobre los métodos de la API, consulte "Gestiona el almacenamiento con la API de Element".

Lo que necesitarás

- Deberías haber habilitado SnapMirror en la interfaz de usuario de Element para el clúster de almacenamiento.
- Conoces las credenciales ONTAP para el punto final.

Pasos

1. Haga clic en **Protección de datos** > *Puntos de conexión de SnapMirror *.
2. Haz clic en **Crear punto de conexión**.
3. En el cuadro de diálogo **Crear un nuevo punto de conexión**, introduzca la dirección IP de administración del clúster del sistema ONTAP .
4. Introduzca las credenciales de administrador de ONTAP asociadas al punto de conexión.
5. Revisar detalles adicionales:
   - LIFs: Enumera las interfaces lógicas intercluster de ONTAP utilizadas para comunicarse con Element.
   - Estado: Muestra el estado actual del punto de conexión de SnapMirror . Los valores posibles son: conectado, desconectado y no administrado.
6. Haz clic en **Crear punto de conexión**.

Crear una relación SnapMirror

Debe crear una relación SnapMirror en la interfaz de usuario de NetApp Element .

> Cuando un volumen aún no está habilitado para SnapMirror y usted selecciona crear una relación desde la interfaz de usuario de Element, SnapMirror se habilita automáticamente en ese volumen.

Lo que necesitarás

SnapMirror está habilitado en el volumen.

Pasos

1. Haz clic en **Administración** > **Volúmenes**.
2. Haga clic en el icono **Acciones** del volumen que formará parte de la relación.
3. Haga clic en *Crear una relación SnapMirror *.
4. En el cuadro de diálogo **Crear una relación SnapMirror *, seleccione un punto de conexión de la lista *Punto de conexión**.
5. Seleccione si la relación se creará utilizando un volumen ONTAP nuevo o un volumen ONTAP existente.
6. Para crear un nuevo volumen ONTAP en la interfaz de usuario de Element, haga clic en **Crear nuevo volumen**.
   a. Seleccione la **Máquina Virtual de Almacenamiento** para esta relación.
   b. Seleccione **Agregado** de la lista desplegable.
   c. En el campo **Sufijo del nombre del volumen**, introduzca un sufijo.

      El sistema detecta el nombre del volumen de origen y lo copia al campo **Nombre del volumen**. El sufijo que introduzcas añadirá un elemento al nombre.

   d. Haga clic en **Crear volumen de destino**.
7. Para utilizar un volumen ONTAP existente, haga clic en **Usar volumen existente**.
   a. Seleccione la **Máquina Virtual de Almacenamiento** para esta relación.
   b. Seleccione el volumen que será el destino de esta nueva relación.
8. En la sección **Detalles de la relación**, seleccione una póliza. Si la política seleccionada tiene reglas de retención, la tabla de reglas muestra las reglas y las etiquetas asociadas.
9. **Opcional**: Seleccione un horario.

   Esto determina con qué frecuencia la relación crea copias.

10. **Opcional**: En el campo **Limitar ancho de banda a**, ingrese la cantidad máxima de ancho de banda que pueden consumir las transferencias de datos asociadas con esta relación.
11. Revisar detalles adicionales:
    - **Estado**: Estado actual de la relación del volumen de destino. Los valores posibles son:
      - no inicializado: El volumen de destino no se ha inicializado.
      - snapmirrered: El volumen de destino se ha inicializado y está listo para recibir actualizaciones de SnapMirror .
      - volumen interrumpido: El volumen de destino es de lectura/escritura y existen instantáneas.
    - **Estado**: Estado actual de la relación. Los valores posibles son: inactivo, transfiriendo, comprobando, en reposo, en reposo, en cola, preparando, finalizando, abortando y rompiendo.
    - **Tiempo de retardo**: Cantidad de tiempo en segundos que el sistema de destino se retrasa con respecto al sistema de origen. El tiempo de demora no debe ser mayor que el intervalo del programa de transferencia.
    - **Límite de ancho de banda**: La cantidad máxima de ancho de banda que pueden consumir las transferencias de datos asociadas con esta relación.

- **Última transferencia**: Marca de tiempo de la última instantánea transferida. Haz clic para obtener más información.
- **Nombre de la política**: El nombre de la política ONTAP SnapMirror para la relación.
- **Tipo de política**: Tipo de política ONTAP SnapMirror seleccionada para la relación. Los valores posibles son:
  - espejo asíncrono
  - bóveda_espejo
- **Nombre de la programación**: Nombre de la programación preexistente en el sistema ONTAP seleccionada para esta relación.

12. Para no inicializar en este momento, asegúrese de que la casilla de verificación **Inicializar** no esté seleccionada.

> La inicialización puede llevar mucho tiempo. Quizás te convenga ejecutarlo durante las horas de menor tráfico. La inicialización realiza una transferencia básica; crea una copia instantánea del volumen de origen y luego transfiere esa copia y todos los bloques de datos a los que hace referencia al volumen de destino. Puede inicializar manualmente o utilizar una programación para iniciar el proceso de inicialización (y las actualizaciones posteriores) según la programación establecida.

13. Haz clic en **Crear relación**.
14. Haz clic en **Protección de datos** > *Relaciones de SnapMirror * para ver esta nueva relación de SnapMirror .

acciones de relación de SnapMirror

Puede configurar una relación desde la página Relaciones de SnapMirror de la pestaña Protección de datos. Aquí se describen las opciones del icono Acciones.

- **Editar**: Modifica la política utilizada o el cronograma para la relación.
- **Eliminar**: Elimina la relación SnapMirror . Esta función no elimina el volumen de destino.
- **Inicializar**: Realiza la primera transferencia inicial de datos de referencia para establecer una nueva relación.
- **Actualización**: Realiza una actualización a petición de la relación, replicando en el destino cualquier dato nuevo y copias de instantáneas incluidas desde la última actualización.
- **Quiesce**: Impide cualquier actualización adicional de una relación.
- **Reanudar**: Reanuda una relación que se encontraba en pausa.
- **Interrupción**: Hace que el volumen de destino sea de lectura y escritura y detiene todas las transferencias actuales y futuras. Compruebe que los clientes no están utilizando el volumen de origen original, ya que la operación de resincronización inversa hace que el volumen de origen original sea de solo lectura.
- **Resincronizar**: Restablece una relación rota en la misma dirección en la que se produjo la ruptura.
- **Resincronización inversa**: Automatiza los pasos necesarios para crear e inicializar una nueva relación en la dirección opuesta. Esto solo puede hacerse si la relación existente está rota. Esta operación no eliminará la relación actual. El volumen de origen original vuelve a la copia Snapshot común más reciente y se resincroniza con el destino. Se perderán todos los cambios realizados en el volumen de origen original desde la última actualización correcta de SnapMirror . Cualquier modificación realizada o nuevos datos escritos en el volumen de destino actual se envían de vuelta al volumen de origen original.

- **Abortar**: Cancela una transferencia en curso. Si se emite una actualización de SnapMirror para una relación interrumpida, la relación continúa con la última transferencia del último punto de control de reinicio que se creó antes de que se produjera la interrupción.

Etiquetas de SnapMirror

Etiquetas de SnapMirror

Una etiqueta SnapMirror sirve como marcador para transferir una instantánea específica de acuerdo con las reglas de retención de la relación.

Al aplicar una etiqueta a una instantánea, esta se marca como objetivo para la replicación de SnapMirror . La función de esta relación es hacer cumplir las reglas durante la transferencia de datos, seleccionando la instantánea etiquetada correspondiente, copiándola al volumen de destino y asegurando que se conserve el número correcto de copias. Se refiere a la política para determinar el número de copias a conservar y el período de retención. La política puede tener cualquier número de reglas y cada regla tiene una etiqueta única. Esta etiqueta sirve de enlace entre la instantánea y la regla de retención.

Es la etiqueta SnapMirror la que indica qué regla se aplica a la instantánea, instantánea de grupo o programación seleccionada.

Agregar etiquetas de SnapMirror a las instantáneas

Las etiquetas de SnapMirror especifican la política de retención de instantáneas en el punto final de SnapMirror . Puedes añadir etiquetas a las instantáneas y agrupar instantáneas.

Puede ver las etiquetas disponibles desde un cuadro de diálogo de relación SnapMirror existente o desde NetApp ONTAP System Manager.

> Al agregar una etiqueta a una instantánea de grupo, se sobrescriben las etiquetas existentes en las instantáneas individuales.

Lo que necesitarás

- SnapMirror está habilitado en el clúster.
- La etiqueta que desea agregar ya existe en ONTAP.

Pasos

1. Haz clic en **Protección de datos** > **Instantáneas** o en la página **Instantáneas de grupo**.
2. Haga clic en el icono **Acciones** de la instantánea o instantánea de grupo a la que desea agregar una etiqueta de SnapMirror .
3. En el cuadro de diálogo **Editar instantánea**, introduzca el texto en el campo *Etiqueta de SnapMirror *. La etiqueta debe coincidir con una etiqueta de regla en la política aplicada a la relación SnapMirror .
4. Haz clic en **Guardar cambios**.

Agregar etiquetas de SnapMirror a las programaciones de instantáneas

Puedes agregar etiquetas SnapMirror a las programaciones de instantáneas para asegurarte de que se aplique una política SnapMirror . Puede ver las etiquetas disponibles desde un cuadro de diálogo de relación SnapMirror existente o desde el

Administrador del sistema NetAppONTAP.

Lo que necesitarás

- SnapMirror debe estar habilitado a nivel de clúster.
- La etiqueta que desea agregar ya existe en ONTAP.

Pasos

1. Haz clic en **Protección de datos** > **Programaciones**.
2. Agregue una etiqueta de SnapMirror a una programación de una de las siguientes maneras:

Opción	Pasos
Crear un nuevo horario	a. Seleccione **Crear horario**. b. Introduzca todos los demás datos relevantes. c. Seleccione **Crear horario**.
Modificar el cronograma existente	a. Haz clic en el icono **Acciones** del calendario al que quieras añadir una etiqueta y selecciona **Editar**. b. En el cuadro de diálogo resultante, introduzca el texto en el campo *Etiqueta de SnapMirror *. c. Seleccione **Guardar cambios**.

Encuentra más información

Crea un cronograma de instantáneas

Recuperación ante desastres mediante SnapMirror

Recuperación ante desastres mediante SnapMirror

En caso de que se produzca un problema con un volumen o clúster que ejecute el software NetApp Element , utilice la funcionalidad SnapMirror para romper la relación y realizar una conmutación por error al volumen de destino.

Si el clúster original ha fallado por completo o no existe, póngase en contacto con el soporte de NetApp para obtener más ayuda.

Realizar una conmutación por error desde un clúster de Element

Puede realizar una conmutación por error desde el clúster Element para que el volumen de destino sea de lectura/escritura y accesible para los hosts en el lado de destino. Antes de realizar una conmutación por error desde el clúster Element, debe romper la relación SnapMirror .

Utilice la interfaz de usuario de NetApp Element para realizar la conmutación por error. Si la interfaz de usuario de Element no está disponible, también puede usar ONTAP System Manager o ONTAP CLI para ejecutar el comando para romper la relación.

Lo que necesitarás

- Existe una relación SnapMirror y tiene al menos una instantánea válida en el volumen de destino.
- Necesitas realizar una conmutación por error al volumen de destino debido a una interrupción no planificada o un evento planificado en el sitio principal.

Pasos

1. En la interfaz de usuario de Element, haga clic en **Protección de datos** > *Relaciones de SnapMirror *.
2. Encuentre la relación con el volumen de origen que desea conmutar por error.
3. Haz clic en el icono **Acciones**.
4. Haga clic en **Interrupción**.
5. Confirma la acción.

   El volumen en el clúster de destino ahora tiene acceso de lectura y escritura y se puede montar en los hosts de la aplicación para reanudar las cargas de trabajo de producción. Como resultado de esta acción, se detiene toda la replicación de SnapMirror . La relación muestra un estado de ruptura.

Realizar una recuperación a Element

Aprenda cómo realizar una recuperación ante fallos a Element

Una vez mitigado el problema en el lado primario, debe volver a sincronizar el volumen de origen original y recurrir al software NetApp Element . Los pasos a seguir varían dependiendo de si el volumen de origen original aún existe o si necesita recurrir a un volumen recién creado.

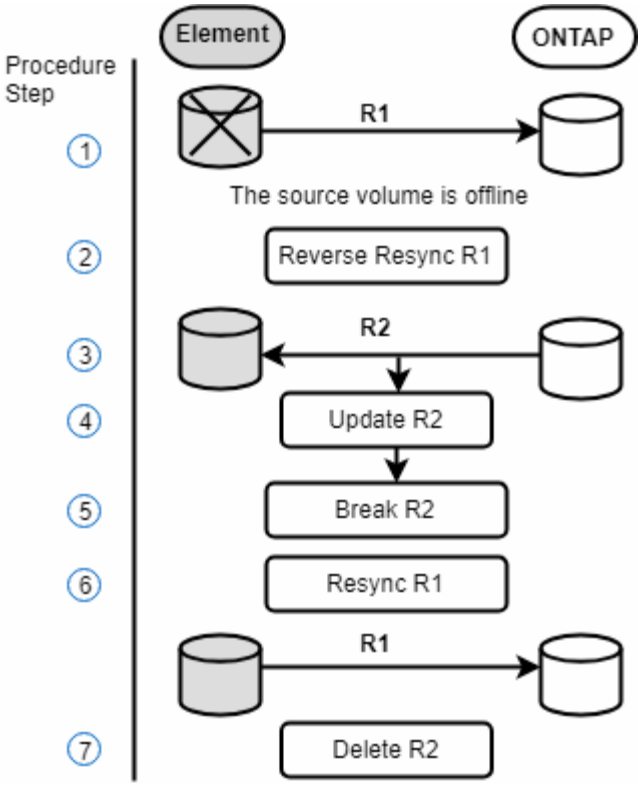
escenarios de recuperación ante fallos de SnapMirror

La funcionalidad de recuperación ante desastres de SnapMirror se ilustra en dos escenarios de recuperación tras fallo. Esto presupone que la relación original ha fracasado (se ha roto).

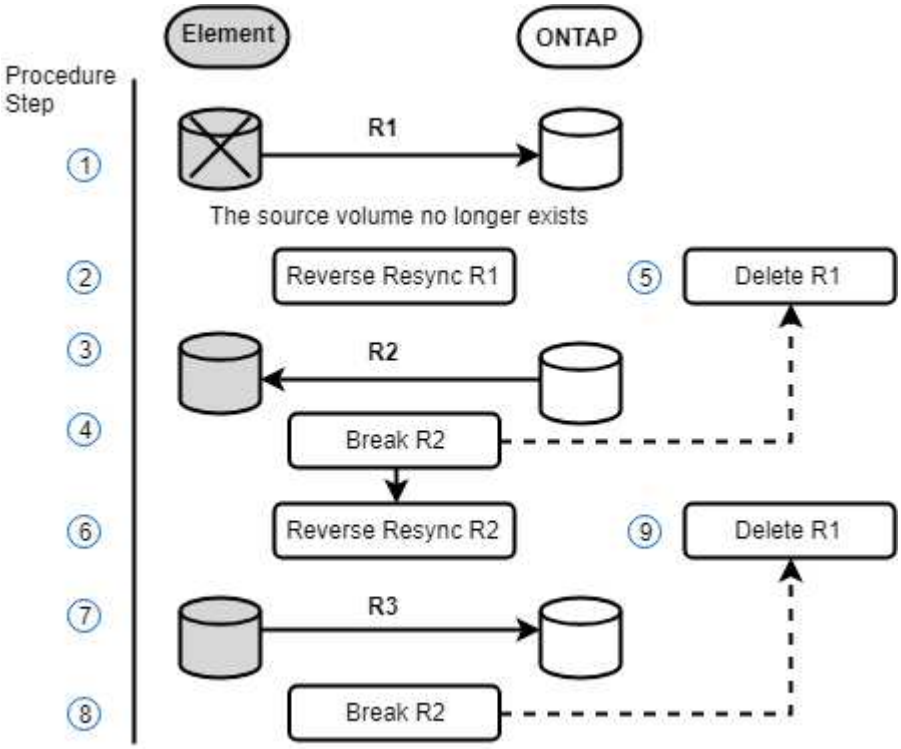
Los pasos de los procedimientos correspondientes se añaden como referencia.

> En los ejemplos aquí presentes, R1 = la relación original en la que el clúster que ejecuta el software NetApp Element es el volumen de origen original (Element) y ONTAP es el volumen de destino original (ONTAP). R2 y R3 representan las relaciones inversas creadas a través de la operación de resincronización inversa.

La siguiente imagen muestra el escenario de recuperación ante fallos cuando el volumen de origen aún existe:



La siguiente imagen muestra el escenario de recuperación ante fallos cuando el volumen de origen ya no existe:



Encuentra más información

- Realizar una recuperación tras fallo cuando el volumen de origen aún exista
- Realizar una recuperación tras fallo cuando el volumen de origen ya no exista

- escenarios de recuperación ante fallos de SnapMirror

Realizar una recuperación tras fallo cuando el volumen de origen aún exista

Puede volver a sincronizar el volumen de origen original y realizar la recuperación tras un fallo utilizando la interfaz de usuario de NetApp Element . Este procedimiento se aplica a escenarios donde el volumen fuente original aún existe.

1. En la interfaz de usuario de Element, busque la relación que rompió para realizar la conmutación por error.
2. Haz clic en el icono Acciones y luego en **Revertir resincronización**.
3. Confirma la acción.

> La operación de resincronización inversa crea una nueva relación en la que se invierten las funciones de los volúmenes de origen y destino originales (esto da como resultado dos relaciones, ya que la relación original persiste). Los nuevos datos procedentes del volumen de destino original se transfieren al volumen de origen original como parte de la operación de resincronización inversa. Puede seguir accediendo y escribiendo datos en el volumen activo en el lado de destino, pero deberá desconectar todos los hosts del volumen de origen y realizar una actualización de SnapMirror antes de redirigir de nuevo al primario original.

4. Haz clic en el icono de Acciones de la relación inversa que acabas de crear y haz clic en **Actualizar**.

   Una vez completada la resincronización inversa y comprobado que no hay sesiones activas conectadas al volumen en el lado de destino y que los datos más recientes se encuentran en el volumen primario original, puede realizar los siguientes pasos para completar la recuperación ante fallos y reactivar el volumen primario original:

5. Haz clic en el icono de Acciones de la relación inversa y haz clic en **Romper**.
6. Haz clic en el icono Acciones de la relación original y haz clic en **Resincronizar**.

> Ahora se puede montar el volumen primario original para reanudar las cargas de trabajo de producción en dicho volumen. La replicación original de SnapMirror se reanuda según la política y la programación configuradas para la relación.

7. Después de confirmar que el estado de la relación original es “snapmirred”, haga clic en el icono de Acciones de la relación inversa y haga clic en **Eliminar**.

Encuentra más información

escenarios de recuperación ante fallos de SnapMirror

Realizar una recuperación tras fallo cuando el volumen de origen ya no exista

Puede volver a sincronizar el volumen de origen original y realizar la recuperación tras un fallo utilizando la interfaz de usuario de NetApp Element . Esta sección se aplica a escenarios en los que se ha perdido el volumen de origen original, pero el clúster original permanece intacto. Para obtener instrucciones sobre cómo restaurar un nuevo clúster, consulte la documentación en el sitio de soporte de NetApp .

Lo que necesitarás

- Existe una relación de replicación interrumpida entre los volúmenes de Element y ONTAP .
- El volumen de Element se ha perdido irremediablemente.
- El nombre del volumen original aparece como NO ENCONTRADO.

