Gestionar el almacenamiento con el software Element

Element Software

NetApp
April 02, 2025

Tabla de contenidos

Gestionar el almacenamiento con el software Element

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

Element es el sistema operativo de almacenamiento como pieza central de un clúster de 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 presenten como un único sistema de almacenamiento a clientes externos. El software Element es responsable de toda la coordinación, escalado y gestión del clúster en su conjunto.

La interfaz de software se creó sobre la API de Element.

- "Acceda a la interfaz de usuario del software Element"
- "Configure las opciones del sistema SolidFire después de la implementación"
- "Actualice los componentes del sistema de almacenamiento"
- "Use las opciones básicas en la interfaz de usuario del software Element"
- "Gestionar cuentas"
- "Gestione su sistema"
- "Gestione volúmenes y volúmenes virtuales"
- "Proteja sus datos"
- "Solucionar los problemas del sistema"

Obtenga más información

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

Acceda a la interfaz de usuario del software Element

Es posible acceder a la interfaz de usuario de Element mediante la dirección IP virtual de gestión (MVIP) del nodo de clúster principal.

Debe asegurarse de que se hayan deshabilitado los bloqueadores de ventanas emergentes y la configuración de NoScript en el navegador.

Según la configuración durante la creación del clúster, es posible acceder a la interfaz de usuario mediante la dirección IPv4 o IPv6.

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

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

- IPv4: Introduzca la dirección https://[IPv4 MVIP] por ejemplo:

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

2. En el caso de DNS, introduzca el nombre de host.
3. Haga clic en los mensajes de certificados de autenticación que aparezcan.

Obtenga más información

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

Configure las opciones del sistema SolidFire después de la implementación

Después de configurar el sistema SolidFire, quizás desee ejecutar algunas tareas opcionales.

Si cambia las credenciales en el sistema, se recomienda conocer el impacto sobre otros componentes.

Además, es posible configurar la autenticación multifactor, la gestión de claves externa y la seguridad de estándar de procesamiento de información federal (FIPS). También debe revisar las contraseñas cuando sea necesario.

Obtenga más información

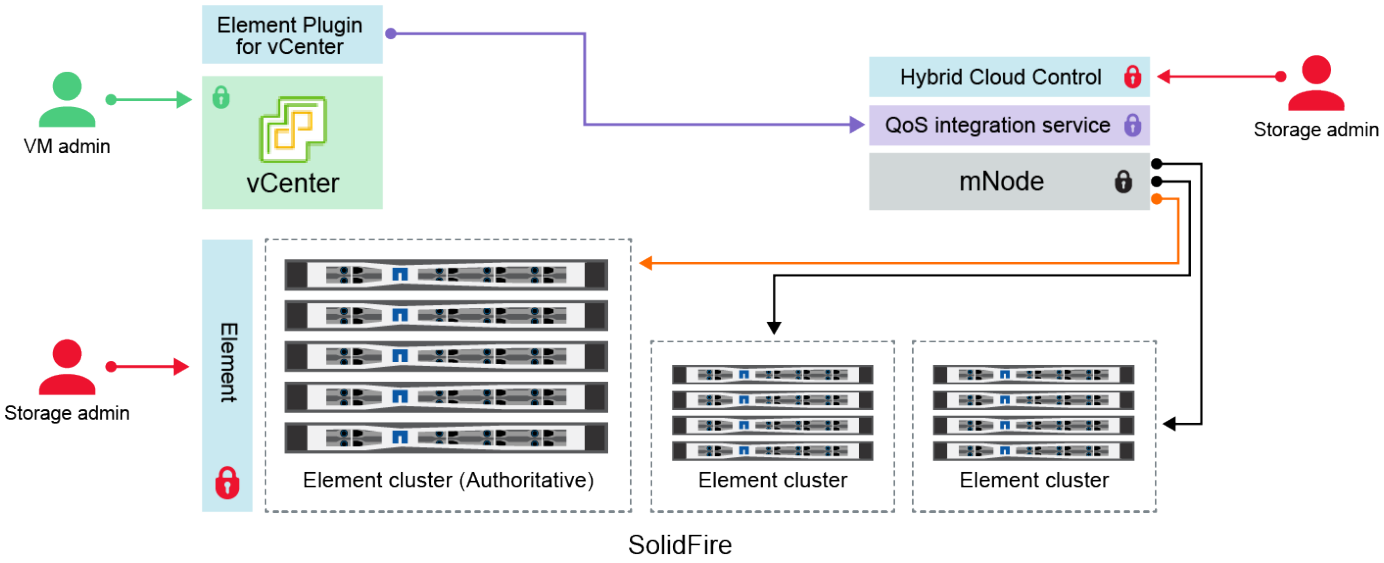
- "Cambie las credenciales en NetApp HCI y SolidFire de NetApp"
- "Cambie el certificado SSL predeterminado del software Element"
- "Cambie la contraseña de IPMI para los nodos"
- "Habilite la autenticación multifactor"
- "Comience con la gestión de claves externas"
- "Cree un clúster que admita unidades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

Cambie las credenciales en NetApp HCI y SolidFire de NetApp

Según las políticas de seguridad de la organización que implementó NetApp HCI o SolidFire de NetApp, los cambios de credenciales o contraseñas suelen formar parte de las prácticas de seguridad. Antes de cambiar las contraseñas, debe tener en cuenta el impacto sobre otros componentes de software en la implementación.

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

Interacciones de componentes de NetApp
SolidFire:



Tipo de credencial e icono	Uso por administrador	Consulte estas instrucciones
Credenciales de Element 	**Se aplica a**: NetApp HCI y SolidFire Los administradores utilizan estas credenciales para iniciar sesión en: • La interfaz de usuario de Element en el clúster de almacenamiento de Element • Control del cloud híbrido en el nodo de gestión (mnode) Cuando Hybrid Cloud Control gestiona varios clústeres de almacenamiento, solo acepta las credenciales de administrador de los clústeres de almacenamiento, conocidas como el *autoritativo cluster* para el que se configuró mnode inicialmente. Para los clústeres de almacenamiento que se añadieron más adelante al control del cloud híbrido, el nodo mnode almacena de forma segura las credenciales de administración. Si se modifican las credenciales para clústeres de almacenamiento añadidos posteriormente, también se deben actualizar las credenciales en mnode con la API mnode.	• "Actualice las contraseñas de administrador del clúster de almacenamiento." • Actualice las credenciales de administrador del clúster de almacenamiento en el nodo mmediante el "API modifyclusteradmin".

Tipo de credencial e icono	Uso por administrador	Consulte estas instrucciones
Credenciales de inicio de sesión único de vSphere 	**Se aplica a**: Sólo NetApp HCI Los administradores utilizan estas credenciales para iniciar sesión en VMware vSphere Client. Cuando vCenter forma parte de la instalación de NetApp HCI, las credenciales se configuran en el motor de implementación de NetApp como lo siguiente: • nombreusuario@vsphere.locloc l con la contraseña especificada, y. • administrator@vsphere.locloc l con la contraseña especificada. Cuando se usa una instancia existente de vCenter para poner en marcha NetApp HCI, los administradores DE TI de VMware gestionan las credenciales de inicio de sesión único de vSphere.	"Actualice las credenciales de vCenter y ESXi".
Credenciales del controlador de administración de la placa base (BMC) 	**Se aplica a**: Sólo NetApp HCI Los administradores utilizan estas credenciales para iniciar sesión en el BMC de los nodos de computación de NetApp en una implementación de NetApp HCI. El BMC proporciona funcionalidades básicas de supervisión de hardware y consola virtual. Las credenciales de BMC (denominadas en ocasiones *IPMI*) para cada nodo de computación de NetApp se almacenan de forma segura en el nodo men las puestas en marcha de NetApp HCI. Control de cloud híbrido de NetApp usa las credenciales de BMC en una capacidad de cuenta de servicio para comunicarse con el BMC en los nodos de computación durante las actualizaciones del firmware de los nodos de computación. Cuando se cambian las credenciales del BMC, también se deben actualizar las credenciales de los nodos de computación respectivos en el mnode para conservar todas las funciones de Hybrid Cloud Control.	• "Configure IPMI para cada nodo en NetApp HCI". • Para los nodos H410C, H610C y H615C, "Cambie la contraseña de IPMI predeterminada". • Para nodos H410S y H610S, "Cambiar la contraseña predeterminada de IPM". • "Cambie las credenciales de BMC en el nodo de gestión".

Tipo de credencial e icono	Uso por administrador	Consulte estas instrucciones
Credenciales de ESXi 	**Se aplica a**: Sólo NetApp HCI Los administradores pueden iniciar sesión en hosts ESXi mediante SSH o la DCUI local con una cuenta raíz local. En implementaciones de NetApp HCI, el nombre de usuario es "raíz" y la contraseña se especificó durante la instalación inicial de ese nodo de computación en el motor de puesta en marcha de NetApp. Las credenciales raíz de ESXi para cada nodo de computación de NetApp se almacenan de forma segura en mnode en puestas en marcha de NetApp HCI. Hybrid Cloud Control de NetApp utiliza las credenciales en una capacidad de cuenta de servicio para comunicarse con hosts ESXi directamente durante las actualizaciones del firmware de los nodos de computación y las comprobaciones del estado. Cuando un administrador de VMware cambia las credenciales raíz de ESXi, las credenciales de los nodos de computación respectivos deben actualizarse en el mnode para mantener la funcionalidad de control de cloud híbrido.	"Actualice las credenciales de para hosts ESXi y vCenter".
Contraseña de integración de la calidad de servicio 	**Se aplica a**: NetApp HCI y opcional en SolidFire No se utiliza para inicios de sesión interactivos por parte de administradores. La integración de calidad de servicio entre VMware vSphere y el software Element se habilita mediante: • Plugin de Element para vCenter Server y. • Servicio QoS en el mnode. Para la autenticación, el servicio QoS utiliza una contraseña que se utiliza exclusivamente en este contexto. La contraseña de calidad de servicio se especifica durante la instalación inicial del plugin de Element para vCenter Server, o bien se genera automáticamente durante la implementación de NetApp HCI. Ningún impacto sobre otros componentes.	"Actualice las credenciales de QoSSIOC en el plugin de NetApp Element para vCenter Server". La contraseña de SIOC del plugin de NetApp Element para vCenter Server también se conoce como *QoSSIOC Password*. Revise el {URL-pico}[plugin de Element para vCenter Server KB].

Tipo de credencial e icono	Uso por administrador	Consulte estas instrucciones
Credenciales de vCenter Service Appliance 	**Se aplica a**: NetApp HCI solo si configura el motor de puesta en marcha de NetApp Los administradores pueden iniciar sesión en las máquinas virtuales del dispositivo de vCenter Server. En implementaciones de NetApp HCI, el nombre de usuario es "raíz" y la contraseña se especificó durante la instalación inicial de ese nodo de computación en el motor de puesta en marcha de NetApp. Según la versión de VMware vSphere implementada, algunos administradores del dominio de inicio de sesión único de vSphere también pueden iniciar sesión en el dispositivo. Ningún impacto sobre otros componentes.	No es necesario realizar cambios.
Credenciales de administrador del nodo de gestión de NetApp 	**Se aplica a**: NetApp HCI y opcional en SolidFire Los administradores pueden iniciar sesión en las máquinas virtuales del nodo de gestión de NetApp para obtener una configuración avanzada y solucionar problemas. Según la versión del nodo de gestión puesta en marcha, el inicio de sesión a través de SSH no se habilita de forma predeterminada. En implementaciones de NetApp HCI, el usuario y la contraseña fueron especificados durante la instalación inicial de ese nodo de computación en el motor de puesta en marcha de NetApp. Ningún impacto sobre otros componentes.	No es necesario realizar cambios.

Obtenga más información

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

Cambie el certificado SSL predeterminado del software Element

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

Cuando se crea un clúster de software de NetApp Element, el clúster crea un certificado único de capa de sockets seguros (SSL) con firma automática y una clave privada que se utiliza para todas las comunicaciones 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 que una entidad de certificación (CA) de confianza emite y verifica.

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

- **GetSSLCertificate**

  Puede utilizar el "Método GetSSLCertificate" Para recuperar información acerca del certificado SSL instalado actualmente, incluidos todos los detalles del certificado.

- **SetSSLCertificate**

  Puede utilizar el "Método SetSSLCertificate" Para establecer los certificados SSL por clúster y por nodo en el certificado y la clave privada que suministre. El sistema valida el certificado y la clave privada para evitar que se aplique un certificado no válido.

- **RemoveSSLCertificate**

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

> El certificado SSL de clúster se aplica automáticamente a todos los nodos nuevos que se añaden al clúster. Cualquier nodo que se quite del clúster se revierte a un certificado autofirmado y toda la información de claves y certificados definidos por el usuario se elimina del nodo.

Obtenga más información

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

Cambie la contraseña de IPMI predeterminada para los nodos

En cuanto tenga acceso IPMI remoto al nodo, puede cambiar la contraseña predeterminada del administrador de la interfaz de gestión de plataformas inteligentes (IPMI). Puede que desee hacerlo si se han actualizado alguna instalación.

Para obtener más información acerca de cómo configurar el acceso IPM para los nodos, consulte "Configure IPMI para cada nodo".

Puede cambiar la contraseña de IPM para estos nodos:

- Nodos H410S
- Nodos H610S

Cambie la contraseña de IPMI predeterminada para los nodos H410S

En cuanto configure el puerto de red IPMI, debe cambiar la contraseña predeterminada de la cuenta de administrador de IPMI en cada nodo de almacenamiento.

Lo que necesitará

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

Pasos

1. Abra un explorador web en un equipo que pueda acceder a la red de IPMI y vaya a la dirección IP de IPMI correspondiente al nodo.
2. Introduzca el nombre de usuario `ADMIN` y contraseña `ADMIN` en la solicitud de inicio de sesión de.
3. Después de iniciar sesión, haga clic en la ficha **Configuración**.
4. Haga clic en **usuarios**.
5. Seleccione la `ADMIN` 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. Haga clic en **Modificar** y, a continuación, haga clic en **Aceptar**.
9. Repita este procedimiento para todos los demás nodos H410S con contraseñas IPMI predeterminadas.

Cambie la contraseña de IPMI predeterminada para los nodos H610S

En cuanto configure el puerto de red IPMI, debe cambiar la contraseña predeterminada de la cuenta de administrador de IPMI en cada nodo de almacenamiento.

Lo que necesitará

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

Pasos

1. Abra un explorador web en un equipo que pueda acceder a la red de IPMI y vaya a la dirección IP de IPMI correspondiente al nodo.
2. Introduzca el nombre de usuario `root` y contraseña `calvin` en la solicitud de inicio de sesión de.
3. Después de iniciar sesión, haga clic en el icono de navegación del menú que aparece en la parte superior izquierda de la página para abrir el cajón de la barra lateral.
4. Haga clic en **Configuración**.
5. Haga clic en **Administración de usuarios**.
6. Seleccione el usuario **Administrador** de la lista.
7. Active la casilla de verificación **Cambiar contraseña**.
8. Introduzca una nueva contraseña segura en los campos **Contraseña** y **Confirmar contraseña**.
9. Haga clic en **Guardar** en la parte inferior de la página.
10. Repita este procedimiento para todos los demás nodos H610S con contraseñas de IPMI predeterminadas.

Obtenga más información

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

Use las opciones básicas en la interfaz de usuario del software Element

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

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

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

Si quiere más información

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

Ver la actividad de la API

El sistema Element usa la API de NetApp Element como base para sus funciones y funcionalidades. La interfaz de usuario de Element le permite ver diversos tipos de actividad de la API en tiempo real en el sistema conforme utiliza la interfaz. Con el registro de la API, puede ver la actividad de la API del sistema en segundo plano y la que ha iniciado el usuario, así como las llamadas API que se han hecho en la página que está viendo en ese momento.

Puede usar el registro de API para identificar qué métodos API se usan en determinadas tareas y cómo se usan los objetos y los métodos API para crear aplicaciones personalizadas.

Para obtener más información sobre cada método, consulte "Referencia de API del software Element".

1. En la barra de navegación de la interfaz de usuario de Element, haga clic en **API Log**.
2. Realice los siguientes pasos para modificar el tipo de actividad de API que se muestra en la ventana API Log:
   a. Seleccione **peticiones** para mostrar el tráfico de solicitud de 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:
      - **Usuario iniciado**: Tráfico API por sus actividades durante esta sesión de interfaz de usuario web.
      - * Sondeo de fondo*: Tráfico de API generado por la actividad del sistema en segundo plano.
      - **Página actual**: Tráfico de API generado por tareas en la página que está viendo actualmente.

Obtenga más información

- "Gestionar el almacenamiento con la API de Element"
- "Documentación de SolidFire y el software Element"

- "Plugin de NetApp Element para vCenter Server"

Tasa de actualización de la interfaz 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 los datos para ciertas porciones de la página de software de NetApp Element que está viendo.

Los valores predeterminados del intervalo de actualización se restablecen cuando la página se vuelve a cargar en el navegador. El intervalo de actualización actual se puede ver si hace clic en el nombre del clúster en la parte superior derecha de la página. Hay que tener en cuenta que el intervalo determina la frecuencia con la que se realizan las solicitudes de API, no la rapidez con la que los datos regresan del servidor.

Cuando la carga del clúster es muy pesada, puede poner en cola las solicitudes de API de la interfaz de usuario de Element. En las pocas ocasiones, cuando la respuesta del sistema se retrasa significativamente, como una conexión de red lenta combinada con un clúster ocupado, puede optar por cerrar la sesión de la interfaz de usuario de Element si el sistema no responde a las solicitudes de API en cola con la suficiente rapidez. Si se le redirige a la pantalla de cierre de sesión, puede volver a iniciar sesión después de desactivar cualquier solicitud de autenticación inicial del navegador. Tras volver a la página de introducción, se le pueden pedir las credenciales del clúster si no las ha guardado en el navegador.

Iconos en la interfaz de Element

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

La tabla siguiente proporciona una referencia rápida:

.	Descripción
	Acciones
	Backup a.
	Clonar o copiar
	Eliminar o purgar
	Editar
	Filtro
	Emparejar

	Actualice
	Restaurar
	Restaurar desde
	Revertir
	Snapshot

Enviar comentarios

Es posible mejorar la interfaz de usuario web del software Element y solucionar cualquier problema con la interfaz de usuario mediante el formulario de comentarios al que se puede acceder en toda la interfaz de usuario.

1. En cualquier página de la interfaz de usuario del elemento, haga clic en el botón **Comentarios**.
2. Introduzca la información que corresponda en los campos Summary y Description.
3. Adjunte las capturas de pantalla que le ayuden.
4. Introduzca un nombre y una dirección de correo electrónico.
5. Active la casilla para incluir datos sobre su entorno actual.
6. Haga clic en **Enviar**.

Obtenga más información

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

Gestionar cuentas

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

- "Trabaje con cuentas que utilicen CHAP"
- "Gestione cuentas de usuario administrador del clúster"

Si quiere más información

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

Trabaje con cuentas que utilicen CHAP

En los sistemas de almacenamiento de SolidFire, los inquilinos pueden utilizar las cuentas para permitir que los clientes se conecten a volúmenes en un clúster. Una cuenta contiene la autenticación mediante protocolo de autenticación por desafío mutuo (CHAP) que se necesita para acceder a los volúmenes que tiene asignados. Cuando crea un volumen, este se asigna a una cuenta específica.

Una cuenta puede tener hasta 2000 volúmenes asignados, pero un volumen solo puede pertenecer a una cuenta.

Crear una cuenta

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

Cada nombre de cuenta del sistema debe ser exclusivo.

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

   Puede dejar los campos de credenciales vacíos para que cualquier contraseña se genere automáticamente.

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

Ver los detalles de la cuenta

La actividad de rendimiento de cada cuenta se puede ver como un gráfico.

El gráfico proporciona información de I/o y rendimiento de la cuenta. Los niveles de actividad promedio y pico se muestran en incrementos de períodos de informe de 10 segundos. Estas estadísticas incluyen la actividad de todos los volúmenes asignados a la cuenta.

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

Estos son algunos de los detalles:

- **Estado**: El estado de la cuenta. Los posibles valores son los siguientes:

- Active: Una cuenta activa.
- Locked: Una cuenta bloqueada.
- Deleted: Una cuenta que se ha eliminado y purgado.

- **Volúmenes activos**: Número de volúmenes activos asignados a la cuenta.
- **Compresión**: La puntuación de eficiencia de compresión para los volúmenes asignados a la cuenta.
- **Deduplicación**: La puntuación de eficiencia de deduplicación para los volúmenes asignados a la cuenta.
- **Thin Provisioning**: La puntuación de eficiencia de thin provisioning para los volúmenes asignados a la cuenta.
- **Eficiencia general**: La puntuación de eficiencia general para los volúmenes asignados a la cuenta.

Editar una cuenta

Una cuenta se puede editar para cambiar el estado, cambiar los secretos de CHAP o modificar el nombre de la cuenta.

Si se modifica la configuración de CHAP en una cuenta o se quitan los iniciadores o los volúmenes de un grupo de acceso, se podría interrumpir el acceso de los iniciadores a los volúmenes de forma inesperada. Para asegurarse de que no se interrumpirá el acceso a los volúmenes de forma inesperada, siempre debe cerrar las sesiones iSCSI afectadas por alguno de los cambios en la cuenta o en el grupo de acceso. Asimismo, compruebe que los iniciadores pueden volver a conectarse con los volúmenes una vez que se hayan realizado los cambios en la configuración del iniciador y la configuración del clúster.

Los volúmenes persistentes asociados con servicios de gestión se asignan a una cuenta nueva que se crea durante la instalación o la actualización. Si utiliza volúmenes persistentes, no modifique o elimine su cuenta asociada.

1. Seleccione **Administración** > **Cuentas**.
2. Haga clic en el icono Actions de una cuenta.
3. En el menú que se abre, seleccione **Editar**.
4. **Opcional:** edite el **Nombre de usuario**.
5. **Opcional:** haga clic en la lista desplegable **Estado** y seleccione un estado diferente.

   Al cambiar el estado a **Locked** se cierran todas las conexiones iSCSI a la cuenta y ya no se puede acceder a ella. Los volúmenes asociados con la cuenta se mantienen, pero ya no se podrán detectar los volúmenes con iSCSI.

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

   Si no cambia las credenciales **Configuración CHAP**, seguirán siendo las mismas. Si deja vacíos los campos de las credenciales, el sistema generará contraseñas nuevas.

7. Haga clic en **Guardar cambios**.

Eliminar una cuenta

Una cuenta se puede eliminar cuando ya no se necesita.

Debe eliminar y purgar los volúmenes asociados con la cuenta antes de eliminarla.

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

1. Seleccione **Administración** > **Cuentas**.
2. Haga clic en el icono Actions de la cuenta que quiera eliminar.
3. En el menú que se abre, seleccione **Eliminar**.
4. Confirme la acción.

Obtenga más información

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

Gestione cuentas de usuario administrador del clúster

Para gestionar las cuentas de administrador de clúster correspondientes a un sistema de almacenamiento de SolidFire, debe crear, eliminar y editar cuentas de administrador de clúster, cambiar la contraseña de administrador de clúster y configurar las opciones de LDAP para gestionar el acceso a los usuarios al sistema.

Tipos de cuenta de administrador del clúster de almacenamiento

Existen dos tipos de cuentas de administrador que pueden existir en un clúster de almacenamiento que ejecuta el software NetApp Element: La cuenta de administrador de clúster principal y una cuenta de administrador de clúster.

- **Cuenta de administrador del clúster principal**

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

- **Cuenta de administrador de clúster**

  Puede conceder a una cuenta de administrador de clúster una gama limitada de accesos de administrador para realizar determinadas tareas dentro de un clúster. Las credenciales que se asignan a cada cuenta de administrador de clúster sirven para autenticar las solicitudes de la API y la interfaz de usuario de Element dentro del sistema de almacenamiento.

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

Ver los detalles de administrador del clúster

1. Si desea crear una cuenta de administrador de clúster (que no sea LDAP) para todo el clúster, realice las siguientes acciones:

a. Haga clic en **usuarios** > **Administradores de clúster**.

2. En la página Cluster Admins de la pestaña Users, puede ver la siguiente información.
   - **ID**: Número secuencial asignado a la cuenta de administrador del clúster.
   - **Nombre de usuario**: El nombre otorgado a la cuenta de administrador del clúster cuando se creó.
   - **Acceso**: Los permisos de usuario asignados a la cuenta de usuario. Los posibles valores son los siguientes:
     - lea
     - creación de informes
     - nodos
     - unidades
     - volúmenes
     - cuentas
     - Administradores de clústeres
     - administrador

     Todos los permisos están disponibles para el tipo de acceso del administrador.
   - **Tipo**: El tipo de administrador de clúster. Los posibles valores son los siguientes:
     - Clúster
     - LDAP
   - **Atributos**: Si la cuenta de administrador de clúster se creó mediante la API de elemento, esta columna muestra cualquier par nombre-valor que se haya establecido utilizando ese método.

     Consulte "Referencia de API del software NetApp Element".

Cree una cuenta de administrador de clúster

Es posible crear nuevas cuentas de administrador de clúster con permisos para conceder o restringir el acceso a determinadas áreas del sistema de almacenamiento. Cuando se configuran los permisos de la cuenta de administrador del clúster, el sistema otorga derechos de solo lectura a aquellos permisos que no se asignen 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 de LDAP con la interfaz de usuario de Element"

Más adelante, los privilegios de la cuenta de administrador de clúster se pueden cambiar para crear informes, nodos, unidades, volúmenes, cuentas y acceso a nivel de clúster. Cuando habilita un permiso, el sistema asigna acceso de escritura para ese nivel. Para los niveles que no se seleccionan, el sistema concede al usuario administrador acceso de solo lectura.

También es posible quitar más adelante cualquier cuenta de usuario administrador de clúster que haya creado un administrador del sistema. Sin embargo, no es posible quitar la cuenta de administrador de clúster principal que se generó al crear el clúster.

1. Si desea crear una cuenta de administrador de clúster (que no sea LDAP) para todo el clúster, realice las

siguientes acciones:

a. Haga clic en **usuarios** > **Administradores de clúster**.
b. Haga clic en **Crear administrador de clúster**.
c. Seleccione el tipo de usuario **Cluster**.
d. Introduzca un nombre de usuario y una contraseña para la cuenta y confirme la contraseña.
e. Seleccione los permisos de usuario que se van a aplicar a la cuenta.
f. Active la casilla con la que se acepta el contrato de licencia para usuario final de.
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 **Cluster** > **LDAP**.
b. Asegúrese de que la autenticación LDAP está habilitada.
c. Haga clic en **probar autenticación de usuario** y copie el nombre completo que aparece para el usuario o uno de los grupos de los que el usuario es miembro para poder pegarlo más tarde.
d. Haga clic en **usuarios** > **Administradores de 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 completo distintivo para el usuario o grupo. Como alternativa, péguela desde el nombre distintivo que copió anteriormente.

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

Para agregar usuarios o grupos de administración de clúster LDAP, el formato general del nombre de usuario es "'LDAP:<Full Distinguished Name>'".

a. Seleccione los permisos de usuario que se van a aplicar a la cuenta.
b. Active la casilla con la que se acepta el contrato de licencia para usuario final de.
c. Haga clic en **Crear administrador de clúster**.

Edite los permisos de administrador del clúster

Los privilegios de la cuenta de administrador de clúster se pueden cambiar para crear informes, nodos, unidades, volúmenes y cuentas. y acceso a nivel de clúster. Cuando habilita un permiso, el sistema asigna acceso de escritura para ese nivel. Para los niveles que no se seleccionan, el sistema concede al usuario administrador acceso de solo lectura.

1. Haga clic en **usuarios** > **Administradores de clúster**.
2. Haga clic en el icono Actions del administrador de clúster que quiera editar.
3. Haga clic en **Editar**.
4. Seleccione los permisos de usuario que se van a aplicar a la cuenta.
5. Haga clic en **Guardar cambios**.

Cambiar contraseñas de las cuentas de administrador del clúster

Es posible usar la interfaz de usuario de Element para cambiar las contraseñas de administrador de clúster.

1. Haga clic en **usuarios** > **Administradores de clúster**.
2. Haga clic en el icono Actions del administrador de clúster que quiera editar.
3. Haga clic en **Editar**.
4. En el campo Change Password, introduzca una contraseña nueva y confírmela.
5. Haga clic en **Guardar cambios**.

Obtenga más información

- "Habilite la autenticación de LDAP con la interfaz de usuario de Element"
- "Deshabilite LDAP"
- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Gestione LDAP

Puede configurar el protocolo ligero de acceso a directorios (LDAP) para habilitar la funcionalidad de inicio de sesión seguro basado en directorios en el almacenamiento de SolidFire. Se puede configurar LDAP en el nivel del clúster y autorizar grupos y usuarios de LDAP.

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

Es posible usar tanto direcciones IPv4 como IPv6.

Habilitar LDAP implica los siguientes pasos de alto nivel, descritos con detalle:

1. **Completar los pasos de preconfiguración para compatibilidad con LDAP**. Valide tener todos los detalles necesarios para configurar la autenticación LDAP.
2. **Activar autenticación LDAP**. Use la interfaz de usuario de Element o la API de Element.
3. **Validar la configuración LDAP**. De manera opcional, compruebe que el clúster se haya configurado con los valores correctos ejecutando el método API GetLdapConfiguration o comprobando la configuración LCAP mediante la interfaz de usuario de Element.
4. **Pruebe la autenticación LDAP** (con la `readonly` usuario). Compruebe que la configuración de LDAP sea correcta mediante la ejecución del método API TestLdapAuthentication o mediante la interfaz de usuario de Element. Para esta prueba inicial, utilice el nombre de usuario «sAMAccountName» del `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. **Pruebe la autenticación LDAP** (con una cuenta de usuario que desea agregar). Repita setp 4 con una cuenta de usuario que desee agregar como administrador de clúster de Element. Copie el `distinguished` Nombre (DN) o usuario (o grupo). Este DN se utilizará en el paso 6.
6. **Agregue el administrador del clúster LDAP** (copie y pegue el DN del paso probar autenticación LDAP). Mediante la interfaz de usuario de Element o el método 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 ha copiado en el paso 5. Esto asegura que el DN está formateado correctamente.

7. **Pruebe el acceso de administrador del clúster**. Inicie sesión en el clúster con el usuario administrador del clúster LDAP recién creado. Si agregó un grupo LDAP, puede iniciar sesión como cualquier usuario de ese grupo.

Complete los pasos previos de configuración para ser compatible con LDAP

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

Pasos

1. Configure un servidor de Active Directory de Windows.
2. **Opcional:** Activar soporte LDAPS.
3. Crear usuarios y grupos.
4. Cree una cuenta de servicio de sólo lectura (como «sfreadonly») que se utilizará para buscar en el directorio LDAP.

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

Puede configurar la integración del sistema de almacenamiento con un servidor LDAP existente. De este modo, los administradores de LDAP pueden gestionar de forma centralizada el acceso al sistema de almacenamiento para los usuarios.

Es posible configurar LDAP con la interfaz de usuario de Element o la API de Element. Este procedimiento describe cómo configurar LDAP mediante la interfaz de usuario de Element.