Pasos

1. En la interfaz de usuario de Element, busque la relación que rompió para realizar la conmutación por error.

   Buenas prácticas: Tome nota de la política de SnapMirror y de los detalles del calendario de la relación original que se interrumpió. Esta información será necesaria para restablecer la relación.

2. Haz clic en el icono **Acciones** y luego en **Revertir resincronización**.
3. Confirma la acción.

   > La operación de resincronización inversa crea una nueva relación en la que se invierten las funciones del volumen de origen original y del volumen de destino (esto da como resultado dos relaciones, ya que la relación original persiste). Dado que el volumen original ya no existe, el sistema crea un nuevo volumen Element con el mismo nombre y tamaño que el volumen de origen original. Al nuevo volumen se le asigna una política QoS predeterminada llamada sm-recovery y se asocia con una cuenta predeterminada llamada sm-recovery. Deberá editar manualmente la cuenta y la política de QoS para todos los volúmenes creados por SnapMirror para reemplazar los volúmenes de origen originales que fueron destruidos.

   Los datos de la última instantánea se transfieren al nuevo volumen como parte de la operación de resincronización inversa. Puede continuar accediendo y escribiendo datos en el volumen activo en el lado de destino, pero deberá desconectar todos los hosts del volumen activo y realizar una actualización de SnapMirror antes de restablecer la relación primaria original en un paso posterior. Después de completar la resincronización inversa y asegurarse de que no haya sesiones activas conectadas al volumen en el lado de destino y que los datos más recientes se encuentren en el volumen primario original, continúe con los siguientes pasos para completar la recuperación ante fallos y reactivar el volumen primario original:

4. Haga clic en el icono **Acciones** de la relación inversa que se creó durante la operación de resincronización inversa y haga clic en **Romper**.
5. Haga clic en el icono **Acciones** de la relación original, en la que no existe el volumen de origen, y haga clic en **Eliminar**.
6. Haz clic en el icono **Acciones** de la relación inversa, que rompiste en el paso 4, y haz clic en **Revertir resincronización**.
7. Esto invierte el origen y el destino, dando como resultado una relación con el mismo origen y destino de volumen que la relación original.
8. Haz clic en el icono **Acciones** y en **Editar** para actualizar esta relación con la política QoS original y la configuración de programación que anotaste.
9. Ahora es seguro eliminar la relación inversa que resincronizaste en el paso 6.

Encuentra más información

escenarios de recuperación ante fallos de SnapMirror

Realice una transferencia o migración única de ONTAP a Element

Normalmente, cuando se utiliza SnapMirror para la recuperación ante desastres desde

un clúster de almacenamiento SolidFire que ejecuta el software NetApp Element al software ONTAP , Element es el origen y ONTAP el destino. Sin embargo, en algunos casos el sistema de almacenamiento ONTAP puede servir como origen y Element como destino.

- Existen dos escenarios:
  - No existe ninguna relación previa de recuperación ante desastres. Siga todos los pasos de este procedimiento.
  - Existe una relación previa de recuperación ante desastres, pero no entre los volúmenes que se utilizan para esta mitigación. En este caso, siga únicamente los pasos 3 y 4 a continuación.

Lo que necesitarás

- El nodo de destino del elemento debe haber sido hecho accesible para ONTAP.
- El volumen Element debe haber estado habilitado para la replicación SnapMirror .

Debe especificar la ruta de destino del elemento en el formato hostip:/lun/<id_number>, donde lun es la cadena real “lun” e id_number es el ID del volumen del elemento.

Pasos

1. Utilizando ONTAP, cree la relación con el clúster Element:

```
snapmirror create -source-path SVM:volume|cluster://SVM/volume
-destination-path hostip:/lun/name -type XDP -schedule schedule -policy
    policy
```

```
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
```

2. Verifique que la relación SnapMirror se haya creado utilizando el comando ONTAP snapmirror show.

   Consulte la información sobre cómo crear una relación de replicación en la documentación de ONTAP y para conocer la sintaxis completa de los comandos, consulte la página del manual de ONTAP .

3. Utilizando el `ElementCreateVolume` API, cree el volumen de destino y configure el modo de acceso al volumen de destino en SnapMirror:

   Crea un volumen de Element utilizando la API de Element.

```
{
   "method": "CreateVolume",
   "params": {
        "name": "SMTargetVolumeTest2",
        "accountID": 1,
        "totalSize": 100000000000,
        "enable512e": true,
        "attributes": {},
        "qosPolicyID": 1,
        "enableSnapMirrorReplication": true,
        "access": "snapMirrorTarget"
    },
    "id": 1
}
```

4. Inicialice la relación de replicación utilizando ONTAP. `snapmirror initialize` dominio:

```
snapmirror initialize -source-path hostip:/lun/name
-destination-path SVM:volume|cluster://SVM/volume
```

Replicación entre el software NetApp Element y ONTAP (CLI de ONTAP)

Descripción general de la replicación entre el software NetApp Element y ONTAP (CLI de ONTAP)

Puede garantizar la continuidad del negocio en un sistema Element utilizando SnapMirror para replicar copias de instantáneas de un volumen Element en un destino ONTAP . En caso de desastre en el sitio de Element, puede proporcionar datos a los clientes desde el sistema ONTAP y luego reactivar el sistema Element cuando se restablezca el servicio.

A partir de ONTAP 9.4, puede replicar copias de instantáneas de una LUN creada en un nodo ONTAP de vuelta a un sistema Element. Es posible que haya creado un LUN durante una interrupción en el sitio de Element, o que esté utilizando un LUN para migrar datos de ONTAP al software de Element.

Deberías trabajar con la copia de seguridad de Element a ONTAP si se cumplen las siguientes condiciones:

- Lo que se busca es utilizar las mejores prácticas, no explorar todas las opciones disponibles.
- Desea utilizar la interfaz de línea de comandos (CLI) de ONTAP , no System Manager ni una herramienta de scripting automatizada.
- Estás utilizando iSCSI para proporcionar datos a los clientes.

Si necesita información adicional sobre la configuración o los conceptos de SnapMirror , consulte"Resumen de protección de datos" .

Acerca de la replicación entre Element y ONTAP

A partir de ONTAP 9.3, puede usar SnapMirror para replicar copias de instantáneas de un volumen Element en un destino ONTAP . En caso de desastre en el sitio de Element, puede proporcionar datos a los clientes desde el sistema ONTAP y luego reactivar el volumen de origen de Element cuando se restablezca el servicio.

A partir de ONTAP 9.4, puede replicar copias de instantáneas de una LUN creada en un nodo ONTAP de vuelta a un sistema Element. Es posible que haya creado un LUN durante una interrupción en el sitio de Element, o que esté utilizando un LUN para migrar datos de ONTAP al software de Element.

Tipos de relación de protección de datos

SnapMirror ofrece dos tipos de relación de protección de datos. Para cada tipo, SnapMirror crea una copia instantánea del volumen de origen del elemento antes de inicializar o actualizar la relación:

- En una relación de protección de datos de *recuperación ante desastres (DR)*, el volumen de destino contiene únicamente la copia instantánea creada por SnapMirror, desde la cual puede continuar sirviendo datos en 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 de instantáneas puntuales creadas por el software Element, así como la copia de instantánea creada por SnapMirror. Por ejemplo, es posible que desee conservar copias de instantáneas mensuales creadas durante un período de 20 años.

Políticas predeterminadas

La primera vez que se invoca SnapMirror, se realiza una transferencia básica desde el volumen de origen al volumen de destino. La política *SnapMirror* define el contenido de la línea base y cualquier actualización.

Puede utilizar una política predeterminada o personalizada al crear una relación de protección de datos. El *tipo de política* determina qué copias de instantáneas se incluirán y cuántas copias se conservarán.

La tabla siguiente muestra las políticas predeterminadas. Utilice el `MirrorLatest` política para crear una relación de DR tradicional. Utilice el `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 póliza	comportamiento de actualización
MirrorLatest	espejo asíncrono	Transfiera la copia de instantánea creada por SnapMirror.
Espejo y bóveda	bóveda de espejos	Transfiera la copia de instantánea creada por SnapMirror y cualquier copia de instantánea menos reciente realizada desde la última actualización, siempre que tengan las etiquetas de SnapMirror “daily” o “weekly”.
Unified7year	bóveda de espejos	Transfiera la copia de instantánea creada por SnapMirror y cualquier copia de instantánea menos reciente realizada desde la última actualización, siempre que tengan las etiquetas de SnapMirror “daily”, “weekly” o “monthly”.

Para obtener información completa sobre las políticas de SnapMirror , incluyendo orientación sobre qué política utilizar, consulte"Resumen de protección de datos" .

Comprender las etiquetas de SnapMirror

Cada política con el tipo de política “mirror-vault” debe tener una regla que especifique qué copias de instantáneas replicar. La regla “daily”, por ejemplo, indica que solo se deben replicar las copias de instantáneas a las que se les haya asignado la etiqueta SnapMirror “daily”. La etiqueta SnapMirror se asigna al configurar las copias de instantáneas de Element.

Replicación desde un clúster de origen Element a un clúster de destino ONTAP

Puede utilizar SnapMirror para replicar copias de instantáneas de un volumen Element en un sistema de destino ONTAP . En caso de desastre en el sitio de Element, puede proporcionar datos a los clientes desde el sistema ONTAP y luego reactivar el volumen de origen de Element cuando se restablezca el servicio.

Un volumen Element es aproximadamente equivalente a un 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 a ONTAP .

Las reglas de replicación son las siguientes:

- Un volumen ONTAP solo puede contener datos de un volumen Element.
- No se pueden replicar datos de un volumen ONTAP a varios volúmenes Element.

Replicación desde un clúster de origen ONTAP a un clúster de destino Element

A partir de ONTAP 9.4, puede replicar copias de instantáneas de una LUN creada en un sistema ONTAP en un volumen Element:

- Si ya existe una relación SnapMirror entre una fuente Element y un destino ONTAP , una LUN creada mientras se sirven datos desde el destino se replica automáticamente cuando se reactiva la fuente.
- De lo contrario, deberá crear e inicializar una relación SnapMirror entre el clúster de origen ONTAP y el clúster de destino Element.

Las reglas de replicación son las siguientes:

- La relación de replicación debe tener una política de tipo “async-mirror”.

  Las políticas de tipo “mirror-vault” no son compatibles.

- Solo se admiten LUN iSCSI.
- No se puede replicar más de un LUN desde un volumen ONTAP a un volumen Element.
- No se puede replicar un LUN desde un volumen ONTAP a varios volúmenes Element.

Prerrequisitos

Debe haber completado las siguientes tareas antes de configurar una relación de protección de datos entre Element y ONTAP:

- El clúster Element debe estar ejecutando el software NetApp Element versión 10.1 o posterior.

- El clúster ONTAP debe estar ejecutando ONTAP 9.3 o posterior.
- SnapMirror debe haber sido licenciado en el clúster ONTAP .
- Debe haber configurado volúmenes en los clústeres Element y ONTAP que sean lo suficientemente grandes como para manejar las transferencias de datos previstas.
- Si está utilizando el tipo de política “mirror-vault”, debe haberse configurado una etiqueta SnapMirror para que se repliquen las copias de instantáneas de Element.

> Solo puedes realizar esta tarea en el"Interfaz web del software Element" o utilizando el"Métodos API" .

- Debes haberte asegurado de que el puerto 5010 esté disponible.
- Si prevé que podría necesitar mover un volumen de destino, debe haberse asegurado de que exista conectividad de malla completa entre el origen y el destino. Cada nodo del clúster de origen Element debe poder comunicarse con cada nodo del clúster de destino ONTAP .

Detalles de soporte

La siguiente tabla muestra los detalles de soporte para la copia de seguridad de Element a ONTAP .

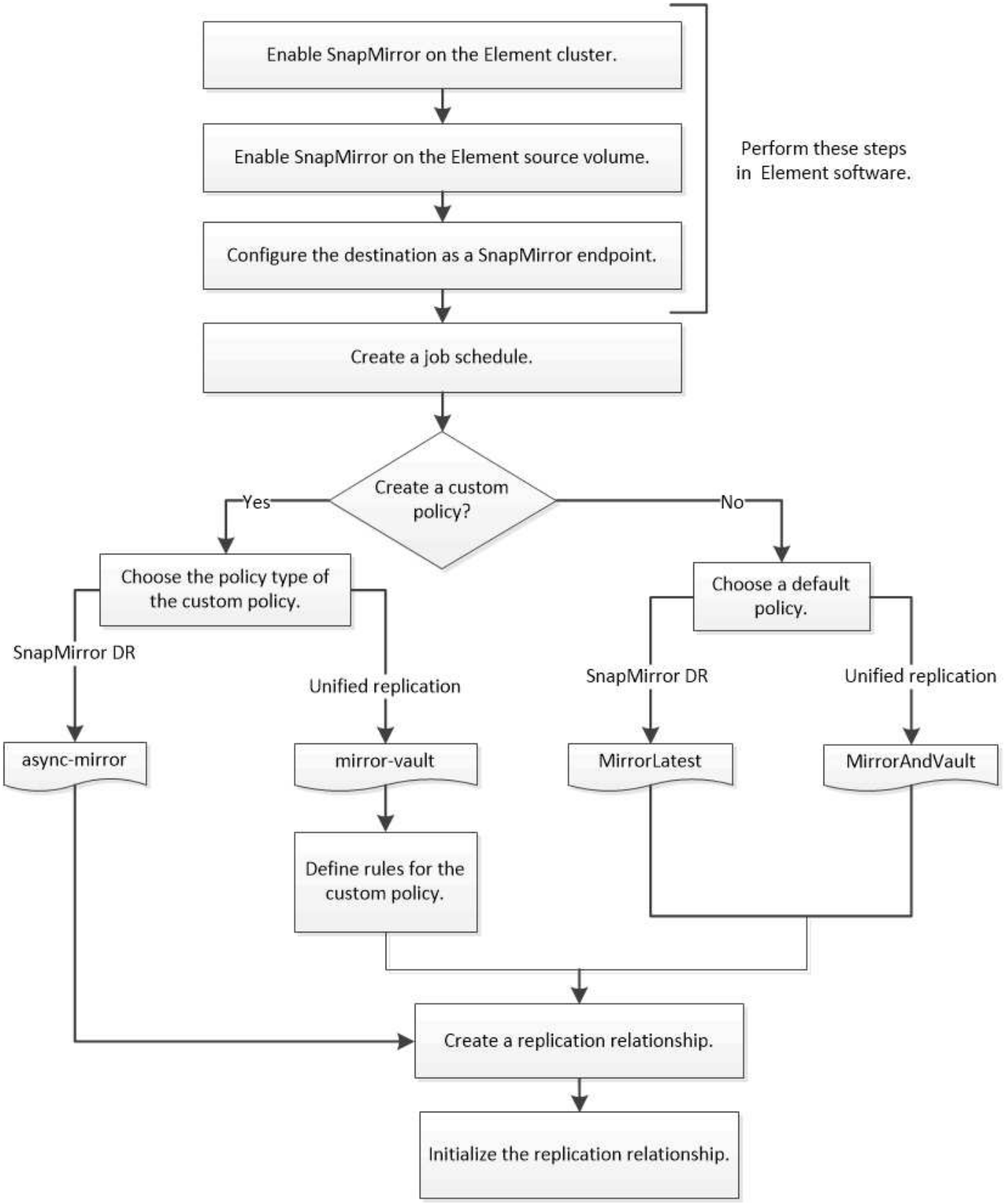
Recurso o función	Detalles de soporte
SnapMirror	• La función de restauración de SnapMirror no es compatible. • El `MirrorAllSnapshots` y `XDPDefault` Las políticas no son compatibles. • El tipo de política “vault” no es compatible. • La regla definida por el sistema “all_source_snapshots” no es compatible. • El tipo de política “mirror-vault” solo es compatible con la replicación desde el software Element a ONTAP. Utilice “async-mirror” para la replicación desde ONTAP al software Element. • El `-schedule` y `-prefix` opciones para `snapmirror policy add-rule` No son compatibles. • El `-preserve` y `-quick-resync` opciones para `snapmirror resync` No son compatibles. • La eficiencia del almacenamiento no se conserva. • No se admiten implementaciones de protección de datos en cascada ni de tipo fan-out.
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 del bloque de volumen debe ser de 512 bytes. No se admite un tamaño de bloque de 4K bytes. • El tamaño del volumen debe ser un múltiplo de 1 MiB. • Los atributos de volumen no se conservan. • El número máximo de copias de instantáneas que se replicarán es 30.
Red	• Se permite una única conexión TCP por transferencia. • El nodo Element debe especificarse como una dirección IP. La búsqueda de nombres de host DNS no es compatible. • Los espacios IP no son compatibles.
SnapLock	Los volúmenes SnapLock no son compatibles.
FlexGroup	Los volúmenes FlexGroup no son compatibles.
SVM DR	Los volúmenes ONTAP en una configuración SVM DR no son compatibles.
MetroCluster	Los volúmenes ONTAP en una configuración MetroCluster no son compatibles.

Flujo de trabajo para la replicación entre Element y ONTAP

Tanto si replica datos de Element a ONTAP como de ONTAP a Element, deberá configurar una programación de trabajos, especificar una política y crear e inicializar la relación. Puede utilizar una política predeterminada o personalizada.

El flujo de trabajo presupone que usted ha completado las tareas previas que se enumeran en"Prerrequisitos" . Para obtener información completa sobre las políticas de SnapMirror , incluyendo orientación sobre qué política utilizar, consulte"Resumen de protección de datos" .



Habilita SnapMirror en el software Element.

Habilite SnapMirror en el clúster de Element.

Debe habilitar SnapMirror en el clúster de Element antes de poder crear una relación de

replicación. Esta tarea solo se puede realizar en la interfaz web del software Element o utilizando "Método API".

Antes de empezar

- El clúster Element debe estar ejecutando el software NetApp Element versión 10.1 o posterior.
- SnapMirror solo se puede habilitar para clústeres Element utilizados con volúmenes NetApp ONTAP .

Acerca de esta tarea

El sistema Element viene con SnapMirror desactivado por defecto. SnapMirror no se habilita automáticamente como parte de una nueva instalación o actualización.

> Una vez activado, SnapMirror no se puede desactivar. Solo puedes desactivar la función SnapMirror y restaurar la configuración predeterminada devolviendo el clúster a la imagen de fábrica.

Pasos

1. Haz clic en **Clústeres** > **Configuración**.
2. Encuentre la configuración específica del clúster para SnapMirror.
3. Haz clic en **Habilitar SnapMirror**.

Habilite SnapMirror en el volumen de origen Element.

Debe habilitar SnapMirror en el volumen de origen Element antes de poder crear una relación de replicación. Esta tarea solo se puede realizar en la interfaz web del software Element o utilizando"Modificar volumen" y"Modificar volúmenes" Métodos de la API.

Antes de empezar

- Debes haber habilitado SnapMirror en el clúster Element.
- El tamaño del bloque de volumen debe ser de 512 bytes.
- El volumen no debe participar en la replicación remota de Element.
- El tipo de acceso al volumen no debe ser “Objetivo de replicación”.

Acerca de esta tarea

El procedimiento que se describe a continuación presupone que el volumen ya existe. También puedes habilitar SnapMirror al crear o clonar un volumen.

Pasos

1. Seleccione **Administración** > **Volúmenes**.
2. Seleccione el botón para el volumen.
3. En el menú desplegable, seleccione **Editar**.
4. En el cuadro de diálogo **Editar volumen**, seleccione **Habilitar SnapMirror**.
5. Seleccione **Guardar cambios**.

Crea un punto de conexión de SnapMirror

Debes crear un punto de conexión SnapMirror antes de poder crear una relación de replicación. Esta tarea solo se puede realizar en la interfaz web del software Element o

utilizando "Métodos de la API de SnapMirror".