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

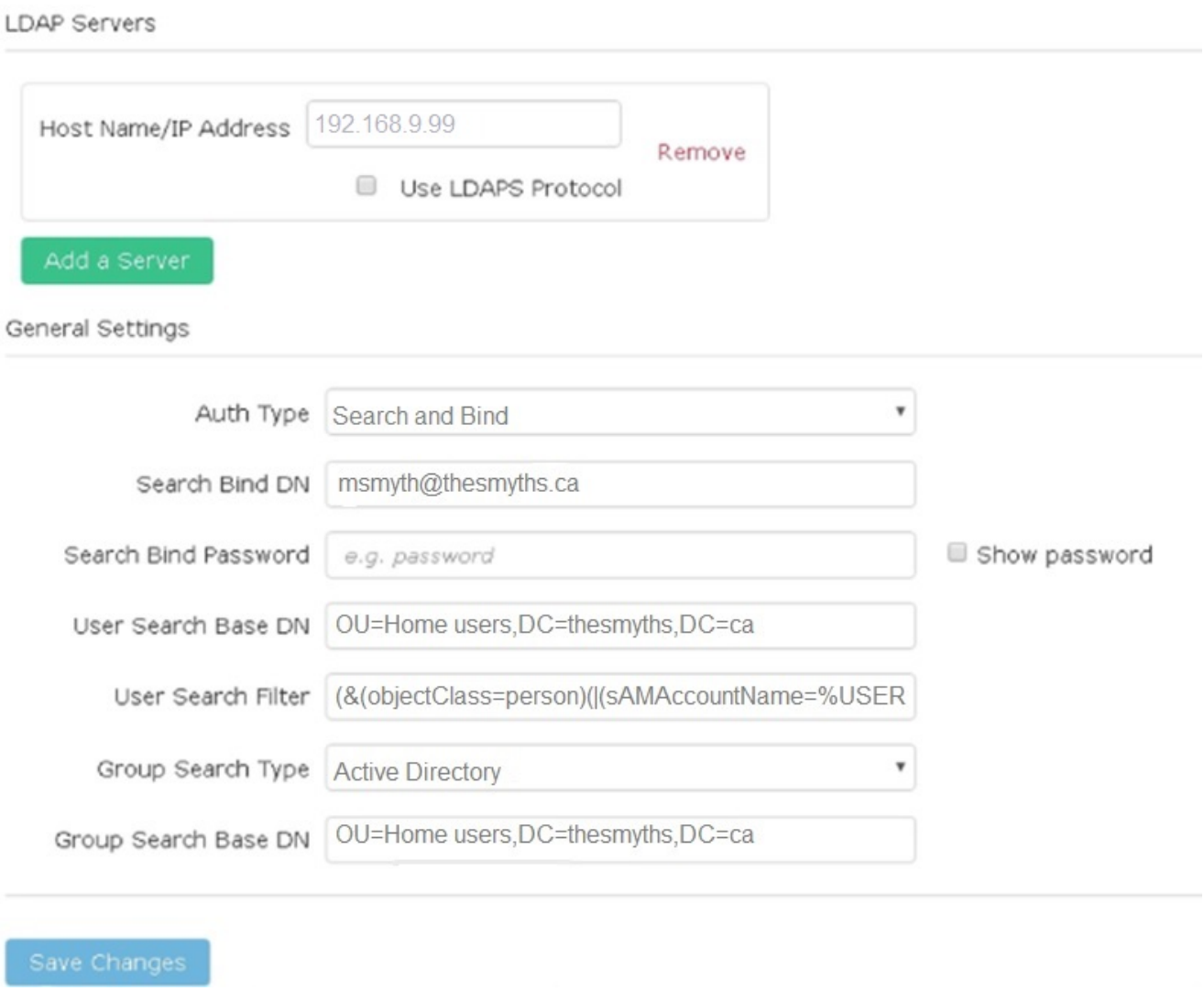
Pasos

1. Haga clic en **Cluster** > **LDAP**.
2. Haga clic en **Sí** para activar la autenticación LDAP.
3. Haga clic en **Agregar un servidor**.
4. Introduzca **Nombre de host/dirección IP**.

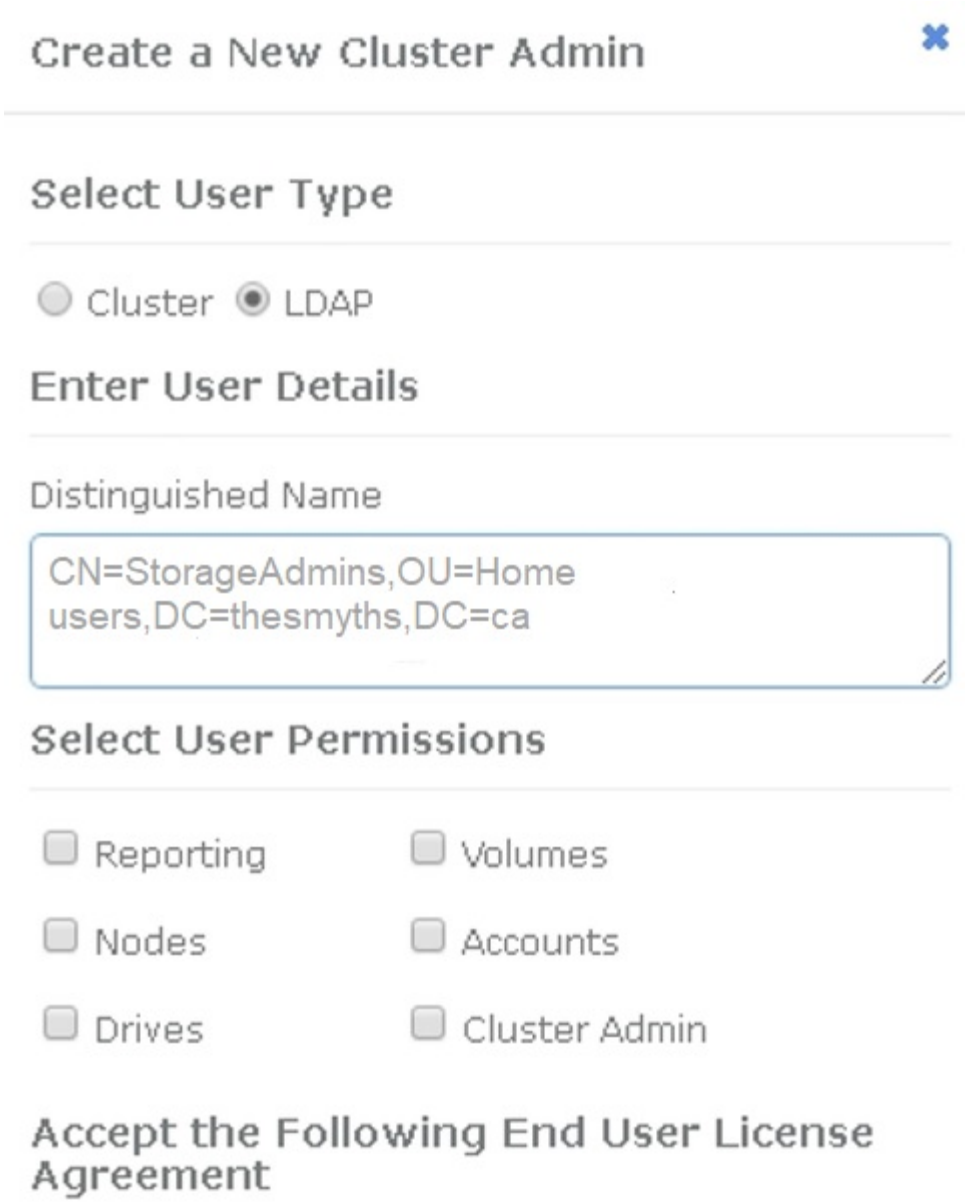
   También puede introducir un número de puerto personalizado opcional.

   Por ejemplo, para añadir un número de puerto personalizado, introduzca <host name or ip address>:<port number>

5. **Opcional:** Seleccione **Use LDAPS Protocol**.
6. Introduzca la información necesaria en **Ajustes generales**.



7. Haga clic en **Activar LDAP**.
8. Haga clic en **probar autenticación de usuario** si desea probar el acceso al servidor para un usuario.
9. Copie la información del nombre distintivo y del grupo de usuarios que aparece para usarla más adelante cuando se crean administradores de clúster.
10. Haga clic en **Guardar cambios** para guardar cualquier configuración nueva.
11. Para crear un usuario en este grupo de modo que cualquiera pueda iniciar sesión, realice lo siguiente:
    a. Haga clic en **Usuario** > **Ver**.



b. Para el nuevo usuario, haga clic en **LDAP** para el tipo de usuario y pegue el grupo que copió en el campo Nombre distintivo.
c. Seleccione los permisos, normalmente todos los permisos.
d. Desplácese hasta el Contrato de licencia para el usuario final y haga clic en **Acepto**.
e. Haga clic en **Crear administrador de clúster**.

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

Para probarlo, cierre sesión en la interfaz de usuario del elemento y vuelva a iniciarla como usuario en ese grupo.

Habilite la autenticación de LDAP con la API de Element

Puede configurar la integración del sistema de almacenamiento con un servidor LDAP existente. De este modo, los administradores de LDAP pueden gestionar de forma centralizada el acceso al sistema de almacenamiento para los usuarios.

Es posible configurar LDAP con la interfaz de usuario de Element o la API de Element. Este procedimiento describe cómo configurar LDAP mediante 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 `EnableLdapAuthentication` Método API.

Pasos

1. Habilite la autenticación LDAP primero en el clúster de mediante el `EnableLdapAuthentication` Método API.
2. Especifique la información obligatoria.

```
{
     "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
AuthType: SearchAndBind	Dicta que el clúster utilizará la cuenta de servicio readonly para buscar primero el usuario que se va a autenticar y, a continuación, enlazar ese usuario si se encuentra y se autentica.
GroupSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	Especifica la ubicación en el árbol LDAP para comenzar a buscar grupos. Para este ejemplo, hemos utilizado la raíz de nuestro árbol. Si su árbol LDAP es muy grande, quizás desee establecer este árbol en un subárbol más granular para reducir los tiempos de búsqueda.

Parámetros utilizados	Descripción
UserSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	Especifica la ubicación en el árbol LDAP para comenzar a buscar usuarios. Para este ejemplo, hemos utilizado la raíz de nuestro árbol. Si su árbol LDAP es muy grande, quizás desee establecer este árbol en un subárbol más granular para reducir los tiempos de búsqueda.
GroupSearchType: ActiveDirectory	Utiliza el servidor de Windows Active Directory como servidor LDAP.

`userSearchFilter: "(&(objectClass=person)(sAMAccountName=%USERNAME%))"`
 	
Para utilizar userPrincipalName (dirección de correo electrónico para el inicio de sesión), puede cambiar userSearchFilter a:
 	
`"(&(objectClass=person)(userPrincipalName=%USERNAME%))"`
 	
O bien, para buscar userPrincipalName y sAMAccountName, puede usar el siguiente usuarioSearchFilter:
 	
`"(&(objectClass=person)(`
	(SAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%))" ----

Utiliza sAMAccountName como nombre de usuario para iniciar sesión en el clúster de SolidFire. Esta configuración indica a LDAP que busque el nombre de usuario especificado durante el inicio de sesión en el atributo sAMAccountName y que también limite la búsqueda a entradas que tengan "'Person'" como valor en el atributo objectClass.	SearchBindDN
Es el nombre completo del usuario readonly que se utilizará para buscar en el directorio LDAP. Para un directorio activo suele ser más fácil utilizar userPrincipalName (formato de dirección de correo electrónico) para el usuario.	SearchBindPassword

Para probarlo, cierre sesión en la interfaz de usuario del elemento y vuelva a iniciarla como usuario en ese grupo.

Ver los detalles de LDAP

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

Debe habilitar LDAP para ver estas opciones de configuración de LDAP.

1. Para ver los detalles de LDAP con la interfaz de usuario de Element, haga clic en **Cluster** > **LDAP**.
   - **Nombre de host/Dirección IP**: Dirección de un servidor de directorio LDAP o LDAPS.
   - **Tipo de autenticación**: El método de autenticación de usuario. Los posibles valores son los siguientes:
     - Enlace directo
     - Búsqueda y vinculación
   - **Buscar Bind DN**: Un DN completo con el que conectarse para realizar una búsqueda LDAP del usuario (necesita acceso de nivel de enlace al directorio LDAP).
   - **Buscar Contraseña de enlace**: Contraseña utilizada para autenticar el acceso al servidor LDAP.
   - **User Search base DN**: El DN base del árbol utilizado para iniciar la búsqueda del usuario. El sistema busca el subárbol de 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. Los posibles valores son los siguientes:
     - Active Directory: Pertenencia anidada de todos los grupos LDAP de un usuario.
     - No hay grupos: Ningún soporte de grupo.
     - DN de miembro: Grupos de tipo DN de miembro (un nivel).
   - **DN base de búsqueda de grupo**: El DN base del árbol utilizado para iniciar la búsqueda de grupo. El sistema busca el subárbol de la ubicación especificada.
   - **Probar autenticación de usuario**: Después de configurar LDAP, utilice esta opción para probar la autenticación de nombre de usuario y contraseña para el servidor LDAP. Introduzca una cuenta que ya existe para probarlo. Se muestra la información relacionada con el nombre distintivo y el grupo de usuarios, que se puede copiar para usarlo más adelante al crear administradores de clúster.

Pruebe la configuración de LDAP

Después de configurar LDAP, debe probarla mediante la interfaz de usuario de Element o la API de Element `TestLdapAuthentication` método.

Pasos

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

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

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

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

b. Revise los resultados. Si la llamada API es correcta, los resultados incluyen el nombre completo del usuario especificado y una lista de grupos en los que el usuario es miembro.

```
{
"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"
     }
}
```

Deshabilite LDAP

Es posible deshabilitar la integración de LDAP con la interfaz de usuario de Element.

Antes de comenzar, debe tener en cuenta todas las opciones de configuración, ya que al deshabilitar LDAP se borran todas las opciones.

Pasos

1. Haga clic en **Cluster** > **LDAP**.
2. Haga clic en **no**.
3. Haga clic en **Desactivar LDAP**.

Obtenga más información

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

Gestione su sistema

Puede gestionar el sistema en la interfaz de usuario de Element. Esto incluye habilitar la autenticación multifactor, gestionar la configuración de clústeres, admitir estándares de

procesamiento de información federal (FIPS) y el uso de gestión de claves externa.

- "Habilite la autenticación multifactor"
- "Configure las opciones del clúster"
- "Cree un clúster que admita unidades FIPS"
- "Comience con la gestión de claves externas"

Si quiere más información

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

Habilite la autenticación multifactor

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

Configure la autenticación de múltiples factores

Es posible usar estos pasos básicos a través de la API de Element para configurar el clúster con el fin de utilizar la autenticación multifactor.

Puede encontrar más detalles de cada método de API en la "Referencia de la API de Element".

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

   Los metadatos de IDP, en formato de texto sin formato, se recuperan del IDP de terceros. Estos metadatos se deben validar para asegurarse de que están formateados correctamente en JSON. Hay numerosas aplicaciones de formateador JSON disponibles que puede utilizar, por ejemplo:https://freeformatter.com/json-escape.html.

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

   SpMetadataUrl es una URL que se utiliza para recuperar metadatos del proveedor de servicios del clúster para el IDP con el fin de establecer una relación de confianza.

3. Configure las afirmaciones SAML en el IDP de terceros para incluir el atributo "'NameID'" para identificar de forma exclusiva a un usuario para el registro de auditorías y para que Single Logout funcione correctamente.
4. Cree una o varias cuentas de usuario administrador del clúster autenticadas por un IDP de terceros para su autorización, llamando al siguiente método API:`AddIdpClusterAdmin`

El nombre de usuario del administrador del clúster IDP debe coincidir con el mapa de nombre/valor del atributo SAML del 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.
- Group=cluster-Administrator: Donde el IDP está configurado para liberar una propiedad de grupo en la que todos los usuarios deberían tener acceso. Tenga en cuenta que el emparejamiento nombre/valor del atributo SAML distingue mayúsculas y minúsculas por motivos de seguridad.

5. Habilite la MFA para el clúster llamando al siguiente método API: `EnableIdpAuthentication`

Obtenga más información

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

Información adicional para la autenticación multifactor

Debe conocer las siguientes advertencias en relación con la autenticación de múltiples factores.

- Para actualizar los certificados de IDP que ya no son válidos, deberá usar un usuario administrador no IDP para llamar al siguiente método API: `UpdateIdpConfiguration`
- La MFA es incompatible con certificados con una longitud inferior a 2048 bits. De manera predeterminada, se crea un certificado SSL de 2048 bits en el clúster. Debe evitar establecer un certificado de menor tamaño cuando llame al método de API: `SetSSLCertificate`

Si el clúster utiliza un certificado que sea inferior a 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 una versión posterior.

- Los usuarios del administrador de IDP no pueden utilizarse para realizar llamadas de API directamente (por ejemplo, mediante SDK o Postman) o para otras integraciones (por ejemplo, OpenStack Cinder o el complemento vCenter). Si necesita crear usuarios que tengan estas capacidades, añada usuarios bien al administrador del clúster LDAP o usuarios de administrador del clúster local.

Obtenga más información

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

Configure las opciones del clúster

Es posible ver y modificar la configuración de todo el clúster y realizar tareas específicas del clúster en la pestaña Cluster de la interfaz de usuario de Element.

Puede configurar ajustes como el umbral de ocupación del clúster, el acceso de soporte, el cifrado en reposo, los volúmenes virtuales, SnapMirror, Y el cliente de retransmisión NTP.

Opciones

- Trabaje con volúmenes virtuales
- Use la replicación de SnapMirror entre clústeres de Element y ONTAP
- Establezca el umbral de ocupación del clúster
- Habilite y deshabilite el acceso al soporte
- "Cómo se calculan los umbrales de blockSpace para el elemento"
- Habilite y deshabilite el cifrado de un clúster
- Gestione el banner de las condiciones de uso
- Configure los servidores de protocolo de tiempo de red para que el clúster consulte
- Gestionar SNMP
- Gestionar unidades
- Gestione los nodos
- Gestionar redes virtuales
- Ver detalles de los puertos Fibre Channel

Obtenga más información

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

Habilite y deshabilite el cifrado en reposo para un clúster

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

Puede habilitar el cifrado de hardware en reposo mediante la interfaz de usuario o la API de Element. La habilitación de la función de cifrado de hardware en reposo no afecta al rendimiento o la eficiencia del clúster. Puede habilitar el cifrado de software en reposo únicamente mediante la API de Element.

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

> En los clústeres de almacenamiento all-flash de SolidFire, el cifrado del software en reposo debe habilitarse durante la creación del clúster y no se puede deshabilitar una vez que se ha creado el clúster.

Lo que necesitará

- Tiene privilegios de administrador de clúster para habilitar o modificar la configuración de cifrado.
- Para el cifrado basado en hardware en reposo, se ha asegurado de que el clúster está en estado correcto antes de cambiar la configuración de cifrado.
- Si va a deshabilitar el cifrado, debe haber dos nodos participando en un clúster para acceder a la clave para deshabilitar el cifrado en una unidad.

Comprobar el cifrado en estado de reposo

Para ver el estado actual del cifrado en reposo y/o el cifrado de software en reposo en el clúster, use el "GetClusterInfo" método. Puede utilizar el "GetSoftwareEncryptionAtRestInfo" método para obtener información que utiliza el clúster para cifrar datos en reposo.

> La consola de interfaz de usuario del software Element en `https://<MVIP>/` actualmente, solo muestra el cifrado en estado de reposo para el cifrado basado en hardware.

Opciones

- Habilite el cifrado basado en hardware en reposo
- Habilite el cifrado basado en software en reposo
- Deshabilite el cifrado basado en hardware en reposo

Habilite el cifrado basado en hardware en reposo

> Para habilitar el cifrado en reposo mediante una configuración de gestión de claves externa, debe habilitar el cifrado en reposo a través de la "API". Al habilitar el uso del botón existente de la interfaz de usuario de Element, se revierten al uso de claves generadas internamente.

1. En la interfaz de usuario de Element, seleccione **Cluster** > **Settings**.
2. Seleccione **Activar cifrado en reposo**.

Habilite el cifrado basado en software en reposo

> El cifrado de software en reposo no se puede deshabilitar una vez que se habilita en el clúster.

1. Durante la creación del clúster, ejecute el "cree el método de clúster" con `enableSoftwareEncryptionAtRest` establezca en `true`.

Deshabilite el cifrado basado en hardware en reposo

1. En la interfaz de usuario de Element, seleccione **Cluster** > **Settings**.
2. Seleccione **Desactivar cifrado en reposo**.

Obtenga más información

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

Establezca el umbral de ocupación del clúster

Puede cambiar el nivel en el que el sistema genera una advertencia de ocupación de la capacidad del clúster de bloques mediante los pasos siguientes. Además, puede utilizar el método API ModifyClusterFullThreshold para cambiar el nivel en el que el sistema genera una advertencia de bloque o metadatos.

Lo que necesitará

Debe tener privilegios de administrador del clúster.

Pasos

1. Haga clic en **Cluster** > **Settings**.
2. En la sección Cluster Full Settings, introduzca un porcentaje en **Raise a warning alert when _% capacity remains before Helix could not recover from a node failure**.
3. Haga clic en **Guardar cambios**.

Obtenga más información

"Cómo se calculan los umbrales de blockSpace para el elemento"

Habilite y deshabilite el acceso al soporte

Es posible habilitar el acceso de soporte para permitir temporalmente el acceso del personal de soporte de NetApp a los nodos de almacenamiento a través de SSH para solucionar problemas.

Para modificar el acceso al soporte, debe tener privilegios de administrador de clúster.

1. Haga clic en **Cluster** > **Settings**.
2. En la sección Habilitar/deshabilitar acceso de soporte, introduzca la duración (en horas) que desea permitir que el soporte tenga acceso.
3. Haga clic en **Activar acceso de soporte**.
4. **Opcional:** para desactivar el acceso al soporte técnico, haga clic en **Desactivar acceso al soporte técnico**.

Gestione el banner de las condiciones de uso

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

Opciones

Habilite el banner de las condiciones de uso Edite el banner con las condiciones de uso Deshabilite el banner con las condiciones de uso

Habilite el banner de las condiciones de uso

Si lo desea, se puede habilitar un banner con las condiciones de uso que aparece cuando un usuario inicia 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 haya configurado para el clúster. El banner se puede descartar cuando desee.

Para poder habilitar la funcionalidad de las condiciones de uso, debe tener privilegios de administrador del clúster.

1. Haga clic en **usuarios** > **Términos de uso**.
2. En el formulario **Términos de uso**, introduzca el texto que desea que aparezca en el cuadro de diálogo Términos de uso.

   No supere los 4096 caracteres.

3. Haga clic en **Activar**.

Edite el banner con las condiciones de uso

Se puede editar el texto que ven los usuarios cuando seleccionan el banner de inicio de sesión de las condiciones de uso.

Lo que necesitará

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

Pasos

1. Haga clic en **usuarios** > **Términos de uso**.
2. En el cuadro de diálogo **Términos de uso**, edite el texto que desea que aparezca.

   No supere los 4096 caracteres.

3. Haga clic en **Guardar cambios**.

Deshabilite el banner con las condiciones de uso

El banner con las condiciones de uso se puede deshabilitar. Cuando se deshabilita el banner, se deja de solicitar al usuario que acepte las condiciones de uso cuando se usa la interfaz de usuario de Element.

Lo que necesitará

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

Pasos

1. Haga clic en **usuarios** > **Términos de uso**.
2. Haga clic en **Desactivar**.

Establezca el protocolo de hora de red

La configuración del protocolo de tiempo de redes (NTP) se puede lograr de dos maneras: Indique a cada nodo de un clúster que escuche las difusiones o indique a cada nodo que consulte un servidor NTP para obtener actualizaciones.

El NTP se utiliza para sincronizar los relojes que hay en toda una red. La conexión con un servidor NTP interno o externo debe formar parte de la configuración inicial del clúster.

Configure los servidores de protocolo de tiempo de red para que el clúster consulte

Puede indicar a cada nodo de un clúster que consulte un servidor de protocolo de tiempo de redes (NTP) en busca de actualizaciones. El clúster solo contacta con los servidores configurados y solicita información NTP de ellos.

Configure el NTP en el clúster para que apunte a un servidor NTP local. Es posible usar la dirección IP o el nombre de host FQDN. El servidor NTP predeterminado en el momento de crear el clúster se establece en us.pool.ntp.org; sin embargo, no siempre es posible establecer una conexión con este sitio en función de la ubicación física del clúster de SolidFire.

El uso del FQDN depende de si la configuración de DNS del nodo de almacenamiento individual está en su

lugar y operativa. Para ello, revise la página requisitos de puerto de red para configurar los servidores DNS en cada nodo de almacenamiento y asegúrese de que los puertos estén abiertos.

Es posible introducir hasta cinco servidores NTP distintos.

Es posible usar tanto direcciones IPv4 como IPv6.

Lo que necesitará

Para poder configurar esta opción, debe tener privilegios de administrador del clúster.

Pasos

1. Configure una lista de IP y/o FQDN en la configuración del servidor.
2. Compruebe que DNS se haya configurado correctamente en los nodos.
3. Haga clic en **Cluster** > **Settings**.
4. En Configuración del protocolo de tiempo de redes, seleccione **no**, que utiliza la configuración NTP estándar.
5. Haga clic en **Guardar cambios**.

Obtenga más información

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

Configure el clúster para que escuche las transmisiones NTP

Con el modo de retransmisión, puede ordenar a cada nodo de un clúster que escuche en la red de mensajes de retransmisión de protocolo de tiempo de redes (NTP) de un servidor determinado.

Lo que necesitará

- Para poder configurar esta opción, debe tener privilegios de administrador del clúster.
- Debe configurar un servidor NTP en la red como servidor de retransmisión.

Pasos

1. Haga clic en **Cluster** > **Settings**.
2. Introduzca en la lista de servidores el servidor NTP o los servidores que utilizan el modo de retransmisión.
3. En Configuración del protocolo de tiempo de redes, seleccione **Sí** para utilizar un cliente de difusión.
4. Para establecer el cliente de difusión, en el campo **servidor**, introduzca el servidor NTP configurado en modo de difusión.
5. Haga clic en **Guardar cambios**.

Obtenga más información

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

Gestionar SNMP

Puede configurar el protocolo simple de gestión de redes (SNMP) en el clúster.

Puede seleccionar un solicitante SNMP, seleccionar la versión de SNMP que desea usar, identificar el usuario de modelo de seguridad basado en usuario de SNMP (USM) y configurar las capturas para supervisar el clúster de SolidFire. También permite ver y acceder a los archivos de base de información de gestión.

Es posible usar tanto direcciones IPv4 como IPv6.

Detalles de SNMP

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

- **MIB SNMP**

  Los archivos MIB que hay disponibles para que pueda verlos o descargarlos.

- **Configuración general de SNMP**

  Es posible habilitar o deshabilitar SNMP. Después de habilitar SNMP, puede elegir qué versión quiere usar. Si utiliza la versión 2, puede añadir solicitantes y, si usa la versión 3, puede configurar usuarios USM.

- **Configuración de la captura SNMP**

  Puede identificar los retos que quiere recibir. Puede establecer el host, el puerto y la cadena de comunidad para cada destinatario de reto.

Configure un solicitante SNMP

Cuando se habilita la versión 2 de SNMP, puede habilitar o deshabilitar un solicitante, así como configurar solicitantes para que reciban solicitudes SNMP autorizadas.

1. Haga clic en MENU:Cluster[SNMP].
2. En **Configuración general de SNMP**, haga clic en **Sí** para activar SNMP.
3. En la lista **Versión**, seleccione **Versión 2**.
4. En la sección **Requestors**, introduzca la información **Community String** y **Network**.

   De forma predeterminada, la cadena de comunidad es public y la red es localhost. No obstante, puede cambiar estas opciones predeterminadas si lo necesita.

5. **Opcional:** para añadir otro solicitante, haga clic en **Añadir un solicitante** e introduzca la información **cadena de comunidad** y **Red**.
6. Haga clic en **Guardar cambios**.

Obtenga más información

- Configurar las capturas SNMP
- Se pueden ver los datos de objetos gestionados mediante los archivos de base de información de gestión

Configure un usuario USM en SNMP

Al habilitar la versión 3 de SNMP, tendrá que configurar un usuario USM para que reciba las solicitudes de SNMP autorizadas.

1. Haga clic en **Cluster** > **SNMP**.
2. En **Configuración general de SNMP**, haga clic en **Sí** para activar SNMP.
3. En la lista **Versión**, seleccione **Versión 3**.
4. En la sección **usuarios USM**, introduzca el nombre, la contraseña y la contraseña.
5. **Opcional:** para añadir otro usuario USM, haga clic en **Añadir usuario USM** e introduzca el nombre, la contraseña y la frase de paso.
6. Haga clic en **Guardar cambios**.

Configurar las capturas SNMP

Los administradores del sistema pueden utilizar capturas SNMP, también denominadas notificaciones, para supervisar el estado del clúster de SolidFire.

Cuando se habilitan los retos SNMP, el clúster de SolidFire genera retos asociados con las entradas del registro de eventos y las alertas del sistema. Para recibir notificaciones SNMP, tiene que elegir los retos que se tendrían que generar e identificar los destinatarios de la información del reto. De forma predeterminada, no se genera ningún reto.

1. Haga clic en **Cluster** > **SNMP**.
2. Seleccione uno o varios tipos de solapamientos en la sección **Configuración de solapamientos SNMP** que el sistema debe generar:
   - Retos de fallo de clúster
   - Retos de fallo resueltos del clúster
   - Retos de evento de clúster
3. En la sección **destinatarios de la captura**, introduzca la información de host, puerto y cadena de comunidad para un destinatario.
4. **Opcional**: Para agregar otro destinatario de captura, haga clic en **Agregar un destinatario de captura** e introduzca la información de host, puerto y cadena de comunidad.
5. Haga clic en **Guardar cambios**.

Se pueden ver los datos de objetos gestionados mediante los archivos de base de información de gestión

Es posible ver y descargar los archivos de la base de datos de información de administración (MIB) que se usan para definir cada uno de los objetos gestionados. La función SNMP admite el acceso de solo lectura a los objetos que se definen en SolidFire-StorageCluster-MIB.

Los datos estadísticos que se proporcionan en el archivo MIB muestran la actividad del sistema en relación a lo siguiente:

- Estadísticas de clúster
- Estadísticas de volumen

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

El sistema también permite acceder al archivo MIB que contenga los puntos de acceso del nivel superior (OIDS) a los productos SF-Series.

Pasos

1. Haga clic en **Cluster** > **SNMP**.
2. En **MIB de SNMP**, haga clic en el archivo MIB que desee descargar.
3. En la ventana de descarga que aparece, abra o guarde el archivo MIB.

Gestionar unidades

Cada nodo contiene una o varias 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 una vez que esta se ha añadido correctamente a un clúster. Es posible usar la interfaz de usuario de Element para gestionar las unidades.

Si quiere más información

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

Detalles de unidades

En la página Drives de la pestaña Cluster, se proporciona una lista de las unidades activas del clúster. La página se puede filtrar si selecciona de las pestañas Active, Available, Removing, Erasing y Failed.

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

Los siguientes elementos se muestran en la lista de unidades activas.

- **ID de unidad**

  El número secuencial asignado a la unidad.

- **ID de nodo**

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

- **Nombre de nodo**

  El nombre del nodo que aloja la unidad.

- **Ranura**

  El número de ranura en la que la unidad se encuentra físicamente.

- **Capacidad**

  El tamaño de la unidad, en GB.

- **Serie**

  El número de serie de la unidad.

- **Desgaste restante**

  El indicador del nivel de desgaste.

  El sistema de almacenamiento informa de la cantidad aproximada de desgaste disponible en cada unidad de estado sólido (SSD) para escribir y borrar datos. Una unidad que ha consumido el 5% de los ciclos de escritura y borrado diseñados informa del 95% de desgaste restante. El sistema no actualiza automáticamente la información de desgaste de la unidad; se puede actualizar o cerrar y volver a cargar la página para actualizar la información.

- **Tipo**

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

Gestione los nodos

Desde la página Nodes de la pestaña Cluster, se pueden gestionar los nodos de almacenamiento SolidFire y Fibre Channel.

Si un nodo que se acaba de añadir supone más del 50 % de la capacidad total del clúster, parte de la capacidad de este nodo se vuelve inutilizable ("trenzado"), de modo que cumpla con la regla de capacidad. Este sigue siendo el caso hasta que se añada más almacenamiento. Si se añade un nodo muy grande que también desobedece la regla de capacidad, el nodo que antes se había abandonado ya no se quedará abandonado, mientras el nodo recién añadido se vuelve abandonado. La capacidad debe añadirse siempre por parejas para evitar que esto suceda. Cuando un nodo se queda sin poner en cadena, se produce un error del clúster adecuado.

Obtenga más información

Añada un nodo a un clúster

Añada un nodo a un clúster

Es posible añadir nodos a un clúster cuando se necesita más almacenamiento o después de crear el clúster. Los nodos requieren una configuración inicial cuando se conectan por primera vez. Una vez que se configura, aparece en la lista de nodos pendientes y puede añadirlos a un clúster.

La versión de software de cada nodo en un clúster tiene que ser compatible. Cuando añade un nodo a un clúster, el clúster instala la versión del clúster del software NetApp Element en el nuevo nodo según sea necesario.

Es posible añadir nodos de capacidad inferior o superior a un clúster existente. Es posible añadir capacidades de nodos superiores a un clúster para aumentar su capacidad. Cuando se añaden nodos más grandes a un clúster con nodos más pequeños, debe hacerse en parejas. De este modo se le otorga suficiente espacio para

que Double Helix pueda mover los datos en caso de que uno de los nodos superiores presente errores. Es posible añadir capacidades de nodos más pequeños a un clúster de nodos más grandes para mejorar el rendimiento.

> Si un nodo que se acaba de añadir supone más del 50 % de la capacidad total del clúster, parte de la capacidad de este nodo se vuelve inutilizable ("trenzado"), de modo que cumpla con la regla de capacidad. Este sigue siendo el caso hasta que se añada más almacenamiento. Si se añade un nodo muy grande que también desobedece la regla de capacidad, el nodo que antes se había abandonado ya no se quedará abandonado, mientras el nodo recién añadido se vuelve abandonado. La capacidad debe añadirse siempre por parejas para evitar que esto suceda. Cuando un nodo se convierte en abandonado, se produce el error del clúster strandedCapacity.

"Vídeo de NetApp: Escale según sus necesidades: Ampliar un clúster de SolidFire"

Puede añadir nodos a dispositivos NetApp HCI.

Pasos

1. Seleccione **Cluster** > **Nodes**.
2. Haga clic en **pendiente** para ver la lista de nodos pendientes.

   Una vez completado el proceso de adición de nodos, aparecen en la lista Active Nodes. Hasta entonces, los nodos pendientes aparecen en la lista Pending Active.

   SolidFire instala la versión del software Element del clúster en los nodos pendientes cuando se añaden a un clúster. Esto puede tardar varios 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 añadir varios nodos, active la casilla de los nodos que desee agregar y, a continuación, **acciones masivas**. **Nota:** Si el nodo que está agregando tiene una versión diferente del software Element que 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 de clústeres. Después de que se actualiza el nodo, se añade automáticamente al clúster. Durante este proceso asíncrono, el nodo tendrá el estado pendingActive.
4. Haga clic en **Agregar**.

   El nodo aparece en la lista de nodos activos.

Obtenga más información

Versiones y compatibilidad de nodos

Versiones y compatibilidad de nodos

La compatibilidad del nodo se basa en la versión del software Element instalada en un nodo. Los clústeres de almacenamiento basados en software Element crean automáticamente la imagen de un nodo en la versión de software Element en el clúster cuando las versiones del nodo y el clúster no son compatibles.

En la siguiente lista, se describen los niveles de importancia de las versiones del software Element que

conforman el número de versión del software Element:

- **Mayor**

  El primer número designa una versión de software. No es posible añadir un nodo con un número de componente principal a un clúster que contenga nodos de otro número de revisión principal ni se puede crear un clúster con nodos de versiones principales mixtas.

- **Menor**

  El segundo número designa mejoras o funciones de software más pequeñas que se aplican en funciones de software existentes que se han incorporado a una versión principal. Este componente aumenta dentro de un componente de versión principal para indicar que esta versión incremental no es compatible con otras versiones incrementales del software Element con un componente secundario distinto. Por ejemplo, 11.0 no es compatible con 11.1 y 11.1 no es compatible con 11.2.

- **Micro**

  El tercer número designa una revisión compatible (versión incremental) con la versión de software Element que representan los componentes principal.secundario. Por ejemplo, 11.0.1 es compatible con 11.0.2 y 11.0 es compatible con 11.0.3.

Los números de versión principal y secundario deben coincidir para ser compatibles. Los números micro no tienen que coincidir para ser compatibles.

Capacidad de clúster en un entorno de nodos mixtos

En un clúster se pueden combinar distintos tipos de nodos. SF-Series 2405, 3010, 4805, 6010, 9605 9010, 19210, 38410 y H-Series pueden coexistir en un clúster.

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

Es mejor no mezclar nodos no cifrados y no cifrados. En un clúster de nodos mixtos, ningún nodo puede superar el 33 % de la capacidad total del clúster. Por ejemplo, en un clúster con cuatro nodos SF-Series 4805, el nodo más grande que se puede añadir solo es un nodo SF-Series 9605. El umbral de capacidad del clúster se calcula en función de la pérdida potencial del nodo más grande en esta situación.

A partir de Element 12.0, los siguientes nodos de almacenamiento SF-Series no son compatibles:

- SF3010
- SF6010
- SF9010

Si actualiza uno de estos nodos de almacenamiento a Element 12.0, verá un error indicando que este nodo no es compatible con Element 12.0.

Ver los detalles del nodo

Puede ver detalles de nodos individuales, como etiquetas de servicio, detalles de unidades y gráficos para la utilización y estadísticas de unidades. La página Nodes de la pestaña Cluster proporciona la columna Version donde puede ver la versión de software de cada nodo.

Pasos

1. Haga clic en **Cluster** > **Nodes**.
2. Para ver los detalles de un nodo específico, haga clic en el icono **acciones** de un nodo.
3. Haga clic en **Ver detalles**.
4. Revise los detalles del nodo:
   - **ID de nodo**: El ID generado por el sistema para el nodo.
   - **Nombre de nodo**: El nombre de host del nodo.
   - **iops 4k** disponible: IOPS configuradas para el nodo.
   - **Función de nodo**: La función que tiene el nodo en el clúster. Los posibles valores son los siguientes:
     - Cluster Master: El nodo que realiza tareas administrativas para todo el clúster y contiene la MVIP y la SVIP.
     - Ensemble Node: Un nodo que participa en el clúster. Hay nodos de 3 o 5 conjuntos, según el tamaño del clúster.
     - Fibre Channel: Un nodo del clúster.
   - **Tipo de nodo**: Tipo de modelo del nodo.
   - **Active Drives**: Número de unidades activas en el nodo.
   - **IP de administración**: La dirección IP de administración (MIP) asignada al nodo para las tareas de administración de red de 1 GbE o 10 GbE.
   - **IP de clúster**: La dirección IP de clúster (CIP) asignada al nodo utilizado para la comunicación entre nodos del mismo clúster.
   - **IP de almacenamiento**: La dirección IP de almacenamiento (SIP) asignada al nodo utilizado para la detección de redes iSCSI y todo el tráfico de red de datos.
   - **ID de VLAN de administración**: ID virtual para la red de área local de administración.
   - **Storage VLAN ID**: El ID virtual de 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 exclusivo asignado al nodo.

Ver detalles de los puertos Fibre Channel

Es posible ver detalles de los puertos Fibre Channel, como el estado, el nombre y la dirección de puerto, desde la página puertos FC.

Permite ver información sobre los puertos Fibre Channel que están conectados al clúster.

Pasos

1. Haga clic en **Cluster** > **puertos FC**.
2. Para filtrar información en esta página, haga clic en **filtro**.
3. Consulte los detalles:
   - **ID de nodo**: El nodo que aloja la sesión de la conexión.
   - **Nombre de nodo**: Nombre de nodo generado por el sistema.
   - **Slot**: Número de ranura donde se encuentra el puerto Fibre Channel.

- **Puerto HBA**: Puerto físico en el adaptador de bus de host (HBA) Fibre Channel.
- **WWNN**: El nombre de nodo mundial.
- **WWPN**: El nombre de puerto de destino para todo el mundo.
- **WWN del conmutador**: Nombre mundial del conmutador Fibre Channel.
- **Estado del puerto**: Estado actual del puerto.
- **NPort ID**: El identificador de puerto del nodo en la estructura Fibre Channel.
- **Velocidad**: La velocidad negociada del canal de fibra. Los valores posibles son los siguientes:
  - 4 Gbps
  - 8 Gbps
  - 16 Gbps

Obtenga más información

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

Gestionar redes virtuales

Las redes virtuales del almacenamiento de SolidFire permiten que el tráfico entre varios clientes en redes lógicas independientes se conecten a un clúster. Las conexiones al clúster se separan en la pila de redes mediante el etiquetado de VLAN.

Obtenga más información

- Añadir una red virtual
- Habilite el enrutamiento y el reenvío virtuales
- Editar una red virtual
- Edite las VLAN de VRF
- Eliminar una red virtual

Añadir una red virtual

Es posible añadir una red virtual nueva a la configuración de un clúster para habilitar una conexión de entorno multi-tenant con un clúster donde se ejecuta el software Element.

Lo que necesitará

- 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 usará como extremo para todo el tráfico de almacenamiento de NetApp Element.

Debe tener en cuenta los siguientes criterios para esta configuración:

- Las VLAN que no están habilitadas para VRF requieren que haya iniciadores en la misma subred que la SVIP.
- Las VLAN que están habilitadas para VRF no requieren que haya iniciadores en la misma subred que la

SVIP y el que enrutamiento esté admitido.

- La SVIP predeterminada no requiere que haya iniciadores en la misma subred que la SVIP y el que enrutamiento esté admitido.

Cuando se añade una red virtual, se crea una interfaz para cada nodo y cada una requiere una dirección IP de red virtual. La cantidad de direcciones IP especificada cuando se crea una red virtual nueva debe ser igual o mayor que la cantidad de nodos del clúster. Las direcciones de red virtuales se aprovisionan de forma masiva y se asignan automáticamente a los nodos individuales. No es necesario asignar manualmente direcciones de red virtual 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 valores en los siguientes campos:
   - **Nombre de VLAN**
   - **Etiqueta VLAN**
   - **SVIP**
   - **Netmask**
   - (Opcional) **Descripción**
4. Introduzca la dirección **IP inicial** para el rango de direcciones IP en **IP Address Blocks**.
5. Introduzca el **Tamaño** del intervalo IP como el número de direcciones IP que se incluirán en el bloque.
6. Haga clic en **Agregar un bloque** para agregar un bloque no continuo de direcciones IP para esta VLAN.
7. Haga clic en **Crear VLAN**.

Ver detalles de redes virtuales

Pasos

1. Haga clic en **clúster** > **Red**.
2. Revise los detalles.
   - **ID**: ID exclusivo de la red VLAN, asignada por el sistema.
   - **Nombre**: Nombre exclusivo 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.
   - **Netmask**: Máscara de red para esta red virtual.
   - **Gateway**: Dirección IP única de una puerta de enlace de red virtual. VRF debe estar habilitado.
   - **VRF Enabled**: Indica si el enrutamiento y reenvío virtuales está activado o no.
   - **IP utilizadas**: El rango de direcciones IP de red virtual que se utiliza para la red virtual.

Habilite el enrutamiento y el reenvío virtuales

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

Solo puede habilitar VRF en el momento de crear una VLAN. Si desea volver a un estado sin VRF, debe eliminar y volver a crear la VLAN.

1. Haga clic en **clúster** > **Red**.
2. Para habilitar VRF en una VLAN nueva, seleccione **Crear VLAN**.
   a. Introduzca la información relevante para la nueva VRF/VLAN. Consulte Añadir una red virtual.
   b. Active la casilla de verificación **Activar VRF**.
   c. **Opcional**: Introduzca una puerta de enlace.
3. Haga clic en **Crear VLAN**.

Obtenga más información

Añadir una red virtual

Editar una red virtual

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

Si existe alguna sesión de iSCSI, replicación remota u otras sesiones de red, se podría producir un error en la modificación.

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

- Solo es posible eliminar direcciones IP del rango de direcciones IP iniciales asignado en el momento en que se creó la VLAN.
- Puede eliminar un bloque de direcciones IP que se agregó después del rango de direcciones IP inicial, pero no puede cambiar el tamaño de un bloque IP eliminando las direcciones IP.
- Cuando intenta quitar direcciones IP, ya sea del rango de direcciones IP inicial o de un bloque IP, que están utilizando los nodos en el clúster, la operación puede generar un error.
- No se pueden reasignar direcciones IP específicas en uso a otros nodos del clúster.

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

1. Seleccione **Cluster** > **Red**.
2. Seleccione el icono Actions de la VLAN que quiera 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 continuo de direcciones IP para la red virtual.
6. Seleccione **Guardar cambios**.

Enlace a artículos de la base de conocimientos de solución de problemas

Enlace a los artículos de la base de conocimientos para obtener ayuda sobre la solución de problemas relacionados con la gestión de los intervalos de direcciones IP de VLAN.

- "Duplique la advertencia de IP después de añadir un nodo de almacenamiento en VLAN en el clúster de Element"
- "Cómo determinar a qué IP de VLAN están en uso y a qué nodos están asignados esas IP en Element"

Edite las VLAN de VRF

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

1. Haga clic en **clúster** > **Red**.
2. Haga clic en el icono Actions de la VLAN que quiera editar.
3. Haga clic en **Editar**.
4. Introduzca los nuevos atributos para la VLAN del VRF en el cuadro de diálogo **Editar VLAN**.
5. Haga clic en **Guardar cambios**.

Eliminar una red virtual

Puede eliminar un objeto de red virtual. Debe añadir los bloques de dirección a otra red virtual antes de eliminar una red virtual.

1. Haga clic en **clúster** > **Red**.
2. Haga clic en el icono Actions de la VLAN que desea eliminar.
3. Haga clic en **Eliminar**.
4. Confirme el mensaje.

Obtenga más información

Editar una red virtual

Cree un clúster que admita unidades FIPS

La seguridad cada vez resulta más importante para la puesta en marcha de soluciones en muchos entornos de cliente. Los estándares de procesamiento de información federal (FIPS) son estándares de interoperabilidad y seguridad informática. El cifrado certificado FIPS 140-2 para datos en reposo es un componente de la solución de seguridad general.

- "Evite combinar nodos para unidades FIPS"
- "Habilite el cifrado en reposo"
- "Identifique si los nodos están listos para la función de unidades FIPS"
- "Habilite la función de unidades FIPS"
- "Compruebe el estado de la unidad FIPS"
- "Solucione problemas de la función de unidad FIPS"

Evite combinar nodos para unidades FIPS

Para prepararse para habilitar la función de unidades FIPS, debe evitar combinar nodos

donde algunos sean compatibles con unidades FIPS y otros no lo sean.

Un clúster se considera compatible con 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.
- Se habilitó la función de unidades FIPS. Todas las unidades y los nodos deben ser compatibles con FIPS, y el cifrado en reposo debe habilitarse para habilitar la función de unidad FIPS.

Habilite el cifrado en reposo

Puede habilitar y deshabilitar el cifrado en todo el clúster en reposo. Esta función no está habilitada de forma predeterminada. Para admitir las 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 **Activar cifrado en reposo**.

Obtenga más información

- Habilite y deshabilite el cifrado de un clúster
- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Identifique si los nodos están listos para la función de unidades FIPS

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

El informe resultante muestra uno de los siguientes Estados:

- None: El nodo no es compatible con la función de unidades FIPS.
- Parcial: El nodo es compatible con FIPS, pero no todas las unidades son unidades FIPS.
- Ready: El nodo es compatible con FIPS y todas las unidades son unidades FIPS o no existen unidades.

Pasos

1. Con la API de Element, compruebe si los nodos y las unidades del clúster de almacenamiento pueden ver las unidades FIPS introduciendo:

   ```
   GetFipsReport
   ```

2. Revise los resultados y consulte los nodos que no muestran el estado de Ready.
3. En el caso de los nodos que no muestren el estado Listo, compruebe si la unidad es compatible con la función de las unidades FIPS:
   - Utilice la API de Element, introduzca: `GetHardwareList`
   - Observe el valor de **DriveEncryptionCapabilityType**. Si es "fips", el hardware puede admitir la

función de unidades FIPS.

Consulte los detalles acerca de `GetFipsReport` o. `ListDriveHardware` en la "Referencia de la API de Element".

4. Si la unidad no puede admitir la función unidades FIPS, reemplace el hardware con hardware FIPS (nodo o unidades).

Obtenga más información

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

Habilite la función de unidades FIPS

Es posible habilitar la función 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, tal y como se indica cuando GetFipsReport muestra el estado Ready para todos los nodos.

Paso

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

```
EnableFeature params: FipsDrives
```

Obtenga más información

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

Compruebe el estado de la unidad FIPS

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

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

```
GetFeatureStatus
```

2. Revise los resultados del `GetFeatureStatus` Llamada a API. Si el valor de unidades FIPS habilitadas es True, se habilita la función de unidades FIPS.

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

Obtenga más información

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

Solucione problemas de la función de unidad FIPS

Con la interfaz de usuario del software NetApp Element, es posible ver alertas sobre errores o errores del clúster en el sistema relacionados con la función de unidades FIPS.

1. Con la interfaz de usuario de Element, seleccione **Informes** > **Alertas**.
2. Busque fallos del clúster, entre los que se incluyen:
   - Las unidades FIPS no coinciden
   - FIPS no cumple las normativas
3. Para obtener sugerencias de resolución, consulte la información sobre el código de avería del clúster.

Obtenga más información

- códigos de error de clúster
- "Gestione el almacenamiento con la API de Element"
- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Habilite FIPS 140-2 para HTTPS en el clúster

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

Con el software NetApp Element, puede optar por habilitar el modo operativo estándar de procesamiento de información federal (FIPS) 140-2 en el clúster. Al habilitar este modo, se activa el módulo de seguridad criptográfica de NetApp (NCSM) y se utiliza el cifrado certificado FIPS 140-2 de nivel 1 para toda la comunicación mediante HTTPS a la interfaz de usuario y la API de NetApp Element.

> Después de habilitar el modo FIPS 140-2-2, no puede deshabilitarse. Cuando se habilita FIPS 140-2-Mode, cada nodo del clúster se reinicia y ejecuta una prueba automática, lo que garantiza que NCSM se habilite correctamente y funcione en el modo certificado FIPS 140-2-2. Esto provoca una interrupción de las conexiones de gestión y almacenamiento en el clúster. Debe planificar con cuidado y activar este modo únicamente si su entorno necesita el mecanismo de cifrado que ofrece.

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

A continuación se muestra un ejemplo de la solicitud de API para habilitar FIPS:

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

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

Obtenga más información

- Cifrados SSL
- "Gestione el almacenamiento con la API de Element"
- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Cifrados SSL

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

Las siguientes listas proporcionan los cifrados estándar de capa de socket seguro (SSL) que admite el software Element y los cifrados SSL que se admiten 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_WITH_AES_128_CBC_SHA256 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (SECP256R1) - A.

  TLS_RSA_WITH_3DES_EDE_CBC_SHA (RSA 2048) - C

  TLS_RSA_WITH_AES_128_CBC_SHA (RSA 2048) - A.

  TLS_RSA_WITH_AES_128_CBC_SHA256 (RSA 2048) - A

TLS_RSA_WITH_AES_128_GCM_SHA256 (RSA 2048) - A

TLS_RSA_WITH_AES_256_CBC_SHA (RSA 2048) - A.

TLS_RSA_WITH_AES_256_CBC_SHA256 (RSA 2048) - A

TLS_RSA_WITH_AES_256_GCM_SHA384 (RSA 2048) - A.

TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (RSA 2048) - A.

TLS_RSA_WITH_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_WITH_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_WITH_AES_128_CBC_SHA256 (SECT571R1) - A.

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (SECT571R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (SECT571R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (SECT571R1) - A.

  TLS_RSA_WITH_3DES_EDE_CBC_SHA (RSA 2048) - C

  TLS_RSA_WITH_AES_128_CBC_SHA (RSA 2048) - A.

  TLS_RSA_WITH_AES_128_CBC_SHA256 (RSA 2048) - A

  TLS_RSA_WITH_AES_128_GCM_SHA256 (RSA 2048) - A

  TLS_RSA_WITH_AES_256_CBC_SHA (RSA 2048) - A.

TLS_RSA_WITH_AES_256_CBC_SHA256 (RSA 2048) - A

TLS_RSA_WITH_AES_256_GCM_SHA384 (RSA 2048) - A.

Obtenga más información

Habilite FIPS 140-2 para HTTPS en el clúster

Comience con la gestión de claves externas

La gestión de claves externas (EKM) ofrece gestión de claves de autenticación seguras (AK) en combinación con un servidor de claves externo (EKS) fuera de clúster. El AKS se utiliza para bloquear y desbloquear unidades de cifrado automático (SED) cuando "cifrado en reposo" está habilitado en el clúster. El EKS proporciona una generación y almacenamiento seguros del AKS. El clúster utiliza el protocolo de interoperabilidad de gestión de claves (KMIP, en inglés "Key Management Interoperability Protocol"), un protocolo estándar definido de OASIS para comunicarse con el EKS.

- "Configurar la administración externa"
- "Vuelva a obtener el cifrado de software en la clave maestra de REST"
- "Recuperación de claves de autenticación no válidas o inaccesibles"
- "Comandos de API de gestión de claves externas"

Obtenga más información

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

Configure la gestión de claves externas

Puede seguir estos pasos y usar los métodos API de Element que aparecen para configurar la función de gestión de claves externa.

Lo que necesitará

- Si va a configurar la gestión de claves externas en combinación con el cifrado de software en reposo, debe habilitar el cifrado de software en reposo con el "CreateCluster" 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 público/privado para el clúster de Element que se utilice para establecer una relación de confianza con el servidor de claves llamando al siguiente método de API: "CreatePublicPrivateKeyPair"
   b. Obtenga la solicitud de firma de certificado (CSR) que la entidad de certificación debe firmar. La CSR permite que el servidor de claves verifique que el clúster de Element que tendrá acceso a las claves se autentique como clúster de Element. Llame al siguiente método API: "GetClientCertificateSignRequest"

c. Utilice la autoridad EKS/Certificate 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 el EKS. Un proveedor de claves define dónde se debe obtener una clave y un servidor define los atributos específicos del EKS con los que se comunicará.

   a. Cree un proveedor de claves en el que residirán los detalles del servidor de claves llamando al siguiente método de API: "CreateKeyProviderKmip"

   b. Cree un servidor de claves que proporcione el certificado firmado y el certificado de clave pública de la entidad emisora de certificados llamando a los siguientes métodos API: "CreateKeyServerKmip" "TestKeyServerKmip"

      Si la prueba falla, verifique la configuración y la conectividad del servidor. A continuación, repita la prueba.

   c. Para agregar el servidor de claves al contenedor de proveedor de claves, llame a los siguientes métodos API:"AddKeyServerToProviderKmip" "TestKeyProviderKmip"

      Si la prueba falla, verifique la configuración y la conectividad del servidor. A continuación, repita la prueba.

3. Realice una de las siguientes acciones como siguiente paso para el cifrado en reposo:

   a. (Para el cifrado de hardware en reposo) Habilitar "cifrado de hardware en reposo" Mediante la identificación del proveedor de claves que contiene el servidor de claves utilizado para almacenar las claves, llame al "EnableEncryptionAtest" Método API.

      > Debe habilitar el cifrado en reposo a través del "API". Si se habilita el cifrado en reposo con el botón existente de interfaz de usuario de Element, la función volverá al uso de claves generadas internamente.

   b. (Para el cifrado de software en reposo) en orden de "cifrado de software en reposo" Para utilizar el proveedor de claves recién creado, pase el ID de proveedor de claves al "RekeySoftwareEncryptionAtRestMasterKey" Método API.

Obtenga más información

- "Habilite y deshabilite el cifrado de un clúster"
- "Documentación de SolidFire y el software Element"
- "Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"

Vuelva a obtener el cifrado de software en la clave maestra de REST

Es posible usar la API de Element para volver a introducir una clave existente. Este proceso crea una nueva clave maestra de reemplazo para el servidor de gestión de claves externo. Las claves maestras siempre se sustituyen por claves maestras nuevas y nunca se duplican ni se sobrescriben.

Es posible que deba volver a introducir la clave como parte de uno de los siguientes procedimientos:

- Cree una nueva clave como parte de un cambio de la gestión de claves interna a la gestión de claves externas.

- Cree una nueva clave como reacción o como protección ante un evento relacionado con la seguridad.

> Este proceso es asíncrono y devuelve una respuesta antes de que se complete la operación de reclave. Puede utilizar el "GetAsyncResult" método para sondear el sistema para ver cuándo se ha completado el proceso.

Lo que necesitará

- Habilitó el cifrado de software en reposo mediante el "CreateCluster" Método en un nuevo clúster que no contiene volúmenes y no tiene I/O. Utilice el enlace:../api/reference_element_api_getsoftwareencryptionatrestinfo.html[`GetSoftwareEncryptionatRestInfo`] para confirmar que el estado es `enabled` antes de continuar.
- Ya tienes "estableció una relación de confianza" Entre el clúster de SolidFire y un servidor de claves externo (EKS). Ejecute el "TestKeyProviderKmip" método para verificar que se ha establecido una conexión con el proveedor de claves.

Pasos

1. Ejecute el "ListKeyProvidersKmip" Y copie el ID del proveedor de claves (`keyProviderID`).
2. Ejecute el "RekeySoftwareEncryptionAtRestMasterKey" con la `keyManagementType` parámetro como `external` y.. `keyProviderID` Como el número de ID del proveedor de claves del paso anterior:

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

3. Copie el `asyncHandle` valor de `RekeySoftwareEncryptionAtRestMasterKey` respuesta del comando.
4. Ejecute el "GetAsyncResult" con el `asyncHandle` valor del paso anterior para confirmar el cambio en la configuración. Desde la respuesta del comando, debe ver que la configuración de la clave maestra anterior se ha actualizado con información de clave nueva. 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. Ejecute el `GetSoftwareEncryptionatRestInfo` comando para confirmar la información de la nueva clave, incluida la `keyProviderID`, se han actualizado.

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

Obtenga más información

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

Recuperación de claves de autenticación no válidas o inaccesibles

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

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

Esto puede suceder cuando el clúster se inicia por primera vez y no se puede acceder al servidor de claves o la clave requerida no está disponible.

1. Siga los pasos de recuperación indicados en los códigos de fallo del clúster (si los hubiera).

Se puede configurar un error slicServiceUnhealthy porque las unidades de metadatos se han marcado como un error y se han colocado en el estado "Available".

Pasos para borrar:

1. Vuelva a añadir las unidades.
2. Después de 3 a 4 minutos, verificar que el `sliceServiceUnhealthy` se borró el error.

Consulte "códigos de error de clúster" si quiere más información.

Comandos de API de gestión de claves externas

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

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

- CreatePublicPrivateKeyPair
- GetClientCertificateSignRequest

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

- CreateKeyServerKmip
- ModifyKeyServerKmip
- DeleteKeyServerKmip
- GetKeyServerKmip
- ListKeyServersKmip
- TestKeyServerKmip

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

- CreateKeyProviderKmip

- DeleteKeyProviderKmip
- AddKeyServerToProviderKmip
- RemoveKeyServerFromProviderKmip
- GetKeyProviderKmip
- ListKeyProvidersKmip
- RekeySoftwareEncryptionAtRestMasterKey
- TestKeyProviderKmip

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

Gestione volúmenes y volúmenes virtuales

Es posible gestionar los datos en un clúster que ejecuta el software Element desde la pestaña Management de la interfaz de usuario de Element. Las funciones de gestión de clúster disponibles incluyen la creación y la gestión de volúmenes de datos, grupos de acceso de volúmenes, iniciadores y políticas de calidad de servicio (QoS).

- "Trabaje con volúmenes"
- "Trabaje con volúmenes virtuales"
- "Trabajar con iniciadores y grupos de acceso de volúmenes"

Si quiere más información

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

Trabaje con volúmenes

El sistema SolidFire aprovisiona el almacenamiento mediante volúmenes. Los volúmenes son dispositivos de bloque a los que los clientes iSCSI o Fibre Channel acceden a través de la red. En la página Volumes de la pestaña Management, puede crear, modificar, clonar y eliminar volúmenes en un nodo. También puede ver estadísticas sobre el ancho de banda de los volúmenes y el uso de I/O.

Obtenga más información

- "Gestione políticas de calidad de servicio"
- "Cree un volumen"
- "Ver detalles de rendimiento de cada volumen"
- "Editar los volúmenes activos"
- "Eliminar un volumen"
- "Restaurar un volumen eliminado"
- "Purgar un volumen"
- "Clonar un volumen"

- "Asigne LUN a volúmenes Fibre Channel"
- "Aplique una política de calidad de servicio en los volúmenes"
- "Quite la asociación de políticas de calidad de servicio de un volumen"

Gestione políticas de calidad de servicio

Una política de calidad de servicio (QoS) permite crear y guardar un ajuste de calidad de servicio estandarizado que se puede aplicar a muchos volúmenes. Las políticas de calidad de servicio se pueden crear, editar y eliminar desde la página QoS Policies de la pestaña Management.

> Si utiliza políticas de calidad de servicio, no use la calidad de servicio personalizada en un volumen. La calidad de servicio personalizada anulará y ajustará los valores de las políticas de calidad de servicio de los volúmenes.

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

Consulte "Rendimiento y calidad del servicio".

- Cree una política de calidad de servicio
- Edite una política de calidad de servicio
- Elimine una política de calidad de servicio

Cree una política de calidad de servicio

Puede crear políticas de calidad de servicio y aplicarlas cuando se creen los volúmenes.

1. Seleccione **Administración** > **políticas QoS**.
2. Haga clic en **Crear directiva QoS**.
3. Introduzca el **Nombre de la directiva**.
4. Introduzca los valores**Min IOPS**, **Max IOPS** y **Burst IOPS**.
5. Haga clic en **Crear directiva QoS**.

Edite una política de calidad de servicio

Una política de calidad de servicio existente se puede cambiar, o bien se pueden editar los valores asociados con esta. Los cambios que se aplican en una política de calidad de servicio afectan a todos los volúmenes asociados con la política.

1. Seleccione **Administración** > **políticas QoS**.
2. Haga clic en el icono Actions de la política de calidad de servicio que quiera editar.
3. En el menú que se abre, seleccione**Edit**.
4. En el cuadro de diálogo **Editar directiva de QoS**, modifique las siguientes propiedades según sea necesario:
   - Nombre de la directiva
   - IOPS mín
   - Tasa máx. De IOPS

- IOPS de ráfaga

5. Haga clic en **Guardar cambios**.

Elimine una política de calidad de servicio

Puede eliminar una política de calidad de servicio si ya no es necesaria. Cuando se elimina una política de calidad de servicio, todos los volúmenes asociados con la política se conservan en la configuración de QoS, pero se desasocian de una política.

> Si desea desasociar en lugar de ello un volumen de una política de calidad de servicio, puede cambiar la configuración de calidad de servicio de ese volumen a personalizado.

1. Seleccione **Administración** > **políticas QoS**.
2. Haga clic en el icono Actions de la política de calidad de servicio que quiera eliminar.
3. En el menú que se abre, seleccione **Eliminar**.
4. Confirme la acción.

Obtenga más información

- "Quite la asociación de políticas de calidad de servicio de un volumen"
- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Gestione los volúmenes

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

En la página Volumes de la pestaña Management, puede crear, modificar, clonar y eliminar volúmenes en un nodo.

Cree un volumen

Es posible crear un volumen y asociarlo con una cuenta determinada. Cada volumen debe estar asociado con una cuenta. Gracias a esta asociación, la cuenta podrá acceder al volumen a través de iniciadores iSCSI con las credenciales de CHAP.

Puede especificar la configuración de calidad de servicio de un volumen mientras lo crea.

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

> El tamaño de volumen predeterminado se selecciona en GB. Los volúmenes se pueden crear con tamaños en GB o GIB:

- 1 GB = 1 000 000 000 bytes

- 1 GIB = 1 073 741 824 bytes

5. Seleccione **Tamaño de bloque** para el volumen.
6. Haga clic en la lista desplegable **cuenta** y seleccione la cuenta que debe tener acceso al volumen.

   Si no existe ninguna cuenta, haga clic en el enlace **Crear cuenta**, escriba un nuevo nombre de cuenta y haga clic en **Crear**. La cuenta se creará y se asociará con el volumen nuevo.

   Si hay más de 50 cuentas, no aparecerá la lista. Comience a escribir y la función de autocompletar mostrará los posibles valores que puede elegir.

7. Para establecer la **calidad del servicio**, realice una de las siguientes acciones:
   a. En **Directiva**, puede seleccionar una directiva QoS existente, si está disponible.
   b. En **Configuración personalizada**, establezca valores mínimos, máximos y de ráfaga personalizados para IOPS o utilice los valores de QoS predeterminados.

      Los volúmenes que tengan un valor de IOPS máximo o de ráfaga superior a 20 20,000 IOPS podrían requerir una profundidad de cola alta o varias sesiones para alcanzar este nivel de IOPS en un único volumen.

8. Haga clic en **Crear volumen**.

Ver los detalles del volumen

1. Seleccione **Gestión** > **volúmenes**.
2. Revise los detalles.
   - **ID**: El ID generado por el sistema para el volumen.
   - **Nombre**: El nombre otorgado al volumen cuando fue creado.
   - **Cuenta**: El nombre de la cuenta asignada al volumen.
   - **Grupos de acceso**: El nombre del grupo o los grupos de acceso de volúmenes a los que pertenece el volumen.
   - **Acceso**: Tipo de acceso asignado al volumen cuando se creó. Los posibles valores son los siguientes:
     - Read/Write: Se aceptan todas las lecturas y las escrituras.
     - Read Only: Se permite toda la actividad de lectura, pero no la de escritura.
     - Locked: Solo se permite el acceso de administrador.
     - ReplicationTarget: Se designa como un volumen de destino en una pareja de volúmenes replicada.
   - **Utilizado**: El porcentaje de espacio utilizado en el volumen.
   - **Tamaño**: El tamaño total (en GB) del volumen.
   - **Instantáneas**: El número de instantáneas creadas para el volumen.
   - **Política de QoS**: Nombre y enlace a la política de QoS definida por el usuario.
   - **Min IOPS**: El número mínimo de IOPS garantizado para el volumen.
   - **Max IOPS**: El número máximo de IOPS permitido para el volumen.
   - **Burst IOPS**: El número máximo de IOPS permitido durante un breve período de tiempo para el volumen. El valor predeterminado es de 15 15,000.
   - **Atributos**: Atributos que se han asignado al volumen como par clave/valor mediante un método API.

- **512e**: Indica si 512e está habilitado en un volumen. Los posibles valores son los siguientes:
  - Sí
  - No
- **Creado el**: Fecha y hora en que se creó el volumen.

Ver los detalles de cada volumen

Es posible ver estadísticas de rendimiento de cada volumen.

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

   Aparecerá una bandeja en la parte inferior de la página 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 y gráficos de rendimiento del volumen.

Editar los volúmenes activos

Es posible modificar atributos de volúmenes, como los valores de calidad de servicio, el tamaño de los volúmenes y la unidad de medida en la que se calculan los valores de bytes. También se puede modificar el acceso de la cuenta para el uso de la replicación o para restringir el acceso al volumen.

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

- Condiciones de funcionamiento normales.
- Se informa de los errores de los volúmenes.
- El volumen se clona.
- El volumen se vuelve a sincronizar.

Pasos

1. Seleccione **Gestión** > **volúmenes**.
2. En la ventana **activo**, haga clic en el icono acciones del volumen que desea editar.
3. Haga clic en **Editar**.
4. **Opcional:** cambie el tamaño total del volumen.
   - Puede aumentar el tamaño del volumen, pero no reducirlo. En cada operación de ajuste de tamaño, solo se puede ajustar el tamaño de un volumen. Las operaciones de recopilación de datos basura y las actualizaciones de software no interrumpen la operación de cambio de tamaño.
   - Si desea ajustar el tamaño del volumen para la replicación, primero debe aumentar el tamaño del volumen asignado como el destino de replicación. Posteriormente, puede cambiar el tamaño del volumen de origen. El tamaño del volumen de destino puede ser mayor o igual que el del volumen de origen, pero no menor.

     El tamaño de volumen predeterminado se selecciona en GB. Los volúmenes se pueden crear con tamaños 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 de cuenta diferente de uno de los siguientes:
   - Solo lectura
   - Lectura/Escritura
   - 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**, escriba un nuevo nombre de cuenta y haga clic en **Crear**. La cuenta se creará y se asociará con el volumen.

   Si hay más de 50 cuentas, no aparecerá la lista. Comience a escribir y la función de autocompletar mostrará los posibles valores que puede elegir.

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

   Si utiliza políticas de calidad de servicio en un volumen, puede establecer la calidad de servicio personalizada para quitar la asociación de la política de calidad de servicio con el volumen. La calidad de servicio personalizada anulará y ajustará los valores de las políticas de calidad de servicio de los volúmenes.

   Cuando cambie los valores de IOPS, debe incrementar sus diez o cien. Los valores de entrada deben ser números enteros válidos.

   Configure los volúmenes con un valor de ráfaga muy alto. De este modo, el sistema podrá procesar grandes cargas de trabajo secuenciales en bloque ocasionales con mayor rapidez, a la vez que se limitan las IOPS sostenidas de un volumen.

8. Haga clic en **Guardar cambios**.

Eliminar un volumen

Es posible eliminar uno o varios volúmenes de un clúster de almacenamiento de Element.

El sistema no purga de manera inmediata un volumen eliminado, sino que este sigue disponible durante aproximadamente ocho horas. Si un volumen se restaura antes de que el sistema lo purgue, el volumen volverá a conectarse y las conexiones iSCSI se restaurarán.

Si se elimina el volumen que se utilizó para crear una snapshot, sus snapshots asociadas pasan a estar inactivas. Cuando se purgan los volúmenes de origen eliminados, también se eliminan del sistema las snapshots inactivas asociadas.

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

Pasos

1. Seleccione **Gestión** > **volúmenes**.
2. Para eliminar un solo volumen, realice los siguientes pasos:
   a. Haga clic en el icono Actions del volumen que desea eliminar.
   b. En el menú que se abre, haga clic en **Eliminar**.
   c. Confirme la acción.

   El sistema mueve el volumen al área **borrada** de la página **Volumes**.
3. Para eliminar varios volúmenes, realice los siguientes pasos:
   a. En la lista de volúmenes, active la casilla junto a los volúmenes que quiera eliminar.
   b. Haga clic en **acciones masivas**.
   c. En el menú que se abre, haga clic en **Eliminar**.
   d. Confirme la acción.

   El sistema mueve los volúmenes al área **Deleted** de la página **Volumes**.

Restaurar un volumen eliminado

Un volumen se puede restaurar en el sistema si se eliminó, pero aún no se purgó. El sistema purga un volumen de manera automática aproximadamente ocho horas después de que fue eliminado. Si el sistema purgó el volumen, no podrá restaurarlo.

1. Seleccione **Gestión** > **volúmenes**.
2. Haga clic en la ficha **eliminado** para ver la lista de volúmenes eliminados.
3. Haga clic en el icono Actions del volumen que desea restaurar.
4. En el menú que se abre, haga clic en **Restaurar**.
5. Confirme la acción.

   El volumen se coloca en la lista **volúmenes activos** y se restauran las conexiones iSCSI con el volumen.

Purgar un volumen

Cuando se purga un volumen, este se quita de forma permanente del sistema y Se pierden todos los datos del volumen.

El sistema purga de manera automática un volumen eliminado ocho horas después de su eliminación. Sin embargo, si desea purgar un volumen antes de la hora programada, puede hacerlo.

1. Seleccione **Gestión** > **volúmenes**.
2. Haga clic en el botón **eliminado**.
3. Ejecute los pasos para purgar un único volumen o varios volúmenes.

Opción	Pasos
Purgar un único volumen	a. Haga clic en el icono Actions del volumen que desea purgar. b. Haga clic en **Purgar**. c. Confirme la acción.
Purgar varios volúmenes	a. Seleccione los volúmenes que desea purgar. b. Haga clic en **acciones masivas**. c. En el menú que se abre, seleccione **Purge**. d. Confirme la acción.

Clonar un volumen

Un clon se puede crear de un solo volumen o de varios volúmenes para hacer una copia de los datos en un momento específico. Cuando se clona un volumen, el sistema crea una copia de Snapshot del volumen y, a continuación, crea una copia de los datos que se indican en la copia de Snapshot. Este es un proceso asíncrono, y la cantidad de tiempo que requiere el proceso depende del tamaño del volumen que se clona y de la carga del clúster actual.

El clúster admite hasta dos solicitudes de clones en ejecución por volumen a la vez y hasta ocho operaciones de clones de volúmenes activos a la vez. Las solicitudes que superen este límite se pondrán en cola para procesarlas más adelante.

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 Snapshot. El volumen será un dispositivo disponible para usar para crear un nuevo almacén de datos. Para obtener más información sobre el montaje de volúmenes de clones y el tratamiento de LUN de copias Snapshot, consulte la documentación de VMware en "Montar una copia de almacén de datos VMFS" y.. "Gestión de almacenes de datos VMFS duplicados".

Antes de truncar un volumen clonado mediante el clonado en un tamaño más pequeño, asegúrese de preparar las particiones de manera que se adapten al volumen inferior.

Pasos

1. Seleccione **Gestión** > **volúmenes**.
2. Para clonar un solo volumen, realice los siguientes pasos:
   a. En la lista de volúmenes de la página **activo**, haga clic en el icono acciones del volumen que desea clonar.
   b. En el menú que se abre, haga clic en **Clonar**.
   c. En la ventana **Clone Volume**, introduzca un nombre de volumen para el volumen recién clonado.
   d. Seleccione un tamaño y una medida para el volumen utilizando el cuadro de número **Tamaño de volumen** y la lista.

      El tamaño de volumen predeterminado se selecciona en GB. Los volúmenes se pueden crear con tamaños 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 que se acaba de clonar.

f. Seleccione una cuenta para asociarla con el volumen recién clonado en la lista **cuenta**.

> Puede crear una cuenta durante este paso si hace clic en el enlace **Crear cuenta**, escribe un nombre de cuenta y hace clic en **Crear**. El sistema agrega automáticamente la cuenta a la lista **cuenta** después de crearla.

3. Para clonar varios volúmenes, realice los siguientes pasos:

a. En la lista de volúmenes de la página **Active**, marque la casilla junto a los volúmenes que desee clonar.

b. Haga clic en **acciones masivas**.

c. En el menú que se abre, 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 asociarla con los volúmenes clonados en la lista **cuenta**.

f. Seleccione el tipo de acceso de los volúmenes clonados.

4. Haga clic en **Iniciar clonación**.

> Al aumentar el tamaño del volumen de un clon, se genera un volumen nuevo con espacio libre adicional al final del volumen. Según cómo use el volumen, podría necesitar ampliar las particiones o crear otras nuevas en el espacio libre para utilizarlo.

Si quiere más información

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

Asigne LUN a volúmenes Fibre Channel

Puede cambiar la asignación de LUN para un volumen Fibre Channel en un grupo de acceso de volúmenes. También puede hacer asignaciones de LUN de volúmenes de Fibre Channel cuando se crea un grupo de acceso de volúmenes.

La asignación de nuevos LUN de Fibre Channel es una función avanzada y podría tener consecuencias desconocidas en el host de conexión. Por ejemplo, el ID del nuevo LUN podría no detectarse automáticamente en el host y este podría requerir un nuevo análisis para detectar el nuevo ID de LUN.

1. Seleccione **Administración** > **grupos de acceso**.
2. Haga clic en el icono Actions del grupo de acceso que quiera editar.
3. En el menú que se abre, seleccione**Edit**.
4. En **asignar ID de LUN** en el cuadro de diálogo **Editar grupo de acceso de volumen**, haga clic en la flecha de la lista **asignaciones de LUN**.
5. Para cada volumen de la lista a la que desea asignar un LUN, introduzca un nuevo valor en el campo **LUN**

correspondiente.

6. Haga clic en **Guardar cambios**.

Aplique una política de calidad de servicio en los volúmenes

Puede aplicar de forma masiva una política de calidad de servicio existente a uno o varios volúmenes.

Debe existir la política de calidad de servicio que desea aplicar de forma masiva.

1. Seleccione **Gestión** > **volúmenes**.
2. En la lista de volúmenes, active la casilla junto a los volúmenes a los que quiera aplicar la política de calidad de servicio.
3. Haga clic en **acciones masivas**.
4. En el menú que aparece, haga clic en **aplicar directiva QoS**.
5. Seleccione la política de calidad de servicio de la lista desplegable.
6. Haga clic en **aplicar**.

Obtenga más información

Políticas de calidad de servicio

Quite la asociación de políticas de calidad de servicio de un volumen

Si desea quitar la asociación de una política de calidad de servicio de un volumen, seleccione una configuración de calidad de servicio personalizada.

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

1. Seleccione **Gestión** > **volúmenes**.
2. Haga clic en el icono Actions de un volumen que contiene una política de calidad de servicio 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 **Min IOPS**, **Max IOPS** y **Burst IOPS**, o mantenga la configuración predeterminada.
6. Haga clic en **Guardar cambios**.

Obtenga más información