Antes de empezar

Debes haber habilitado SnapMirror en el clúster Element.

Pasos

1. Haga clic en **Protección de datos** > *Puntos de conexión de SnapMirror *.
2. Haz clic en **Crear punto de conexión**.
3. En el cuadro de diálogo **Crear un nuevo punto de conexión**, introduzca la dirección IP de administración del clúster ONTAP .
4. Introduzca el ID de usuario y la contraseña del administrador del clúster ONTAP .
5. Haz clic en **Crear punto de conexión**.

Configurar una relación de replicación

Cree un programa de trabajo de replicación.

Tanto si replica datos de Element a ONTAP como de ONTAP a Element, deberá configurar una programación de trabajos, especificar una política y crear e inicializar la relación. Puede utilizar una política predeterminada o personalizada.

Puedes usar el `job schedule cron create` comando para crear una programación de trabajos de replicación. La programación de tareas determina cuándo SnapMirror actualiza automáticamente la relación de protección de datos a la que está asignada dicha programación.

Acerca de esta tarea

Se asigna un cronograma de trabajo al crear una relación de protección de datos. Si no asigna un horario de trabajo, deberá actualizar la relación manualmente.

Paso

1. Crear un horario 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` , puedes especificar `all` para ejecutar el trabajo cada mes, día de la semana y hora, respectivamente.

   A partir de ONTAP 9.10.1, puede incluir el Vserver en su planificación de trabajos:

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

   El siguiente ejemplo crea una programación de trabajos llamada `my_weekly` que se emite los sábados a las 3:00 am:

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

Crear una política de replicación personalizada

Puede utilizar una política predeterminada o personalizada al crear una relación de replicación. Para una política de replicación unificada personalizada, debe definir una o más *reglas* que determinen qué copias de instantáneas se transfieren durante la inicialización y la actualización.

Puede crear una política de replicación personalizada si la política predeterminada para una relación no es adecuada. Es posible que desee comprimir los datos en una transferencia de red, por ejemplo, o modificar el número de intentos que realiza SnapMirror para transferir copias de instantáneas.

Acerca de esta tarea

El *tipo de política* de la política de replicación determina el tipo de relación que admite. La tabla siguiente muestra los tipos de pólizas disponibles.

Tipo de póliza	Tipo de relación
espejo asíncrono	SnapMirror DR
bóveda de espejos	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 conocer la sintaxis completa del comando, consulte la página del manual.

   A partir de ONTAP 9.5, puede especificar la programación para crear una programación de copia de instantánea común para las relaciones síncronas de SnapMirror mediante el uso de `-common-snapshot-schedule` parámetro. Por defecto, la programación común de copia de instantáneas para las relaciones síncronas de SnapMirror es de una hora. Puede especificar un valor de entre 30 minutos y dos horas para la programación de copia de instantáneas para las relaciones síncronas de SnapMirror .

   El siguiente ejemplo crea una política de replicación personalizada para SnapMirror DR que habilita 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
   ```

   El siguiente ejemplo 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

Para los tipos de políticas “mirror-vault”, debe definir reglas que determinen qué copias de instantáneas se transfieren durante la inicialización y la actualización.

Utilice el `snapmirror policy show` comando para verificar que se creó la política de SnapMirror . Para conocer la sintaxis completa del comando, consulte la página del manual.

Defina una regla para una política

Para las políticas personalizadas con el tipo de política “mirror-vault”, debe definir al menos una regla que determine qué copias de instantáneas se transfieren durante la inicialización y la actualización. También puede definir reglas para políticas predeterminadas con el tipo de política “mirror-vault”.

Acerca de esta tarea

Cada política con el tipo de política “mirror-vault” debe tener una regla que especifique qué copias de instantáneas replicar. La regla “bimensual”, por ejemplo, indica que solo deben replicarse las copias de instantáneas a las que se les haya asignado la etiqueta SnapMirror “bimensual”. La etiqueta SnapMirror se asigna al configurar las copias de instantáneas de Element.

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

regla definida por el sistema	Utilizado en tipos de políticas	Resultado
sm_creado	espejo asíncrono, bóveda de espejos	Una copia instantánea creada por SnapMirror se transfiere durante la inicialización y la actualización.
a diario	bóveda de espejos	Las nuevas copias de instantáneas en la fuente con la etiqueta SnapMirror “daily” se transfieren durante la inicialización y la actualización.
semanalmente	bóveda de espejos	Las nuevas copias de instantáneas en la fuente con la etiqueta SnapMirror “weekly” se transfieren durante la inicialización y la actualización.

mensual	bóveda de espejos	Las nuevas copias de instantáneas en la fuente con la etiqueta SnapMirror “mensual” se transfieren durante la inicialización y la actualización.

Puede especificar reglas adicionales según sea necesario, para políticas predeterminadas o personalizadas. Por ejemplo:

- Por defecto `MirrorAndVault` En cuanto a la política, podría crear una regla llamada “bimensual” para que coincidan las copias de instantáneas en la fuente con la etiqueta SnapMirror “bimensual”.
- Para una política personalizada con el tipo de política “mirror-vault”, puede crear una regla llamada “bi-weekly” para que coincida con las copias de instantáneas en el origen con la etiqueta SnapMirror “bi-weekly”.

Paso

1. Defina una regla para una política:

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

   Para conocer la sintaxis completa del comando, consulte la página del manual.

   El siguiente ejemplo agrega una regla con la etiqueta SnapMirror. `bi-monthly` al valor predeterminado `MirrorAndVault` política:

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

   El siguiente ejemplo agrega una regla con la etiqueta SnapMirror. `bi-weekly` a la costumbre `my_snapvault` política:

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

   El siguiente ejemplo agrega una regla con la etiqueta SnapMirror. `app_consistent` a la costumbre `Sync` política:

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

   A continuación, puede replicar copias de instantáneas 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
```

Crear una relación de replicación

Cree una relación desde un origen Element a un destino ONTAP .

La relación entre el volumen de origen en el almacenamiento primario y el volumen de destino en el almacenamiento secundario se denomina *relación de protección de datos*. Puedes usar el `snapmirror create` comando para crear una relación de protección de datos desde una fuente Element a un destino ONTAP , o desde una fuente ONTAP a un destino Element.

Puede utilizar SnapMirror para replicar copias de instantáneas de un volumen Element en un sistema de destino ONTAP . En caso de desastre en el sitio de Element, puede proporcionar datos a los clientes desde el sistema ONTAP y luego reactivar el volumen de origen de Element cuando se restablezca el servicio.

Antes de empezar

- El nodo Element que contiene el volumen que se va a replicar debe haber sido hecho accesible para ONTAP.
- El volumen Element debe haber estado habilitado para la replicación SnapMirror .
- Si está utilizando el tipo de política “mirror-vault”, debe haberse configurado una etiqueta SnapMirror para que se repliquen las copias de instantáneas de Element.

> Solo puedes realizar esta tarea en el"Interfaz web del software Element" o utilizando el"Métodos API" .

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 Element es aproximadamente equivalente a un 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 los datos a una LUN existente si la LUN cumple los requisitos para la replicación desde el software Element a ONTAP.

Las reglas de replicación son las siguientes:

- Un volumen ONTAP solo puede contener datos de un volumen Element.
- No se pueden replicar datos de un volumen ONTAP a varios volúmenes Element.

En ONTAP 9.3 y versiones anteriores, un volumen de destino puede contener hasta 251 copias de instantáneas. En ONTAP 9.4 y versiones posteriores, un volumen de destino puede contener hasta 1019 copias de instantáneas.

Paso

1. Desde el clúster de destino, cree una relación de replicación desde un origen Element a un destino ONTAP :

```
snapmirror create -source-path <hostip:>/lun/<name> -destination-path
<SVM:volume>|<cluster://SVM/volume> -type XDP -schedule schedule -policy
<policy>
```

Para conocer la sintaxis completa del comando, consulte la página del manual.

El siguiente ejemplo crea una relación de recuperación ante desastres de SnapMirror utilizando la configuración predeterminada. `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
```

El siguiente ejemplo crea una relación de replicación unificada utilizando la configuración 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
```

El siguiente ejemplo crea una relación de replicación unificada utilizando `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
```

El siguiente ejemplo crea una relación de replicación unificada utilizando la opción personalizada. `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 el `snapmirror show` comando para verificar que se creó la relación SnapMirror . Para conocer la sintaxis completa del comando, consulte la página del manual.

Cree una relación desde un origen ONTAP a un destino Element.

A partir de ONTAP 9.4, puede usar SnapMirror para replicar copias de instantáneas de una LUN creada en una fuente ONTAP de vuelta a un destino Element. Es posible que esté utilizando la LUN para migrar datos desde ONTAP al software Element.

Antes de empezar

- El nodo de destino del elemento debe haber sido hecho accesible para ONTAP.
- El volumen Element debe haber estado habilitado para la replicación 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 “async-mirror”.

  Puede utilizar una política predeterminada o personalizada.

- Solo se admiten LUN iSCSI.
- No se puede replicar más de un LUN desde un volumen ONTAP a un volumen Element.
- No se puede replicar un LUN desde un volumen ONTAP a varios volúmenes Element.

Paso

1. Cree una relación de replicación desde un origen ONTAP a un destino Element:

   ```
   snapmirror create -source-path <SVM:volume>|<cluster://SVM/volume>
   -destination-path <hostip:>/lun/<name> -type XDP -schedule schedule -policy
   <policy>
   ```

   Para conocer la sintaxis completa del comando, consulte la página del manual.

   El siguiente ejemplo crea una relación de recuperación ante desastres de SnapMirror utilizando la configuración predeterminada. `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
   ```

   El siguiente ejemplo crea una relación de recuperación ante desastres de SnapMirror utilizando la configuración personalizada. `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 el `snapmirror show` comando para verificar que se creó la relación SnapMirror . Para conocer la sintaxis completa del comando, consulte la página del manual.

Inicializar una relación de replicación

Para todos los tipos de relaciones, la inicialización realiza una *transferencia de línea*

base: crea una copia instantánea del volumen de origen y luego transfiere esa copia y todos los bloques de datos a los que hace referencia al volumen de destino.

Antes de empezar

- El nodo Element que contiene el volumen que se va a replicar debe haber sido hecho accesible para ONTAP.
- El volumen Element debe haber estado habilitado para la replicación SnapMirror .
- Si está utilizando el tipo de política “mirror-vault”, debe haberse configurado una etiqueta SnapMirror para que se repliquen las copias de instantáneas de Element.

Solo puedes realizar esta tarea en el"Interfaz web del software Element" o utilizando el"Métodos API" .

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 llevar mucho tiempo. Quizás te interese realizar la transferencia de referencia en horas de menor tráfico.

Si la inicialización de una relación desde una fuente ONTAP a un destino Element falla por cualquier motivo, seguirá fallando incluso después de que haya corregido el problema (un nombre de LUN no válido, por ejemplo). La solución alternativa es la siguiente:

1. Eliminar la relación.
2. Elimine el volumen de destino del elemento.
3. Crea un nuevo volumen de destino de Elemento.
4. Cree e inicialice una nueva relación desde la fuente ONTAP al volumen de destino Element.

Paso

1. Inicializar una relación de replicación:

   ```
   snapmirror initialize -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume|cluster://SVM/volume>
   ```

   Para conocer la sintaxis completa del comando, consulte la página del manual.

   El siguiente ejemplo inicializa la relación entre el volumen fuente `0005` en la dirección IP 10.0.0.11 y el volumen de destino `volA_dst` en `svm_backup` :

   ```
   cluster_dst::> snapmirror initialize -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

Servir datos desde un volumen de destino de SnapMirror DR

Haga que el volumen de destino sea escribible.

Cuando un desastre inhabilita el sitio principal para una relación de recuperación ante desastres de SnapMirror , puede servir datos desde el volumen de destino con una interrupción mínima. Puede reactivar el volumen de origen cuando se restablezca el servicio en el sitio principal.

Debes hacer que el volumen de destino sea escribible antes de poder servir datos desde el volumen a los clientes. Puedes usar el `snapmirror quiesce` comando para detener las transferencias programadas al destino, el `snapmirror abort` orden de detener las transferencias en curso, y la `snapmirror break` comando para hacer que el destino sea escribible.

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. Suspender los traslados programados al destino:

   ```
   snapmirror quiesce -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume>|<cluster://SVM/volume>
   ```

   Para conocer la sintaxis completa del comando, consulte la página del manual.

   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` en `svm_backup` :

   ```
   cluster_dst::> snapmirror quiesce -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

2. Detener las transferencias en curso al destino:

   ```
   snapmirror abort -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume>|<cluster://SVM/volume>
   ```

   Para conocer la sintaxis completa del comando, consulte la página del manual.

   El siguiente ejemplo detiene las transferencias en curso entre el volumen de origen `0005` en la dirección IP 10.0.0.11 y el volumen de destino `volA_dst` en `svm_backup` :

   ```
   cluster_dst::> snapmirror abort -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

3. Romper la relación de recuperación ante desastres de SnapMirror :

   ```
   snapmirror break -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume>|<cluster://SVM/volume>
   ```

   Para conocer la sintaxis completa del comando, consulte la página del manual.

El siguiente ejemplo rompe la relación entre el volumen de origen `0005` en la dirección IP 10.0.0.11 y el volumen de destino `volA_dst` en `svm_backup` y el volumen de destino `volA_dst` en `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 el acceso a datos.

Después de habilitar la escritura en el volumen de destino, debe configurar el volumen para el acceso a los datos. Los hosts SAN pueden acceder a los datos del volumen de destino hasta que se reactive el volumen de origen.

1. Asigne el LUN del elemento al grupo iniciador apropiado.
2. Cree sesiones iSCSI desde los iniciadores del host SAN a las LIF de la SAN.
3. En el cliente SAN, realice un nuevo escaneo de almacenamiento para detectar la LUN conectada.

Reactivar el volumen de la fuente original

Puede restablecer la relación original de protección de datos entre los volúmenes de origen y destino cuando ya no necesite servir datos desde el destino.

Acerca de esta tarea

El procedimiento que se describe a continuación presupone que la línea base en el volumen de la fuente original está intacta. Si la línea base no está intacta, debe crear e inicializar la relación entre el volumen desde el que está sirviendo 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 de instantáneas de una LUN creadas mientras se sirven datos desde el destino ONTAP se replican automáticamente cuando se reactiva la fuente Element.

Las reglas de replicación son las siguientes:

- Solo se admiten LUN iSCSI.
- No se puede replicar más de un LUN desde un volumen ONTAP a un volumen Element.
- No se puede replicar un LUN desde un volumen ONTAP a varios volúmenes Element.

Pasos

1. Eliminar la relación original de protección de datos:

   ```
   snapmirror delete -source-path <SVM:volume>|<cluster://SVM/volume>
   -destination-path <hostip:>/lun/<name> -policy <policy>
   ```

   Para conocer la sintaxis completa del comando, consulte la página del manual.

   El siguiente ejemplo elimina la relación con el volumen fuente original, `0005` en la dirección IP 10.0.0.11 y el volumen desde el que está sirviendo datos, `volA_dst` en `svm_backup` :

```
cluster_dst::> snapmirror delete -source-path 10.0.0.11:/lun/0005
-policy MirrorLatest -destination-path svm_backup:volA_dst
```

2. Invertir la relación original de protección de datos:

   ```
   snapmirror resync -source-path <SVM:volume>|<cluster://SVM/volume>
   -destination-path <hostip:>/lun/<name> -policy <policy>
   ```

   Para conocer la sintaxis completa del comando, consulte la página del manual.

   Aunque la resincronización no requiere una transferencia de referencia, puede llevar mucho tiempo. Quizás te convenga ejecutar la resincronización en horas de menor actividad.

   El siguiente ejemplo invierte la relación entre el volumen de la fuente original, `0005` en la dirección IP 10.0.0.11 y el volumen desde el que está sirviendo datos, `volA_dst` en `svm_backup` :

   ```
   cluster_dst::> snapmirror resync -source-path svm_backup:volA_dst
   -destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
   ```

3. Actualizar la relación inversa:

   ```
   snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>
   -destination-path <hostip:>/lun/<name>
   ```

   Para conocer la sintaxis completa del comando, consulte la página del manual.

   > El comando falla si no existe una copia de instantánea común en el origen y el destino. Usar `snapmirror initialize` para reiniciar la relación.

   El siguiente ejemplo actualiza la relación entre el volumen desde el que se sirven los datos, `volA_dst` en `svm_backup` , y el volumen fuente 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. Detener las transferencias programadas para la relación inversa:

   ```
   snapmirror quiesce -source-path <SVM:volume>|<cluster://SVM/volume>
   -destination-path <hostip:>/lun/<name>
   ```

   Para conocer la sintaxis completa del comando, consulte la página del manual.

   El siguiente ejemplo detiene las transferencias programadas entre el volumen desde el que se están sirviendo los datos, `volA_dst` en `svm_backup` , y el volumen fuente 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. Detener las transferencias en curso para la relación inversa:

   `snapmirror abort -source-path <SVM:volume>|<cluster://SVM/volume> -destination -path <hostip:>/lun/<name>`

   Para conocer la sintaxis completa del comando, consulte la página del manual.

   El siguiente ejemplo detiene las transferencias en curso entre el volumen desde el que se están sirviendo los datos, `volA_dst` en `svm_backup` , y el volumen fuente 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. Romper la relación inversa:

   `snapmirror break -source-path <SVM:volume>|<cluster://SVM/volume> -destination -path <hostip:>/lun/<name>`

   Para conocer la sintaxis completa del comando, consulte la página del manual.

   El siguiente ejemplo rompe la relación entre el volumen desde el que se sirven los datos, `volA_dst` en `svm_backup` , y el volumen fuente 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. Eliminar la relación de protección de datos invertida:

   `snapmirror delete -source-path <SVM:volume>|<cluster://SVM/volume> -destination-path <hostip:>/lun/<name> -policy <policy>`

   Para conocer la sintaxis completa del comando, consulte la página del manual.

   El siguiente ejemplo elimina la relación inversa entre el volumen fuente original, `0005` en la dirección IP 10.0.0.11 y el volumen desde el que está sirviendo datos, `volA_dst` en `svm_backup` :

```
cluster_src::> snapmirror delete -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
```

8. Restablecer la relación original de protección de datos:

   `snapmirror resync -source-path <hostip:>/lun/<name> -destination-path <SVM:volume>|<cluster://SVM/volume>`

Para conocer la sintaxis completa del comando, consulte la página del manual.

El siguiente ejemplo restablece la relación entre el volumen fuente original, `0005` en la dirección IP 10.0.0.11 y el volumen de destino original, `volA_dst` en `svm_backup` :

```
cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst
```

Después de terminar

Utilice el `snapmirror show` comando para verificar que se creó la relación SnapMirror . Para conocer la sintaxis completa del comando, consulte la página del manual.

Actualizar manualmente una relación de replicación.

Es posible que deba actualizar manualmente una relación de replicación si una actualización falla 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. Actualizar manualmente una relación de replicación:

   ```
   snapmirror update -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume>|<cluster://SVM/volume>
   ```

   Para conocer la sintaxis completa del comando, consulte la página del manual.

   > El comando falla si no existe una copia de instantánea común en el origen y el destino. Usar `snapmirror initialize` para reiniciar la relación.

   El siguiente ejemplo actualiza la relación entre el volumen de origen `0005` en la dirección IP 10.0.0.11 y el volumen de destino `volA_dst` en `svm_backup` :

   ```
   cluster_src::> snapmirror update -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

Resincronizar una relación de replicación

Es necesario resincronizar una relación de replicación después de hacer que un volumen de destino sea escribible, después de que falle una actualización porque no existe una copia Snapshot común en los volúmenes de origen y destino, o si se desea cambiar la política de replicación para la relación.