Elimine una política de calidad de servicio

Trabaje con volúmenes virtuales

Es posible ver información y realizar tareas en relación con los volúmenes virtuales y sus contenedores de almacenamiento, extremos de protocolo, vinculaciones y hosts asociados mediante la interfaz de usuario de Element.

El sistema de almacenamiento del software NetApp Element se envía con la función Virtual Volumes (VVol)

deshabilitada. Debe realizar una tarea puntual que realice la habilitación manual de la funcionalidad VVol de vSphere a través de la interfaz de usuario de Element.

Después de habilitar la funcionalidad VVol, aparecerá una pestaña VVols en la interfaz de usuario de que ofrece opciones de gestión limitada y supervisión relacionadas con VVol. Además, un componente de software del almacenamiento que se conoce como "proveedor VASA" actúa como un servicio de reconocimiento de almacenamiento de vSphere. La mayoría de los comandos de VVol, como la creación, el clonado y la edición de VVol, se inician en un host de vCenter Server o ESXi y se traducen en el proveedor VASA de API de Element para el sistema de almacenamiento del software Element. Los comandos para crear, eliminar y gestionar contenedores de almacenamiento y eliminar volúmenes virtuales se pueden iniciar mediante la interfaz de usuario de Element.

La mayoría de las configuraciones que se necesitan para usar la funcionalidad Virtual Volumes con los sistemas de almacenamiento del software Element se establecen en vSphere. Consulte la guía de configuración de Virtual Volumes de VMware vSphere para el almacenamiento SolidFire_ para registrar el proveedor VASA en vCenter, crear y gestionar almacenes de datos de VVol, y gestionar el almacenamiento en función de políticas.

No se deben registrar más de un proveedor de VASA de NetApp Element en una sola instancia de vCenter. Cuando se añade un segundo proveedor de VASA NetApp Element, esto hace que no se pueda acceder a todos los almacenes de datos DE VVOL.

La compatibilidad CON VASA para varias vCenter está disponible como revisión de actualización si ya se registró un proveedor de VASA en el para vCenter. Para instalar, descargue el archivo VASA39 .tar.gz de "Descargas de software de NetApp" el sitio y siga las instrucciones en el manifiesto. El proveedor VASA de NetApp Element utiliza un certificado de NetApp. Con este parche, vCenter utiliza el certificado sin modificar para admitir varias instancias de vCenter para que usen VASA y VVol. No modifique el certificado. VASA no admite los certificados SSL personalizados.

Obtenga más información

- Habilite Virtual Volumes
- Ver los detalles de los volúmenes virtuales
- Eliminar un volumen virtual
- Cree un contenedor de almacenamiento
- Editar un contenedor de almacenamiento
- Eliminar un contenedor de almacenamiento
- Extremos de protocolo
- Vinculaciones
- Detalles del host

Habilite Virtual Volumes

Debe habilitar manualmente la funcionalidad vSphere Virtual Volumes (VVol) de a través del software NetApp Element. El sistema de software Element viene con la funcionalidad VVol deshabilitada de forma predeterminada y no se habilita automáticamente como parte de una nueva instalación o actualización. Habilitar la función VVol es una tarea de configuración que solo debe hacer una vez.

Lo que necesitará

- El clúster debe ejecutar Element 9.0 o una versión posterior.
- El clúster de debe estar conectado a un entorno ESXi 6.0 o posterior que sea compatible con VVol.
- Si se utiliza Element 11.3 o una versión posterior, el clúster debe estar conectado a un entorno de ESXi 6.0 Update 3 o posterior.

> Al habilitar la funcionalidad vSphere Virtual Volumes, la configuración del software Element se modifica irreversiblemente. Solo debe habilitar la funcionalidad VVol si el clúster está conectado a un entorno de VMware ESXi compatible con VVol. Puede deshabilitar la función VVol y restaurar la configuración predeterminada solo si devuelve el clúster a la imagen de fábrica, lo que elimina todos los datos del sistema.

Pasos

1. Seleccione **Clusters** > **Ajustes**.
2. Busque la configuración específica del clúster para Virtual Volumes.
3. Haga clic en **Activar volúmenes virtuales**.
4. Haga clic en **Sí** para confirmar el cambio de configuración de Virtual Volumes.

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

   > Cuando se habilita la funcionalidad VVol, el clúster de SolidFire inicia el proveedor VASA, abre el puerto 8444 para el tráfico VASA y crea extremos de protocolo que vCenter y todos los hosts ESXi puedan detectar.

5. Copie la URL del proveedor VASA de la configuración de Virtual Volumes (VVols) en **Clusters** > **Settings**. Esta URL se usará 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 se puedan aprovisionar las máquinas virtuales en un almacén de datos de VVol.

7. Seleccione **VVols** > **Protocol Endpoints**.
8. Compruebe que se ha creado un extremo de protocolo para cada nodo del clúster.

   > Se requieren tareas adicionales de configuración en vSphere. Consulte la guía de configuración de Virtual Volumes de VMware vSphere para el almacenamiento SolidFire_ para registrar el proveedor VASA en vCenter, crear y gestionar almacenes de datos de VVol, y gestionar el almacenamiento en función de políticas.

Obtenga más información

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

Ver los detalles de los volúmenes virtuales

En la interfaz de usuario de Element, se puede revisar la información relacionada con los volúmenes virtuales activos del clúster. También se puede ver la actividad de rendimiento de cada volumen virtual, como la entrada, la salida, el rendimiento y la latencia,

profundidad de cola e información de volumen.

Lo que necesitará

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

Pasos

1. Haga clic en **VVols** > **Virtual Volumes**.

   Se muestra la información de todos los volúmenes virtuales activos.

2. Haga clic en el icono **acciones** del volumen virtual que desee revisar.
3. En el menú que se abre, seleccione **Ver detalles**.

Detalles

La página Virtual Volumes de la pestaña VVols proporciona información sobre cada volumen virtual activo en el clúster, como el ID de volumen, el ID de snapshot, el ID de volumen virtual primario y el ID de 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 snapshot de SolidFire.
- **Id. De volumen virtual principal**: El ID de volumen virtual del volumen virtual principal. Si el ID solo está formado por ceros, indica que el volumen virtual es independiente y no tiene ningún enlace a un volumen principal.
- **Virtual Volume ID**: El UUID del volumen virtual.
- **Nombre**: 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**: Tipo de volumen virtual: Config, datos, memoria, intercambio u otro.
- **Access**: 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. Haga clic en el número para vincular a detalles de instantánea.
- **Min IOPS**: El valor mínimo de QoS de IOPS del volumen virtual.
- **Max IOPS**: El valor máximo de QoS para IOPS del volumen virtual.
- **Burst IOPS**: El valor máximo de QoS de ráfaga del volumen virtual.
- **VMW_VMID**: VMware define la información de los campos que van precedidos por "VMW_".
- **Crear tiempo**: La hora en que se completó la tarea de creación de volumen virtual.

Detalles de cada volumen virtual

La página Virtual Volumes de la pestaña VVols proporciona la siguiente información sobre volúmenes virtuales cuando selecciona un volumen virtual y desea ver sus detalles.

- **VMW_XXX**: VMware define la información de los campos que van precedidos por "VMW_".
- **Id. De volumen virtual principal**: El ID de volumen virtual del volumen virtual principal. Si el ID solo está formado por ceros, indica que el volumen virtual es independiente y no tiene ningún enlace a un volumen principal.
- **Virtual Volume ID**: El UUID del volumen virtual.
- **Tipo de volumen virtual**: Tipo de volumen virtual: Config, datos, memoria, intercambio u otro.
- **ID de volumen**: El ID del volumen subyacente.
- **Access**: Los permisos de lectura y escritura asignados al volumen virtual.
- **Nombre de cuenta**: Nombre de la cuenta que contiene el volumen.
- **Grupos de acceso**: Grupos de acceso de volúmenes asociados.
- **Tamaño total del volumen**: Capacidad total aprovisionada en bytes.
- * Bloques no cero*: Número total de bloques de 4 KiB con datos después de haber completado la última operación de recopilación de basura.
- * Cero bloques*: Número total de bloques de 4 KiB sin datos después de haber completado la última ronda de recolección de basura.
- **Instantáneas**: El número de instantáneas asociadas. Haga clic en el número para vincular a detalles de instantánea.
- **Min IOPS**: El valor mínimo de QoS de IOPS del volumen virtual.
- **Max IOPS**: El valor máximo de QoS para IOPS del volumen virtual.
- **Burst IOPS**: El valor máximo de QoS de ráfaga del volumen virtual.
- **Activar 512**: Debido a que los volúmenes virtuales siempre utilizan emulación de tamaño de bloque de 512 bytes, el valor es siempre yes.
- **Volúmenes emparejados**: Indica si un volumen está emparejado.
- **Crear tiempo**: La hora en que se completó la tarea de creación de 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 ámbito de sector 4k. Si el número de escrituras no alineadas es grande, puede indicar que la alineación de las particiones no es la adecuada.
- **Lecturas no alineadas**: Para los volúmenes 512e, el número de operaciones de lectura que no estaban en un ámbito del sector 4k. Si el número de lecturas no alineadas es grande, puede indicar que la alineación de las particiones no es la adecuada.
- **SsiEUIDeviceID**: Identificador único global de dispositivo SCSI para el volumen en formato de 16 bytes basado en EUI-64.
- **SscsiNAADeviceID**: Identificador de dispositivo SCSI exclusivo global para el volumen en el formato extendido registrado de NAA según IEEE.
- **Atributos**: Lista de pares nombre-valor en formato de objeto JSON.

Eliminar un volumen virtual

Si bien los volúmenes virtuales se deben eliminar siempre en el nivel de gestión de VMware, la funcionalidad que le permite eliminar volúmenes virtuales se habilita en la interfaz de usuario de Element. Solo debe eliminar un volumen virtual en la interfaz de usuario de Element cuando sea absolutamente necesario, como cuando vSphere no logra limpiar los volúmenes virtuales en el almacenamiento de SolidFire.

1. Seleccione **VVols** > **Virtual Volumes**.
2. Haga clic en el icono Actions del volumen virtual que desee eliminar.
3. En el menú que se abre, seleccione **Eliminar**.

> Debe eliminar un volumen virtual en el nivel de gestión de VMware para garantizar que el volumen virtual esté correctamente desvinculado antes de su eliminación. Solo debe eliminar un volumen virtual en la interfaz de usuario de Element cuando sea absolutamente necesario, como cuando vSphere no logra limpiar los volúmenes virtuales en el almacenamiento de SolidFire. Si elimina un volumen virtual en la interfaz de usuario de Element, el volumen se depurará inmediatamente.

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

Gestione los contenedores de almacenamiento

Un contenedor de almacenamiento es una representación de almacén de datos de vSphere creada en un clúster donde se ejecuta el software Element.

Los contenedores de almacenamiento se crean y están ligados a cuentas de NetApp Element. Un contenedor de almacenamiento que se crea en el almacenamiento Element se muestra como un almacén de datos de vSphere en vCenter y ESXi. Los contenedores de almacenamiento no asignan espacio en el almacenamiento de Element. Simplemente se utilizan para asociar volúmenes virtuales de forma lógica.

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

Cree un contenedor de almacenamiento

Los contenedores de almacenamiento se pueden crear en la interfaz de usuario de Element y se pueden detectar en vCenter. Es necesario crear al menos un contenedor de almacenamiento para comenzar a aprovisionar máquinas virtuales respaldadas por VVol.

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

Pasos

1. Seleccione **VVols** > **contenedores de almacenamiento**.
2. Haga clic en el botón **Crear contenedores de almacenamiento**.
3. Introduzca la información del contenedor de almacenamiento en el cuadro de diálogo **Crear un contenedor de almacenamiento nuevo**:

a. Escriba un nombre para el contenedor de almacenamiento.

b. Configure el iniciador y los secretos de destino para CHAP.

> Deje los campos CHAP Settings vacíos para que los secretos se generen automáticamente.

c. Haga clic en el botón **Crear contenedor de almacenamiento**.

4. Compruebe que el nuevo contenedor de almacenamiento aparece en la lista de la subpestaña **contenedores de almacenamiento**.

> Dado que el ID de cuenta de NetApp Element se crea automáticamente y se asigna al contenedor de almacenamiento, no es necesario crear una cuenta de forma manual.

Ver los detalles del contenedor de almacenamiento

En la página Storage Containers de la pestaña VVols, puede ver información relativa a todos los contenedores de almacenamiento activos del clúster.

- **ID de cuenta**: El ID de la cuenta NetApp Element asociada con el contenedor de almacenamiento.
- **Nombre**: El nombre del contenedor de almacenamiento.
- **Estado**: El estado del contenedor de almacenamiento. Los posibles valores son los siguientes:
  - Active: El contenedor de almacenamiento está en uso.
  - Locked: El contenedor de almacenamiento está bloqueado.
- **Tipo PE**: Tipo de extremo de 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.
- **Active Virtual Volumes**: El número de volúmenes virtuales activos asociados con el contenedor de almacenamiento.

Ver los detalles de cada contenedor de almacenamiento

Si desea ver la información de un contenedor de almacenamiento específico, selecciónelo en la página Storage Containers de la pestaña VVols.

- **ID de cuenta**: El ID de la cuenta NetApp Element asociada con el contenedor de almacenamiento.
- **Nombre**: El nombre del contenedor de almacenamiento.
- **Estado**: El estado del contenedor de almacenamiento. Los posibles valores son los siguientes:
  - Active: El contenedor de almacenamiento está en uso.
  - Locked: El contenedor de almacenamiento está bloqueado.
- **Secreto CHAP del iniciador**: El secreto CHAP único para el iniciador.
- **Secreto objetivo CHAP**: El secreto CHAP único para el destino.
- **ID del contenedor de almacenamiento**: El UUID del contenedor de almacenamiento del volumen virtual.
- **Tipo de extremo de protocolo**: Indica el tipo de extremo de protocolo (SCSI es el único protocolo disponible).

Editar un contenedor de almacenamiento

La autenticación CHAP del contenedor de almacenamiento se puede modificar en la interfaz de usuario de Element.

1. Seleccione **VVols** > **contenedores de almacenamiento**.
2. Haga clic en el icono **acciones** del contenedor de almacenamiento que desee editar.
3. En el menú que se abre, seleccione **Editar**.
4. En CHAP Settings, edite las credenciales de Initiator Secret y Target Secret que se han usado para la autenticación.

   Si no se modifican las credenciales en CHAP Settings, seguirán siendo las mismas. Si deja vacíos los campos de las credenciales, el sistema generará automáticamente secretos nuevos.

5. Haga clic en **Guardar cambios**.

Eliminar un contenedor de almacenamiento

Los contenedores de almacenamiento se pueden eliminar de la interfaz de usuario de Element.

Lo que necesitará

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

Pasos

1. Seleccione **VVols** > **contenedores de almacenamiento**.
2. Haga clic en el icono **acciones** del contenedor de almacenamiento que desea eliminar.
3. En el menú que se abre, seleccione **Eliminar**.
4. Confirme la acción.
5. Actualice la lista de contenedores de almacenamiento en la subpestaña **contenedores de almacenamiento** para confirmar que se ha eliminado el contenedor de almacenamiento.

Extremos de protocolo

Los extremos de protocolo son puntos de acceso que utiliza un host para abordar el almacenamiento de un clúster que ejecuta el software NetApp Element. Los usuarios no pueden eliminar ni modificar los extremos de protocolo. Tampoco se pueden asociar con una cuenta ni se pueden añadir a un grupo de acceso de volúmenes.

Un clúster que ejecuta el software Element crea automáticamente un extremo de protocolo por nodo de almacenamiento en el clúster. Por ejemplo, un clúster de almacenamiento de seis nodos tiene seis extremos de protocolo que se asignan a cada host ESXi. Los extremos de protocolo se gestionan dinámicamente con el software Element y se crean, mueven o eliminan según sea necesario sin intervención. Los extremos de protocolo son el objetivo para las rutas múltiples y actúan como proxy I/o para las LUN subsidiarias. Cada extremo de protocolo consume una dirección SCSI disponible, al igual que un destino iSCSI estándar. Los extremos de protocolo aparecen como un dispositivo de almacenamiento de bloque único (512 bytes) en el cliente vSphere, pero este dispositivo de almacenamiento no está disponible para formatearse o usarse como almacenamiento.

ISCSI es el único protocolo compatible. No se admite el protocolo Fibre Channel.

Detalles de los extremos de protocolo

La página Protocol Endpoints en la pestaña VVols proporciona información sobre extremos de protocolo.

- **ID de proveedor primario**

  El ID del proveedor de extremo de protocolo principal.

- **ID de proveedor secundario**

  El ID del proveedor de extremo de protocolo secundario.

- **ID de extremo de protocolo**

  El UUID del extremo de protocolo.

- **Estado del extremo de protocolo**

  El estado del extremo de protocolo. Los valores posibles son los siguientes:

  - Active: El extremo de protocolo está en uso.
  - Start: El extremo de protocolo se está iniciando.
  - Failover: El extremo de protocolo se conmutó al nodo de respaldo.
  - Reserved: El extremo de protocolo está reservado.

- **Tipo de proveedor**

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

  - Primario
  - Secundario

- **SCSI NAA DEVICE ID**

  El identificador exclusivo de dispositivo SCSI para el extremo de protocolo a nivel global en el formato extendido registrado de NAA según la norma IEEE.

Vinculaciones

Para realizar operaciones de I/o con un volumen virtual, el volumen virtual se debe vincular primero a un host ESXi.

El clúster de SolidFire elige un extremo de protocolo adecuado, crea una vinculación que asocia el host ESXi y el volumen virtual con el extremo del protocolo, y devuelve la vinculación al host ESXi. Una vez enlazados, el host ESXi puede llevar a cabo operaciones de I/o con el volumen virtual vinculado.

Detalles de vinculaciones

La página Bindings de la pestaña VVols proporciona información relacionada con la vinculación de cada volumen virtual.

Se muestra la siguiente información:

- **ID de host**

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

- **ID de extremo de protocolo**

  Los ID de extremo de protocolo que corresponden a cada nodo del clúster de SolidFire.

- **Protocol Endpoint in Band ID**

  El ID de dispositivo SCSI de NAA según el extremo de protocolo.

- **Tipo de extremo de protocolo**

  El tipo de extremo de protocolo.

- **ID de enlace de VVol**

  El UUID de vinculación del volumen virtual.

- **ID de VVol**

  El identificador único universal (UUID) del volumen virtual.

- **ID secundario de VVol**

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

Detalles del host

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

Se muestra la siguiente información:

- **ID de host**

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

- **Dirección de host**

  La dirección IP o el nombre DNS del host ESXi.

- **Enlaces**

  Los ID de vinculación de todos los volúmenes virtuales que están vinculados por el host ESXi.

- **ID de clúster ESX**

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

- **IQN del iniciador**

  Los IQN de iniciador para el host de volúmenes virtuales.

- **ID de extremo de protocolo de SolidFire**

  Los extremos del protocolo que el host ESXi puede ver en ese momento.

Trabajar con iniciadores y grupos de acceso de volúmenes

Es posible usar iniciadores iSCSI o iniciadores de Fibre Channel para acceder a los volúmenes definidos dentro de los grupos de acceso de volúmenes.

Los grupos de acceso se pueden crear asignando IQN de iniciadores de iSCSI o WWPN de Fibre Channel en una colección de volúmenes. Cada IQN que se añade a un grupo de acceso puede acceder a cada volumen del grupo sin necesidad de contar con autenticación CHAP.

Existen dos tipos de métodos de autenticación CHAP:

- Autenticación CHAP en el nivel de la cuenta: Se puede asignar la autenticación CHAP para la cuenta.
- Autenticación CHAP a nivel de iniciador: Puede asignar secretos y destino CHAP únicos para iniciadores específicos sin estar enlazados a una única cuenta en. Esta autenticación CHAP a nivel de iniciador sustituye las credenciales de nivel de cuenta.

De manera opcional, con CHAP por iniciador, puede aplicar la autorización de iniciador y la autenticación CHAP por iniciador. Estas opciones se pueden definir por iniciador y un grupo de acceso puede contener una combinación de iniciadores con diferentes opciones.

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

Los grupos de acceso de volúmenes presentan los siguientes límites:

- Se permiten hasta 64 IQN o WWPN en un grupo de acceso.
- Un grupo de acceso puede estar formado por un máximo de 2000 volúmenes.
- Un IQN o un WWPN solo pueden pertenecer a un grupo de acceso.
- Un volumen puede pertenecer a hasta cuatro grupos de acceso.

Obtenga más información

- Cree un grupo de acceso de volúmenes
- Añada volúmenes a un grupo de acceso
- Quite volúmenes de un grupo de acceso
- Cree un iniciador
- Edite un iniciador
- Añada un único iniciador a un grupo de acceso de volúmenes
- Añada varios iniciadores a un grupo de acceso de volúmenes
- Quite los iniciadores de un grupo de acceso
- Eliminar un grupo de acceso
- Eliminar un iniciador

Cree un grupo de acceso de volúmenes

Los grupos de acceso de volúmenes se pueden crear asignando iniciadores a una colección de volúmenes para garantizar el acceso seguro. A continuación, podrá 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 añadir credenciales de CHAP para un único iniciador en un grupo de acceso de volúmenes, lo que proporciona más seguridad. Esto permite aplicar esta opción a los grupos de acceso de volúmenes que ya existen.

Pasos

1. Haga clic en **Administración** > **grupos de acceso**.
2. Haga clic en **Crear grupo de acceso**.
3. Escriba un nombre para el grupo de acceso de volúmenes en el campo **Nombre**.
4. Añada un iniciador al grupo de acceso de volúmenes de una de las siguientes maneras:

Opción	Descripción
Se añade un iniciador de Fibre Channel	a. En Add Initiators, seleccione un iniciador de Fibre Channel existente en la lista Unbound Fibre Channel Initiators. b. Haga clic en **Agregar iniciador FC**. Puede crear un iniciador durante este paso si hace clic en el enlace **Crear iniciador**, escribe un nombre de iniciador y hace clic en **Crear**. El sistema añade automáticamente el iniciador a la lista Initiators después de crearlo. A continuación, se ofrece un ejemplo de formato: `5f:47:ac:c0:5c:74:d4:02`

Opción	Descripción
Adición de un iniciador de iSCSI	En Add Initiators, seleccione un iniciador de existente en la lista Initiators. **Nota:** puede crear un iniciador durante este paso si hace clic en el enlace **Crear iniciador**, introduce un nombre de iniciador y haz clic en **Crear**. El sistema añade automáticamente el iniciador a la lista Initiators después de crearlo. A continuación, se ofrece un ejemplo de formato: `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 **Gestión** > **volúmenes** > **activo**. Al modificar un iniciador, puede cambiar el atributo requiredCHAP a True, lo que permite configurar el secreto de iniciador de destino. Para obtener más información, consulte la información de API acerca del método API ModifyInitiator. "Gestione 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 **volúmenes adjuntos**.
7. **Opcional:** Agregue más volúmenes según sea necesario.
8. Haga clic en **Crear grupo de acceso**.

Obtenga más información

Añada volúmenes a un grupo de acceso

Ver detalles de cada grupo de acceso

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

1. Haga clic en **Administración** > **grupos de acceso**.
2. Haga clic en el icono Actions de un grupo de acceso.
3. Haga clic en **Ver detalles**.

Detalles del grupo de acceso de volúmenes

En la página Access Groups de la pestaña Management, se proporciona información sobre los grupos de acceso de volúmenes.

Se muestra la siguiente información:

- **ID**: El ID generado por el sistema para el grupo de acceso.
- **Nombre**: El nombre otorgado al grupo de acceso cuando se creó.
- **Volúmenes activos**: Número de volúmenes activos en el grupo de acceso.
- **Compresión**: La puntuación de eficiencia de compresión del grupo de acceso.
- **Deduplicación**: La puntuación de eficiencia de deduplicación del grupo de acceso.
- **Thin Provisioning**: Puntuación de eficiencia de thin provisioning para el grupo de acceso.
- **Eficiencia general**: La puntuación de eficiencia general del grupo de acceso.
- **Initiators**: El número de iniciadores conectados al grupo de acceso.

Añada volúmenes a un grupo de acceso

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

También puede usar este procedimiento para añadir volúmenes a un grupo de acceso de volúmenes de Fibre Channel.

1. Haga clic en **Administración** > **grupos de acceso**.
2. Haga clic en el icono Actions del grupo de acceso al que desea añadir volúmenes.
3. Haga clic en el botón **Editar**.
4. En Agregar volúmenes, seleccione un volumen de la lista **volúmenes**.

   Puede añadir más volúmenes repitiendo este paso.

5. Haga clic en **Guardar cambios**.

Quite volúmenes de un grupo de acceso

Cuando se quita un volumen de un grupo de acceso, el grupo ya no puede acceder a dicho volumen.

Si se modifica la configuración de CHAP en una cuenta o se quitan los iniciadores o los volúmenes de un grupo de acceso, se podría interrumpir el acceso de los iniciadores a los volúmenes de forma inesperada. Para asegurarse de que no se interrumpirá el acceso a los volúmenes de forma inesperada, siempre debe cerrar las sesiones iSCSI afectadas por alguno de los cambios en la cuenta o en el grupo de acceso. Asimismo, compruebe que los iniciadores pueden volver a conectarse con los volúmenes una vez que se hayan realizado los cambios en la configuración del iniciador y la configuración del clúster.

1. Haga clic en **Administración** > **grupos de acceso**.
2. Haga clic en el icono Actions del grupo de acceso del que desea quitar volúmenes.
3. Haga clic en **Editar**.
4. En Agregar volúmenes en el cuadro de diálogo **Editar grupo de acceso de volumen**, haga clic en la flecha de la lista **volúmenes adjuntos**.
5. Seleccione el volumen que desea eliminar de la lista y haga clic en el icono **x** para eliminar el volumen de

la lista.

Puede eliminar más volúmenes repitiendo este paso.

6. Haga clic en **Guardar cambios**.

Cree un iniciador

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

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

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

Pasos

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

Opción	Pasos
Cree un solo iniciador	a. Haga clic en **Crear un único iniciador**. b. Introduzca el IQN o el WWPN del iniciador en el campo **IQN/WWPN**. c. Introduzca un nombre descriptivo para el iniciador en el campo **Alias**. d. Haga clic en **Crear iniciador**.
Cree varios iniciadores	a. Haga clic en **Bulk Create Initiators**. b. Introduzca una lista de varios IQN o WWPN en el cuadro de texto. c. Haga clic en **Add Initiators**. d. Elija un iniciador de la lista resultante y haga clic en el icono Agregar correspondiente en la columna **Alias** para añadir un alias para el iniciador. e. Haga clic en la Marca de verificación para confirmar el nuevo alias. f. Haga clic en **Crear iniciadores**.

Edite un iniciador

Es posible cambiar el alias de un iniciador existente o añadir un alias si aún no hay ninguno.

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

Consulte "Gestione el almacenamiento con la API de Element".

Pasos

1. Haga clic en **Administración** > **iniciadores**.
2. Haga clic en el icono Actions del iniciador que quiera editar.
3. Haga clic en **Editar**.
4. Introduzca un nuevo alias para el iniciador en el campo **Alias**.
5. Haga clic en **Guardar cambios**.

Añada un único iniciador a un grupo de acceso de volúmenes

Es posible añadir un iniciador a un grupo de acceso de volúmenes existente.

Cuando se añade un iniciador a un grupo de acceso de volúmenes, el iniciador tiene acceso a todos los volúmenes en ese grupo de acceso de volúmenes.

Para buscar el iniciador de cada volumen, haga clic en el icono Actions y seleccione **View Details** para el volumen en la lista de volúmenes activos.

Si utiliza CHAP basado en iniciador, puede añadir credenciales de CHAP para un único iniciador en un grupo de acceso de volúmenes, lo que proporciona más seguridad. Esto permite aplicar esta opción a los grupos de acceso de volúmenes que ya existen.

Pasos

1. Haga 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 añadir un iniciador de Fibre Channel al grupo de acceso de volúmenes, realice los pasos siguientes:

   a. En Add Initiators, seleccione un iniciador de Fibre Channel existente en la lista **Unbound Fibre Channel Initiators**.

   b. Haga clic en **Agregar iniciador FC**.

   Puede crear un iniciador durante este paso si hace clic en el enlace **Crear iniciador**, escribe un nombre de iniciador y hace clic en **Crear**. El sistema agrega automáticamente el iniciador a la lista **Initiators** después de crearlo.

   A continuación, se ofrece un ejemplo de formato:

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

5. Para añadir un iniciador iSCSI al grupo de acceso de volúmenes, en Add Initiators, seleccione un iniciador existente en la lista **Initiators**.

   Puede crear un iniciador durante este paso si hace clic en el enlace **Crear iniciador**, escribe un nombre de iniciador y hace clic en **Crear**. El sistema agrega automáticamente el iniciador a la lista **Initiators** después de crearlo.

El formato aceptado de un IQN de iniciador es el siguiente: iqn.aaaa-mm, en el cual a y m son dígitos, seguidos de texto que solo puede contener dígitos, caracteres alfabéticos en minúscula, un punto (.), dos puntos (:) o un guion (-).

A continuación, se ofrece un ejemplo de formato:

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

Puede encontrar el IQN del iniciador para cada volumen desde la página **Management** > **Volumes** Active Volumes haciendo clic en el icono Actions y, a continuación, seleccionando **View Details** para el volumen.

6. Haga clic en **Guardar cambios**.

Añada varios iniciadores a un grupo de acceso de volúmenes