Acerca de esta tarea

Aunque la resincronización no requiere una transferencia de referencia, puede llevar mucho tiempo. Quizás te convenga 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. Resincronizar 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 conocer la sintaxis completa del comando, consulte la página del manual.

   El siguiente ejemplo resincroniza la relación entre el volumen de origen `0005` en la dirección IP 10.0.0.11 y el volumen de destino `volA_dst` en `svm_backup` :

   ```
   cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005
   -policy MirrorLatest -destination-path svm_backup:volA_dst
   ```

Copia de seguridad y restauración de volúmenes

Copia de seguridad y restauración de volúmenes

Puede realizar copias de seguridad y restaurar volúmenes en otros almacenamientos SolidFire , así como en almacenes de objetos secundarios compatibles con Amazon S3 u OpenStack Swift.

Al restaurar volúmenes desde OpenStack Swift o Amazon S3, se necesita la información del manifiesto del proceso de copia de seguridad original. Si está restaurando un volumen del que se realizó una copia de seguridad en un sistema de almacenamiento SolidFire , no se requiere información de manifiesto.

Encuentra más información

- Realizar una copia de seguridad de un volumen en un almacenamiento de objetos de Amazon S3
- Realizar una copia de seguridad de un volumen en un almacén de objetos Swift de OpenStack
- Realizar una copia de seguridad de un volumen en un clúster de almacenamiento SolidFire
- Restaurar un volumen desde una copia de seguridad en un almacenamiento de objetos de Amazon S3
- Restaurar un volumen desde una copia de seguridad en un almacén de objetos OpenStack Swift
- Restaurar un volumen desde una copia de seguridad en un clúster de almacenamiento SolidFire

Realizar una copia de seguridad de un volumen en un almacenamiento de objetos de Amazon S3

Puede realizar copias de seguridad de volúmenes en almacenes de objetos externos que sean compatibles con Amazon S3.

1. Haz clic en **Administración** > **Volúmenes**.

2. Haz clic en el icono Acciones del volumen que deseas respaldar.
3. En el menú resultante, haga clic en **Realizar copia de seguridad en**.
4. En el cuadro de diálogo **Copia de seguridad integrada**, en **Realizar copia de seguridad en**, seleccione **S3**.
5. Seleccione una opción en **Formato de datos**:
   - **Nativo**: Un formato comprimido legible únicamente por los sistemas de almacenamiento SolidFire .
   - **Sin comprimir**: Un formato sin comprimir compatible con otros sistemas.
6. Introduzca un nombre de host para acceder al almacén de objetos en el campo **Nombre de host**.
7. Introduzca un ID de clave de acceso para la cuenta en el campo **ID de clave de acceso**.
8. Introduzca la clave de acceso secreta de la cuenta en el campo **Clave de acceso secreta**.
9. Introduzca el bucket de S3 en el que se almacenará la copia de seguridad en el campo **Bucket de S3**.
10. Introduzca una etiqueta de identificación para añadir al prefijo en el campo **Etiqueta de identificación**.
11. Haz clic en **Iniciar lectura**.

Realizar una copia de seguridad de un volumen en un almacén de objetos Swift de OpenStack

Puede realizar copias de seguridad de volúmenes en almacenes de objetos externos que sean compatibles con OpenStack Swift.

1. Haz clic en **Administración** > **Volúmenes**.
2. Haz clic en el icono de Acciones del volumen que deseas respaldar.
3. En el menú resultante, haga clic en **Realizar copia de seguridad en**.
4. En el cuadro de diálogo **Copia de seguridad integrada**, en **Realizar copia de seguridad en**, seleccione **Swift**.
5. Seleccione un formato de datos en **Formato de datos**:
   - **Nativo**: Un formato comprimido legible únicamente por los sistemas de almacenamiento SolidFire .
   - **Sin comprimir**: Un formato sin comprimir compatible con otros sistemas.
6. Introduzca una URL para acceder al almacén de objetos en el campo **URL**.
7. Introduzca un nombre de usuario para la cuenta en el campo **Nombre de usuario**.
8. Introduzca la clave de autenticación de la cuenta en el campo **Clave de autenticación**.
9. Introduzca el contenedor en el que desea almacenar la copia de seguridad en el campo **Contenedor**.
10. **Opcional**: Introduzca una etiqueta de nombre para añadir al prefijo en el campo **Etiqueta de nombre**.
11. Haz clic en **Iniciar lectura**.

Realizar una copia de seguridad de un volumen en un clúster de almacenamiento SolidFire

Puede realizar copias de seguridad de los volúmenes que residen en un clúster en un clúster remoto para clústeres de almacenamiento que ejecutan el software Element.

Asegúrese de que los clústeres de origen y destino estén emparejados.

Ver"Agrupaciones de pares para replicación" .

Al realizar copias de seguridad o restauraciones de un clúster a otro, el sistema genera una clave que se utilizará para la autenticación entre los clústeres. Esta clave de escritura de volumen masivo permite que el clúster de origen se autentique con el clúster de destino, proporcionando un nivel de seguridad al escribir en el volumen de destino. Como parte del proceso de copia de seguridad o restauración, debe generar una clave de escritura de volumen masivo desde el volumen de destino antes de iniciar la operación.

1. En el clúster de destino, **Administración** > **Volúmenes**.
2. Haz clic en el icono Acciones del volumen de destino.
3. En el menú que aparece, haga clic en **Restaurar desde**.
4. En el cuadro de diálogo **Restauración integrada**, en **Restaurar desde**, seleccione * SolidFire*.
5. Seleccione una opción en **Formato de datos**:
   - **Nativo**: Un formato comprimido legible únicamente por los sistemas de almacenamiento SolidFire .
   - **Sin comprimir**: Un formato sin comprimir compatible con otros sistemas.
6. Haz clic en **Generar clave**.
7. Copie la clave del cuadro **Clave de escritura de volumen masivo** al portapapeles.
8. En el clúster de origen, vaya a **Administración** > **Volúmenes**.
9. Haz clic en el icono de Acciones del volumen que deseas respaldar.
10. En el menú resultante, haga clic en **Realizar copia de seguridad en**.
11. En el cuadro de diálogo **Copia de seguridad integrada**, en **Realizar copia de seguridad en**, seleccione * SolidFire*.
12. Seleccione la misma opción que seleccionó anteriormente en el campo **Formato de datos**.
13. Introduzca la dirección IP virtual de gestión del clúster del volumen de destino en el campo **MVIP de clúster remoto**.
14. Introduzca el nombre de usuario del clúster remoto en el campo **Nombre de usuario del clúster remoto**.
15. Introduzca la contraseña del clúster remoto en el campo **Contraseña del clúster remoto**.
16. En el campo **Clave de escritura de volumen masivo**, pegue la clave que generó anteriormente en el clúster de destino.
17. Haz clic en **Iniciar lectura**.

Restaurar un volumen desde una copia de seguridad en un almacenamiento de objetos de Amazon S3

Puede restaurar un volumen desde una copia de seguridad en un almacenamiento de objetos de Amazon S3.

1. Haz clic en **Informes** > **Registro de eventos**.
2. Localice el evento de copia de seguridad que creó la copia de seguridad que necesita restaurar.
3. En la columna **Detalles** del evento, haga clic en **Mostrar detalles**.
4. Copie la información del manifiesto al portapapeles.
5. Haz clic en **Administración** > **Volúmenes**.
6. Haz clic en el icono Acciones del volumen que deseas restaurar.
7. En el menú que aparece, haga clic en **Restaurar desde**.
8. En el cuadro de diálogo **Restauración integrada**, en **Restaurar desde**, seleccione **S3**.

9. Seleccione la opción que coincida con la copia de seguridad en **Formato de datos**:
    - **Nativo**: Un formato comprimido legible únicamente por los sistemas de almacenamiento SolidFire .
    - **Sin comprimir**: Un formato sin comprimir compatible con otros sistemas.
10. Introduzca un nombre de host para acceder al almacén de objetos en el campo **Nombre de host**.
11. Introduzca un ID de clave de acceso para la cuenta en el campo **ID de clave de acceso**.
12. Introduzca la clave de acceso secreta de la cuenta en el campo **Clave de acceso secreta**.
13. Introduzca el bucket de S3 en el que se almacenará la copia de seguridad en el campo **Bucket de S3**.
14. Pegue la información del manifiesto en el campo **Manifiesto**.
15. Haz clic en **Comenzar a escribir**.

Restaurar un volumen desde una copia de seguridad en un almacén de objetos OpenStack Swift

Puede restaurar un volumen desde una copia de seguridad en un almacén de objetos OpenStack Swift.

1. Haz clic en **Informes** > **Registro de eventos**.
2. Localice el evento de copia de seguridad que creó la copia de seguridad que necesita restaurar.
3. En la columna **Detalles** del evento, haga clic en **Mostrar detalles**.
4. Copie la información del manifiesto al portapapeles.
5. Haz clic en **Administración** > **Volúmenes**.
6. Haz clic en el icono Acciones del volumen que deseas restaurar.
7. En el menú que aparece, haga clic en **Restaurar desde**.
8. En el cuadro de diálogo **Restauración integrada**, en **Restaurar desde**, seleccione **Swift**.
9. Seleccione la opción que coincida con la copia de seguridad en **Formato de datos**:
    - **Nativo**: Un formato comprimido legible únicamente por los sistemas de almacenamiento SolidFire .
    - **Sin comprimir**: Un formato sin comprimir compatible con otros sistemas.
10. Introduzca una URL para acceder al almacén de objetos en el campo **URL**.
11. Introduzca un nombre de usuario para la cuenta en el campo **Nombre de usuario**.
12. Introduzca la clave de autenticación de la cuenta en el campo **Clave de autenticación**.
13. Introduzca el nombre del contenedor en el que se almacena la copia de seguridad en el campo **Contenedor**.
14. Pegue la información del manifiesto en el campo **Manifiesto**.
15. Haz clic en **Comenzar a escribir**.

Restaurar un volumen desde una copia de seguridad en un clúster de almacenamiento SolidFire

Puede restaurar un volumen desde una copia de seguridad en un clúster de almacenamiento SolidFire .

Al realizar copias de seguridad o restauraciones de un clúster a otro, el sistema genera una clave que se utilizará para la autenticación entre los clústeres. Esta clave de escritura de volumen masivo permite que el clúster de origen se autentique con el clúster de destino, proporcionando un nivel de seguridad al escribir en el

volumen de destino. Como parte del proceso de copia de seguridad o restauración, debe generar una clave de escritura de volumen masivo desde el volumen de destino antes de iniciar la operación.

1. En el clúster de destino, haga clic en **Administración** > **Volúmenes**.
2. Haz clic en el icono Acciones del volumen que deseas restaurar.
3. En el menú que aparece, haga clic en **Restaurar desde**.
4. En el cuadro de diálogo **Restauración integrada**, en **Restaurar desde**, seleccione * SolidFire*.
5. Seleccione la opción que coincida con la copia de seguridad en **Formato de datos**:
   - **Nativo**: Un formato comprimido legible únicamente por los sistemas de almacenamiento SolidFire .
   - **Sin comprimir**: Un formato sin comprimir compatible con otros sistemas.
6. Haz clic en **Generar clave**.
7. Copie la información de la **Clave de escritura de volumen masivo** al portapapeles.
8. En el clúster de origen, haga clic en **Administración** > **Volúmenes**.
9. Haz clic en el icono Acciones del volumen que deseas usar para la restauración.
10. En el menú resultante, haga clic en **Realizar copia de seguridad en**.
11. En el cuadro de diálogo **Copia de seguridad integrada**, seleccione * SolidFire* en **Realizar copia de seguridad en**.
12. Seleccione la opción que coincida con la copia de seguridad en **Formato de datos**.
13. Introduzca la dirección IP virtual de gestión del clúster del volumen de destino en el campo **MVIP de clúster remoto**.
14. Introduzca el nombre de usuario del clúster remoto en el campo **Nombre de usuario del clúster remoto**.
15. Introduzca la contraseña del clúster remoto en el campo **Contraseña del clúster remoto**.
16. Pegue la clave desde su portapapeles en el campo **Clave de escritura de volumen masivo**.
17. Haz clic en **Iniciar lectura**.

Configurar dominios de protección personalizados

Para los clústeres de Element que contienen más de dos nodos de almacenamiento, puede configurar dominios de protección personalizados para cada nodo. Cuando configure dominios de protección personalizados, deberá asignar todos los nodos del clúster a un dominio.

Cuando se asignan dominios de protección, se inicia una sincronización de datos entre nodos y algunas operaciones del clúster no están disponibles hasta que se complete la sincronización de datos. Después de configurar un dominio de protección personalizado para un clúster, cuando agregue un nuevo nodo de almacenamiento, no podrá agregar unidades para el nuevo nodo hasta que le asigne un dominio de protección y permita que se complete la sincronización de datos. Visita el"Documentación de dominios de protección" Para obtener más información sobre los dominios de protección.

Para que un esquema de dominio de protección personalizado sea útil para un clúster, todos los nodos de almacenamiento dentro de cada chasis deben estar asignados al mismo dominio de protección personalizado. Debe crear tantos dominios de protección personalizados como sean necesarios para que esto ocurra (el esquema de dominio de protección personalizado más pequeño posible es de tres dominios). Como práctica recomendada, configure el mismo número de nodos por dominio y procure que cada nodo asignado a un dominio en particular sea del mismo tipo.

Pasos

1. Haz clic en **Clúster** > **Nodos**.
2. Haga clic en **Configurar dominios de protección**.

   En la ventana **Configurar dominios de protección personalizados**, puede ver los dominios de protección configurados actualmente (si los hay), así como las asignaciones de dominios de protección para nodos individuales.

3. Introduzca un nombre para el nuevo dominio de protección personalizado y haga clic en **Crear**.

   Repita este paso para todos los nuevos dominios de protección que necesite crear.

4. Para cada nodo de la lista **Asignar nodos**, haga clic en el menú desplegable de la columna **Dominio de protección** y seleccione un dominio de protección para asignar a ese nodo.

   Asegúrese de comprender la disposición de su nodo y chasis, el esquema de dominio de protección personalizado que ha configurado y los efectos del esquema en la protección de datos antes de aplicar los cambios. Si aplica un esquema de dominio de protección e inmediatamente necesita realizar cambios, podría pasar algún tiempo antes de que pueda hacerlo debido a la sincronización de datos que se produce una vez que se aplica una configuración.

5. Haga clic en **Configurar dominios de protección**.

Resultado

Dependiendo del tamaño de su clúster, la sincronización de datos entre dominios podría tardar algún tiempo. Una vez completada la sincronización de datos, puede ver las asignaciones de dominio de protección personalizadas en la página **Clúster** > **Nodos**, y el panel de la interfaz de usuario web de Element muestra el estado de protección del clúster en el panel **Estado del dominio de protección personalizado**.

Posibles errores

Aquí tienes algunos errores que podrías ver después de aplicar una configuración de dominio de protección personalizada:

Error	Descripción	Resolución
Falló SetProtectionDomainLayout: ProtectionDomainLayout dejaría el NodeID {9} inutilizable. No se pueden usar nombres predeterminados y no predeterminados al mismo tiempo.	Un nodo no tiene asignado un dominio de protección.	Asigne un dominio de protección al nodo.

Error al establecer el diseño del dominio de protección: el tipo de dominio de protección 'custom' divide el tipo de dominio de protección 'chassis'.	A un nodo en un chasis multinodo se le asigna un Dominio de Protección diferente al de los demás nodos del chasis.	Asegúrese de que todos los nodos del chasis tengan asignado el mismo dominio de protección.

Encuentra más información

- "Dominios de protección personalizados"
- "Gestiona el almacenamiento con la API de Element"

Soluciona los problemas de tu sistema

Eventos del sistema

Ver información sobre eventos del sistema

Puedes ver información sobre diversos eventos detectados en el sistema. El sistema actualiza los mensajes de eventos cada 30 segundos. El registro de eventos muestra los eventos clave del clúster.

1. En la interfaz de usuario de Element, seleccione **Informes** > **Registro de eventos**.

   Para cada evento, verá la siguiente información:

Artículo	Descripción
IDENTIFICACIÓN	Identificador único asociado a cada evento.
Tipo de evento	El tipo de evento que se registra, por ejemplo, eventos de API o eventos de clonación.
Mensaje	Mensaje asociado al evento.
Detalles	Información que ayuda a identificar por qué ocurrió el suceso.
Service ID	El servicio que informó del suceso (si procede).
Node	El nodo que informó del evento (si corresponde).
ID de unidad	La unidad que informó del evento (si corresponde).
Hora del evento	La hora en que ocurrió el suceso.

Encuentra más información

Tipos de eventos

Tipos de eventos

El sistema informa de múltiples tipos de eventos; cada evento es una operación que el sistema ha completado. Los eventos pueden ser rutinarios, normales o que requieran la atención del administrador. La columna "Tipos de evento" en la página del registro de eventos indica en qué parte del sistema ocurrió el evento.

El sistema no registra los comandos de API de solo lectura en el registro de eventos.

La siguiente lista describe los tipos de eventos que aparecen en el registro de eventos:

- **apiEvent**

  Eventos iniciados por un usuario a través de una API o interfaz web que modifican la configuración.

- **binAssignmentsEvent**

  Eventos relacionados con la asignación de intervalos de datos. Los bins son esencialmente contenedores que almacenan datos y se distribuyen por todo el clúster.

- **binSyncEvent**

  Eventos del sistema relacionados con una reasignación de datos entre servicios de bloques.

- **bsCheckEvent**

  Eventos del sistema relacionados con comprobaciones de servicio de bloqueo.

- **bsKillEvent**

  Eventos del sistema relacionados con la finalización del servicio de bloqueo.

- **Evento de operación masiva**

  Eventos relacionados con operaciones realizadas en un volumen completo, como una copia de seguridad, restauración, instantánea o clonación.

- **clonación de evento**

  Eventos relacionados con la clonación de volúmenes.

- **Evento maestro de clúster**

  Eventos que aparecen al inicializar el clúster o al realizar cambios en su configuración, como agregar o eliminar nodos.

- **cSumEvent**

  Eventos relacionados con la detección de una discrepancia en la suma de comprobación durante la validación de la suma de comprobación de extremo a extremo.

Los servicios que detectan una discrepancia en la suma de comprobación se detienen automáticamente y no se reinician después de generar este evento.

- **evento de datos**

  Eventos relacionados con la lectura y escritura de datos.

- **Evento de base de datos**

  Eventos relacionados con la base de datos global mantenida por los nodos del conjunto en el clúster.

- **driveEvent**

  Eventos relacionados con las operaciones de conducción.

- **Evento de cifrado en reposo**

  Eventos relacionados con el proceso de cifrado en un clúster.

- **evento de conjunto**

  Eventos relacionados con el aumento o la disminución del número de nodos en un conjunto.

- **Evento del canal de fibra**

  Eventos relacionados con la configuración y las conexiones a los nodos.

- **gcEvento**

  Los eventos relacionados con los procesos se ejecutan cada 60 minutos para recuperar espacio de almacenamiento en las unidades de bloque. Este proceso también se conoce como recogida de basura.

- **ieEvento**

  Error interno del sistema.

- **Evento de instalación**

  Eventos de instalación automática de software. El software se está instalando automáticamente en un nodo pendiente.

- **Evento iSCSIE**

  Eventos relacionados con problemas de iSCSI en el sistema.

- **limitEvento**

  Eventos relacionados con el número de volúmenes o volúmenes virtuales en una cuenta o en el clúster que se acercan al máximo permitido.

- **Evento de modo de mantenimiento**

  Eventos relacionados con el modo de mantenimiento del nodo, como la desactivación del nodo.

- **evento_de_red**

Eventos relacionados con el informe de errores de red para cada interfaz de tarjeta de interfaz de red (NIC) física.

Estos eventos se activan cuando cualquier recuento de errores para una interfaz supera un umbral predeterminado de 1000 durante un intervalo de monitoreo de 10 minutos. Estos eventos se aplican a errores de red como fallos de recepción, errores de comprobación de redundancia cíclica (CRC), errores de longitud, errores de desbordamiento y errores de trama.

- **Evento de hardware de plataforma**

  Eventos relacionados con problemas detectados en dispositivos de hardware.

- **evento de clúster remoto**

  Eventos relacionados con el emparejamiento de clústeres remotos.

- **evento del planificador**

  Eventos relacionados con instantáneas programadas.

- **evento de servicio**

  Eventos relacionados con el estado del servicio del sistema.

- **sliceEvent**

  Eventos relacionados con el servidor Slice, como la eliminación de una unidad o volumen de metadatos.

  Existen tres tipos de eventos de reasignación de segmentos, que incluyen información sobre el servicio al que se asigna un volumen:

  - cambio: modificar el servicio principal a un nuevo servicio principal.

    ```
    sliceID oldPrimaryServiceID->newPrimaryServiceID
    ```

  - traslado: cambio del servicio secundario a un nuevo servicio secundario

    ```
    sliceID {oldSecondaryServiceID(s)}->{newSecondaryServiceID(s)}
    ```

  - poda: eliminar un volumen de un conjunto de servicios

    ```
    sliceID {oldSecondaryServiceID(s)}
    ```

- **snmpTrapEvent**

  Eventos relacionados con las trampas SNMP.

- **estadoEvento**

  Eventos relacionados con las estadísticas del sistema.

- **tsEvento**

  Eventos relacionados con el servicio de transporte del sistema.

- **Excepción inesperada**

  Eventos relacionados con excepciones inesperadas del sistema.

- **ureEvento**

  Eventos relacionados con errores de lectura irrecuperables que ocurren durante la lectura desde el dispositivo de almacenamiento.

- **Evento del proveedor vasa**

  Eventos relacionados con un proveedor VASA (vSphere APIs for Storage Awareness).

Ver el estado de las tareas en ejecución

En la interfaz web, puede consultar el progreso y el estado de finalización de las tareas en ejecución que se reportan mediante los métodos API ListSyncJobs y ListBulkVolumeJobs. Puedes acceder a la página Tareas en ejecución desde la pestaña Informes de la interfaz de usuario de Element.

Si hay una gran cantidad de tareas, el sistema podría ponerlas en cola y ejecutarlas por lotes. La página Tareas en ejecución muestra los servicios que se están sincronizando actualmente. Cuando una tarea finaliza, se reemplaza por la siguiente tarea de sincronización en cola. Es posible que las tareas de sincronización sigan apareciendo en la página de Tareas en ejecución hasta que no haya más tareas por completar.

Puedes ver los datos de sincronización de replicación para los volúmenes que se están replicando en la página Tareas en ejecución del clúster que contiene el volumen de destino.

Alertas del sistema

Ver alertas del sistema

Puede consultar las alertas para obtener información sobre fallos del clúster o errores en el sistema. Las alertas pueden ser informativas, de advertencia o de error, y son un buen indicador del buen funcionamiento del clúster. La mayoría de los errores se resuelven automáticamente.

Puede utilizar el método de la API ListClusterFaults para automatizar la supervisión de alertas. Esto le permite recibir notificaciones sobre todas las alertas que se produzcan.

1. En la interfaz de usuario de Element, seleccione **Informes** > **Alertas**.

   El sistema actualiza las alertas en la página cada 30 segundos.

   Para cada evento, verá la siguiente información:

Artículo	Descripción

IDENTIFICACIÓN	Identificador único asociado a una alerta de clúster.
Gravedad	El grado de importancia de la alerta. Valores posibles: • Advertencia: Un problema menor que podría requerir atención pronto. Todavía se permiten las actualizaciones del sistema. • error: Un fallo que podría causar una degradación del rendimiento o la pérdida de alta disponibilidad (HA). En general, los errores no deberían afectar al servicio. • crítico: Una falla grave que afecta el servicio. El sistema no puede atender solicitudes de API o de E/S de cliente. Operar en este estado podría conllevar una posible pérdida de datos. • bestPractice: No se está utilizando una práctica recomendada de configuración del sistema.
Tipo	El componente afectado por la falla. Puede ser un nodo, una unidad, un clúster, un servicio o un volumen.
Node	Identificador del nodo al que se refiere este fallo. Incluido para fallos de nodo y unidad, de lo contrario establecido en - (guion).
ID de unidad	Identificación de la unidad a la que se refiere este fallo. Incluido en caso de fallos de la unidad, de lo contrario establecido en - (guion).
Código de error	Un código descriptivo que indica la causa del fallo.
Detalles	Descripción de la avería con detalles adicionales.
Fecha	Fecha y hora en que se registró la falla.

2. Haz clic en **Mostrar detalles** para ver información sobre una alerta individual.
3. Para ver los detalles de todas las alertas en la página, haga clic en la columna Detalles.

   Una vez que el sistema resuelve una alerta, toda la información sobre la misma, incluida la fecha en que se resolvió, se traslada al área de Resueltas.

Encuentra más información

- Códigos de falla del clúster
- "Gestiona el almacenamiento con la API de Element"

Códigos de falla del clúster

El sistema informa de un error o un estado que podría ser de interés mediante la generación de un código de fallo, que aparece en la página de Alertas. Estos códigos le ayudan a determinar qué componente del sistema experimentó la alerta y por qué se generó.

La siguiente lista describe los diferentes tipos de códigos:

- **Fallo del servicio de autenticación**

  El servicio de autenticación en uno o más nodos del clúster no funciona como se esperaba.

  Póngase en contacto con el soporte de NetApp para obtener ayuda.

- **Direcciones IP de red virtual disponibles bajas**

  El número de direcciones de red virtuales en el bloque de direcciones IP es bajo.

  Para resolver este fallo, agregue más direcciones IP al bloque de direcciones de red virtual.

- **bloqueoClústerCompleto**

  No hay suficiente espacio de almacenamiento de bloques libre para soportar la pérdida de un solo nodo. Consulte el método de la API GetClusterFullThreshold para obtener detalles sobre los niveles de plenitud del clúster. Este fallo en clúster indica una de las siguientes condiciones:

  - etapa3Baja (Advertencia): Se superó el umbral definido por el usuario. Ajuste la configuración de Cluster Full o agregue más nodos.
  - etapa4Crítica (Error): No hay suficiente espacio para recuperarse de una falla de 1 nodo. No se permite la creación de volúmenes, instantáneas ni clones.
  - etapa5CompletamenteConsumido (Crítico)1; No se permiten escrituras ni nuevas conexiones iSCSI. Las conexiones iSCSI actuales se mantendrán. Las escrituras fallarán hasta que se agregue más capacidad al clúster.

  Para resolver este fallo, purgue o elimine volúmenes o agregue otro nodo de almacenamiento al clúster de almacenamiento.

- **bloquesDegradados**

  Los datos del bloque ya no se replican completamente debido a una falla.

Gravedad	Descripción
Advertencia	Solo se puede acceder a dos copias completas de los datos del bloque.
Error	Solo se puede acceder a una única copia completa de los datos del bloque.
Crítico	No se puede acceder a copias completas de los datos del bloque.

Nota: El estado de advertencia solo puede ocurrir en un sistema Triple Helix.

Para resolver este fallo, restaure los nodos o servicios fuera de línea o bloquee los servicios, o póngase en contacto con el soporte de NetApp para obtener ayuda.

- **bloqueoServicioDemasiadoLleno**

  Un servicio de bloques está utilizando demasiado espacio.

  Para resolver este fallo, añada más capacidad aprovisionada.

- **bloquear servicio no saludable**

  Se ha detectado que un servicio de bloqueo no funciona correctamente:

  - Gravedad = Advertencia: No se toma ninguna medida. Este período de advertencia expirará en cTimeUntilBSIsKilledMSec=330000 milisegundos.
  - Gravedad = Error: El sistema está desactivando automáticamente los datos y replicándolos en otras unidades en buen estado.
  - Gravedad = Crítica: Hay servicios de bloque fallidos en varios nodos mayores o iguales al recuento de replicación (2 para doble hélice). Los datos no están disponibles y la sincronización del contenedor no finalizará.

    Compruebe si hay problemas de conectividad de red y errores de hardware. Si fallan componentes de hardware específicos, se producirán otras averías. La avería desaparecerá cuando se pueda acceder al servicio de bloqueo o cuando el servicio haya sido desactivado.

- **Error en la autocomprobación de Bmc**

  El controlador de gestión de la placa base (BMC) falló una autocomprobación.

  Póngase en contacto con el soporte técnico de NetApp para obtener ayuda.

  Durante una actualización a Element 12.5 o posterior, `BmcSelfTestFailed` No se genera ningún fallo para un nodo que tenga un BMC defectuoso preexistente, o cuando el BMC de un nodo falla durante la actualización. Los BMC que no superen las autocomprobaciones durante la actualización emitirán un `BmcSelfTestFailed` Se produce un fallo de advertencia después de que todo el clúster complete la actualización.

- **La asimetría del reloj supera el umbral de fallos**

  La diferencia horaria entre el nodo maestro del clúster y el nodo que presenta un token supera el umbral recomendado. El clúster de almacenamiento no puede corregir automáticamente la diferencia horaria entre los nodos.

  Para resolver este problema, utilice servidores NTP internos de su red, en lugar de los servidores predeterminados de la instalación. Si está utilizando un servidor NTP interno, póngase en contacto con el soporte de NetApp para obtener ayuda.

- **clusterCannotSync**

  Existe una condición de falta de espacio y los datos de las unidades de almacenamiento en bloque fuera de línea no se pueden sincronizar con las unidades que aún están activas.

  Para solucionar este problema, agregue más almacenamiento.

- **clusterFull**

  No hay más espacio de almacenamiento libre en el clúster de almacenamiento.

  Para solucionar este problema, agregue más almacenamiento.

- **El clúster tiene sobreaprovisionamiento**

  Las IOPS del clúster están sobreaprovisionadas. La suma de todas las IOPS mínimas de QoS es mayor que las IOPS esperadas del clúster. No se puede mantener un nivel mínimo de QoS para todos los volúmenes simultáneamente.

  Para resolver este problema, reduzca la configuración mínima de IOPS de QoS para los volúmenes.

- **Umbral de evento térmico de la CPU**

  El número de eventos térmicos de la CPU en una o más CPU supera el umbral configurado.

  Si no se detectan nuevos eventos térmicos de la CPU en diez minutos, la advertencia desaparecerá automáticamente.

- **Error al deshabilitar la seguridad de la unidad**

  El clúster no está configurado para habilitar la seguridad de la unidad (cifrado en reposo), pero al menos una unidad tiene habilitada la seguridad de la unidad, lo que significa que deshabilitar la seguridad de la unidad en esas unidades falló. Este fallo se registra con gravedad “Advertencia”.

  Para resolver este fallo, compruebe los detalles del fallo para conocer el motivo por el cual no se pudo desactivar la seguridad de la unidad. Las posibles razones son:

  - No se pudo obtener la clave de cifrado; investigue el problema de acceso a la clave o al servidor de claves externo.
  - La operación de desactivación falló en la unidad; determine si posiblemente se adquirió una clave incorrecta.

    Si ninguna de estas es la causa de la avería, es posible que haya que sustituir la unidad.

  Puede intentar recuperar una unidad que no logra deshabilitar la seguridad incluso cuando se proporciona la clave de autenticación correcta. Para realizar esta operación, retire la(s) unidad(es) del sistema moviéndola(s) a Disponible, realice un borrado seguro en la unidad y vuelva a moverla(s) a Activo.

- **Par de clústeres desconectado**

  Un par de clústeres está desconectado o configurado incorrectamente.

  Comprobar la conectividad de red entre los clústeres.

- **nodo remoto desconectado**

  Un nodo remoto está desconectado o configurado incorrectamente.

  Comprobar la conectividad de red entre los nodos.

- **punto final SnapMirror desconectado**

Un punto final remoto de SnapMirror está desconectado o configurado incorrectamente.

Compruebe la conectividad de red entre el clúster y el SnapMirrorEndpoint remoto.

- **Conductor disponible**

  En el clúster hay disponible una o más unidades. En general, todos los clústeres deberían tener todas las unidades agregadas y ninguna en estado disponible. Si este fallo aparece de forma inesperada, póngase en contacto con el soporte de NetApp .

  Para resolver este fallo, agregue las unidades disponibles al clúster de almacenamiento.

- **fallo de la unidad**

  El clúster devuelve este fallo cuando una o más unidades han fallado, lo que indica una de las siguientes condiciones:

  - El administrador de la unidad no puede acceder a la unidad.
  - El servicio de segmentación o bloque ha fallado demasiadas veces, presumiblemente debido a fallos de lectura o escritura en la unidad, y no puede reiniciarse.
  - Falta la unidad.
  - El servicio maestro del nodo es inaccesible (todas las unidades del nodo se consideran faltantes/fallidas).
  - La unidad está bloqueada y no se puede obtener la clave de autenticación.
  - La unidad está bloqueada y la operación de desbloqueo falla.

    Para resolver este problema:

  - Compruebe la conectividad de red del nodo.
  - Reemplace la unidad.
  - Asegúrese de que la clave de autenticación esté disponible.
- **fallo de estado de la unidad**

  La unidad no ha superado la comprobación de estado SMART y, como resultado, sus funciones se han visto reducidas. Existe un nivel de gravedad crítico para esta falla:

  - La unidad con número de serie: <número de serie> en la ranura: <ranura del nodo><ranura de la unidad> no ha superado la comprobación general de estado SMART.

  Para solucionar este problema, sustituya la unidad.

- **Fallo de desgaste de la unidad**

  La vida útil restante de la unidad ha caído por debajo de los umbrales establecidos, pero aún funciona. Existen dos posibles niveles de gravedad para esta falla: Crítica y Advertencia.

  - La unidad con número de serie: <número de serie> en la ranura: <ranura del nodo><ranura de la unidad> tiene niveles de desgaste críticos.
  - La unidad con número de serie: <número de serie> en la ranura: <ranura del nodo><ranura de la unidad> tiene bajas reservas de desgaste.

    Para solucionar este problema, sustituya la unidad lo antes posible.

- **candidatos duplicados de maestro de clúster**

  Se ha detectado más de un candidato a maestro de clúster de almacenamiento.

  Póngase en contacto con el soporte de NetApp para obtener ayuda.

- **Error al habilitar la seguridad de la unidad**

  El clúster está configurado para requerir seguridad de la unidad (cifrado en reposo), pero no se pudo habilitar la seguridad de la unidad en al menos una unidad. Este fallo se registra con gravedad "Advertencia".

  Para resolver este fallo, compruebe los detalles del fallo para conocer el motivo por el que no se pudo habilitar la seguridad de la unidad. Las posibles razones son:

  - No se pudo obtener la clave de cifrado; investigue el problema de acceso a la clave o al servidor de claves externo.
  - La operación de habilitación falló en la unidad; determine si posiblemente se adquirió la clave incorrecta. Si ninguna de estas es la causa de la avería, es posible que haya que sustituir la unidad.

  Puede intentar recuperar una unidad que no habilita correctamente la seguridad incluso cuando se proporciona la clave de autenticación correcta. Para realizar esta operación, retire la(s) unidad(es) del sistema moviéndola(s) a Disponible, realice un borrado seguro en la unidad y vuelva a moverla(s) a Activo.

- **conjunto degradado**

  Se ha perdido la conectividad de red o el suministro eléctrico en uno o más de los nodos del conjunto.

  Para resolver esta falla, restablezca la conectividad de red o la alimentación eléctrica.

- **excepción**

  Se ha reportado una avería que no es una avería rutinaria. Estas fallas no se borran automáticamente de la cola de fallas.

  Póngase en contacto con el soporte de NetApp para obtener ayuda.

- **falló EspacioDemasiadoLleno**

  Un servicio de bloques no responde a las solicitudes de escritura de datos. Esto provoca que el servicio de segmentación se quede sin espacio para almacenar las escrituras fallidas.

  Para resolver este fallo, restaure la funcionalidad de los servicios de bloques para permitir que las escrituras continúen normalmente y que el espacio fallido se elimine del servicio de segmentación.

- **sensor de ventilador**

  Un sensor del ventilador ha fallado o falta.

  Para solucionar este problema, sustituya cualquier componente de hardware defectuoso.

- **Acceso Fibre Channel degradado**

  Un nodo Fibre Channel no responde a otros nodos del clúster de almacenamiento a través de su IP de almacenamiento durante un período de tiempo. En este estado, el nodo se considerará no responsivo y generará un fallo de clúster.

Comprobar la conectividad de red.

- **Acceso a Fibre Channel no disponible**

  Todos los nodos Fibre Channel no responden. Se muestran los identificadores de los nodos.

  Comprobar la conectividad de red.

- **fibreChannelActiveIxL**

  El recuento de IxL Nexus se está acercando al límite admitido de 8000 sesiones activas por nodo Fibre Channel.

  - El límite recomendado es de 5500.
  - El límite de advertencia es de 7500.
  - El límite máximo (no aplicado) es 8192.

  Para resolver este fallo, reduzca el recuento de IxL Nexus por debajo del límite de mejores prácticas de 5500.

- **Configuración de canal de fibra**

  Este fallo en clúster indica una de las siguientes condiciones:

  - Hay un puerto Fibre Channel inesperado en una ranura PCI.
  - Existe un modelo de HBA de canal de fibra inesperado.
  - Existe un problema con el firmware de un HBA de canal de fibra.
  - Un puerto Fibre Channel no está en línea.
  - Existe un problema persistente al configurar el paso de Fibre Channel.

  Póngase en contacto con el soporte de NetApp para obtener ayuda.

- **IOPS de canal de fibra**

  El recuento total de IOPS se está acercando al límite de IOPS para los nodos Fibre Channel en el clúster. Los límites son:

  - FC0025: Límite de 450K IOPS con un tamaño de bloque de 4K por nodo Fibre Channel.
  - FCN001: Límite de 625K OPS con un tamaño de bloque de 4K por nodo Fibre Channel.

  Para resolver este fallo, equilibre la carga entre todos los nodos Fibre Channel disponibles.

- **fibreChannelStaticIxL**

  El recuento de IxL Nexus se está acercando al límite admitido de 16000 sesiones estáticas por nodo Fibre Channel.

  - El límite recomendado es de 11000.
  - El límite de advertencia es de 15000.
  - El límite máximo (aplicable) es 16384.

  Para resolver este fallo, reduzca el recuento de IxL Nexus por debajo del límite de mejores prácticas de 11000.

- **Capacidad del sistema de archivos baja**

  No hay suficiente espacio en uno de los sistemas de archivos.

  Para resolver este fallo, añada más capacidad al sistema de archivos.

- **El sistema de archivos es de solo lectura**

  El sistema de archivos ha entrado en modo de solo lectura.

  Póngase en contacto con el soporte de NetApp para obtener ayuda.

- **FipsDrivesMismatch**

  Se ha insertado físicamente una unidad no FIPS en un nodo de almacenamiento compatible con FIPS o se ha insertado físicamente una unidad FIPS en un nodo de almacenamiento no FIPS. Se genera un único fallo por nodo y se enumeran todas las unidades afectadas.

  Para solucionar este problema, retire o sustituya la unidad o unidades incompatibles en cuestión.

- **fipsDrivesOutOfCompliance**

  El sistema ha detectado que el cifrado en reposo se desactivó después de que se habilitara la función de unidades FIPS. Este fallo también se genera cuando la función de unidades FIPS está habilitada y hay una unidad o nodo que no sea FIPS en el clúster de almacenamiento.