Es posible añadir varios iniciadores a un grupo de acceso de volúmenes existente para permitir el acceso a volúmenes en el grupo de acceso de volúmenes con o sin necesidad de contar con autenticación CHAP.

Cuando se añaden un iniciador a un grupo de acceso de volúmenes, los iniciadores tienen acceso a todos los volúmenes en ese grupo de acceso de volúmenes.

Para buscar el iniciador de cada volumen, haga clic en el icono Actions y, a continuación, en **View Details** para el volumen en la lista de volúmenes activos.

Es posible añadir varios iniciadores a un grupo de acceso de volúmenes existente para habilitar el acceso a volúmenes y asignar credenciales CHAP únicas para cada iniciador de ese grupo de acceso de volúmenes. Esto permite aplicar esta opción a los grupos de acceso de volúmenes que ya existen.

Puede asignar atributos CHAP basados en iniciadores mediante una llamada API. Para añadir un nombre de cuenta CHAP y credenciales por iniciador, debe utilizar la llamada API ModifyInitiator para quitar y agregar acceso y atributos de CHAP.

Para obtener más información, consulte "Gestione el almacenamiento con la API de Element".

Pasos

1. Haga clic en **Administración** > **iniciadores**.
2. Seleccione los iniciadores que desea añadir a un grupo de acceso.
3. Haga clic en el botón **acciones masivas**.
4. Haga clic en **Agregar a grupo de acceso de volumen**.
5. En el cuadro de diálogo Add to Volume Access Group, seleccione un grupo de acceso en la lista **Volume Access Group**.
6. Haga clic en **Agregar**.

Quite los iniciadores de un grupo de acceso

Cuando se quita un iniciador de un grupo de acceso, este ya no puede acceder a los

volúmenes de ese grupo de acceso de volúmenes. El acceso normal de cuenta al volumen no se interrumpe.

Si se modifica la configuración de CHAP en una cuenta o se quitan los iniciadores o los volúmenes de un grupo de acceso, se podría interrumpir el acceso de los iniciadores a los volúmenes de forma inesperada. Para asegurarse de que no se interrumpirá el acceso a los volúmenes de forma inesperada, siempre debe cerrar las sesiones iSCSI afectadas por alguno de los cambios en la cuenta o en el grupo de acceso. Asimismo, compruebe que los iniciadores pueden volver a conectarse con los volúmenes una vez que se hayan realizado los cambios en la configuración del iniciador y la configuración del clúster.

Pasos

1. Haga clic en **Administración** > **grupos de acceso**.
2. Haga clic en el icono **acciones** del grupo de acceso que desea quitar.
3. En el menú que se abre, seleccione **Editar**.
4. En Add Initiators en el cuadro de diálogo **Edit Volume Access Group**, haga clic en la flecha de la lista **Initiators**.
5. Seleccione el icono de x para cada iniciador que desea quitar del grupo de acceso.
6. Haga clic en **Guardar cambios**.

Eliminar un grupo de acceso

Puede eliminar un grupo de acceso cuando ya no sea necesario. No hace falta que elimine los ID de iniciador ni los ID de volumen del grupo de acceso de volúmenes antes de eliminar el grupo. Una vez que se elimine el grupo de acceso, se interrumpirá el acceso del grupo al volumen.

1. Haga clic en **Administración** > **grupos de acceso**.
2. Haga clic en el icono **acciones** del grupo de acceso que desea eliminar.
3. En el menú que se abre, haga clic en **Eliminar**.
4. Para eliminar también los iniciadores asociados con este grupo de acceso, active la casilla de verificación **Eliminar iniciadores de este grupo de acceso** .
5. Confirme la acción.

Eliminar un iniciador

Es posible eliminar un iniciador cuando ya no se necesita. Cuando se elimina un iniciador, el sistema la quita de los grupos de acceso de volúmenes asociados. Las conexiones que usan el iniciador siguen siendo válidas hasta que se restablece la conexión.

Pasos

1. Haga clic en **Administración** > **iniciadores**.
2. Siga los pasos para eliminar un solo iniciador o varios iniciadores:

Opción	Pasos
Elimine un solo iniciador	a. Haga clic en el icono **acciones** del iniciador que desea eliminar. b. Haga clic en **Eliminar**. c. Confirme la acción.
Elimine varios iniciadores	a. Seleccione las casillas junto a los iniciadores que desea eliminar. b. Haga clic en el botón **acciones masivas**. c. En el menú que se abre, seleccione **Eliminar**. d. Confirme la acción.

Proteja sus datos

El software NetApp Element permite proteger los datos de diversos modos con funcionalidades como copias de Snapshot de volúmenes o grupos de volúmenes individuales, replicación entre clústeres y volúmenes que se ejecutan en Element y replicación en sistemas ONTAP.

- **Instantáneas**

  La protección de datos con Snapshot replica los datos modificados en momentos específicos a un clúster remoto. Solo se replican las copias de Snapshot que se crean en el clúster de origen. No se producen las escrituras activas del volumen de origen.

  Use copias Snapshot de volumen para la protección de datos

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

  Es posible replicar datos de volúmenes de forma síncrona o asíncrona desde un clúster de una pareja de clústeres, tanto en ejecución en Element para los escenarios de conmutación por error y conmutación tras recuperación.

  Llevar a cabo la replicación remota entre los clústeres que ejecutan el software NetApp Element

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

  Con la tecnología SnapMirror de NetApp, puede replicar copias de Snapshot que se hayan realizado utilizando Element en ONTAP con fines de recuperación ante desastres. En una relación de SnapMirror, Element es un extremo y ONTAP es el otro.

  Use la replicación de SnapMirror entre clústeres de Element y ONTAP

- **Copia de seguridad y restauración de volúmenes desde almacenes de objetos SolidFire, S3 o Swift**

  Es posible realizar backups y restaurar volúmenes en otro almacenamiento de SolidFire, así como en almacenes de objetos secundarios que sean compatibles con OpenStack Swift o Amazon S3.

  Realizar backups y restaurar volúmenes en almacenes de objetos SolidFire, S3 o Swift

Si quiere más información

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

Use copias Snapshot de volumen para la protección de datos

Una copia de Snapshot de volumen es una copia de un momento específico de un volumen. Puede realizar una copia de Snapshot de un volumen y usarla más adelante si se tiene que revertir un volumen al estado que tenía en el momento de creación de la copia de Snapshot.

Las copias Snapshot son similares a los clones de volúmenes. No obstante, las copias de Snapshot son réplicas de los metadatos del volumen, por lo que no es posible montarlas ni escribir en ellas. Además, para crear una copia de Snapshot de volumen, solo se requiere una pequeña cantidad de espacio y recursos del sistema, lo cual es más rápido crear una copia de Snapshot que clonar.

Es posible realizar una copia de Snapshot de un volumen individual o un conjunto de volúmenes.

Opcionalmente, replique las snapshots en un clúster de remoto y utilícelos como copia de backup del volumen. Gracias a ello, es posible revertir un volumen a un momento específico mediante la copia de Snapshot replicada. Como alternativa, es posible crear un clon de un volumen a partir de una copia de Snapshot replicada.

Obtenga más información

- Use copias de Snapshot de volumen individuales para la protección de datos
- El uso de copias de Snapshot de grupo para la tarea de protección de datos
- Programar una copia de Snapshot

Use copias de Snapshot de volumen individuales para la protección de datos

Una copia de Snapshot de volumen es una copia de un momento específico de un volumen. Se puede usar un volumen individual en lugar de un grupo de volúmenes para la copia de Snapshot.

Obtenga más información

- Cree una copia de Snapshot de volumen
- Editar la retención de snapshot
- Eliminar una copia de Snapshot
- Clonar un volumen a partir de una copia de Snapshot
- Revertir un volumen a una copia de Snapshot
- Realizar backups de una copia de Snapshot de volumen en un almacén de objetos Amazon S3
- Realizar backups de una copia de Snapshot de volumen en un almacén de objetos OpenStack Swift
- Realizar backups de una copia de Snapshot de volumen en un clúster de SolidFire

Cree una copia de Snapshot de volumen

Se puede crear una copia de Snapshot de un volumen activo para conservar la imagen del volumen en un momento determinado. Es posible crear hasta 32 copias de Snapshot de un solo volumen.

1. Haga clic en **Administración** > **volúmenes**.
2. Haga clic en el icono **acciones** del volumen que desea utilizar para la instantánea.
3. En el menú que se abre, seleccione **Snapshot**.
4. En el cuadro de diálogo **Crear instantánea del volumen**, introduzca el nuevo nombre de instantánea.
5. **Opcional:** Active la casilla de verificación **incluir instantánea en la replicación cuando se empareja** para asegurarse de que la instantánea se captura en la replicación cuando el volumen principal está emparejado.
6. Para configurar la retención de la copia de Snapshot, seleccione una de las siguientes opciones:
   - Haga clic en **mantener siempre** para conservar la instantánea en el sistema indefinidamente.
   - Haga clic en **establecer período de retención** y utilice los cuadros de número de fecha para elegir un período de tiempo durante el cual el sistema retendrá la instantánea.
7. Para crear una sola snapshot de forma inmediata, realice los siguientes pasos:
   a. Haga clic en **tomar instantánea ahora**.
   b. Haga clic en **Crear Snapshot**.
8. Para programar que la copia de Snapshot se ejecute en el futuro, realice los siguientes pasos:
   a. Haga clic en **Crear programación Snapshot**.
   b. Introduzca un **Nuevo nombre de programa**.
   c. Seleccione un **Tipo de programación** de la lista.
   d. **Opcional:** Active la casilla de verificación **Programación periódica** para repetir periódicamente la instantánea programada.
   e. Haga clic en **Crear programación**.

Obtenga más información

Programar una copia de Snapshot

Editar la retención de snapshot

Puede cambiar el período de retención de una snapshot y determinar si el sistema elimina las snapshots y cuándo. El período de retención que se especifica comienza cuando se introduce el nuevo intervalo. Cuando se establece un período de retención, se puede seleccionar un período que comience en ese mismo momento (la retención no se calcula a partir del momento de creación de la copia de Snapshot). Los intervalos se pueden especificar en minutos, horas y días.

Pasos

1. Haga clic en **Protección de datos** > **instantáneas**.
2. Haga clic en el icono **acciones** de la instantánea que desea editar.

3. En el menú que se abre, haga clic en **Editar**.
4. **Opcional:** Active la casilla de verificación **incluir instantánea en la replicación cuando se empareje** para asegurarse de que la instantánea se capture en la replicación cuando el volumen primario se empareje.
5. **Opcional:** Seleccione una opción de retención para la instantánea:
   - Haga clic en **mantener siempre** para conservar la instantánea en el sistema indefinidamente.
   - Haga clic en **establecer período de retención** y utilice los cuadros de número de fecha para seleccionar un período de tiempo durante el cual el sistema retendrá la instantánea.
6. Haga clic en **Guardar cambios**.

Eliminar una copia de Snapshot

Es posible eliminar una copia de Snapshot de volumen de un clúster de almacenamiento donde se ejecuta el software Element. Cuando se elimina una copia de Snapshot, el sistema la quita de forma inmediata.

Es posible eliminar del clúster de origen copias de Snapshot que se están replicando. Si una snapshot se está sincronizando en el clúster de destino cuando se la elimina, se completa la replicación sincrónica y la snapshot se elimina del clúster de origen. La copia de Snapshot no se elimina del clúster de destino.

También es posible eliminar del clúster de destino las copias de Snapshot que se hayan replicado en el destino. La copia de Snapshot eliminada se guarda en una lista de copias de Snapshot eliminadas en el destino hasta que el sistema detecta que se ha eliminado la copia de Snapshot en el clúster de origen. Cuando el destino detecta que se ha eliminado la copia de Snapshot de origen, el destino detiene la replicación de la copia de Snapshot.

Cuando se elimina una snapshot del clúster de origen, la snapshot del clúster de destino no se ve afectada (lo contrario también aplica).

1. Haga clic en **Protección de datos** > **instantáneas**.
2. Haga clic en el icono **acciones** de la instantánea que desea eliminar.
3. En el menú que se abre, seleccione **Eliminar**.
4. Confirme la acción.

Clonar un volumen a partir de una copia de Snapshot

Es posible crear un nuevo volumen a partir de una copia de Snapshot de un volumen. En ese caso, el sistema utiliza la información de la copia de Snapshot para clonar un volumen nuevo con los datos que contenía el volumen en el momento en el que se creó la copia de Snapshot. En este proceso se almacena información sobre otras copias de Snapshot del volumen en el volumen que se acaba de crear.

1. Haga clic en **Protección de datos** > **instantáneas**.
2. Haga clic en el icono **acciones** de la instantánea que desee utilizar para la clonación de volumen.
3. En el menú que se abre, haga clic en **Clone Volume from Snapshot**.
4. Introduzca un **Nombre de volumen** en el cuadro de diálogo **Clonar volumen desde Snapshot**.
5. Seleccione una **Tamaño total** y unidades de tamaño para el nuevo volumen.

6. Seleccione un tipo **Access** para el volumen.
7. Seleccione una **cuenta** de la lista para asociarla con el nuevo volumen.
8. Haga clic en **Iniciar clonación**.

Revertir un volumen a una copia de Snapshot

Siempre que lo desee, es posible revertir un volumen a una snapshot anterior. De este modo se revierten los cambios que se hayan hecho al volumen desde el momento de la creación de la snapshot.

Pasos

1. Haga clic en **Protección de datos** > **instantáneas**.
2. Haga clic en el icono **acciones** de la instantánea que desee utilizar para la reversión de volumen.
3. En el menú que se abre, seleccione **revertir volumen a instantánea**.
4. **Opcional:** para guardar el estado actual del volumen antes de retroceder a la instantánea:
   a. En el cuadro de diálogo **revertir a instantánea**, seleccione **Guardar estado actual del volumen como instantánea**.
   b. Escriba un nombre para la snapshot nueva.
5. Haga clic en **revertir Snapshot**.

Realice un backup de una copia de Snapshot de volumen

La función integrada de backup se puede usar para realizar un backup de una copia de Snapshot de volumen. Es posible realizar backups de snapshots de un clúster de SolidFire en un almacén de objetos externo o en otro clúster de SolidFire. Cuando se crea un backup de una copia de Snapshot en un almacén de objetos externo, debe haber una conexión con el almacén de objetos que permita realizar operaciones de lectura y escritura.

- "Realice backups de una copia de Snapshot de volumen en un almacén de objetos Amazon S3"
- "Realice backups de una copia de Snapshot de volumen en un almacén de objetos OpenStack Swift"
- "Realice backups de una copia de Snapshot de volumen en un clúster de SolidFire"

Realice backups de una copia de Snapshot de volumen en un almacén de objetos Amazon S3

Es posible realizar backups de snapshots de SolidFire en almacenes de objetos externos que sean compatibles con Amazon S3.

1. Haga clic en**Protección de datos** > **Snapshots**.
2. Haga clic en el icono **acciones** de la instantánea de la que desea realizar la copia de seguridad.
3. En el menú que se abre, haga clic en **copia de seguridad en**.
4. En el cuadro de diálogo **copia de seguridad integrada** en **copia de seguridad a**, seleccione **S3**.
5. Seleccione una opción en **Formato de datos**:
   - **Original**: Formato comprimido que sólo pueden leer los sistemas de almacenamiento SolidFire.

- **Sin comprimir**: Formato sin comprimir compatible con otros sistemas.

6. Introduzca un nombre de host para acceder al almacén de objetos en el campo **Hostname**.
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 bloque S3 en el que desea almacenar la copia de seguridad en el campo **S3 Bucket**.
10. **Opcional**: Introduzca una etiqueta de nombre para adjuntarla al prefijo en el campo **etiqueta de nombre**.
11. Haga clic en **Iniciar lectura**.

Realice backups de una copia de Snapshot de volumen en un almacén de objetos OpenStack Swift

Es posible realizar backups de snapshots de SolidFire en almacenes de objetos secundarios que sean compatibles con OpenStack Swift.

1. Haga clic en **Protección de datos** > **instantáneas**.
2. Haga clic en el icono **acciones** de la instantánea de la que desea realizar la copia de seguridad.
3. En el menú que se abre, haga clic en **copia de seguridad en**.
4. En el cuadro de diálogo **Backup integrado**, en **Backup to**, seleccione **Swift**.
5. Seleccione una opción en **Formato de datos**:
   - **Original**: Formato comprimido que sólo pueden leer los sistemas de almacenamiento SolidFire.
   - **Sin comprimir**: Formato sin comprimir compatible con otros sistemas.
6. Introduzca una **URL** para acceder al almacén de objetos.
7. Introduzca un **Nombre de usuario** para la cuenta.
8. Introduzca **clave de autenticación** para la cuenta.
9. Introduzca el **contenedor** en el que desea almacenar la copia de seguridad.
10. **Opcional**: Introduzca una **etiqueta de nombre**.
11. Haga clic en **Iniciar lectura**.

Realice backups de una copia de Snapshot de volumen en un clúster de SolidFire

Puede realizar backups de snapshots de volumen que residen en un clúster de SolidFire en un clúster de SolidFire remoto.

Debe confirmar que los clústeres de origen y destino están emparejados.

Cuando se crea un backup o se restaura de un clúster a otro, el sistema genera una clave que se debe usar como autenticación entre los clústeres. Con esta clave de escritura masiva de volúmenes, el clúster de origen puede autenticarse con el clúster de destino, lo que permite ofrecer un nivel de seguridad cuando se escribe en el volumen de destino. Como parte del proceso de backup o restauración, debe generar una clave de escritura masiva de volúmenes 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 se abre, haga clic en **Restaurar de**.
4. En el cuadro de diálogo **Restauración integrada**, en **Restaurar de**, seleccione **SolidFire**.

5. Seleccione un formato de datos en **Formato de datos**:
   - **Original**: Formato comprimido que sólo pueden leer los sistemas de almacenamiento SolidFire.
   - **Sin comprimir**: Formato sin comprimir compatible con otros sistemas.
6. Haga clic en **generar clave**.
7. Copie la clave del cuadro **Bulk Volume Write Key** en el portapapeles.
8. En el clúster de origen, haga clic en **Protección de datos** > **instantáneas**.
9. Haga clic en el icono Actions de la snapshot que quiera usar para el backup.
10. En el menú que se abre, haga clic en **copia de seguridad en**.
11. En el cuadro de diálogo**copia de seguridad integrada**, en **copia de seguridad en**, seleccione **SolidFire**.
12. Seleccione el mismo formato de datos que haya seleccionado anteriormente en el campo **Formato de datos**.
13. Introduzca la dirección IP virtual de administración del clúster del volumen de destino en el campo **Remote Cluster MVIP**.
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 **Remote Cluster Password**.
16. En el campo **Bulk Volume Write Key**, pegue la clave que ha generado en el clúster de destino anteriormente.
17. Haga clic en **Iniciar lectura**.

El uso de copias de Snapshot de grupo para la tarea de protección de datos

Se puede crear una copia de Snapshot de grupo de un conjunto relacionado de volúmenes para conservar una copia de un momento específico de los metadatos de cada volumen. La snapshot de grupo se puede usar más adelante como un backup o una reversión para restaurar el estado del grupo de volúmenes en un estado anterior.

Obtenga más información

- Crear una copia de Snapshot de grupo
- Editar copias de Snapshot de grupo
- Editar los miembros de la copia de Snapshot de grupo
- Eliminar una copia de Snapshot de grupo
- Revertir volúmenes a una copia de Snapshot de grupo
- Clone varios volúmenes
- Clone varios volúmenes a partir de una copia de Snapshot de grupo

Detalles de la copia de Snapshot de grupo

En la página Group Snapshots de la pestaña Data Protection, se proporciona información sobre las snapshots de grupo.

- **ID**

  El ID que genera el sistema para la copia de Snapshot de grupo.

- **UUID**

  El ID único de la copia de Snapshot de grupo.

- **Nombre**

  El nombre definido por el usuario para la snapshot de grupo.

- **Crear tiempo**

  La hora en la que se ha creado la snapshot de grupo.

- **Estado**

  El estado actual de la copia de Snapshot de grupo. Los posibles valores son los siguientes:

  - Preparing: La copia de Snapshot se está preparando para poder usarla y aún no se puede escribir en ella.
  - Done: Esta snapshot se ha terminado de preparar y se puede usar.
  - Active: La snapshot es la rama activa.

- **# volúmenes**

  El número de volúmenes en el grupo.

- **Mantener hasta**

  La fecha y la hora en las que se eliminó la copia de Snapshot.

- **Replicación remota**

  Indica si la snapshot se habilita para la replicación en un clúster de SolidFire remoto. Los posibles valores son los siguientes:

  - Enabled: La snapshot está habilitada para la replicación remota.
  - Disabled: La snapshot no está habilitada para la replicación remota.

Crear una copia de Snapshot de grupo

Puede crear una snapshot de un grupo de volúmenes, así como planificar snapshots de grupo para automatizarlas. Una copia de Snapshot de grupo puede realizar copias de forma constante de hasta 32 volúmenes a la vez.

Pasos

1. Haga clic en **Administración** > **volúmenes**.
2. Use las casillas para seleccionar varios volúmenes de un grupo de volúmenes.
3. Haga clic en **acciones masivas**.
4. Haga clic en **instantánea de grupo**.
5. Introduzca un nombre de snapshot de grupo nuevo en el cuadro de diálogo Create Group Snapshot of Volumes.
6. **Opcional:** Active la casilla de verificación **incluir cada miembro de instantánea de grupo en**

replicación cuando se empareja para asegurarse de que cada instantánea se captura en la replicación cuando el volumen principal está emparejado.

7. Seleccione una opción de retención para la copia de Snapshot de grupo:
   - Haga clic en **mantener siempre** para conservar la instantánea en el sistema indefinidamente.
   - Haga clic en **establecer período de retención** y utilice los cuadros de número de fecha para elegir un período de tiempo durante el cual el sistema retendrá la instantánea.
8. Para crear una sola snapshot de forma inmediata, realice los siguientes pasos:
   a. Haga clic en **tomar instantánea de grupo ahora**.
   b. Haga clic en **Crear instantánea de grupo**.
9. Para programar que la copia de Snapshot se ejecute en el futuro, realice los siguientes pasos:
   a. Haga clic en **Crear programación Snapshot de grupo**.
   b. Introduzca un **Nuevo nombre de programa**.
   c. Seleccione un **Tipo de programación** de la lista.
   d. **Opcional:** Active la casilla de verificación **Programación periódica** para repetir periódicamente la instantánea programada.
   e. Haga clic en **Crear programación**.

Editar copias de Snapshot de grupo

La configuración de la replicación y la retención se puede editar para las snapshots de grupos existentes.

1. Haga clic en **Protección de datos** > **instantáneas de grupo**.
2. Haga clic en el icono Actions de la snapshot de grupo que quiera editar.
3. En el menú que se abre, 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. Active la casilla de verificación **incluir cada miembro de Snapshot de grupo en replicación cuando se empareja** para asegurarse de que cada instantánea se capture en la replicación cuando el volumen primario esté emparejado.
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 copia de Snapshot de grupo:
      - Haga clic en **mantener siempre** para conservar la instantánea en el sistema indefinidamente.
      - Haga clic en **establecer período de retención** y utilice los cuadros de número de fecha para elegir un período de tiempo durante el cual el sistema retendrá la instantánea.
6. Haga clic en **Guardar cambios**.

Eliminar una copia de Snapshot de grupo

Es posible eliminar una copia de Snapshot de grupo del sistema. Cuando se elimina la copia de Snapshot de grupo, se puede elegir si se eliminarán todas las copias de

Snapshot asociadas al grupo o si se retendrán como copias de Snapshot individuales.

Si elimina un volumen o una copia de Snapshot que forma parte de una copia de Snapshot de grupo, no se puede revertir a la copia de Snapshot de grupo. Sin embargo, se puede revertir a cada volumen de forma individual.

1. Haga clic en **Protección de datos** > **instantáneas de grupo**.
2. Haga clic en el icono Actions de la snapshot que quiera eliminar.
3. En el menú que se abre, 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 instantánea de grupo** para eliminar la instantánea de grupo y todas las instantáneas de miembro.
   - Haga clic en **retener miembros de instantánea de grupo como instantáneas individuales** para eliminar la instantánea de grupo pero conservar todas las instantáneas de miembro.
5. Confirme la acción.

Revertir volúmenes a una copia de Snapshot de grupo

Siempre que lo desee, puede revertir un grupo de volúmenes a una snapshot de grupo.

Cuando se restaura un grupo de volúmenes, todos los volúmenes del grupo se restauran con el estado que tenían en el momento en que se creó la snapshot de grupo. La reversión también restaura el tamaño registrado en la snapshot original de los volúmenes. Si el sistema ha purgado un volumen, todas las copias de Snapshot de dicho volumen se eliminan durante la purga. Por ello, el sistema no restaura ninguna de las copias de Snapshot de volumen eliminadas.

1. Haga clic en **Protección de datos** > **instantáneas de grupo**.
2. Haga clic en el icono Actions de la snapshot de grupo que desee usar para revertir el volumen.
3. En el menú que se abre, seleccione **revertir volúmenes a Group Snapshot**.
4. **Opcional**: Para guardar el estado actual de los volúmenes antes de revertir a la instantánea:
   a. En el cuadro de diálogo **revertir a instantánea**, seleccione **Guardar volúmenes' Estado actual como una instantánea de grupo**.
   b. Escriba un nombre para la snapshot nueva.
5. Haga clic en **revertir Snapshot de grupo**.

Editar miembros de la copia de Snapshot de grupo

La configuración de retención se puede editar para los miembros de una copia de Snapshot de grupo existente.

1. Haga clic en **Protección de datos** > **instantáneas**.
2. Haga clic en la ficha **Miembros**.
3. Haga clic en el icono Actions del miembro de la snapshot de grupo que desea editar.
4. En el menú que se abre, seleccione **Editar**.
5. Para cambiar la configuración de replicación de la snapshot, seleccione una de las siguientes opciones:
   - Haga clic en **mantener siempre** para conservar la instantánea en el sistema indefinidamente.

- Haga clic en **establecer período de retención** y utilice los cuadros de número de fecha para elegir un período de tiempo durante el cual el sistema retendrá la instantánea.

6. Haga clic en **Guardar cambios**.

Clone varios volúmenes

Es posible crear varios clones de volúmenes en una única operación para crear una copia de los datos de un momento específico en un grupo de volúmenes.

Cuando se clona un volumen, el sistema crea una copia Snapshot del volumen y, a continuación, crea un nuevo volumen a partir de los datos de la copia. Es posible montar el nuevo clon de volumen y escribir en él. El clonado de varios volúmenes es un proceso asíncrono cuya duración puede variar en función del tamaño y el número de volúmenes que se van a clonar.

El tamaño del volumen y la carga del clúster actual influirán en el tiempo que se necesite para completar una operación de clonado.

Pasos

1. Haga clic en **Administración** > **volúmenes**.
2. Haga clic en la ficha **activo**.
3. Use las casillas para seleccionar varios volúmenes con el fin de crear un grupo de volúmenes.
4. Haga clic en **acciones masivas**.
5. Haga clic en **Clonar** en el menú que aparece.
6. Introduzca un * prefijo de nombre de nuevo volumen* en el cuadro de diálogo **Clonar varios volúmenes**.

   El prefijo se aplica a todos los volúmenes del grupo.

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

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

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

   Si no selecciona ninguno, el sistema usará el acceso de volumen actual.

9. Haga clic en **Iniciar clonación**.

Clonar varios volúmenes a partir de una copia de Snapshot de grupo

Es posible clonar un grupo de volúmenes desde una copia de Snapshot de grupo específica. Esta operación requiere la existencia de una snapshot de grupo de los volúmenes, puesto que la snapshot de grupo sirve como base para crear los volúmenes. Después de crear los volúmenes, es posible usarlos como cualquier otro volumen del sistema.

El tamaño del volumen y la carga del clúster actual influirán en el tiempo que se necesite para completar una operación de clonado.

1. Haga clic en **Protección de datos** > **instantáneas de grupo**.

2. Haga clic en el icono Actions de la snapshot de grupo que desee usar para los clones de volúmenes.
3. En el menú que se abre, seleccione **Clonar volúmenes desde Group Snapshot**.
4. Introduzca un * prefijo de nombre de nuevo volumen* en el cuadro de diálogo **Clonar volúmenes desde Snapshot de grupo**.

   El prefijo se aplica a todos los volúmenes que se creen a partir de la copia de Snapshot de grupo.

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

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

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

   Si no selecciona ninguno, el sistema usará el acceso de volumen actual.

7. Haga clic en **Iniciar clonación**.

Programar una copia de Snapshot

Se pueden proteger datos en un volumen o un grupo de volúmenes mediante la programación de copias de Snapshot de volumen para que se produzcan en intervalos concretos. Se pueden programar las copias de Snapshot de un solo volumen o las copias de Snapshot de grupo para que se ejecuten automáticamente.

Cuando se configura una programación de Snapshot, se puede elegir entre intervalos de tiempo basados en los días de la semana o los días del mes. También es posible especificar los días, las horas y los minutos antes de que se produzca la siguiente copia de Snapshot. Las snapshots resultantes se pueden almacenar en un sistema de almacenamiento de remoto si el volumen se está replicando.

Obtenga más información

- Crear una programación de Snapshot
- Editar una programación de Snapshot
- Eliminar una programación de Snapshot
- Copiar una programación de Snapshot

Detalles de la programación de Snapshot