  Para resolver este fallo, habilite el cifrado en reposo o retire el hardware no FIPS del clúster de almacenamiento.

- **fallo en la autocomprobación de fips**

  El subsistema FIPS ha detectado un fallo durante la autocomprobación.

  Póngase en contacto con el soporte de NetApp para obtener ayuda.

- **Desajuste de configuración de hardware**

  Este fallo en clúster indica una de las siguientes condiciones:

  - La configuración no coincide con la definición del nodo.
  - El tamaño de la unidad es incorrecto para este tipo de nodo.
  - Se ha detectado una unidad no compatible. Una posible razón es que la versión de Element instalada no reconoce esta unidad. Se recomienda actualizar el software Element en este nodo.
  - Existe una incompatibilidad en el firmware del controlador.
  - El estado de capacidad de cifrado de la unidad no coincide con el nodo.

  Póngase en contacto con el soporte de NetApp para obtener ayuda.

- **Fecha de vencimiento del certificado idPC**

  El certificado SSL del proveedor de servicios del clúster para su uso con un proveedor de identidad (IdP) de terceros está próximo a caducar o ya ha caducado. Esta falla utiliza los siguientes niveles de gravedad según su urgencia:

Gravedad	Descripción
Advertencia	El certificado caduca en 30 días.
Error	El certificado caduca en 7 días.
Crítico	El certificado caduca en 3 días o ya ha caducado.

Para solucionar este problema, actualice el certificado SSL antes de que caduque. Utilice el método de la API UpdateIdpConfiguration con `refreshCertificateExpirationTime=true` para proporcionar el certificado SSL actualizado.

- **modos de enlace inconsistentes**

  Faltan los modos de enlace en el dispositivo VLAN. Este fallo mostrará el modo de enlace esperado y el modo de enlace que se está utilizando actualmente.

- **Mtus inconsistente**

  Este fallo en clúster indica una de las siguientes condiciones:

  - Desajuste en Bond1G: Se han detectado MTU inconsistentes en las interfaces Bond1G.
  - Desajuste de Bond10G: Se han detectado MTU inconsistentes en las interfaces Bond10G.

  Este error muestra el nodo o nodos en cuestión junto con el valor MTU asociado.

- **reglas de enrutamiento inconsistentes**

  Las reglas de enrutamiento para esta interfaz son inconsistentes.

- **máscaras de subred inconsistentes**

  La máscara de red del dispositivo VLAN no coincide con la máscara de red registrada internamente para la VLAN. Este error muestra la máscara de red esperada y la máscara de red que se está utilizando actualmente.

- **recuento incorrecto de puertos de enlace**

  El número de puertos de enlace es incorrecto.

- **Recuento de nodos de canal de fibra configurado no válido**

  Una de las dos conexiones de nodo Fibre Channel previstas está degradada. Este fallo aparece cuando solo está conectado un nodo Fibre Channel.

  Para resolver esta falla, verifique la conectividad de la red del clúster y el cableado de red, y compruebe si hay servicios que hayan fallado. Si no hay problemas de red o de servicio, póngase en contacto con el soporte de NetApp para solicitar un reemplazo del nodo Fibre Channel.

- **Error de balanceo de interrupciones**

  Se produjo una excepción al intentar equilibrar las interrupciones.

  Póngase en contacto con el soporte de NetApp para obtener ayuda.

- **kmipCertificateFault**
  - El certificado de la Autoridad de Certificación (CA) raíz está próximo a caducar.

    Para resolver este fallo, adquiera un nuevo certificado de la CA raíz con una fecha de vencimiento de al menos 30 días y utilice ModifyKeyServerKmip para proporcionar el certificado actualizado de la CA raíz.

  - El certificado del cliente está próximo a caducar.

    Para resolver este problema, cree una nueva CSR utilizando GetClientCertificateSigningRequest, fírmela asegurándose de que la nueva fecha de vencimiento sea al menos 30 días posterior, y utilice ModifyKeyServerKmip para reemplazar el certificado de cliente KMIP que vence con el nuevo certificado.

  - El certificado de la Autoridad de Certificación (CA) raíz ha caducado.

    Para resolver este fallo, adquiera un nuevo certificado de la CA raíz con una fecha de vencimiento de al menos 30 días y utilice ModifyKeyServerKmip para proporcionar el certificado actualizado de la CA raíz.

  - El certificado del cliente ha caducado.

    Para resolver este problema, cree una nueva CSR utilizando GetClientCertificateSigningRequest, fírmela asegurándose de que la nueva fecha de vencimiento sea al menos 30 días posterior y utilice ModifyKeyServerKmip para reemplazar el certificado de cliente KMIP vencido con el nuevo certificado.

  - Error en el certificado de la Autoridad de Certificación (CA) raíz.

    Para resolver este fallo, compruebe que se ha proporcionado el certificado correcto y, si es necesario, vuelva a adquirir el certificado de la CA raíz. Utilice ModifyKeyServerKmip para instalar el certificado de cliente KMIP correcto.

  - Error en el certificado del cliente.

    Para resolver este fallo, compruebe que esté instalado el certificado de cliente KMIP correcto. La CA raíz del certificado del cliente debe estar instalada en el EKS. Utilice ModifyKeyServerKmip para instalar el certificado de cliente KMIP correcto.

- **kmipServerFault**
  - Fallo de conexión

    Para resolver este fallo, compruebe que el servidor de claves externo está activo y accesible a través de la red. Utilice TestKeyServerKimp y TestKeyProviderKmip para probar su conexión.

  - Fallo de autenticación

    Para resolver este fallo, compruebe que se están utilizando los certificados de CA raíz y de cliente KMIP correctos, y que la clave privada y el certificado de cliente KMIP coinciden.

  - Error del servidor

    Para resolver este fallo, compruebe los detalles del error. Es posible que sea necesario solucionar problemas en el servidor de claves externo según el error devuelto.

- **umbral de error de memoria**

  Se ha detectado un gran número de errores ECC corregibles e incorregibles. Esta falla utiliza los siguientes niveles de gravedad según su urgencia:

Evento	Gravedad	Descripción
Un único DIMM cErrorCount alcanza cDimmCorrectableErrWarnThreshold.	Advertencia	Errores de memoria ECC corregibles por encima del umbral en DIMM: <Procesador> <Ranura DIMM>
Un único valor de cErrorCount de DIMM permanece por encima de cDimmCorrectableErrWarnThreshold hasta que expire cErrorFaultTimer para el DIMM.	Error	Errores de memoria ECC corregibles por encima del umbral en DIMM: <Procesador> <DIMM>
Un controlador de memoria informa que cErrorCount supera cMemCtlrCorrectableErrWarnThreshold, y se especifica cMemCtlrCorrectableErrWarnDuration.	Advertencia	Errores de memoria ECC corregibles por encima del umbral en el controlador de memoria: <Procesador> <Controlador de memoria>
Un controlador de memoria informa que cErrorCount está por encima de cMemCtlrCorrectableErrWarnThreshold hasta que expire cErrorFaultTimer para el controlador de memoria.	Error	Errores de memoria ECC corregibles por encima del umbral en DIMM: <Procesador> <DIMM>
Un único DIMM informa un uErrorCount superior a cero, pero inferior a cDimmUncorrectableErrFaultThreshold.	Advertencia	Se han detectado errores de memoria ECC no corregibles en el módulo DIMM: <Procesador> <Ranura DIMM>
Un único DIMM informa un uErrorCount de al menos cDimmUncorrectableErrFaultThreshold.	Error	Se han detectado errores de memoria ECC no corregibles en el módulo DIMM: <Procesador> <Ranura DIMM>
Un controlador de memoria informa un uErrorCount superior a cero, pero inferior a cMemCtlrUncorrectableErrFaultThreshold.	Advertencia	Se han detectado errores de memoria ECC no corregibles en el controlador de memoria: <Procesador> <Controlador de memoria>

Un controlador de memoria informa un uErrorCount de al menos cMemCtlrUncorrectableErrFaultThreshold.	Error	Se han detectado errores de memoria ECC no corregibles en el controlador de memoria: <Procesador> <Controlador de memoria>

Para resolver este problema, póngase en contacto con el soporte técnico de NetApp para obtener ayuda.

- **umbral de uso de memoria**

  El uso de memoria es superior a lo normal. Esta falla utiliza los siguientes niveles de gravedad según su urgencia:

  > Consulte el apartado **Detalles** del error para obtener información más detallada sobre el tipo de fallo.

Gravedad	Descripción
Advertencia	La memoria del sistema es baja.
Error	La memoria del sistema es muy baja.
Crítico	La memoria del sistema está completamente agotada.

  Para resolver este problema, póngase en contacto con el soporte técnico de NetApp para obtener ayuda.

- **metadataClusterFull**

  No hay suficiente espacio libre de almacenamiento de metadatos para soportar la pérdida de un solo nodo. Consulte el método de la API GetClusterFullThreshold para obtener detalles sobre los niveles de plenitud del clúster. Este fallo en clúster indica una de las siguientes condiciones:

  - etapa3Baja (Advertencia): Se superó el umbral definido por el usuario. Ajuste la configuración de Cluster Full o agregue más nodos.
  - etapa4Crítica (Error): No hay suficiente espacio para recuperarse de una falla de 1 nodo. No se permite la creación de volúmenes, instantáneas ni clones.
  - etapa5CompletamenteConsumido (Crítico)1; No se permiten escrituras ni nuevas conexiones iSCSI. Las conexiones iSCSI actuales se mantendrán. Las escrituras fallarán hasta que se agregue más capacidad al clúster. Elimine o borre datos o agregue más nodos.

  Para resolver este fallo, purgue o elimine volúmenes o agregue otro nodo de almacenamiento al clúster de almacenamiento.

- **Fallo en la comprobación de mtu**

  Un dispositivo de red no está configurado con el tamaño MTU adecuado.

  Para resolver este fallo, asegúrese de que todas las interfaces de red y los puertos del conmutador estén configurados para tramas jumbo (MTU de hasta 9000 bytes).

- **Configuración de red**

  Este fallo en clúster indica una de las siguientes condiciones:

  - No se encuentra presente la interfaz esperada.
  - Existe una interfaz duplicada.
  - Una interfaz configurada está inactiva.
  - Es necesario reiniciar la red.

  Póngase en contacto con el soporte de NetApp para obtener ayuda.

- **noHayDireccionesIPdeRedVirtualDisponibles**

  No hay direcciones de red virtual disponibles en el bloque de direcciones IP.

  - virtualNetworkID # TAG(###) no tiene direcciones IP de almacenamiento disponibles. No se pueden agregar nodos adicionales al clúster.

  Para resolver este fallo, agregue más direcciones IP al bloque de direcciones de red virtual.

- **fallo de hardware del nodo (la interfaz de red <nombre> está inactiva o el cable está desconectado)**

  La interfaz de red está inactiva o el cable está desconectado.

  Para resolver este fallo, compruebe la conectividad de red del nodo o nodos.

- **Fallo de hardware del nodo (El estado de capacidad de cifrado de la unidad no coincide con el estado de capacidad de cifrado del nodo para la unidad en la ranura <ranura del nodo><ranura de la unidad>)**

  Una unidad no tiene las capacidades de cifrado compatibles con el nodo de almacenamiento en el que está instalada.

- **Fallo de hardware del nodo (Tamaño incorrecto de la unidad <tipo de unidad> <tamaño real> para la unidad en la ranura <ranura del nodo><ranura de la unidad> para este tipo de nodo - se esperaba <tamaño esperado>)**

  Un nodo de almacenamiento contiene una unidad de almacenamiento cuyo tamaño no es el adecuado para este nodo.

- **Fallo de hardware del nodo (Se ha detectado una unidad no compatible en la ranura <ranura del nodo><ranura de la unidad>; las estadísticas y la información de estado de la unidad no estarán disponibles)**

  Un nodo de almacenamiento contiene una unidad que no admite.

- **fallo de hardware del nodo (La unidad en la ranura <ranura del nodo><ranura de la unidad> debería estar usando la versión de firmware <versión esperada>, pero está usando una versión no compatible <versión actual>)**

  Un nodo de almacenamiento contiene una unidad que ejecuta una versión de firmware no compatible.

- **modo de mantenimiento del nodo**

  Un nodo ha sido puesto en modo de mantenimiento. Esta falla utiliza los siguientes niveles de gravedad

según su urgencia:

Gravedad	Descripción
Advertencia	Indica que el nodo aún está en modo de mantenimiento.
Error	Indica que el modo de mantenimiento no se ha podido desactivar, muy probablemente debido a fallos o sistemas en espera activos.

Para solucionar este problema, desactive el modo de mantenimiento una vez finalizado el mantenimiento. Si el fallo de nivel de error persiste, póngase en contacto con el soporte de NetApp para obtener ayuda.

- **nodo fuera de línea**

  El software Element no puede comunicarse con el nodo especificado. Comprobar la conectividad de red.

- **no se usa el modo de puente LACP**

  El modo de enlace LACP no está configurado.

  Para resolver este problema, utilice el enlace LACP al implementar nodos de almacenamiento; los clientes podrían experimentar problemas de rendimiento si LACP no está habilitado y configurado correctamente.

- **Servidor ntp inaccesible**

  El clúster de almacenamiento no puede comunicarse con el servidor o servidores NTP especificados.

  Para resolver este fallo, compruebe la configuración del servidor NTP, la red y el cortafuegos.

- **ntpTimeNoEstáSincronizado**

  La diferencia entre la hora del clúster de almacenamiento y la hora del servidor NTP especificado es demasiado grande. El clúster de almacenamiento no puede corregir la diferencia automáticamente.

  Para resolver este problema, utilice servidores NTP internos de su red, en lugar de los servidores predeterminados de la instalación. Si está utilizando servidores NTP internos y el problema persiste, póngase en contacto con el soporte de NetApp para obtener ayuda.

- **Estado del dispositivo nvram**

  Un dispositivo NVRAM tiene un error, está fallando o ha fallado. Esta falla presenta las siguientes severidades:

Gravedad	Descripción

Advertencia	El hardware ha detectado una advertencia. Esta condición puede ser transitoria, como por ejemplo una alerta de temperatura. • nvmLifetimeError • nvmLifetimeStatus • Estado de la vida útil de la fuente de energía • Estado de la temperatura de la fuente de energía • Se superó el umbral de advertencia
Error	El hardware ha detectado un error o un estado crítico. El maestro del clúster intenta retirar la unidad de partición de funcionamiento (esto genera un evento de extracción de unidad). Si no están disponibles los servicios de partición secundaria, la unidad no se extraerá. Errores devueltos además de los errores de nivel de advertencia: • No existe un punto de montaje para el dispositivo NVRAM . • La partición del dispositivo NVRAM no existe. • La partición del dispositivo NVRAM existe, pero no está montada.
Crítico	El hardware ha detectado un error o un estado crítico. El maestro del clúster intenta retirar la unidad de partición de funcionamiento (esto genera un evento de extracción de unidad). Si no están disponibles los servicios de partición secundaria, la unidad no se extraerá. • persistencia perdida • estado del brazo GuardarN Armado • Error de estado de csave

Reemplace cualquier componente de hardware defectuoso en el nodo. Si esto no resuelve el problema, póngase en contacto con el soporte técnico de NetApp para obtener ayuda.

- **Error de fuente de alimentación**

  Este fallo en clúster indica una de las siguientes condiciones:

  - No hay fuente de alimentación.
  - Se ha producido un fallo en la fuente de alimentación.
  - Falta una entrada de alimentación o está fuera de rango.

  Para resolver esta falla, verifique que se suministre alimentación redundante a todos los nodos. Póngase en contacto con el soporte de NetApp para obtener ayuda.

- **espacio aprovisionado demasiado lleno**

  La capacidad total aprovisionada del clúster está demasiado llena.

  Para resolver este fallo, agregue más espacio aprovisionado o elimine y purgue volúmenes.

- **remoteRepAsyncDelayExceeded**

  Se ha superado el retardo asíncrono configurado para la replicación. Comprobar la conectividad de red entre clústeres.

- **remoteRepClusterFull**

  Los volúmenes han pausado la replicación remota porque el clúster de almacenamiento de destino está demasiado lleno.

  Para resolver este fallo, libere algo de espacio en el clúster de almacenamiento de destino.

- **remoteRepSnapshotClusterFull**

  Los volúmenes han pausado la replicación remota de instantáneas porque el clúster de almacenamiento de destino está demasiado lleno.

  Para resolver este fallo, libere algo de espacio en el clúster de almacenamiento de destino.

- **Se ha superado el límite de instantáneas de representantes remotos**

  Los volúmenes han pausado la replicación remota de instantáneas porque el volumen del clúster de almacenamiento de destino ha superado su límite de instantáneas.

  Para resolver este fallo, aumente el límite de instantáneas en el clúster de almacenamiento de destino.

- **Error de acción programada**

  Una o más de las actividades programadas se ejecutaron, pero fallaron.

  El fallo se soluciona si la actividad programada se ejecuta de nuevo y tiene éxito, si se elimina la actividad programada o si se pausa y se reanuda.

- **Error al leer el sensor**

  Un sensor no pudo comunicarse con el controlador de gestión de la placa base (BMC).

  Póngase en contacto con el soporte de NetApp para obtener ayuda.

- **servicio no en ejecución**

  Un servicio necesario no está en funcionamiento.

  Póngase en contacto con el soporte de NetApp para obtener ayuda.

- **sliceServiceTooFull**

  Un servicio de segmentación tiene asignada muy poca capacidad aprovisionada.

  Para resolver este fallo, añada más capacidad aprovisionada.

- **sliceServicePoco saludable**

  El sistema ha detectado que un servicio de segmentación no funciona correctamente y lo está desactivando automáticamente.

  - Gravedad = Advertencia: No se toma ninguna medida. Este periodo de advertencia expirará en 6 minutos.
  - Gravedad = Error: El sistema está desactivando automáticamente los datos y replicándolos en otras unidades en buen estado.

  Compruebe si hay problemas de conectividad de red y errores de hardware. Si fallan componentes de hardware específicos, se producirán otras averías. El fallo se solucionará cuando el servicio de segmentación esté accesible o cuando el servicio haya sido desactivado.

- **ssh habilitado**

  El servicio SSH está habilitado en uno o más nodos del clúster de almacenamiento.

  Para resolver este fallo, deshabilite el servicio SSH en el nodo o nodos correspondientes o póngase en contacto con el soporte de NetApp para obtener ayuda.

- **Caducidad del certificado SSL**

  El certificado SSL asociado a este nodo está próximo a caducar o ya ha caducado. Esta falla utiliza los siguientes niveles de gravedad según su urgencia:

Gravedad	Descripción
Advertencia	El certificado caduca en 30 días.
Error	El certificado caduca en 7 días.
Crítico	El certificado caduca en 3 días o ya ha caducado.

  Para solucionar este problema, renueve el certificado SSL. Si necesita ayuda, póngase en contacto con el soporte técnico de NetApp .

- **capacidad varada**

  Un solo nodo representa más de la mitad de la capacidad del clúster de almacenamiento.

  Para mantener la redundancia de datos, el sistema reduce la capacidad del nodo más grande, de modo que parte de su capacidad de bloque queda inactiva (sin utilizar).

  Para resolver este fallo, agregue más unidades a los nodos de almacenamiento existentes o agregue nodos de almacenamiento al clúster.

- **sensor de temperatura**

  Un sensor de temperatura está registrando temperaturas superiores a lo normal. Esta falla puede producirse junto con fallas de powerSupplyError o fanSensor.

  Para resolver este fallo, compruebe si hay obstrucciones en el flujo de aire cerca del clúster de almacenamiento. Si es necesario, póngase en contacto con el soporte de NetApp para obtener ayuda.

- **mejora**

  La actualización lleva en curso más de 24 horas.