En la página Data Protection > Schedules, puede ver la siguiente información en la lista de programaciones de snapshots.

- **ID**

  El ID que genera el sistema para la copia de Snapshot.

- **Tipo**

  El tipo de programación. Actualmente, Snapshot es el único tipo admitido.

- **Nombre**

El nombre que se le dio a la programación cuando se creó. Los nombres de las programaciones de snapshots pueden tener hasta 223 caracteres y contener a-z, 9 y guion (-).

- **Frecuencia**

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

- **Recurrente**

  Indicación de si el programa se ejecutará sólo una vez o a intervalos regulares.

- **Pausado manualmente**

  Indica si la programación se pausó manualmente o no.

- **ID de volumen**

  El ID del volumen que usará la programación cuando se ejecute.

- **Última ejecución**

  La última vez que se ejecutó la programación.

- **Estado de la última ejecución**

  El resultado de la última ejecución de la programación. Los posibles valores son los siguientes:

  - Correcto
  - Fallo

Crear una programación de Snapshot

Se puede programar la ejecución automática de una copia de Snapshot de un volumen o de varios volúmenes en intervalos concretos.

Cuando se configura una programación de Snapshot, se puede elegir entre intervalos de tiempo basados en los días de la semana o los días del mes. Igualmente, se puede crear una programación recurrente y especificar los días, las horas y los minutos antes de que se ejecute la siguiente snapshot.

Si se programa la ejecución de una copia de Snapshot en un período que no sea divisible entre 5 minutos, la copia de Snapshot se ejecutará en el siguiente período que lo sea 5. Por ejemplo, si se programa la ejecución de una copia de Snapshot a las 12:42:00 UTC, se realizará a las 12:45:00 UTC. No se podrá programar la ejecución de una copia de Snapshot en intervalos inferiores a 5 minutos.

Pasos

1. Haga clic en **Protección de datos** > **programas**.
2. Haga clic en **Crear programación**.
3. En el campo **ID de volumen CSV**, introduzca un ID de volumen único o una lista separada por comas con los ID de volumen que desea incluir en la operación de instantánea.
4. Introduzca un nombre de programación nuevo.
5. Seleccione un tipo de programación y establezca la programación entre las opciones proporcionadas.

6. **Opcional:** Seleccione **Recurring Schedule** para repetir la programación de la instantánea de forma indefinida.
7. **Opcional:** Escriba un nombre para la nueva instantánea en el campo **Nuevo nombre de instantánea**.

   Si se deja el campo vacío, el sistema usará como nombre la hora y la fecha de la creación de la copia de Snapshot.

8. **Opcional:** Active la casilla de verificación **incluir instantáneas en replicación cuando se empareja** para asegurarse de que las instantáneas se capturan en la replicación cuando el volumen principal está emparejado.
9. Para configurar la retención de la snapshot, seleccione una de las siguientes opciones:
   - Haga clic en **mantener siempre** para conservar la instantánea en el sistema indefinidamente.
   - Haga clic en **establecer período de retención** y utilice los cuadros de número de fecha para elegir un período de tiempo durante el cual el sistema retendrá la instantánea.
10. Haga clic en **Crear programación**.

Editar una programación de Snapshot

Puede modificar las programaciones de Snapshot que ya tenga. Después de modificarlas, la próxima vez que se ejecute la programación, se utilizarán los atributos actualizados. Las copias de Snapshot que se crean con la programación original siguen en el sistema de almacenamiento.

Pasos

1. Haga clic en **Protección de datos** > **programas**.
2. Haga clic en el icono **acciones** de la programación que desea cambiar.
3. En el menú que se abre, haga clic en **Editar**.
4. En el campo **ID de volumen CSV**, modifique el ID de volumen único o la lista separada por comas de los ID de volumen actualmente incluidos 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** en la lista **Pausa manual**.
   - Para reanudar una programación pausada, seleccione **no** en la lista **Pausa Manual**.
6. Introduzca otro nombre para la programación en el campo **Nombre de programación nuevo** si lo desea.
7. Para cambiar la programación para que se ejecute en distintos días de la semana o del mes, seleccione **Tipo de programación** y cambie la programación de las opciones proporcionadas.
8. **Opcional:** Seleccione **Recurring Schedule** para repetir la programación de la instantánea de forma indefinida.
9. **Opcional:** Introduzca o modifique el nombre de la nueva instantánea en el campo **Nuevo nombre de instantánea**.

   Si se deja el campo vacío, el sistema usará como nombre la hora y la fecha de la creación de la copia de Snapshot.

10. **Opcional:** Active la casilla de verificación **incluir instantáneas en replicación cuando se empareja** para asegurarse de que las instantáneas se capturan en la replicación cuando el volumen principal está emparejado.

11. Para cambiar la configuración de retención, seleccione una de las siguientes opciones:
    - Haga clic en **mantener siempre** para conservar la instantánea en el sistema indefinidamente.
    - Haga clic en **establecer período de retención** y utilice los cuadros de número de fecha para seleccionar un período de tiempo durante el cual el sistema retendrá la instantánea.
12. Haga clic en **Guardar cambios**.

Copiar una programación de Snapshot

Puede copiar una programación y mantener sus atributos actuales.

1. Haga clic en **Protección de datos** > **programas**.
2. Haga clic en el icono Actions de la programación que quiera copiar.
3. En el menú que se abre, haga clic en **hacer una copia**.

   Aparece el cuadro de diálogo **Crear programación**, con los atributos actuales de la programación.

4. **Opcional:** Introduzca un nombre y atributos actualizados para la nueva programación.
5. Haga clic en **Crear programación**.

Eliminar una programación de Snapshot

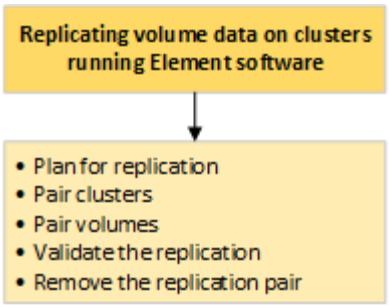
Es posible eliminar programaciones de Snapshot. Después de eliminar una programación, no se ejecutan las siguientes copias de Snapshot programadas. Las copias de Snapshot creadas con la programación permanecen en el sistema de almacenamiento.

1. Haga clic en **Protección de datos** > **programas**.
2. Haga clic en el icono **acciones** de la programación que desea eliminar.
3. En el menú que se abre, haga clic en **Eliminar**.
4. Confirme la acción.

Llevar a cabo la replicación remota entre los 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. Un clúster de almacenamiento se puede emparejar con hasta otros cuatro clústeres de almacenamiento. Es posible replicar datos de volúmenes de forma síncrona o asíncrona desde un clúster de una pareja de clústeres para escenarios de conmutación por error y conmutación tras recuperación.

El proceso de replicación incluye los siguientes pasos:



- "Planifique el emparejamiento de clústeres y volúmenes para la replicación en tiempo real"
- "Emparejar clústeres para la replicación"
- "Emparejar volúmenes"
- "Validar la replicación de volúmenes"
- "Eliminar una relación de volumen después de la replicación"
- "Gestionar relaciones de volumen"

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

La replicación remota en tiempo real requiere emparejar dos clústeres de almacenamiento que ejecutan el software Element, emparejar volúmenes en cada clúster y validar la replicación. Una vez que se completa la replicación, se debe eliminar la relación de volumen.

Lo que necesitará

- Debe tener privilegios de administrador del clúster en uno de los clústeres que se está emparejando, o en ambos.
- Todas las direcciones IP de nodos en las redes de gestión y almacenamiento para los clústeres emparejados se deben enrutar entre sí.
- La MTU de todos los nodos emparejados debe ser la misma y debe ser compatible entre clústeres de un extremo a otro.
- Ambos clústeres de almacenamiento deben tener nombres de clúster únicos, MVIP, SVIP y todas las direcciones IP de los nodos.
- La diferencia entre las versiones del software Element en los clústeres no debe ser superior a la versión principal. Si la diferencia es superior, se debe actualizar uno de los clústeres para ejecutar la replicación de datos.

> NetApp no ha autorizado los dispositivos aceleradores WAN para usarlos al replicar datos. Estos dispositivos pueden interferir con la compresión y la deduplicación si se implementan entre dos clústeres que están replicando datos. Asegúrese de autorizar por completo los efectos de cualquier dispositivo acelerador WAN antes de implementarlo en un entorno de producción.

Obtenga más información

- Emparejar clústeres para la replicación

- Emparejar volúmenes
- Asigne un origen y un destino de replicación a los volúmenes emparejados

Emparejar clústeres para la replicación

Debe emparejar dos clústeres como primer paso para utilizar la funcionalidad de replicación en tiempo real. Después de emparejar y conectar dos clústeres, es posible configurar volúmenes activos en un clúster para que se repliquen continuamente en un segundo clúster; esto proporciona protección de datos continua (CDP).

Lo que necesitará

- Debe tener privilegios de administrador del clúster en uno de los clústeres que se está emparejando, o en ambos.
- Todos los MIPs y SIPs de nodos están enrutados 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 todas las direcciones IP de los nodos.
- La diferencia entre las versiones del software Element en los clústeres no debe ser superior a la versión principal. Si la diferencia es superior, se debe actualizar uno de los clústeres para ejecutar la replicación de datos.

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

Un clúster se puede emparejar con hasta otros cuatro clústeres para replicar volúmenes. De igual manera, los clústeres que pertenecen a un grupo de clústeres se pueden emparejar entre sí.

Obtenga más información

Requisitos de puerto de red

Emparejar clústeres con la MVIP o una clave de emparejamiento

Es posible emparejar un clúster de origen y de destino mediante la dirección MVIP de un clúster de destino si ambos clústeres ofrece acceso de administrador de clúster. Si solo un clúster en una pareja de clústeres ofrece acceso de administrador del clúster, se puede usar una clave de emparejamiento en el clúster de destino para completar el emparejamiento de clústeres.

1. Seleccione uno de los siguientes métodos para emparejar clústeres:
   - Emparejar clústeres con la MVIP: Utilice este método si ambos clústeres tienen acceso de administrador del clúster. Este método utiliza la dirección MVIP del clúster remoto para emparejar dos clústeres.
   - Emparejar clústeres con una clave de emparejamiento: Utilice este método si solo uno de los clústeres ofrece acceso de administrador del clúster. Este método genera una clave de emparejamiento que se puede usar en el clúster de destino para completar el emparejamiento de clústeres.

Obtenga más información

- Emparejar clústeres con la MVIP
- Emparejar clústeres con una clave de emparejamiento

Emparejar clústeres con la MVIP

Es posible emparejar dos clústeres para la replicación en tiempo real mediante la dirección MVIP de un clúster para establecer una conexión con el otro clúster. Para usar este método, debe tener acceso de administrador de clúster en ambos clústeres. La contraseña y el nombre de usuario del administrador de clúster se usan para autenticar el acceso a los clústeres antes de que estos se puedan emparejar.

1. En el clúster local, seleccione **Data Protection** > **Cluster Pairs**.
2. Haga clic en **Pair Cluster**.
3. Haga clic en **Iniciar emparejamiento** y haga clic en **Sí** para indicar que tiene acceso al clúster remoto.
4. Introduzca la dirección de MVIP del clúster remoto.
5. Haga clic en **emparejamiento completo en clúster remoto**.

   En la ventana **autenticación requerida**, introduzca 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 **Pair Cluster**.
8. Haga clic en **Complete Pairing**.
9. Haga clic en el botón **Complete Pairing**.

Obtenga más información

- Emparejar clústeres con una clave de emparejamiento
- "Emparejar clústeres con la MVIP (vídeo)"

Emparejar clústeres con una clave de emparejamiento

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

1. En el clúster local, seleccione **Data Protection** > **Cluster Pairs**.
2. Haga clic en **Pair Cluster**.
3. Haga clic en **Iniciar emparejamiento** y haga clic en **no** para indicar que no tiene acceso al clúster remoto.
4. Haga clic en **generar clave**.

Esta acción genera una clave de texto para el emparejamiento y crea una pareja de clústeres sin configurar en el clúster local. Si no completa el procedimiento, deberá eliminar manualmente la pareja de clústeres.

5. Copie la clave de emparejamiento del clúster en el portapapeles.
6. Ponga la clave de emparejamiento a disposición del administrador de clúster en el sitio del clúster remoto.

La clave de emparejamiento de clústeres contiene una versión de la dirección MVIP, el nombre de usuario, la contraseña y la información de la base de datos para permitir las conexiones de volúmenes para la replicación remota. Esta clave se debe tratar de una forma segura y no se debe almacenar de manera que se pueda acceder de forma accidental o insegura al nombre de usuario o a la contraseña.

No modifique ningún carácter de la clave de emparejamiento. La clave pierde su validez si se modifica.

7. En el clúster remoto, seleccione **Protección de datos** > **pares de clústeres**.
8. Haga clic en **Pair Cluster**.
9. Haga clic en **Complete Pairing** e introduzca la clave de emparejamiento en el campo **Pairing Key** (pegue es el método recomendado).
10. Haga clic en **Complete Pairing**.

Obtenga más información

- Emparejar clústeres con la MVIP
- "Emparejamiento de clústeres con una clave de emparejamiento de clúster (vídeo)"

Valide la conexión de la pareja de clústeres

Una vez que se ha completado el emparejamiento de clústeres, es posible que desee verificar la conexión de la pareja de clústeres para garantizar que la replicación se haya realizado correctamente.

1. En el clúster local, seleccione **Data Protection** > **Cluster Pairs**.
2. En la ventana **Cluster Pairs**, compruebe que el par de clústeres esté conectado.
3. **Opcional:** vuelva al clúster local y a la ventana **Cluster Pairs** y compruebe que el par de clústeres esté conectado.

Emparejar volúmenes

Después de establecer una conexión entre los clústeres de una pareja de clústeres, es posible emparejar un volumen de un clúster con un volumen en el otro clúster de la pareja. Cuando se establece una relación de emparejamiento de volúmenes, es necesario identificar qué volumen es el destino de replicación.

Es posible emparejar dos volúmenes para replicación en tiempo real si están almacenados en clústeres de almacenamiento diferentes en una pareja de clústeres conectados. Después de emparejar dos clústeres, es posible configurar volúmenes activos en un clúster para que se repliquen continuamente en un segundo

clúster; esto proporciona protección de datos continua (CDP). También es posible asignar cada volumen como origen o destino de la replicación.

Los emparejamientos de volúmenes se realizan siempre de uno a uno. Una vez que un volumen forma parte de un emparejamiento con un volumen de otro clúster, no se puede volver a emparejar con otro volumen.

Lo que necesitará

- Estableció una conexión entre los clústeres de una pareja de clústeres.
- Tiene privilegios de administrador del clúster en uno de los clústeres que se está emparejando, o en ambos.

Pasos

1. Cree un volumen objetivo con acceso de lectura o escritura
2. Emparejar volúmenes con un ID de volumen o una clave de emparejamiento
3. Asigne un origen y un destino de replicación a los volúmenes emparejados

Cree un volumen objetivo con acceso de lectura o escritura

El proceso de replicación implica dos extremos: El volumen de origen y el de destino. Cuando se crea el volumen objetivo, el volumen se establece automáticamente en el modo de lectura/escritura para aceptar los datos durante la replicación.

1. Seleccione **Gestión** > **volúmenes**.
2. Haga clic en **Crear volumen**.
3. En el cuadro de diálogo Create a New Volume, introduzca el nombre del volumen en Volume Name.
4. Introduzca el tamaño total del volumen, seleccione un tamaño de bloque para el volumen y seleccione la cuenta que debe tener acceso al volumen.
5. Haga clic en **Crear volumen**.
6. En la ventana Active, haga clic en el icono Actions del volumen.
7. Haga clic en **Editar**.
8. Cambie el nivel de acceso de cuenta a destino de replicación.
9. Haga clic en **Guardar cambios**.

Emparejar volúmenes con un ID de volumen o una clave de emparejamiento

El proceso de emparejamiento implica el emparejamiento de dos volúmenes mediante un ID de volumen o una clave de emparejamiento.

1. Emparejar volúmenes seleccionando uno de los siguientes métodos:
   - Usar un ID de volumen: Utilice este método si tiene acceso de administrador de clúster a los dos clústeres donde planea emparejar volúmenes. Este método utiliza el ID de volumen del volumen en el clúster remoto para iniciar una conexión.
   - Usar una clave de emparejamiento: Utilice este método si solo tiene acceso de administrador del clúster al clúster de origen. Este método genera una clave de emparejamiento que se puede usar en el clúster remoto para completar el emparejamiento de volúmenes.

La clave de emparejamiento de volúmenes contiene una versión cifrada de la información de los volúmenes y puede contener información confidencial. Únicamente comparta esta clave de forma segura.

Obtenga más información

- Emparejar volúmenes con un ID de volumen
- Emparejar volúmenes con una clave de emparejamiento

Emparejar volúmenes con un ID de volumen

Es posible emparejar un volumen con otro volumen en un clúster remoto si tiene credenciales de administrador de clústeres para el clúster remoto.

Lo que necesitará

- Confirme que los clústeres que contienen los volúmenes están emparejados.
- Cree un nuevo volumen en el clúster remoto.

Puede asignar un origen y un destino de replicación después del proceso de emparejamiento. Un origen u objetivo de replicación pueden ser un volumen de una pareja de volúmenes. Debe crear un volumen de destino que no contenga datos y que tenga las mismas características que el volumen de origen, como el tamaño, la configuración de tamaño de bloque para los volúmenes (512e o 4k) y la configuración de calidad de servicio. Si asigna un volumen existente como objetivo de replicación, los datos de ese volumen se sobrescriben. El tamaño del volumen de destino puede ser mayor o igual que el del volumen de origen, pero no menor.

- Determine el ID del volumen de destino.

Pasos

1. Seleccione **Gestión** > **volúmenes**.
2. Haga clic en el icono **acciones** del volumen que desea emparejar.
3. Haga clic en **par**.
4. En el cuadro de diálogo **volumen de par**, seleccione **Iniciar emparejamiento**.
5. Seleccione **i do** para indicar que tiene acceso al clúster remoto.
6. Seleccione un **modo de replicación** de la lista:
   - **Tiempo real (asíncrono)**: Las escrituras se reconocen en el cliente después de que se aplican en el clúster de origen.
   - **Real-Time (Synchronous)**: Las escrituras se reconocen en el cliente después de que se aplican tanto en los clústeres de origen como de destino.
   - **Sólo instantáneas**: Sólo se replican las instantáneas creadas en el clúster de origen. No se replican las escrituras activas del volumen de origen.
7. Seleccione un clúster remoto de la lista Remote Cluster.
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 de Element del clúster remoto. Es posible que se le pida iniciar sesión en el clúster remoto con las credenciales de administrador de clúster.

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

    Después de confirmar el emparejamiento, los dos clústeres comienzan 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**. Se muestra la pareja de volúmenes `PausedMisconfigured` hasta que se asignan el origen y el destino de la pareja de volúmenes.

    Después de completar correctamente el emparejamiento, debe actualizar la tabla Volumes para eliminar la opción **Pair** de la lista **Actions** del volumen emparejado. Si no actualiza la tabla, la opción **par** permanece disponible para su selección. Si vuelve a seleccionar la opción **par**, se abre una nueva pestaña y, dado que el volumen ya está emparejado, el sistema informa un `StartVolumePairing Failed: xVolumeAlreadyPaired` Mensaje de error en la ventana **Pair Volume** de la página UI de Element.

Obtenga más información

- Mensajes sobre el emparejamiento de volúmenes
- Advertencias sobre el emparejamiento de volúmenes
- Asigne un origen y un destino de replicación a los volúmenes emparejados

Emparejar volúmenes con una clave de emparejamiento

Si no tiene credenciales de administrador del clúster para un clúster remoto, puede emparejar un volumen con otro volumen en un clúster remoto mediante una clave de emparejamiento.

Lo que necesitará

- Confirme que los clústeres que contienen los volúmenes están emparejados.
- Compruebe que haya un volumen en el clúster remoto que utilice para el emparejamiento.

> Puede asignar un origen y un destino de replicación después del proceso de emparejamiento. Un origen u objetivo de replicación pueden ser un volumen de una pareja de volúmenes. Debe crear un volumen de destino que no contenga datos y que tenga las mismas características que el volumen de origen, como el tamaño, la configuración de tamaño de bloque para los volúmenes (512e o 4k) y la configuración de calidad de servicio. Si asigna un volumen existente como objetivo de replicación, los datos de ese volumen se sobrescriben. El tamaño del volumen de destino puede ser mayor o igual que el del volumen de origen, pero no menor.

Pasos

1. Seleccione **Gestión** > **volúmenes**.
2. Haga clic en el icono **acciones** del volumen que desea emparejar.
3. Haga clic en **par**.

4. En el cuadro de diálogo **volumen de par**, seleccione **Iniciar emparejamiento**.
5. Seleccione **no** para indicar que no tiene acceso al clúster remoto.
6. Seleccione un **modo de replicación** de la lista:
   - **Tiempo real (asíncrono)**: Las escrituras se reconocen en el cliente después de que se aplican en el clúster de origen.
   - **Real-Time (Synchronous)**: Las escrituras se reconocen en el cliente después de que se aplican tanto en los clústeres de origen como de destino.
   - **Sólo instantáneas**: Sólo se replican las instantáneas creadas en el clúster de origen. No se replican las escrituras activas del volumen de origen.
7. Haga clic en **generar clave**.

   Esta acción genera una clave de texto para el emparejamiento y crea una pareja de volúmenes sin configurar en el clúster local. Si no completa el procedimiento, deberá eliminar manualmente la pareja de volúmenes.

8. Copie la clave de emparejamiento en el portapapeles de su equipo.
9. Ponga la clave de emparejamiento a disposición del administrador del clúster en el sitio del clúster remoto.

   La clave de emparejamiento se debe tratar de una forma segura y no se debe utilizar de manera que se pueda acceder de forma accidental o insegura a ella.

   No modifique ningún carácter de la clave de emparejamiento. La clave pierde su validez si se modifica.

10. En la interfaz de usuario de elemento de clúster remoto, seleccione **Administración** > **volúmenes**.
11. Haga clic en el icono Actions del volumen que quiere emparejar.
12. Haga clic en **par**.
13. En el cuadro de diálogo **volumen de par**, seleccione **emparejamiento completo**.
14. Pegue la clave de emparejamiento del otro clúster en el cuadro **clave de emparejamiento**.
15. Haga clic en **Complete Pairing**.

    Después de confirmar el emparejamiento, los dos clústeres comienzan 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**. Se muestra la pareja de volúmenes `PausedMisconfigured` hasta que se asignan el origen y el destino de la pareja de volúmenes.

    Después de completar correctamente el emparejamiento, debe actualizar la tabla Volumes para eliminar la opción **Pair** de la lista **Actions** del volumen emparejado. Si no actualiza la tabla, la opción **par** permanece disponible para su selección. Si vuelve a seleccionar la opción **par**, se abre una nueva pestaña y, dado que el volumen ya está emparejado, el sistema informa un `StartVolumePairing Failed: xVolumeAlreadyPaired` Mensaje de error en la ventana **Pair Volume** de la página UI de Element.

Obtenga más información

- Mensajes sobre el emparejamiento de volúmenes
- Advertencias sobre el emparejamiento de volúmenes

- Asigne un origen y un destino de replicación a los volúmenes emparejados

Asigne un origen y un destino de replicación a los volúmenes emparejados

Después de emparejar los volúmenes, debe asignar un volumen de origen y su volumen de destino de replicación. Un origen u objetivo de replicación pueden ser un volumen de una pareja de volúmenes. Este procedimiento también se puede usar para redirigir los datos enviados a un volumen de origen hacia un volumen de destino remoto en caso de que no esté disponible el volumen de origen.

Lo que necesitará

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

Pasos

1. Prepare el volumen de origen:
   a. En el clúster que contiene el volumen que desea asignar como origen, seleccione **Administración** > **volúmenes**.
   b. Haga clic en el icono **acciones** del volumen que desea asignar como origen y haga clic en **Editar**.
   c. En la lista desplegable **Access**, seleccione **Read/Write**.

   > Si va a revertir la asignación de origen y objetivo, esta acción hará que la pareja de volúmenes muestre el siguiente mensaje hasta que se asigne un nuevo objetivo de replicación: `PausedMisconfigured`

   Cambiar el acceso pone en pausa la replicación de volumen y provoca el cese de la transmisión de datos. Asegúrese de haber coordinado estos cambios en ambos sitios.

   a. Haga clic en **Guardar cambios**.
2. Prepare el volumen objetivo:
   a. Desde el clúster que contiene el volumen que desea asignar como destino, seleccione **Gestión** > **volúmenes**.
   b. Haga clic en el icono Actions del volumen que desea asignar como destino y haga clic en **Editar**.
   c. En la lista desplegable **Access**, seleccione **destino de replicación**.

   > Si asigna un volumen existente como objetivo de replicación, los datos de ese volumen se sobrescriben. Debe usar un nuevo volumen de destino que no contiene datos y que tenga las mismas características que el volumen de origen, como el tamaño, la configuración 512e y la configuración de calidad de servicio. El tamaño del volumen de destino puede ser mayor o igual que el del volumen de origen, pero no menor.

   d. Haga clic en **Guardar cambios**.

Obtenga más información

- Emparejar volúmenes con un ID de volumen
- Emparejar volúmenes con una clave de emparejamiento

Validar la replicación de volúmenes

Una vez que se replica un volumen, los volúmenes de origen y objetivo deben estar activos. Cuando en un estado activo, los volúmenes se emparejan, los datos se envían del volumen de origen al de destino y los datos están sincronizados.

1. En ambos clústeres, seleccione **Protección de datos** > **pares de volúmenes**.
2. Compruebe que el estado del volumen sea Active.

Obtenga más información

Advertencias sobre el emparejamiento de volúmenes

Eliminar una relación de volumen después de la replicación

Una vez que se completa la replicación y ya no se necesita la relación de pareja de volúmenes, es posible eliminar la relación de volumen.

1. Seleccione **Protección de datos** > **pares de volúmenes**.
2. Haga clic en el icono **acciones** del par de volúmenes que desee eliminar.
3. Haga clic en **Eliminar**.
4. Confirme el mensaje.

Gestionar relaciones de volumen

Es posible gestionar las relaciones de volúmenes de muchas maneras, como pausar la replicación, revertir el emparejamiento de volúmenes, cambiar el modo de replicación, eliminar una pareja de volúmenes o eliminar una pareja de clústeres.

Obtenga más información

- Detenga la replicación
- Cambie el modo de replicación
- Eliminar parejas de volúmenes

Detenga la replicación

Puede pausar manualmente la replicación si necesita detener el procesamiento de I/o durante un breve periodo de tiempo. Puede que desee pausar la replicación si hay un aumento en el procesamiento de I/o y desea reducir la carga de procesamiento.

1. Seleccione **Protección de datos** > **pares de volúmenes**.
2. Haga clic en el icono Actions de la pareja de volúmenes.
3. Haga clic en **Editar**.
4. En el panel **Editar par de volúmenes**, detenga manualmente el proceso de replicación.

Cuando se pausa o se reanuda manualmente una replicación de volumen, se detiene o se reanuda la transmisión de datos. Asegúrese de haber coordinado estos cambios en ambos sitios.

5. Haga clic en **Guardar cambios**.

Cambie el modo de replicación

Es posible editar las propiedades de una pareja de volúmenes para cambiar el modo de replicación de la relación de pareja de volúmenes.

1. Seleccione **Protección de datos** > **pares de volúmenes**.
2. Haga clic en el icono Actions de la pareja 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 reconocen en el cliente después de que se aplican en el clúster de origen.
   - **Real-Time (Synchronous)**: Las escrituras se reconocen en el cliente después de que se aplican tanto en los clústeres de origen como de destino.
   - **Sólo instantáneas**: Sólo se replican las instantáneas creadas en el clúster de origen. No se replican las escrituras activas del volumen de origen. **Atención:** al cambiar el modo de replicación, se cambia el modo inmediatamente. Asegúrese de haber coordinado estos cambios en ambos sitios.
5. Haga clic en **Guardar cambios**.

Eliminar parejas de volúmenes

Es posible eliminar una pareja de volúmenes si se desea quitar una asociación de pareja entre dos volúmenes.

1. Seleccione **Protección de datos** > **pares de volúmenes**.
2. Haga clic en el icono Actions de la pareja de volúmenes que desea eliminar.
3. Haga clic en **Eliminar**.
4. Confirme el mensaje.

Elimine una pareja de clústeres

Es posible eliminar una pareja de clústeres desde la interfaz de usuario de Element de cualquiera de los clústeres que componen la pareja.

1. Haga clic en **Protección de datos** > **pares de clústeres**.
2. Haga clic en el icono Actions de una pareja de clústeres.
3. En el menú que se abre, haga clic en **Eliminar**.
4. Confirme la acción.
5. Repita los pasos desde el segundo clúster de la pareja de clústeres.

Detalles de parejas de clústeres

La página Cluster Pairs de la pestaña Data Protection proporciona información sobre los clústeres que se hayan emparejado o que estén en proceso de emparejarse. El sistema muestra mensajes de emparejamiento y progreso en la columna Status.

- **ID**

  Un ID generado por el sistema que se otorga a cada pareja de clústeres.