  Para resolver este problema, reanude la actualización o póngase en contacto con el soporte de NetApp para obtener ayuda.

- **Servicio que no responde**

  Un servicio ha dejado de responder.

  Póngase en contacto con el soporte de NetApp para obtener ayuda.

- **Configuración de red virtual**

  Este fallo en clúster indica una de las siguientes condiciones:

  - No hay ninguna interfaz presente.
  - Existe un espacio de nombres incorrecto en una interfaz.
  - Existe una máscara de red incorrecta.
  - Existe una dirección IP incorrecta.
  - Una interfaz no está operativa.
  - Existe una interfaz superflua en un nodo.

  Póngase en contacto con el soporte de NetApp para obtener ayuda.

- **volúmenes degradados**

  Los volúmenes secundarios no han terminado de replicarse y sincronizarse. El mensaje se borra cuando finaliza la sincronización.

- **volúmenesDesconectados**

  Uno o más volúmenes del clúster de almacenamiento están fuera de línea. También estará presente el fallo **volumeDegraded**.

  Póngase en contacto con el soporte de NetApp para obtener ayuda.

Ver actividad de rendimiento del nodo

Puede visualizar la actividad de rendimiento de cada nodo en formato gráfico. Esta información proporciona estadísticas en tiempo real sobre la CPU y las operaciones de E/S de lectura/escritura por segundo (IOPS) para cada unidad del nodo. El gráfico de utilización se actualiza cada cinco segundos, y el gráfico de estadísticas de la unidad se actualiza cada diez segundos.

1. Haz clic en **Clúster** > **Nodos**.
2. Haz clic en **Acciones** para el nodo que deseas ver.
3. Haga clic en **Ver detalles**.

Puedes ver puntos específicos en el tiempo en los gráficos de líneas y barras colocando el cursor sobre la línea o la barra.

Rendimiento de volumen

Rendimiento del volumen de visualización

Puede consultar información detallada sobre el rendimiento de todos los volúmenes del clúster. Esta información se puede ordenar por ID de volumen o por cualquier otra de las columnas de rendimiento. También puedes filtrar la información según ciertos criterios.

Puedes cambiar la frecuencia con la que el sistema actualiza la información de rendimiento en la página haciendo clic en la lista **Actualizar cada** y eligiendo un valor diferente. El intervalo de actualización predeterminado es de 10 segundos si el clúster tiene menos de 1000 volúmenes; de lo contrario, el valor predeterminado es de 60 segundos. Si selecciona el valor Nunca, la actualización automática de la página se desactiva.

Puedes volver a habilitar la actualización automática haciendo clic en **Activar actualización automática**.

1. En la interfaz de usuario de Element, seleccione **Informes** > **Rendimiento de volumen**.
2. En la lista de volúmenes, haga clic en el icono Acciones de un volumen.
3. Haga clic en **Ver detalles**.

   En la parte inferior de la página se muestra una bandeja con información general sobre el volumen.
4. Para ver información más detallada sobre el volumen, haga clic en **Ver más detalles**.

   El sistema muestra información detallada, así como gráficos de rendimiento del volumen.

Encuentra más información

Detalles del rendimiento del volumen

Detalles del rendimiento del volumen

Puede consultar las estadísticas de rendimiento de los volúmenes en la página Rendimiento del volumen de la pestaña Informes en la interfaz de usuario de Element.

La siguiente lista describe los detalles que están a su disposición:

- **IDENTIFICACIÓN**

  El identificador generado por el sistema para el volumen.
- **Nombre**

  El nombre que se le dio al volumen cuando fue creado.
- **Cuenta**

  El nombre de la cuenta asignada al volumen.

- **Grupos de acceso**

  El nombre del grupo o grupos de acceso al volumen al que pertenece el volumen.

- **Utilización del volumen**

  Un valor porcentual que describe cuánto volumen está utilizando el cliente.

  Valores posibles:

  - 0 = El cliente no usa el volumen
  - 100 = El cliente está utilizando el máximo
  - >100 = El cliente está utilizando la ráfaga.

- **Total de IOPS**

  El número total de IOPS (lectura y escritura) que se están ejecutando actualmente en el volumen.

- **Leer IOPS**

  El número total de IOPS de lectura que se están ejecutando actualmente en el volumen.

- **Escribir IOPS**

  El número total de IOPS de escritura que se están ejecutando actualmente en el volumen.

- **Rendimiento total**

  Cantidad total de operaciones de lectura y escritura que se están ejecutando actualmente en el volumen.

- **Rendimiento de lectura**

  Cantidad total de operaciones de lectura que se están ejecutando actualmente en el volumen.

- **Rendimiento de escritura**

  Cantidad total de operaciones de escritura que se están ejecutando actualmente en el volumen.

- **Latencia total**

  El tiempo promedio, en microsegundos, para completar las operaciones de lectura y escritura en un volumen.

- **Latencia de lectura**

  Tiempo promedio, en microsegundos, para completar las operaciones de lectura del volumen en los últimos 500 milisegundos.

- **Latencia de escritura**

  Tiempo promedio, en microsegundos, para completar las operaciones de escritura en un volumen en los últimos 500 milisegundos.

- **Profundidad de la cola**

  Número de operaciones de lectura y escritura pendientes en el volumen.

- **Tamaño promedio de E/S**

  Tamaño promedio en bytes de las operaciones de E/S recientes en el volumen en los últimos 500 milisegundos.

Sesiones iSCSI

Ver sesiones iSCSI

Puede ver las sesiones iSCSI que están conectadas al clúster. Puedes filtrar la información para incluir solo las sesiones deseadas.

1. En la interfaz de usuario de Element, seleccione **Informes** > **Sesiones iSCSI**.
2. Para ver los campos de criterios de filtro, haga clic en **Filtrar**.

Encuentra más información

Detalles de la sesión iSCSI

Detalles de la sesión iSCSI

Puede ver información sobre las sesiones iSCSI que están conectadas al clúster.

La siguiente lista describe la información que puede encontrar sobre las sesiones iSCSI:

- **Nodo**

  El nodo que aloja la partición de metadatos principal del volumen.

- **Cuenta**

  El nombre de la cuenta propietaria del volumen. Si el valor está en blanco, se muestra un guion (-).

- **Volumen**

  El nombre del volumen identificado en el nodo.

- **ID de volumen**

  Identificación del volumen asociado con el IQN objetivo.

- **ID del iniciador**

  Un identificador generado por el sistema para el iniciador.

- **Alias del iniciador**

  Un nombre opcional para el iniciador que facilita su búsqueda en una lista larga.

- **Dirección IP del iniciador**

  La dirección IP del punto final que inicia la sesión.

- **Iniciador IQN**

  El IQN del punto final que inicia la sesión.

- **IP de destino**

  La dirección IP del nodo que aloja el volumen.

- **IQN objetivo**

  El IQN del volumen.

- **CAP**

  El algoritmo CHAP para una sesión iSCSI. Si no se está utilizando un algoritmo CHAP, se muestra un guion (-). Disponible a partir del Elemento 12.8.

- **Creado el**

  Fecha en que se estableció la sesión.

Sesiones de Fibre Channel

Ver sesiones de Fibre Channel

Puede ver las sesiones de Fibre Channel (FC) que están conectadas al clúster. Puede filtrar la información para incluir solo las conexiones que desea que se muestren en la ventana.

1. En la interfaz de usuario de Element, seleccione **Informes** > **Sesiones FC**.
2. Para ver los campos de criterios de filtro, haga clic en **Filtrar**.

Encuentra más información

Detalles de la sesión de Fibre Channel

Detalles de la sesión de Fibre Channel

Puede encontrar información sobre las sesiones Fibre Channel (FC) activas que están conectadas al clúster.

La siguiente lista describe la información que puede encontrar sobre las sesiones FC conectadas al clúster:

- **ID del nodo**

  El nodo que aloja la sesión para la conexión.

- **Nombre del nodo**

  Nombre del nodo generado por el sistema.

- **ID del iniciador**

Un identificador generado por el sistema para el iniciador.

- **Iniciador WWPN**

  El nombre del puerto mundial inicial.

- **Alias del iniciador**

  Un nombre opcional para el iniciador que facilita su búsqueda en una lista larga.

- **WWPN objetivo**

  Nombre del puerto mundial de destino.

- **Grupo de acceso por volumen**

  Nombre del grupo de acceso al volumen al que pertenece la sesión.

- **ID de grupo de acceso por volumen**

  ID generado por el sistema para el grupo de acceso.

Solucionar problemas de las unidades

Solucionar problemas de las unidades

Puedes reemplazar una unidad de estado sólido (SSD) defectuosa por una unidad de reemplazo. Las unidades SSD para nodos de almacenamiento SolidFire son intercambiables en caliente. Si sospecha que una unidad SSD ha fallado, póngase en contacto con el soporte de NetApp para verificar la falla y que le guíen a través del procedimiento de resolución adecuado. El soporte de NetApp también trabaja con usted para obtener una unidad de reemplazo de acuerdo con su acuerdo de nivel de servicio.

En este caso, "intercambiable" significa que puede extraer una unidad defectuosa de un nodo activo y reemplazarla con una nueva unidad SSD de NetApp. No se recomienda extraer unidades que no hayan fallado en un clúster activo.

Debe mantener repuestos in situ sugeridos por el soporte de NetApp para permitir el reemplazo inmediato de la unidad en caso de falla.

> Para fines de prueba, si está simulando una falla de la unidad extrayendo una unidad de un nodo, debe esperar 30 segundos antes de volver a insertar la unidad en la ranura de la unidad.

Si falla una unidad, Double Helix redistribuye los datos de la unidad entre los nodos restantes del clúster. Las fallas en múltiples unidades en el mismo nodo no representan un problema, ya que el software Element protege contra la existencia de dos copias de datos en el mismo nodo. Un fallo en el disco duro provoca los siguientes eventos:

- Los datos se migran fuera de la unidad.
- La capacidad total del clúster se reduce en la capacidad de la unidad.
- La protección de datos Double Helix garantiza que existan dos copias válidas de los datos.

Los sistemas de almacenamiento SolidFire no admiten la extracción de una unidad si esto resulta en una cantidad de almacenamiento insuficiente para migrar los datos.

Para más información

- Retire las unidades defectuosas del clúster.
- Solución de problemas básicos de la unidad MDSS
- Retire las unidades MDSS
- "Sustitución de unidades para nodos de almacenamiento SolidFire"
- "Sustitución de unidades para nodos de almacenamiento de la serie H600S"
- "Información de hardware H410S y H610S"
- "Información sobre el hardware de la serie SF"

Retire las unidades defectuosas del clúster.

El sistema SolidFire marca una unidad como averiada si su autodiagnóstico indica al nodo que ha fallado o si la comunicación con la unidad se interrumpe durante cinco minutos y medio o más. El sistema muestra una lista de las unidades que han fallado. Debe eliminar una unidad defectuosa de la lista de unidades defectuosas en el software NetApp Element .

Las unidades en la lista **Alertas** se muestran como **blockServiceUnhealthy** cuando un nodo está fuera de línea. Al reiniciar el nodo, si el nodo y sus unidades vuelven a estar en línea en un plazo de cinco minutos y medio, las unidades se actualizan automáticamente y continúan como unidades activas en el clúster.

1. En la interfaz de usuario de Element, seleccione **Clúster** > **Unidades**.
2. Haz clic en **Error** para ver la lista de unidades que han fallado.
3. Anote el número de ranura de la unidad averiada.

   Necesitas esta información para localizar la unidad averiada en el chasis.

4. Retire las unidades defectuosas utilizando uno de los siguientes métodos:

Opción	Pasos
Para extraer unidades individuales	a. Haz clic en **Acciones** para la unidad que deseas eliminar. b. Haga clic en **Eliminar**.
Para extraer varias unidades	a. Seleccione todas las unidades que desea eliminar y haga clic en **Acciones en lote**. b. Haga clic en **Eliminar**.

Solución de problemas básicos de la unidad MDSS

Puede recuperar las unidades de metadatos (o particiones) volviéndolas a agregar al

clúster en caso de que falle una o ambas unidades de metadatos. Puede realizar la operación de recuperación en la interfaz de usuario de NetApp Element si la función MDSS ya está habilitada en el nodo.

Si una o ambas unidades de metadatos de un nodo experimentan una falla, el servicio de segmentación se apagará y los datos de ambas unidades se respaldarán en unidades diferentes del nodo.

Los siguientes escenarios describen posibles situaciones de fallo y proporcionan recomendaciones básicas para corregir el problema:

La unidad de partición del sistema falla

- En este escenario, se verifica la ranura 2 y se devuelve a un estado disponible.
- Es necesario volver a llenar la unidad de partición del sistema antes de que se pueda volver a poner en línea el servicio de partición.
- Debes reemplazar la unidad de partición del sistema; cuando esté disponible, agrega esta unidad y la unidad de la ranura 2 al mismo tiempo.

> No se puede agregar la unidad en la ranura 2 por sí sola como unidad de metadatos. Debes volver a agregar ambas unidades al nodo al mismo tiempo.

La ranura 2 falla

- En este escenario, se verifica la unidad de partición del sistema y se devuelve a un estado disponible.
- Debes reemplazar la ranura 2 con una de repuesto; cuando la ranura 2 esté disponible, agrega la unidad de partición del sistema y la unidad de la ranura 2 al mismo tiempo.

La unidad de partición del sistema y la ranura 2 fallan

- Debes reemplazar tanto la unidad de partición del sistema como la ranura 2 con una unidad de repuesto. Cuando ambas unidades estén disponibles, agregue la unidad de partición del sistema y la unidad de la ranura 2 al mismo tiempo.

Orden de operaciones

- Reemplace la unidad de hardware defectuosa con una unidad de repuesto (reemplace ambas unidades si ambas han fallado).
- Vuelva a agregar las unidades al clúster cuando se hayan repoblado y estén disponibles.

Verificar operaciones

- Verifique que las unidades en la ranura 0 (o interna) y la ranura 2 se identifiquen como unidades de metadatos en la lista de Unidades Activas.
- Verifique que se haya completado todo el balanceo de segmentos (no debe haber más mensajes de movimiento de segmentos en el registro de eventos durante al menos 30 minutos).

Para más información

Agregar unidades MDSS

Agregar unidades MDSS

Puede agregar una segunda unidad de metadatos en un nodo SolidFire convirtiendo la unidad de bloques en la ranura 2 en una unidad de partición. Esto se logra habilitando la función de servicio de segmentación de múltiples unidades (MDSS). Para habilitar esta función, debe ponerse en contacto con el soporte de NetApp .

Para que una unidad de partición esté disponible, puede ser necesario reemplazar una unidad averiada por una unidad nueva o de repuesto. Debe agregar la unidad de partición del sistema al mismo tiempo que agrega la unidad para la ranura 2. Si intenta agregar la unidad de partición de la ranura 2 sola o antes de agregar la unidad de partición del sistema, el sistema generará un error.

1. Haz clic en **Clúster** > **Unidades**.
2. Haz clic en **Disponible** para ver la lista de unidades disponibles.
3. Seleccione las unidades de partición que desea agregar.
4. Haz clic en **Acciones en lote**.
5. Haga clic en **Agregar**.
6. Confirme en la pestaña **Unidades activas** que las unidades se han agregado.

Retire las unidades MDSS

Puede extraer las unidades del servicio de segmentación de unidades múltiples (MDSS). Este procedimiento se aplica únicamente si el nodo tiene varias unidades de partición.

> Si fallan la unidad de partición del sistema y la unidad de la ranura 2, el sistema apagará los servicios de partición y extraerá las unidades. Si no se produce ningún fallo y se extraen las unidades, ambas deben extraerse al mismo tiempo.

1. Haz clic en **Clúster** > **Unidades**.
2. Desde la pestaña **Unidades disponibles**, haga clic en la casilla de verificación de las unidades de partición que se van a eliminar.
3. Haz clic en **Acciones en lote**.
4. Haga clic en **Eliminar**.
5. Confirma la acción.

Solucionar problemas de nodos

Eliminar nodos de un clúster

Puedes eliminar nodos de un clúster para realizar mantenimiento o reemplazo. Debe utilizar la interfaz de usuario o la API de NetApp Element para eliminar nodos antes de desconectarlos.

A continuación se ofrece una descripción general del procedimiento para eliminar nodos de almacenamiento:

- Asegúrese de que el clúster tenga capacidad suficiente para crear una copia de los datos en el nodo.
- Elimine las unidades del clúster utilizando la interfaz de usuario o el método API RemoveDrives.

Esto provoca que el sistema migre datos desde las unidades del nodo a otras unidades del clúster. El tiempo que tarda este proceso depende de la cantidad de datos que deban migrarse.

- Elimine el nodo del clúster.

Tenga en cuenta las siguientes consideraciones antes de apagar o encender un nodo:

- Apagar nodos y clústeres conlleva riesgos si no se realiza correctamente.

  El apagado de un nodo debe realizarse bajo la dirección del soporte de NetApp .

- Si un nodo ha estado inactivo durante más de 5,5 minutos bajo cualquier tipo de condición de apagado, la protección de datos Double Helix comienza la tarea de escribir bloques replicados individuales en otro nodo para replicar los datos. En este caso, póngase en contacto con el soporte de NetApp para obtener ayuda con el análisis del nodo que ha fallado.
- Para reiniciar o apagar un nodo de forma segura, puede utilizar el comando de la API Shutdown.
- Si un nodo está inactivo o apagado, debe ponerse en contacto con el soporte de NetApp antes de volver a conectarlo.
- Una vez que un nodo vuelve a estar en línea, debe volver a agregar las unidades al clúster, dependiendo del tiempo que haya estado fuera de servicio.

Para más información

"Sustitución de un chasis SolidFire averiado"

"Sustitución de un nodo de la serie H600S averiado"

Apagar un grupo

Realice el siguiente procedimiento para apagar un clúster completo.

Pasos

1. (Opcional) Comuníquese con el soporte de NetApp para obtener ayuda para completar los pasos preliminares.
2. Verifique que todas las operaciones de E/S se hayan detenido.
3. Desconectar todas las sesiones iSCSI:
   a. Navegue hasta la dirección IP virtual de administración (MVIP) en el clúster para abrir la interfaz de usuario de Element.
   b. Observe los nodos que aparecen en la lista de nodos.
   c. Ejecute el método de la API Shutdown con la opción de detención especificada en cada ID de nodo del clúster.

Al reiniciar el clúster, debe seguir ciertos pasos para verificar que todos los nodos se conecten:

1. Verifique que toda la gravedad crítica y `volumesOffline` Se han resuelto los fallos del clúster.
2. Espere de 10 a 15 minutos para que el grupo se asiente.
3. Comience a iniciar los hosts para acceder a los datos.

Si desea disponer de más tiempo al encender los nodos y verificar que estén en buen estado después del mantenimiento, póngase en contacto con el soporte técnico para obtener ayuda para retrasar la sincronización de datos y evitar la sincronización innecesaria de contenedores.

Encuentra más información

"Cómo apagar y encender correctamente un clúster de almacenamiento NetApp Solidfire/HCI"

Trabajar con utilidades por nodo para nodos de almacenamiento

Trabajar con utilidades por nodo para nodos de almacenamiento

Puede utilizar las utilidades por nodo para solucionar problemas de red si las herramientas de supervisión estándar de la interfaz de usuario del software NetApp Element no le proporcionan suficiente información para la resolución de problemas. Las utilidades por nodo proporcionan información y herramientas específicas que pueden ayudarle a solucionar problemas de red entre nodos o con el nodo de administración.

Encuentra más información

- Acceda a la configuración de cada nodo mediante la interfaz de usuario correspondiente.
- Detalles de la configuración de red desde la interfaz de usuario de cada nodo.
- Detalles de configuración del clúster desde la interfaz de usuario por nodo
- Ejecute pruebas del sistema utilizando la interfaz de usuario por nodo.
- Ejecute las utilidades del sistema mediante la interfaz de usuario de cada nodo.

Acceda a la configuración de cada nodo mediante la interfaz de usuario correspondiente.

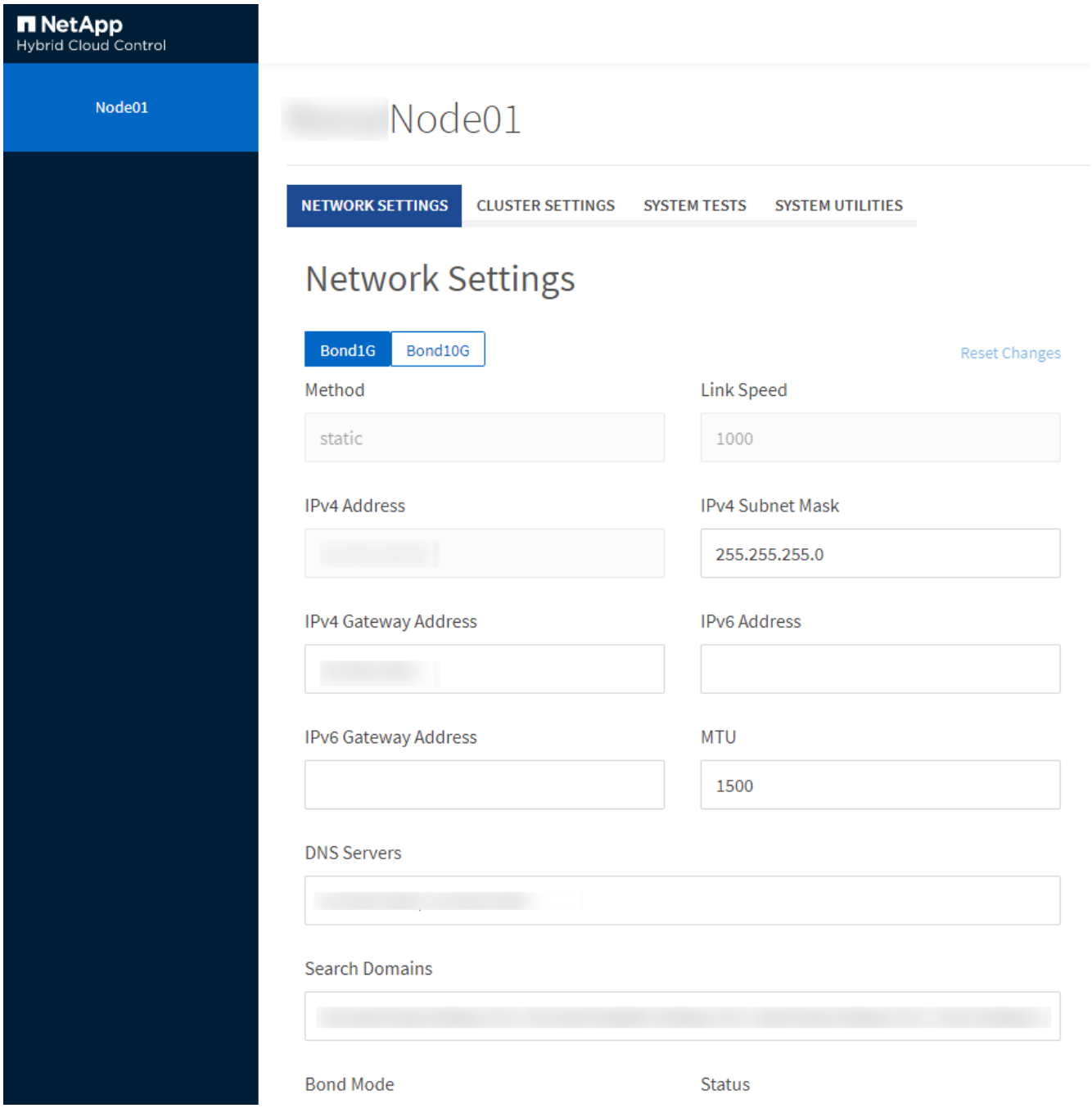
Puede acceder a la configuración de red, la configuración del clúster y las pruebas y utilidades del sistema en la interfaz de usuario por nodo después de ingresar la IP del nodo de administración y autenticarse.

Si desea modificar la configuración de un nodo en estado Activo que forma parte de un clúster, debe iniciar sesión como usuario administrador del clúster.

Debe configurar o modificar un nodo a la vez. Debe asegurarse de que la configuración de red especificada tenga el efecto esperado y de que la red sea estable y funcione correctamente antes de realizar modificaciones en otro nodo.

1. Abra la interfaz de usuario por nodo utilizando uno de los siguientes métodos:

- Ingrese la dirección IP de administración seguida de :442 en una ventana del navegador e inicie sesión con un nombre de usuario y contraseña de administrador.
- En la interfaz de usuario de Element, seleccione **Clúster** > **Nodos** y haga clic en el enlace de la dirección IP de administración del nodo que desea configurar o modificar. En la ventana del navegador que se abre, puede editar la configuración del nodo.



Detalles de la configuración de red desde la interfaz de usuario de cada nodo.

Puede cambiar la configuración de red del nodo de almacenamiento para asignarle un nuevo conjunto de atributos de red.

Puedes ver la configuración de red de un nodo de almacenamiento en la página **Configuración de red** cuando inicies sesión en el nodo. (`https://<node_IP>:442/hcc/node/network-settings`). Puede

seleccionar la configuración **Bond1G** (gestión) o **Bond10G** (almacenamiento). La siguiente lista describe la configuración que puede modificar cuando un nodo de almacenamiento se encuentra en estado Disponible, Pendiente o Activo:

- **Método**

  El método utilizado para configurar la interfaz. Métodos posibles:

  - loopback: Se utiliza para definir la interfaz loopback IPv4.
  - manual: Se utiliza para definir interfaces para las que no se realiza ninguna configuración por defecto.
  - dhcp: Se utiliza para obtener una dirección IP mediante DHCP.
  - estático: Se utiliza para definir interfaces Ethernet con direcciones IPv4 asignadas estáticamente.

- **Velocidad de enlace**

  La velocidad negociada por la NIC virtual.

- **Dirección IPv4**

  La dirección IPv4 para la red eth0.

- **Máscara de subred IPv4**

  Subdivisiones de direcciones de la red IPv4.

- **Dirección de puerta de enlace IPv4**

  Dirección de red del router para enviar paquetes fuera de la red local.

- **Dirección IPv6**

  La dirección IPv6 para la red eth0.

- **Dirección de puerta de enlace IPv6**

  Dirección de red del router para enviar paquetes fuera de la red local.

- **MTU**

  Tamaño máximo de paquete que un protocolo de red puede transmitir. Debe ser mayor o igual a 1500. Si agrega una segunda NIC de almacenamiento, el valor debería ser 9000.

- **Servidores DNS**

  Interfaz de red utilizada para la comunicación del clúster.

- **Dominios de búsqueda**

  Busque direcciones MAC adicionales disponibles para el sistema.

- **Modo de vínculo**

  Puede ser uno de los siguientes modos:

  - ActivoPasivo (predeterminado)

- ALBA
- LACP

- **Estado**

  Valores posibles:

  - En funcionamiento
  - Abajo
  - Arriba

- **Etiqueta de red virtual**

  Etiqueta asignada al crear la red virtual.

- **Rutas**

  Rutas estáticas a hosts o redes específicas a través de la interfaz asociada que las rutas están configuradas para usar.

Detalles de configuración del clúster desde la interfaz de usuario por nodo

Puede verificar la configuración del clúster para un nodo de almacenamiento después de la configuración del clúster y modificar el nombre de host del nodo.

La siguiente lista describe la configuración del clúster para un nodo de almacenamiento indicado en la página **Configuración del clúster** de la interfaz de usuario por nodo. (`https://<node_IP>:442/hcc/node/cluster-settings`).

- **Role**

  Función que desempeña el nodo en el clúster. Valores posibles:

  - Almacenamiento: Nodo de almacenamiento o de canal de fibra.
  - Gestión: Nodo es un nodo de gestión.

- **Nombre de host**

  Nombre del nodo.

- **Grupo**

  Nombre del clúster.

- **Membresía de grupo**

  Estado del nodo. Valores posibles:

  - Disponible: El nodo no tiene un nombre de clúster asociado y aún no forma parte de un clúster.
  - Pendiente: El nodo está configurado y se puede agregar a un clúster designado. No se requiere autenticación para acceder al nodo.
  - PendienteActivo: El sistema está en proceso de instalar software compatible en el nodo. Una vez completado, el nodo pasará al estado Activo.

- Activo: El nodo participa en un clúster. Se requiere autenticación para modificar el nodo.

- **Versión**

  Versión del software Element que se ejecuta en el nodo.

- **Conjunto**

  Nodos que forman parte del conjunto de la base de datos.

- **ID del nodo**

  Se asigna un ID cuando se agrega un nodo al clúster.

- **Interfaz de clúster**

  Interfaz de red utilizada para la comunicación del clúster.

- **Interfaz de gestión**

  Interfaz de red de gestión. Por defecto se utiliza Bond1G, pero también se puede usar Bond10G.

- **Interfaz de almacenamiento**

  Interfaz de red de almacenamiento mediante Bond10G.

- **Capacidad de cifrado**

  Indica si el nodo admite o no el cifrado de unidades.

Ejecute pruebas del sistema utilizando la interfaz de usuario por nodo.

Puedes probar los cambios en la configuración de red después de confirmarlos en la configuración de red. Puedes ejecutar las pruebas para asegurarte de que el nodo de almacenamiento es estable y se puede poner en línea sin problemas.

Has iniciado sesión en la interfaz de usuario por nodo para el nodo de almacenamiento.

1. Haz clic en **Pruebas del sistema**.
2. Haz clic en **Ejecutar prueba** junto a la prueba que deseas ejecutar o selecciona **Ejecutar todas las pruebas**.

   La ejecución de todas las operaciones de prueba puede consumir mucho tiempo y solo debe realizarse bajo la dirección del Soporte de NetApp .

   - **Prueba de conjunto conectado**

     Prueba y verifica la conectividad a un conjunto de bases de datos. Por defecto, la prueba utiliza el conjunto para el clúster con el que está asociado el nodo. Alternativamente, puede proporcionar un conjunto diferente para probar la conectividad.

   - **Prueba Connect Mvip**

     Hace ping a la dirección IP virtual de administración (MVIP) especificada y luego ejecuta una llamada

API simple a la MVIP para verificar la conectividad. Por defecto, la prueba utiliza el MVIP para el clúster con el que está asociado el nodo.

- **Prueba Connect Svip**

  Hace ping a la dirección IP virtual de almacenamiento (SVIP) especificada utilizando paquetes del Protocolo de mensajes de control de Internet (ICMP) que coinciden con el tamaño de la Unidad de transmisión máxima (MTU) configurado en el adaptador de red. Luego se conecta al SVIP como un iniciador iSCSI. Por defecto, la prueba utiliza la SVIP del clúster con el que está asociado el nodo.

- **Configuración de hardware de prueba**

  Comprueba que todas las configuraciones de hardware sean correctas, valida que las versiones de firmware sean correctas y confirma que todas las unidades estén instaladas y funcionando correctamente. Esto es lo mismo que las pruebas de fábrica.

  Esta prueba consume muchos recursos y solo debe ejecutarse si lo solicita el soporte de NetApp .

- **Prueba de conectividad local**

  Prueba la conectividad con todos los demás nodos del clúster haciendo ping a la IP del clúster (CIP) en cada nodo. Esta prueba solo se mostrará en un nodo si este forma parte de un clúster activo.

- **Prueba de localización de clúster**

  Valida que el nodo pueda localizar el clúster especificado en la configuración del clúster.

- **Configuración de red de prueba**

  Verifica que la configuración de red configurada coincida con la configuración de red que se está utilizando en el sistema. Esta prueba no está diseñada para detectar fallos de hardware cuando un nodo participa activamente en un clúster.

- **Prueba de ping**

  Envía un ping a una lista específica de hosts o, si no se especifica ninguna, crea dinámicamente una lista de todos los nodos registrados en el clúster y envía un ping a cada uno para comprobar la conectividad simple.

- **Prueba de conectividad remota**

  Prueba la conectividad a todos los nodos en clústeres emparejados remotamente haciendo ping a la IP del clúster (CIP) en cada nodo. Esta prueba solo se mostrará en un nodo si este forma parte de un clúster activo.

Ejecute las utilidades del sistema mediante la interfaz de usuario de cada nodo.

Puede utilizar la interfaz de usuario por nodo para el nodo de almacenamiento para crear o eliminar paquetes de soporte, restablecer la configuración de las unidades y reiniciar los servicios de red o de clúster.

Has iniciado sesión en la interfaz de usuario por nodo para el nodo de almacenamiento.

1. Haz clic en **Utilidades del sistema**.
2. Haz clic en el botón de la utilidad del sistema que deseas ejecutar.
   - **Control de potencia**

     Reinicia, apaga o desconecta el nodo.

     > Esta operación provoca una pérdida temporal de la conectividad de red.

     Especifique los siguientes parámetros:

     - Acción: Las opciones incluyen Reiniciar y Detener (apagar).
     - Retardo de activación: Cualquier tiempo adicional antes de que el nodo vuelva a estar en línea.
   - **Recopilar registros de nodos**

     Crea un paquete de soporte en el directorio /tmp/bundles del nodo.

     Especifique los siguientes parámetros:

     - Nombre del paquete: Nombre único para cada paquete de soporte creado. Si no se proporciona ningún nombre, se utilizará "supportbundle" y el nombre del nodo como nombre de archivo.
     - Argumentos adicionales: Este parámetro se pasa al script sf_make_support_bundle. Este parámetro solo debe utilizarse a petición del soporte de NetApp .
     - Tiempo de espera (seg.): Especifique el número de segundos que se esperarán para cada respuesta de ping individual.
   - **Eliminar registros del nodo**

     Elimina cualquier paquete de soporte actual en el nodo que se haya creado utilizando **Create Cluster Support Bundle** o el método de API CreateSupportBundle.
   - **Restablecer unidades**

     Inicializa las unidades y elimina todos los datos que residen actualmente en la unidad. Puedes reutilizar la unidad en un nodo existente o en un nodo actualizado.

     Especifique el siguiente parámetro:

     - Unidades: Lista de nombres de dispositivos (no identificadores de unidad) para restablecer.
   - **Restablecer configuración de red**

     Ayuda a resolver problemas de configuración de red para un nodo individual y restablece la configuración de red de un nodo individual a la configuración predeterminada de fábrica.
   - **Reiniciar nodo**

     Restablece un nodo a la configuración de fábrica. Durante esta operación se eliminan todos los datos, pero se conservan los ajustes de red del nodo. Los nodos solo se pueden reiniciar si no están asignados a un clúster y se encuentran en estado Disponible.

     > Al utilizar esta opción, se eliminan del nodo todos los datos, paquetes (actualizaciones de software), configuraciones y archivos de registro.

- **Reiniciar la conexión de red**

  Reinicia todos los servicios de red en un nodo.

  > Esta operación puede provocar una pérdida temporal de la conectividad de la red.

- **Reiniciar servicios**

  Reinicia los servicios de software Element en un nodo.

  > Esta operación puede provocar una interrupción temporal del servicio del nodo. Esta operación solo debe realizarse bajo la dirección del soporte de NetApp .

  Especifique los siguientes parámetros:

  - Servicio: Nombre del servicio que se reiniciará.
  - Acción: Acción a realizar en el servicio. Las opciones incluyen iniciar, detener y reiniciar.

Trabajar con el nodo de gestión

Puede utilizar el nodo de administración (mNode) para actualizar los servicios del sistema, administrar los activos y la configuración del clúster, ejecutar pruebas y utilidades del sistema, configurar Active IQ para la supervisión del sistema y habilitar el acceso al soporte de NetApp para la resolución de problemas.

> Como práctica recomendada, asocie solo un nodo de administración con una instancia de VMware vCenter y evite definir los mismos recursos de almacenamiento y computación o instancias de vCenter en varios nodos de administración.

Ver"Documentación del nodo de gestión" Para más información.

Comprender los niveles de plenitud del clúster

El clúster que ejecuta el software Element genera fallos de clúster para advertir al administrador de almacenamiento cuando el clúster se está quedando sin capacidad. Existen tres niveles de llenado del clúster, todos los cuales se muestran en la interfaz de usuario de NetApp Element : advertencia, error y crítico.

El sistema utiliza el código de error BlockClusterFull para advertir sobre la saturación del almacenamiento de bloques del clúster. Puede consultar los niveles de gravedad de la ocupación del clúster en la pestaña Alertas de la interfaz de usuario de Element.

La siguiente lista incluye información sobre los niveles de gravedad de BlockClusterFull:

- **Advertencia**

  Se trata de una advertencia configurable por el cliente que aparece cuando la capacidad de bloques del clúster se acerca al nivel de gravedad del error. Por defecto, este nivel está establecido en un tres por ciento por debajo del nivel de error y se puede ajustar a través de la interfaz de usuario y la API de Element. Debes añadir más capacidad o liberar capacidad lo antes posible.

- **Error**

  Cuando el clúster se encuentra en este estado, si se pierde un nodo, no habrá suficiente capacidad en el clúster para reconstruir la protección de datos Double Helix. La creación de nuevos volúmenes, clones y snapshots está bloqueada mientras el clúster se encuentra en este estado. Este no es un estado seguro ni recomendable para ningún clúster. Debe agregar más capacidad o liberar capacidad de inmediato.

- **Crítico**

  Este error crítico se ha producido porque el clúster está consumido al 100 por ciento. Se encuentra en estado de solo lectura y no se pueden establecer nuevas conexiones iSCSI al clúster. Cuando se llega a esta etapa, debe liberar o agregar más capacidad de inmediato.

El sistema utiliza el código de error MetadataClusterFull para advertir sobre la falta de espacio de almacenamiento para los metadatos del clúster. Puede consultar el nivel de almacenamiento de metadatos del clúster en la sección Capacidad del clúster de la página Resumen de la pestaña Informes en la interfaz de usuario de Element.

La siguiente lista incluye información sobre los niveles de gravedad de MetadataClusterFull:

- **Advertencia**

  Se trata de una advertencia configurable por el cliente que aparece cuando la capacidad de metadatos del clúster se acerca al nivel de gravedad del error. Por defecto, este nivel está establecido en un tres por ciento por debajo del nivel de error y se puede ajustar a través de la API de Element. Debes añadir más capacidad o liberar capacidad lo antes posible.

- **Error**

  Cuando el clúster se encuentra en este estado, si se pierde un nodo, no habrá suficiente capacidad en el clúster para reconstruir la protección de datos Double Helix. La creación de nuevos volúmenes, clones y snapshots está bloqueada mientras el clúster se encuentra en este estado. Este no es un estado seguro ni recomendable para ningún clúster. Debe agregar más capacidad o liberar capacidad de inmediato.

- **Crítico**

  Este error crítico se ha producido porque el clúster está consumido al 100 por ciento. Se encuentra en estado de solo lectura y no se pueden establecer nuevas conexiones iSCSI al clúster. Cuando se llega a esta etapa, debe liberar o agregar más capacidad de inmediato.

Lo siguiente se aplica a los umbrales de clústeres de dos nodos:

- El error de integridad de metadatos es un 20% inferior al crítico.
- El error de llenado de bloque se produce cuando 1 bloque de capacidad (incluida la capacidad no utilizada) está por debajo del nivel crítico; es decir, cuando la capacidad equivale a dos bloques de capacidad por debajo del nivel crítico.