- **Nombre de clúster remoto**

  El nombre del otro clúster de la pareja.

- **MVIP remoto**

  La dirección IP virtual de gestión del otro clúster en la pareja.

- **Estado**

  El estado de replicación del clúster remoto

- **Replicación de volúmenes**

  La cantidad de volúmenes que contiene el clúster emparejados para la replicación.

- **UUID**

  Un ID único que se otorga a cada clúster en la pareja.

Detalles de parejas de volúmenes

La página Volume Pairs de la pestaña Data Protection proporciona información sobre los volúmenes que se hayan emparejado o que estén en proceso de emparejarse. El sistema muestra los mensajes de emparejamiento y progreso en la columna Volume Status.

- **ID**

  El ID que genera el sistema para el volumen.

- **Nombre**

  El nombre que se le dio al volumen cuando se creó. Los nombres de volumen pueden tener hasta 223 caracteres y contener a-z, 9 y guion (-).

- **Cuenta**

  El nombre de la cuenta asignada al volumen.

- **Estado del volumen**

  El estado de replicación del volumen

- **Estado de instantánea**

  El estado del volumen de snapshot.

- **Modo**

  El método de replicación de escritura del cliente. Los valores posibles son los siguientes:

  - Asincrónica
  - Solo Snapshot
  - Sincr

- **Dirección**

  La dirección de los datos del volumen:

  - Icono de volumen de origen ( ) indica que los datos se escriben en un objetivo fuera del clúster.
  - Icono de volumen de destino ( ) indica que los datos se escriben en el volumen local desde un origen externo.

- **Retraso asíncrono**

  El tiempo transcurrido desde que el volumen se sincronizó por última vez con el clúster remoto. Si el volumen no se empareja, el valor es nulo.

- **Cluster remoto**

  El nombre del clúster remoto en el que reside el volumen.

- **ID de volumen remoto**

  El ID de volumen del volumen en el clúster remoto.

- **Nombre del volumen remoto**

  El nombre que se le dio al volumen remoto cuando se creó.

Mensajes sobre el emparejamiento de volúmenes

Es posible ver mensajes de emparejamiento de volúmenes durante el proceso inicial de emparejamiento desde la página Volume Pairs de la pestaña Data Protection. Estos mensajes pueden aparecer tanto en los extremos de origen como de destino de la pareja en la vista de lista Replicating Volumes.

- **PausedDisconnected**

  Se agotó el tiempo de ejecución de la replicación de origen o los RPC de sincronización. Se perdió la conexión con el clúster remoto. Compruebe las conexiones de red con el clúster.

- **ResumingConnected**

  La sincronización de replicación remota está activa. Se inicia el proceso de sincronización y se esperan los datos.

- **ResumingRRSync**

  Se hace una copia sencilla de Helix de los metadatos del volumen en el clúster emparejado.

- **ResumingLocalSync**

  Se hace una copia doble de Helix de los metadatos del volumen en el clúster emparejado.

- **ReumingDataTransfer**

  Se reanudó 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 produce ninguna actividad de replicación.

Advertencias sobre el emparejamiento de volúmenes

Lapágina Volume Pairs en la pestaña Data Protection proporciona estos mensajes después de emparejar volúmenes. Estos mensajes pueden aparecer tanto en los extremos de origen como de destino de la pareja (a menos que se indique lo contrario) en la vista de lista Replicating Volumes.

- **PausedaClusterFull**

  Dado que el clúster de destino está lleno, la replicación de origen y la transferencia de datos masivos no pueden continuar. El mensaje aparece solamente en el extremo de origen de la pareja.

- **PausedExceedededededMaxSnapshotCount**

  El volumen de destino ya cuenta con el número máximo de copias de Snapshot y no puede replicar copias de Snapshot adicionales.

- **PausedManual**

  El volumen local se pausó manualmente. La pausa se debe cancelar antes de que se reanude la replicación.

- **PausedManualRemote**

  El volumen remoto se pausó manualmente. Se requiere intervención manual para cancelar la pausa del volumen remoto antes de que se reanude la replicación.

- **PausedMisconfigured**

  Se esperan un origen y un destino activos. Se requiere intervención manual para reanudar la replicación.

- **PausedQoS**

La calidad de servicio de destino no pudo sostener el I/o de entrada. La replicación se reanuda automáticamente. El mensaje aparece solamente en el extremo de origen de la pareja.

- **PausedSlowLink**

  Se detectó un enlace lento y se detuvo la replicación. La replicación se reanuda automáticamente. El mensaje aparece solamente en el extremo de origen de la pareja.

- **PausedVolumeSizediscordancia**

  El volumen de destino no tiene el mismo tamaño que el volumen de origen.

- **PausedXCopy**

  Se envía un comando SCSI XCOPY a un volumen de origen. El comando debe completarse antes de que la replicación se pueda reanudar. El mensaje aparece solamente en el extremo de origen de la pareja.

- **StoppedMisconfigured**

  Se detectó un error de configuración permanente. El volumen remoto se purgó o se desemparejó. No se puede realizar ninguna acción correctiva y se debe establecer un nuevo emparejamiento.

Use la replicación de SnapMirror entre clústeres de Element y ONTAP

Las relaciones de SnapMirror se pueden crear en la pestaña Data Protection de la interfaz de usuario de NetApp Element. La funcionalidad de SnapMirror debe estar habilitada para poder verla en la interfaz de usuario de.

IPv6 no es compatible con la replicación de SnapMirror entre el software NetApp Element y los clústeres de ONTAP.

"Vídeo de NetApp: SnapMirror para software NetApp HCI y Element"

Los sistemas que ejecutan el software NetApp Element admiten la funcionalidad SnapMirror para copiar y restaurar copias Snapshot con sistemas ONTAP de NetApp. El principal motivo para usar esta tecnología es la recuperación ante desastres de NetApp HCI a ONTAP. Los extremos incluyen ONTAP, ONTAP Select y Cloud Volumes ONTAP. Consulte TR-4641 Protección de datos de NetApp HCI.

"Informe técnico de NetApp 4641: Protección de datos de NetApp HCI"

Obtenga más información

- "Crear una estructura de datos con NetApp HCI, ONTAP e infraestructura convergente"
- "Replicación entre software de NetApp Element y ONTAP"

Información general de SnapMirror

Los sistemas que ejecutan el software NetApp Element admiten la funcionalidad SnapMirror para copiar y restaurar copias Snapshot con los sistemas ONTAP de NetApp.

Los sistemas que ejecutan Element pueden comunicarse directamente con SnapMirror en los sistemas ONTAP 9.3 o posteriores. La API de NetApp Element proporciona métodos para habilitar la funcionalidad de SnapMirror en clústeres, volúmenes y snapshots. Además, la interfaz de usuario de Element incluye toda la

funcionalidad necesaria para gestionar las relaciones de SnapMirror entre el software Element y los sistemas ONTAP.

Es posible replicar volúmenes originados de ONTAP en volúmenes de Element en casos de uso específicos con funcionalidad limitada. Para obtener más información, consulte la documentación de ONTAP.

Obtenga más información

"Replicación entre software de Element y ONTAP"

Habilite SnapMirror en el clúster

Debe habilitar manualmente la funcionalidad de SnapMirror en el nivel del clúster a través de la interfaz de usuario de NetApp Element. El sistema viene con la funcionalidad de SnapMirror deshabilitada de forma predeterminada y no se habilita automáticamente como parte de una nueva instalación o actualización. Habilitar la función SnapMirror es una tarea de configuración que solo debe hacer una vez.

SnapMirror solo se puede habilitar en clústeres que ejecutan el software Element que se usa junto con volúmenes de un sistema ONTAP de NetApp. Solo debe habilitar la funcionalidad SnapMirror si el clúster está conectado para usarlo con volúmenes de ONTAP de NetApp.

Lo que necesitará

El clúster de almacenamiento debe ejecutar el software NetApp Element.

Pasos

1. Haga clic en **Clusters** > **Configuración**.
2. Busque la configuración específica del clúster para SnapMirror.
3. Haga clic en **Activar SnapMirror**.

> Al habilitar la funcionalidad SnapMirror, se modifica la configuración del software Element de forma permanente. Puede deshabilitar la función SnapMirror y restaurar la configuración predeterminada solo si devuelve el clúster a la imagen de fábrica.

4. Haga clic en **Sí** para confirmar el cambio de configuración de SnapMirror.

Habilite 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 de ONTAP especificados. Se trata de un permiso del administrador del clúster donde se ejecuta el software NetApp Element para que SnapMirror controle un volumen.

Lo que necesitará

- Debe habilitar SnapMirror en la interfaz de usuario de Element para el clúster.
- Existe un extremo de SnapMirror disponible.
- El volumen debe ser el tamaño de bloque 512e.
- El volumen no participa en la replicación remota.

- El tipo de acceso de volumen no es destino de replicación.

> También puede establecer esta propiedad al crear o clonar un volumen.

Pasos

1. Haga clic en **Administración** > **volúmenes**.
2. Haga clic en el icono **acciones** del volumen para el que desea activar SnapMirror.
3. En el menú que se abre, seleccione **Editar**.
4. En el cuadro de diálogo **Editar volumen**, active la casilla de verificación **Activar SnapMirror**.
5. Haga clic en **Guardar cambios**.

Cree un extremo de SnapMirror

Debe crear un extremo de SnapMirror en la interfaz de usuario de NetApp Element para poder crear una relación.

Un extremo de SnapMirror es un clúster de ONTAP que funciona como destino de replicación para un clúster que ejecuta el software Element. Antes de crear una relación de SnapMirror, primero se debe crear un extremo de SnapMirror.

Es posible crear y gestionar hasta cuatro extremos de SnapMirror en un clúster de almacenamiento que ejecuta el software Element.

> Si originalmente se creó un extremo existente mediante la API y no se guardaron las credenciales, puede ver el extremo en la interfaz de usuario de Element y verificar su existencia, pero no se puede gestionar mediante la interfaz de usuario de Element. Este extremo solo puede gestionarse mediante la API de Element.

Para obtener más información sobre los métodos API, consulte "Gestione el almacenamiento con la API de Element".

Lo que necesitará

- Debe haber habilitado SnapMirror en la interfaz de usuario de Element para el clúster de almacenamiento.
- Conoce las credenciales de ONTAP para el extremo.

Pasos

1. Haga clic en **Protección de datos** > **terminales de SnapMirror**.
2. Haga clic en **Crear extremo**.
3. En el cuadro de diálogo **Crear un nuevo extremo**, introduzca la dirección IP de administración del clúster del sistema ONTAP.
4. Introduzca las credenciales de administrador de ONTAP asociadas con el extremo.
5. Consulte información adicional:
   - LIF: Enumera las interfaces lógicas de interconexión de clústeres de ONTAP que se utilizan para comunicarse con Element.
   - Status: Muestra el estado actual del extremo de SnapMirror. Los valores posibles son: Conectado, desconectado y no administrado.
6. Haga clic en **Crear extremo**.

Crear una relación de SnapMirror

Debe crear una relación de SnapMirror en la interfaz de usuario de NetApp Element.

> Cuando aún no se habilita un volumen para SnapMirror y seleccione para crear una relación desde la interfaz de usuario de Element, se habilita automáticamente SnapMirror en ese volumen.

Lo que necesitará

Está habilitado SnapMirror en el volumen.

Pasos

1. Haga clic en **Administración** > **volúmenes**.
2. Haga clic en el icono **acciones** del volumen que va a formar parte de la relación.
3. Haga clic en **Crear una relación de SnapMirror**.
4. En el cuadro de diálogo **Crear una relación de SnapMirror**, seleccione un extremo de la lista **Endpoint**.
5. Seleccione si la relación se creará con un volumen de ONTAP nuevo o con un volumen de ONTAP existente.
6. Para crear un nuevo volumen ONTAP en la interfaz de usuario de Element, haga clic en **Crear nuevo volumen**.
   a. Seleccione **Storage Virtual Machine** para esta relación.
   b. Seleccione **aggregate** en la lista desplegable.
   c. En el campo **sufijo de nombre de volumen**, introduzca un sufijo.

      > El sistema detecta el nombre del volumen de origen y lo copia en el campo **Nombre de volumen**. El sufijo que introduzca anexa el nombre.

   d. Haga clic en **Crear volumen de destino**.
7. Para utilizar un volumen de ONTAP existente, haga clic en **utilizar volumen existente**.
   a. Seleccione **Storage Virtual Machine** 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 directiva. Si la directiva seleccionada tiene reglas de mantenimiento, la tabla Reglas muestra las reglas y las etiquetas asociadas.
9. **Opcional**: Selecciona un horario.

   Esto determina la frecuencia con la que la relación crea copias.
10. **Opcional**: En el campo **limitar ancho de banda a**, introduzca la cantidad máxima de ancho de banda que pueden consumir las transferencias de datos asociadas con esta relación.
11. Consulte información adicional:
    - **Estado**: Estado actual de la relación del volumen de destino. Los valores posibles son:
      - Inicializado: El volumen de destino no se ha inicializado.
      - snapmirror: El volumen de destino se ha inicializado y está listo para recibir actualizaciones de SnapMirror.

        - Roto-off: El volumen de destino es de lectura/escritura y existen snapshots.
    - **Estado**: Estado actual de la relación. Los valores posibles son ralentí, transferencia, comprobación, desactivación, inactivo, puesta en cola, preparación, finalización, anulación y ruptura.
    - **Tiempo de retardo**: La cantidad de tiempo en segundos que el sistema de destino está retrasado con respecto al sistema de origen. El tiempo de desfase no debe superar el intervalo de programación de transferencia.
    - **Límite de ancho de banda**: La cantidad máxima de ancho de banda que pueden consumir las transferencias de datos asociadas a esta relación.
    - **Última transferencia**: Marca de hora de la última instantánea transferida. Haga clic para obtener más información.
    - **Nombre de la política**: Nombre de la política de SnapMirror de ONTAP para la relación.
    - **Tipo de directiva**: Tipo de política de SnapMirror de ONTAP seleccionada para la relación. Los valores posibles son:
        - async_mirror
        - mirror_vault
    - **Nombre del programa**: Nombre del programa preexistente del sistema ONTAP seleccionado para esta relación.
12. Para no inicializar en este momento, asegúrese de que la casilla de verificación **inicializar** no está activada.

    La inicialización puede requerir mucho tiempo. Tal vez desee ejecutarlo durante las horas de menor actividad. La inicialización realiza una transferencia básica; realiza una copia Snapshot del volumen de origen y, a continuación, transfiere esa copia y todos los bloques de datos a los que hace referencia al volumen de destino. Puede inicializar manualmente o utilizar una programación para iniciar el proceso de inicialización (y las actualizaciones posteriores) según la programación.

13. Haga clic en **Crear relación**.
14. Haga clic en **Protección de datos** > **Relaciones de SnapMirror** para ver esta nueva relación de SnapMirror.

Acciones de relaciones con SnapMirror

Puede configurar una relación desde la página SnapMirror Relationships de la pestaña Data Protection. Las opciones del icono acciones se describen aquí.

- **Edición**: Edita la directiva utilizada o la programación de la relación.
- **Eliminar**: Elimina la relación de SnapMirror. Esta función no elimina el volumen de destino.
- **Inicializar**: Realiza la primera transferencia inicial de datos de línea de base para establecer una nueva relación.
- **Actualizar**: Realiza una actualización bajo demanda de la relación, replicando los datos nuevos y las copias Snapshot incluidas desde la última actualización al destino.
- **Quiesce**: Previene cualquier actualización adicional para una relación.
- **Reanudar**: Reanuda una relación que se detiene.
- **Break**: Hace que el volumen de destino sea de lectura y escritura y detiene todas las transferencias actuales y futuras. Determine que los clientes no utilizan el volumen de origen original, ya que la operación

de resincronización inversa hace que el volumen de origen original sea de solo lectura.

- **Resync**: Restablece una relación rota en la misma dirección antes de que se produjera la ruptura.
- **Resync inversa**: Automatiza los pasos necesarios para crear e inicializar una nueva relación en la dirección opuesta. Esto sólo se puede hacer si la relación existente se encuentra en un estado roto. Esta operación no eliminará la relación actual. El volumen de origen original se revierte a la copia Snapshot común más reciente y se vuelve a sincronizar con el destino. Se perderán todos los cambios realizados en el volumen de origen original desde la última actualización correcta de SnapMirror. Los cambios realizados o los nuevos datos escritos en el volumen de destino actual se devuelven al volumen de origen original.
- **Anular**: Cancela una transferencia actual en curso. Si se emite una actualización de SnapMirror para una relación abortada, la relación continúa con la última transferencia desde el último punto de comprobación de reinicio que se creó antes de que se produjera la anulación.

Etiquetas de SnapMirror

Una etiqueta de SnapMirror sirve como marcador para la transferencia de una copia de Snapshot específica según las reglas de retención de la relación.

Si se aplica una etiqueta a una copia de Snapshot, esta se Marca como destino de la replicación de SnapMirror. El rol de la relación es aplicar las reglas sobre la transferencia de datos seleccionando la snapshot con la etiqueta correspondiente, copiándola al volumen de destino y garantizando que se conserva el número correcto de copias. Se refiere a la política para determinar el recuento de retenciones y el período de retención. La directiva puede tener un número cualquiera de reglas y cada regla tiene una etiqueta única. Esta etiqueta actúa como enlace entre la snapshot y la regla de retención.

Es la etiqueta de SnapMirror que indica qué regla se aplica a la snapshot, la snapshot de grupo o la programación seleccionada.

Añada etiquetas de SnapMirror a snapshots

Las etiquetas de SnapMirror especifican la política de retención de snapshots en el extremo de SnapMirror. Se pueden añadir etiquetas a las copias de Snapshot y las copias de Snapshot de grupo.

Puede ver las etiquetas disponibles en un cuadro de diálogo existente de relación de SnapMirror o en el Administrador del sistema ONTAP de NetApp.

> Cuando se añade una etiqueta a una copia de Snapshot de grupo, se sobrescriben todas las etiquetas existentes a copias de Snapshot individuales.

Lo que necesitará

- Se habilita SnapMirror en el clúster.
- La etiqueta que desea añadir ya existe en ONTAP.

Pasos

1. Haga clic en **Protección de datos** > **Snapshots** o **instantánea de grupo**.
2. Haga clic en el icono **acciones** de la instantánea o la instantánea de grupo a la que desea agregar una etiqueta de SnapMirror.
3. En el cuadro de diálogo **Editar instantánea**, introduzca texto en el campo **etiqueta de SnapMirror**. La etiqueta debe coincidir con una etiqueta de regla de la política aplicada a la relación de SnapMirror.

4. Haga clic en **Guardar cambios**.

Añadir etiquetas de SnapMirror a las programaciones de Snapshot

Puede añadir etiquetas de SnapMirror a programaciones de Snapshot para garantizar que se aplique una política de SnapMirror. Puede ver las etiquetas disponibles en un cuadro de diálogo existente de relación de SnapMirror o en ONTAP System Manager de NetApp.

Lo que necesitará

- Se debe habilitar SnapMirror en el nivel de clúster.
- La etiqueta que desea añadir ya existe en ONTAP.

Pasos

1. Haga clic en **Protección de datos** > **programas**.
2. Añada una etiqueta de SnapMirror a una programación de una de las siguientes maneras:

Opción	Pasos
Crear una nueva programación	a. Seleccione **Crear programación**. b. Introduzca todos los demás detalles relevantes. c. Seleccione **Crear programación**.
Modificación de la programación existente	a. Haga clic en el icono **acciones** de la programación a la que desea agregar una etiqueta y seleccione **Editar**. b. En el cuadro de diálogo que aparece, introduzca texto en el campo **etiqueta de SnapMirror**. c. Seleccione **Guardar cambios**.

Obtenga más información

Crear una programación de Snapshot

Recuperación ante desastres mediante SnapMirror

En caso de producirse un problema con un volumen o un clúster que ejecuta el software NetApp Element, utilice la funcionalidad SnapMirror para dividir la relación y la conmutación por error al volumen de destino.

Si el clúster original ha fallado completamente o no existe, póngase en contacto con el soporte de NetApp para obtener ayuda.

Ejecute una conmutación al nodo de respaldo desde un clúster de Element

Puede realizar una conmutación al nodo de respaldo desde el clúster de Element para hacer que el volumen de destino sea de lectura/escritura y accesible para los hosts en el lado de destino. Antes de realizar una conmutación al nodo de respaldo del clúster de

Element, debe interrumpir la relación de SnapMirror.

Use la interfaz de usuario de NetApp Element para realizar la conmutación al respaldo. Si la interfaz de usuario de Element no está disponible, también es posible usar ONTAP System Manager o la CLI de ONTAP para ejecutar el comando break Relationship.

Lo que necesitará

- Existe una relación de SnapMirror y tiene al menos una snapshot válida en el volumen de destino.
- Necesita una conmutación al nodo de respaldo en el volumen de destino debido a una interrupción del servicio 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. Busque la relación con el volumen de origen que desea conmutar al nodo de respaldo.
3. Haga clic en el icono **acciones**.
4. Haga clic en **descanso**.
5. Confirme la acción.

   El volumen del clúster de destino ahora tiene acceso de lectura/escritura y se puede montar en los hosts de la aplicación para reanudar las cargas de trabajo de producción. Toda la replicación de SnapMirror se detiene como resultado de esta acción. La relación muestra un estado de ruptura.

Realice una conmutación tras recuperación al elemento

Cuando se mitigó el problema en el lado primario, se debe volver a sincronizar el volumen de origen original y conmutar al software NetApp Element. Los pasos que realice varían en función de si todavía existe el volumen de origen original o si necesita realizar la conmutación tras recuperación en un volumen recién creado.

Obtenga más información

- Realice una conmutación tras recuperación cuando el volumen de origen siga existiendo
- Realice una conmutación tras recuperación cuando el volumen de origen ya no exista
- Escenarios de conmutación tras recuperación de SnapMirror

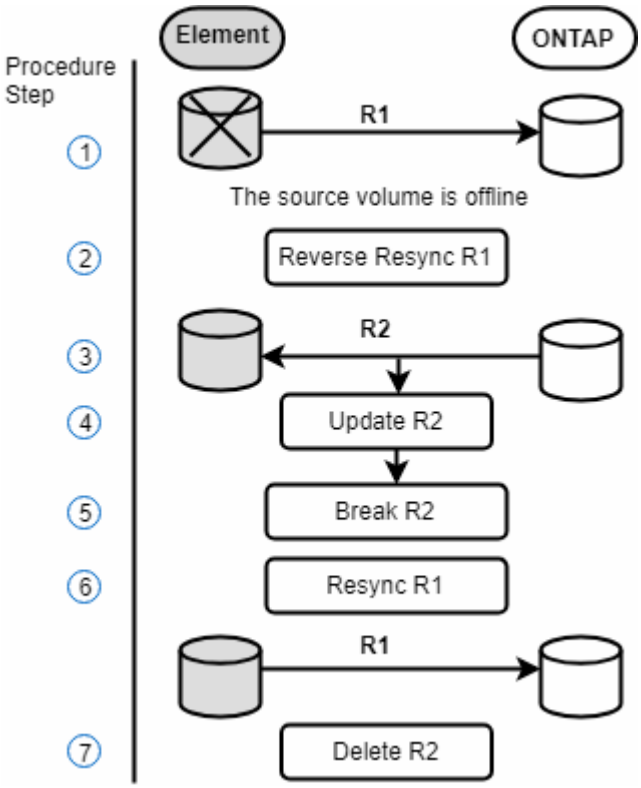
Escenarios de conmutación tras recuperación de SnapMirror

La funcionalidad de recuperación ante desastres de SnapMirror se ilustra en dos escenarios de conmutación tras recuperación. Se asume que la relación original ha sido fallida (rota).

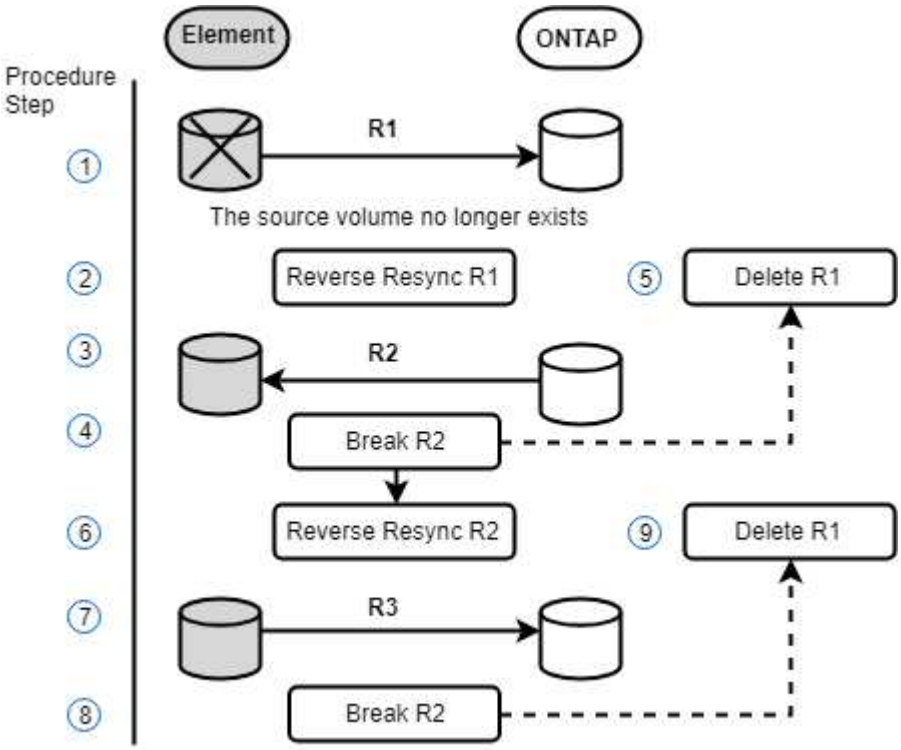
Los pasos de los procedimientos correspondientes se añaden como referencia.

En los ejemplos que se muestran aquí, R1 = la relación original en la que el clúster que ejecuta el software NetApp Element es el volumen de origen original (elemento) 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 conmutación por recuperación cuando el volumen de origen sigue existiendo:



La siguiente imagen muestra el escenario de conmutación por recuperación cuando el volumen de origen ya no existe:



Obtenga más información

- Realice una conmutación tras recuperación cuando el volumen de origen siga existiendo
- Realice una conmutación tras recuperación cuando el volumen de origen ya no exista

Realice una conmutación tras recuperación cuando el volumen de origen siga existiendo

Es posible resincronizar el volumen de origen original y conmutar por error con la interfaz de usuario de NetApp Element. Este procedimiento se aplica a situaciones en las que aún existe el volumen de origen original.

1. En la interfaz de usuario de Element, busque la relación que rompió para realizar la conmutación al respaldo.
2. Haga clic en el icono acciones y haga clic en **Reverse Resync**.
3. Confirme la acción.

> La operación de resincronización inversa crea una nueva relación en la que se invierten los roles de los volúmenes de origen y de destino originales (esto provoca dos relaciones a medida que persiste la relación original). Los datos nuevos del volumen de destino original se transfieren al volumen de origen original como parte de la operación de resincronización inversa. Puede seguir accediendo al volumen activo y escribiendo datos en el lado de destino, pero deberá desconectar todos los hosts del volumen de origen y realizar una actualización de SnapMirror antes de volver a redirigir al volumen primario original.

4. Haga clic en el icono acciones de la relación inversa que acaba de crear y haga clic en **Actualizar**.

   Ahora que ha completado la resincronización inversa y aseguró 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, es posible realizar los siguientes pasos para completar la conmutación tras recuperación y reactivar el volumen primario original:

5. Haga clic en el icono Actions de la relación inversa y haga clic en **Break**.
6. Haga clic en el icono Actions de la relación original y haga clic en **Resync**.

> El volumen primario original ahora se puede montar para reanudar las cargas de trabajo de producción en el volumen primario original. La replicación original de SnapMirror se reanuda a partir de la normativa y el programa que se ha configurado para la relación.

7. Después de confirmar que el estado original de la relación es "sinreflejado", haga clic en el icono acciones de la relación inversa y haga clic en **Eliminar**.

Obtenga más información

Escenarios de conmutación tras recuperación de SnapMirror

Realice una conmutación tras recuperación cuando el volumen de origen ya no exista

Es posible resincronizar el volumen de origen original y conmutar por error con la interfaz de usuario de NetApp Element. Esta sección se aplica a situaciones en las que se ha perdido el volumen de origen original, pero el clúster original sigue intacto. Para obtener

instrucciones sobre cómo restaurar en un clúster nuevo, consulte la documentación en el sitio de soporte de NetApp.

Lo que necesitará

- Tiene una relación de replicación despareja entre los volúmenes de Element y ONTAP.
- El volumen de Element se pierde de forma irreversiblemente.
- El nombre del volumen original se muestra como NO ENCONTRADO.

Pasos

1. En la interfaz de usuario de Element, busque la relación que rompió para realizar la conmutación al respaldo.

   Mejor práctica: anote la política de SnapMirror y los detalles del horario de la relación original de compensación. Esta información será necesaria al recrear la relación.

2. Haga clic en el icono **acciones** y haga clic en **Reverse Resync**.
3. Confirme la acción.

   La operación de resincronización inversa crea una nueva relación en la que se revierten los roles del volumen de origen y del volumen de destino (esto provoca dos relaciones a medida que persiste la relación original). Como el volumen original ya no existe, el sistema crea un nuevo volumen de Element con el mismo nombre de volumen y tamaño de volumen que el volumen de origen original. Al nuevo volumen se le asigna una política de calidad de servicio predeterminada denominada recuperación sm y se asocia a una cuenta predeterminada denominada recuperación sm. Deberá editar manualmente la cuenta y la política de calidad de servicio de todos los volúmenes creados por SnapMirror para reemplazar los volúmenes de origen originales destruidos.

   Los datos de la copia snapshot más reciente se transfieren al nuevo volumen como parte de la operación de resincronización inversa. Puede seguir accediendo al volumen activo y escribiendo datos 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. Una vez finalizada la resincronización inversa y asegúrese de que no haya sesiones activas conectadas al volumen en el lado de destino y que los últimos datos estén en el volumen primario original, siga estos pasos para completar la conmutación por recuperación y reactivar el volumen primario original:

4. Haga clic en el icono **acciones** de la relación inversa que se creó durante la operación Reverse Resync y haga clic en **Break**.
5. Haga clic en el icono **acciones** de la relación original, en la que el volumen de origen no existe, y haga clic en **Eliminar**.
6. Haga clic en el icono **acciones** de la relación inversa, que rompió en el paso 4, y haga clic en **Resync inversa**.
7. De este modo, se revierte el origen y el destino y se establece una relación con el mismo origen y el mismo destino de volumen que la relación original.
8. Haga clic en el icono **acciones** y en **Editar** para actualizar esta relación con la directiva QoS original y la configuración de programación de la que tomó nota.
9. Ahora es seguro eliminar la relación inversa que usted reynced en el paso 6.

Obtenga más información

Escenarios de conmutación tras recuperación de SnapMirror

Realice una transferencia o una migración puntual de ONTAP a Element

Generalmente, cuando se usa SnapMirror para la recuperación ante desastres de un clúster de almacenamiento de 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 actuar como el origen y elemento como el destino.

- Existen dos situaciones hipotéticas:
  - No existe ninguna relación anterior de recuperación ante desastres. Siga todos los pasos de este procedimiento.
  - Existe una relación anterior de recuperación ante desastres, pero no entre los volúmenes que se utilizan para esta mitigación. En este caso, siga sólo los pasos 3 y 4 que se indican a continuación.

Lo que necesitará

- ONTAP debe haber accesible el nodo de destino de Element.
- El volumen de Element debe estar habilitado para la replicación de SnapMirror.

Debe especificar la ruta de destino del elemento en el formato hotip:/lun/<id_number>, donde lun es la cadena real "'lun'" e id_number es el ID del volumen del elemento.

Pasos

1. Con ONTAP, cree la relación con el clúster de 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. Compruebe que la relación de SnapMirror se ha creado mediante el comando ONTAP snapmirror show.

   Consulte la información sobre la creación de una relación de replicación en la documentación de ONTAP y, para obtener una sintaxis de comando completa, consulte la página man de ONTAP.

3. Con el `ElementCreateVolume` API, cree el volumen objetivo y establezca el modo de acceso del volumen de destino en SnapMirror:

   Cree un volumen de Element mediante 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 mediante la ONTAP `snapmirror initialize` comando:

```
snapmirror initialize -source-path hostip:/lun/name
-destination-path SVM:volume|cluster://SVM/volume
```

Realice backups y restaure volúmenes

Es posible realizar backups y restaurar volúmenes en otro almacenamiento de SolidFire, así como en almacenes de objetos secundarios que sean compatibles con OpenStack Swift o Amazon S3.

Cuando se restauran volúmenes desde OpenStack Swift o Amazon S3, se necesita información de manifiesto desde el proceso de backup original. Si desea restaurar un volumen de del cual se había realizado un backup en un sistema de almacenamiento de SolidFire, no será necesaria ninguna información de manifiesto.

Obtenga más información

- Realice backups de un volumen en un almacén de objetos Amazon S3
- Realice backups de un volumen en un almacén de objetos OpenStack Swift
- Realice backups de un volumen en un clúster de almacenamiento de SolidFire
- Restaure un volumen a partir de un backup en un almacén de objetos Amazon S3
- Restaure un volumen a partir de un backup en un almacén de objetos OpenStack Swift
- Restaure un volumen a partir de un backup en un clúster de almacenamiento de SolidFire

Realice backups de un volumen en un almacén de objetos Amazon S3

Es posible realizar backups de volúmenes de en almacenes de objetos externos que sean compatibles con Amazon S3.

1. Haga clic en **Administración** > **volúmenes**.
2. Haga clic en el icono Actions del volumen del que desea realizar un backup.
3. En el menú que se abre, haga clic en **copia de seguridad en**.
4. En el cuadro de diálogo **copia de seguridad integrada** en **copia de seguridad a**, seleccione **S3**.
5. Seleccione una opción en **Formato de datos**:
   - **Original**: Formato comprimido que sólo pueden leer los sistemas de almacenamiento SolidFire.
   - **Sin comprimir**: Formato sin comprimir compatible con otros sistemas.
6. Introduzca un nombre de host para acceder al almacén de objetos en el campo **Hostname**.
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 bloque S3 en el que desea almacenar la copia de seguridad en el campo **S3 Bucket**.
10. Introduzca una etiqueta de nombre para adjuntarla al prefijo en el campo **etiqueta de nombre**.
11. Haga clic en **Iniciar lectura**.

Realice backups de un volumen en un almacén de objetos OpenStack Swift

Es posible realizar backups de volúmenes de en almacenes de objetos externos que sean compatibles con OpenStack Swift.

1. Haga clic en **Administración** > **volúmenes**.
2. Haga clic en el icono Actions del volumen del que desea realizar un backup.
3. En el menú que se abre, haga clic en **copia de seguridad en**.
4. En el cuadro de diálogo **copia de seguridad integrada** en **copia de seguridad a**, seleccione **Swift**.
5. Seleccione un formato de datos en **Formato de datos**:
   - **Original**: Formato comprimido que sólo pueden leer los sistemas de almacenamiento SolidFire.
   - **Sin comprimir**: Formato sin comprimir compatible con otros sistemas.
6. Introduzca una dirección 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 **Container**.
10. **Opcional**: Introduzca una etiqueta de nombre para adjuntarla al prefijo en el campo **nametag**.
11. Haga clic en **Iniciar lectura**.

Realice backups de un volumen en un clúster de almacenamiento de SolidFire

Es posible realizar backups de volúmenes que residen en un clúster de en un clúster remoto de para los clústeres de almacenamiento que ejecutan el software Element.

Debe confirmar que los clústeres de origen y destino están emparejados.

Consulte "Emparejar clústeres para la replicación".

Cuando se crea un backup o se restaura de un clúster a otro, el sistema genera una clave que se debe usar

como autenticación entre los clústeres. Con esta clave de escritura masiva de volúmenes, el clúster de origen puede autenticarse con el clúster de destino, lo que permite ofrecer un nivel de seguridad cuando se escribe en el volumen de destino. Como parte del proceso de backup o restauración, debe generar una clave de escritura masiva de volúmenes desde el volumen de destino antes de iniciar la operación.

1. En el clúster de destino, **Administración** > **volúmenes**.
2. Haga clic en el icono Actions del volumen de destino.
3. En el menú que se abre, haga clic en **Restaurar de**.
4. En el cuadro de diálogo **Restauración integrada**, en **Restaurar de**, seleccione **SolidFire**.
5. Seleccione una opción en **Formato de datos**:
   - **Original**: Formato comprimido que sólo pueden leer los sistemas de almacenamiento SolidFire.
   - **Sin comprimir**: Formato sin comprimir compatible con otros sistemas.
6. Haga clic en **generar clave**.
7. Copie la clave del cuadro **Bulk Volume Write Key** en el portapapeles.
8. En el clúster de origen, vaya a **Administración** > **volúmenes**.
9. Haga clic en el icono Actions del volumen del que desea realizar un backup.
10. En el menú que se abre, haga clic en **copia de seguridad en**.
11. En el cuadro de diálogo **copia de seguridad integrada**, en **copia de seguridad a**, seleccione **SolidFire**.
12. Seleccione la misma opción que seleccionó anteriormente en el campo **Formato de datos**.
13. Introduzca la dirección IP virtual de administración del clúster del volumen de destino en el campo **Remote Cluster MVIP**.
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 **Remote Cluster Password**.
16. En el campo **Bulk Volume Write Key**, pegue la clave que ha generado en el clúster de destino anteriormente.
17. Haga clic en **Iniciar lectura**.

Restaure un volumen a partir de un backup en un almacén de objetos Amazon S3

Es posible restaurar un volumen a partir de un backup en un almacén de objetos Amazon S3.

1. Haga clic en **Informes** > **Registro de sucesos**.
2. Busque el evento de backup que creó el backup que debe restaurar.
3. En la columna **Detalles** del evento, haga clic en **Mostrar detalles**.
4. Copie la información de manifiesto en el portapapeles.
5. Haga clic en **Administración** > **volúmenes**.
6. Haga clic en el icono Actions del volumen que desea restaurar.
7. En el menú que se abre, haga clic en **Restaurar de**.
8. En el cuadro de diálogo **Restauración integrada** en **Restaurar de**, seleccione **S3**.
9. Seleccione la opción que coincide con la copia de seguridad en **Formato de datos**:

- **Original**: Formato comprimido que sólo pueden leer los sistemas de almacenamiento SolidFire.
- **Sin comprimir**: Formato sin comprimir compatible con otros sistemas.

10. Introduzca un nombre de host para acceder al almacén de objetos en el campo **Hostname**.
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 bloque S3 en el que desea almacenar la copia de seguridad en el campo **S3 Bucket**.
14. Pegue la información del manifiesto en el campo **manifiesto**.
15. Haga clic en **Iniciar escritura**.

Restaure un volumen a partir de un backup en un almacén de objetos OpenStack Swift

Es posible restaurar un volumen a partir de un backup en un almacén de objetos OpenStack Swift.

1. Haga clic en **Informes** > **Registro de sucesos**.
2. Busque el evento de backup que creó el backup que debe restaurar.
3. En la columna **Detalles** del evento, haga clic en **Mostrar detalles**.
4. Copie la información de manifiesto en el portapapeles.
5. Haga clic en **Administración** > **volúmenes**.
6. Haga clic en el icono Actions del volumen que desea restaurar.
7. En el menú que se abre, haga clic en **Restaurar de**.
8. En el cuadro de diálogo **Integrated Restore**, en **Restore from**, seleccione **Swift**.
9. Seleccione la opción que coincide con la copia de seguridad en **Formato de datos**:
   - **Original**: Formato comprimido que sólo pueden leer los sistemas de almacenamiento SolidFire.
   - **Sin comprimir**: Formato sin comprimir compatible con otros sistemas.
10. Introduzca una dirección 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 **Container**.
14. Pegue la información del manifiesto en el campo **manifiesto**.
15. Haga clic en **Iniciar escritura**.

Restaure un volumen a partir de un backup en un clúster de almacenamiento de SolidFire

Es posible restaurar un volumen a partir de un backup en un clúster de almacenamiento de SolidFire.

Cuando se crea un backup o se restaura de un clúster a otro, el sistema genera una clave que se debe usar como autenticación entre los clústeres. Con esta clave de escritura masiva de volúmenes, el clúster de origen puede autenticarse con el clúster de destino, lo que permite ofrecer un nivel de seguridad cuando se escribe en el volumen de destino. Como parte del proceso de backup o restauración, debe generar una clave de escritura masiva de volúmenes 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 Actions del volumen que desea restaurar.
3. En el menú que se abre, haga clic en **Restaurar de**.
4. En el cuadro de diálogo **Restauración integrada**, en **Restaurar de**, seleccione **SolidFire**.
5. Seleccione la opción que coincide con la copia de seguridad en **Formato de datos**:
   - **Original**: Formato comprimido que sólo pueden leer los sistemas de almacenamiento SolidFire.
   - **Sin comprimir**: Formato sin comprimir compatible con otros sistemas.
6. Haga clic en **generar clave**.
7. Copie la información de **Bulk Volume Write Key** en el portapapeles.
8. En el clúster de origen, haga clic en **Administración** > **volúmenes**.
9. Haga clic en el icono Actions del volumen que quiera usar para la restauración.
10. En el menú que se abre, haga clic en **copia de seguridad en**.
11. En el cuadro de diálogo **copia de seguridad integrada**, seleccione **SolidFire** en **copia de seguridad**.
12. Seleccione la opción que coincide con la copia de seguridad en **Formato de datos**.
13. Introduzca la dirección IP virtual de administración del clúster del volumen de destino en el campo **Remote Cluster MVIP**.
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 **Remote Cluster Password**.
16. Pegue la clave del portapapeles en el campo **Bulk Volume Write Key**.
17. Haga clic en **Iniciar lectura**.

Solucionar los problemas del sistema

Debe supervisar el sistema para realizar diagnósticos y obtener información acerca de las tendencias y los Estados de rendimiento de varios operaciones del sistema. Puede que deba sustituir nodos o SSD por motivos de mantenimiento.

- "Ver información acerca de los eventos del sistema"
- "Ver el estado de las tareas en ejecución"
- "Ver las alertas del sistema"
- "Ver la actividad de rendimiento del nodo"
- "Ver el rendimiento del volumen"
- "Ver sesiones iSCSI"
- "Consulte las sesiones Fibre Channel"
- "Solucione problemas de unidades"
- "Solucione los problemas de los nodos"
- "Trabaje con utilidades por nodo para los nodos de almacenamiento"
- "Trabaje con el nodo de gestión"
- "Comprender los niveles de llenado de clústeres"

Si quiere más información

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

Ver información acerca de los eventos del sistema

Es posible ver información sobre varios eventos detectados en el sistema. El sistema actualiza los mensajes de evento cada 30 segundos. El registro de eventos muestra eventos clave para el clúster.

1. En la interfaz de usuario de Element, seleccione **Reporting** > **Event Log**.

   Para cada evento, verá la siguiente información:

Elemento	Descripción
ID	ID exclusivo asociado con cada evento.
Tipo de evento	Tipo de evento que se está registrando; por ejemplo, eventos de API o eventos de clon.
Mensaje	Mensaje asociado con el evento.
Detalles	Información que ayuda a identificar por qué ocurre el evento.
ID de servicio	El servicio que notificó el evento (si corresponde).
Nodo	El nodo que notificó el evento (si corresponde).
ID de unidad	La unidad que notificó el evento (si corresponde).
Hora del evento	La hora en la que ocurrió el evento.

Obtenga más información

Tipos de evento

Tipos de evento

El sistema informa de varios tipos de eventos, cada uno de los cuales es una operación que completó el sistema. Los eventos son rutinarios y normales, o bien eventos que requieren la atención del administrador. La columna Event Types en la página Event Log indica en qué parte del sistema se ha producido el evento.

El sistema no registra comandos de API de solo lectura en el registro de eventos.

En la siguiente lista, se describen los tipos de eventos que aparecen en el registro de eventos:

- **ApiEvent**

  Eventos que inicia un usuario a través de una API o una interfaz de usuario web que modifican la configuración.

- **BinAssignmentEvent**

  Eventos relacionados con la asignación de ubicaciones de datos. En esencia, las ubicaciones son contenedores que incluyen datos que se asignan en el clúster.

- **BinSyncEvent**

  Eventos del sistema relacionados con una reasignación de los datos entre los servicios de bloques.

- **BsCheckEvent**

  Eventos del sistema relacionados con las comprobaciones de servicios de bloques.

- **BsKillEvent**

  Eventos del sistema relacionados con las terminaciones de servicios de bloques.

- **BulkOpEvent**

  Eventos relacionados con operaciones realizadas en un volumen completo, como un backup, una restauración, una copia de Snapshot o un clon.

- **ClonEvent**

  Eventos relacionados con el clonado de volúmenes.

- **ClusterMasterEvent**

  Eventos que aparecen tras la inicialización del clúster o tras los cambios de configuración en el clúster, como la adición o la eliminación de nodos.

- **CsumEvent**

  Eventos relacionados con sumas de comprobación de datos no válidas en el disco.

- **DataEvent**

  Eventos relacionados con la lectura y la escritura de datos.

- **DbEvent**

  Eventos relacionados con la base de datos global que mantienen los nodos del conjunto en el clúster.

- **DriveEvent**

  Eventos relacionados con las operaciones de unidades.

- **EncryptionAtRestEvent**

Eventos relacionados con el proceso de cifrado en un clúster.

- **EnsembleEvent**

  Eventos relacionados con el aumento o la reducción del número de nodos en un conjunto.

- **FiberChannelEvent**

  Eventos relacionados con la configuración de los nodos y las conexiones con ellos.

- **GcEvent**

  Eventos relacionados con los procesos que se ejecutan cada 60 minutos para reclamar almacenamiento en las unidades de bloques. Este proceso también se conoce como recolección de basura.

- **IeEvent**

  Error interno del sistema.

- **InstallEvent**

  Eventos de instalación automática del software. El software se instala automáticamente en un nodo pendiente.

- **ISCSIEvent**

  Eventos relacionados con los problemas de iSCSI en el sistema.

- **LimitEvent**

  Eventos relacionados con el número de volúmenes o volúmenes virtuales en una cuenta o en el clúster que se acercan al máximo permitido.

- **MantenimientoModeEvent**

  Eventos relacionados con el modo de mantenimiento de los nodos, como deshabilitar el nodo.

- **NetworkEvent**

  Eventos relacionados con el estado de las redes virtuales.

- **PlatformHardwarwareEvent**

  Eventos relacionados con los problemas detectados en los dispositivos de hardware.

- **RemoteClusterEvent**

  Eventos relacionados con el emparejamiento de clústeres remotos.

- **PlaneerEvent**

  Eventos relacionados con las copias de Snapshot programadas.

- **ServiceEvent**

  Eventos relacionados con el estado de servicio del sistema.

- **SliceEvent**

  Eventos relacionados con el servidor de segmentos, como la eliminación de un volumen o una unidad de metadatos.

  Existen tres tipos de eventos de reasignación de segmentos, que incluyen información acerca del servicio al que se asigna un volumen:

  - voltear: cambiar el servicio primario a un nuevo servicio primario

    ```
    sliceID oldPrimaryServiceID->newPrimaryServiceID
    ```

  - mover: cambiar el servicio secundario a un nuevo servicio secundario

    ```
    sliceID {oldSecondaryServiceID(s)}->{newSecondaryServiceID(s)}
    ```

  - eliminar: eliminar un volumen de un conjunto de servicios

    ```
    sliceID {oldSecondaryServiceID(s)}
    ```

- **SnmpTrapEvent**

  Eventos relacionados con capturas SNMP.

- **StatEvent**

  Eventos relacionados con las estadísticas del sistema.

- **TsEvent**

  Eventos relacionados con el servicio de transporte del sistema.

- **Inesperado Exception**

  Eventos relacionados con las excepciones del sistema inesperadas.

- **UreEvent**

  Eventos relacionados con errores de lectura irrecuperables que se producen durante la lectura desde el dispositivo de almacenamiento.

- **VasaProviderEvent**

  Eventos relacionados con un proveedor de VASA (API de vSphere para el reconocimiento del almacenamiento).

Ver el estado de las tareas en ejecución

Puede ver el progreso y el estado de finalización de las tareas en ejecución de la interfaz

de usuario web que notifican los métodos API ListSyncJobs y ListBulkVolumeJobs. Puede acceder a la página Running Tasks desde la pestaña Reporting de la interfaz de usuario de Element.

En el caso de que haya un gran número de tareas, el sistema puede ponerlas en cola y ejecutarlas en lotes. En la página Running Tasks se muestran los servicios que se están sincronizando en ese momento. Cuando una tarea se completa, se reemplaza por la siguiente tarea de sincronización en la cola. Las tareas de sincronización pueden seguir apareciendo en la página Running Tasks hasta que no haya más tareas pendientes.

Los datos de las sincronizaciones de replicación de los volúmenes que se están replicando se pueden ver en la página Running Tasks del clúster que contiene el volumen de destino.

Ver las alertas del sistema

Puede ver las alertas para obtener información sobre errores del clúster en el sistema. Las alertas pueden tratarse de información, advertencias o errores, y son un buen indicador del funcionamiento del clúster. La mayoría de errores se resuelven automáticamente por sí mismos.

Puede usar el método API ListClusterFaults para automatizar la supervisión de alertas. De este modo podrá recibir notificaciones sobre todas las alertas que se produzcan.

1. En la interfaz de usuario de Element, seleccione **Reporting** > **Alerts**.

   El sistema actualiza las alertas de la página cada 30 segundos.

   Para cada evento, verá la siguiente información:

Elemento	Descripción
ID	ID único asociado con una alerta de clúster.
Gravedad	El grado de importancia de la alerta. Los posibles valores son los siguientes: • Warning: Un problema menor que podría requerir su atención pronto. Las actualizaciones del sistema todavía están permitidas. • Error: Un error que puede provocar la degradación del rendimiento o la pérdida de alta disponibilidad (ha). En general, los errores no deben afectar el servicio de otro modo. • Critical: Un error grave que afecta el servicio. El sistema no es capaz de atender las solicitudes de I/o de la API o el cliente. El funcionamiento en este estado podría provocar la pérdida potencial de datos. • BestPractice: No se utiliza una práctica recomendada de configuración del sistema.

Tipo	El componente al que afecta el fallo. Puede ser nodo, unidad, clúster, servicio o volumen.
Nodo	ID de nodo para el nodo al que hace referencia este error. Se incluye para los errores de nodo y de unidad; de lo contrario se establece como - (guion).
ID de unidad	ID de unidad para la unidad a la que hace referencia este error. Se incluye para los errores drive; de lo contrario se establece como - (guion).
Código de error	Código descriptivo que indica cuál es la causa del error.
Detalles	Una descripción del error con detalles adicionales.
Fecha	La fecha y la hora en la que se registró el error.

2. Haga clic en **Mostrar detalles** para ver una alerta individual y ver información sobre la alerta.
3. Para ver los detalles de todas las alertas de la página, haga clic en la columna Details.

   Una vez que el sistema resuelve una alerta, toda la información sobre la alerta, incluida la fecha en la que se solucionó, se traslada al área Resolved.

Obtenga más información

- códigos de error de clúster
- "Gestione el almacenamiento con la API de Element"

códigos de error de clúster

El sistema informa de un error o un estado que puede ser de su interés al generar un código de error, que se incluye en la página Alerts. Estos códigos ayudan a determinar en qué componente del sistema se generó la alerta y por qué se generó.

En la siguiente lista se describen los distintos tipos de códigos:

- **AutenticaciónServiceFault**

  El servicio de autenticación en uno o más nodos del clúster no funciona según lo esperado.

  Comuníquese con el soporte de NetApp para obtener ayuda.

- **Disponible VirtualNetworkIPAddressLow**

  El número de direcciones de red virtual en el bloque de direcciones IP es bajo.

  Para resolver esta falla, añada más direcciones IP al bloque de direcciones de red virtual.

- **BlockBlockClusterFull**

  No hay suficiente espacio libre de almacenamiento basado en bloques para admitir la pérdida de un solo nodo. Consulte el método API GetClusterFullThreshold para obtener detalles sobre los niveles de ocupación de los clústeres. Esta falla del clúster indica una de las siguientes condiciones:

  - Stage3Low (Advertencia): Se superó el umbral definido por el usuario. Ajuste la configuración del clúster lleno o añada más nodos.
  - Stage4Critical (error): No hay espacio suficiente para recuperar el sistema de un fallo de 1 nodo. No se permite la creación de volúmenes, snapshots y clones.
  - Stage5CompletelyConsumed (crítico)1; no se permiten escrituras ni nuevas conexiones iSCSI. Se mantendrán las conexiones iSCSI actuales. Las escrituras fallarán hasta que se añada más capacidad al clúster. Para resolver esta falla, purgue o elimine volúmenes o añada otro nodo de almacenamiento al clúster de almacenamiento.

- * BlocksDegraded*

  Los datos de bloques ya no se replican por completo debido a un fallo.

Gravedad	Descripción
Advertencia	Solo se puede acceder a dos copias completas de datos en bloques.
Error	Solo se puede acceder a una única copia completa de los datos en bloque.
Crítico	No se puede acceder a ninguna copia completa de los datos en bloque.

  Nota: el estado de aviso sólo puede ocurrir en un sistema de Triple Helix.

  Para resolver esta falla, restaure los nodos sin conexión o los servicios de bloques, o póngase en contacto con el soporte de NetApp para obtener ayuda.

- **BlockServiceTooFull**

  Un servicio de bloques está utilizando demasiado espacio.

  Para resolver esta falla, añada más capacidad aprovisionada.

- **BlockServiceUnhealthy**

  Se detectó que un servicio de bloques está en mal estado:

  - Gravedad = Advertencia: No se realiza ninguna acción. Este período de advertencia caducará en cTimeUntilBSIsKilledMSec=330000 milisegundos.
  - Gravedad = error: El sistema decomisiona automáticamente los datos y vuelve a replicar los datos en otras unidades en buen estado.
  - Severidad = crítico: Hay servicios de bloque con errores en varios nodos mayores o iguales al número de replicación (2 para Double Helix). Los datos no están disponibles y la sincronización de bandejas no finalizará. Compruebe si existen problemas de conectividad de red y errores de hardware. Si se han

producido errores en componentes de hardware específicos, habrá otros errores. El fallo se borrará cuando se pueda acceder al servicio de bloqueo o cuando se haya retirado el servicio.

- **RelojSkewExceedsFaultThreshold**

  El desfase de tiempo entre el maestro de clústeres y el nodo que presenta un token supera el umbral recomendado. El clúster de almacenamiento no puede corregir el desfase de hora entre los nodos automáticamente.

  Para resolver esta falla, use los servidores NTP internos a la red en lugar de los que vienen predeterminados en la instalación. Si usa un servidor NTP interno, comuníquese con el soporte de NetApp para obtener ayuda.

- **ClusterCannotSync**

  Hay una condición de falta de espacio y los datos en las unidades de almacenamiento en bloque desconectadas no pueden sincronizarse con las unidades que siguen activas.

  Para resolver esta falla, añada más almacenamiento.

- **ClusterFull**

  No hay más espacio de almacenamiento libre en el clúster de almacenamiento.

  Para resolver esta falla, añada más almacenamiento.

- **ClusterIOPSAreOverProvisioned**

  Hay un sobreaprovisionamiento de IOPS en el clúster. La suma de todas las IOPS de calidad de servicio mínima es mayor que el número de IOPS que se espera del clúster. No puede mantenerse una calidad de servicio mínima para todos los volúmenes en simultáneo.

  Para resolver este problema, reduzca la configuración mínima de IOPS de calidad de servicio para los volúmenes.

- **DisableDriveSecurityFailed**

  El clúster no se configura para habilitar la seguridad de la unidad (cifrado en reposo), pero al menos una unidad tiene la seguridad de la unidad habilitada, lo cual significa que se deshabilita la seguridad de la unidad en esas unidades. Este fallo se registra con la gravedad "'Advertencia'".

  Para resolver esta falla, compruebe los detalles de la falla por el motivo por el que no se pudo deshabilitar la seguridad de la unidad. Los posibles motivos son:

  - No se pudo adquirir la clave de cifrado, investigue el problema de acceso a la clave o al servidor de claves externo.
  - Se produjo un error en la operación de desactivación de la unidad, determine si es posible que se haya adquirido una clave incorrecta. Si ninguno de estos son el motivo del fallo, es posible que sea necesario sustituir la unidad.

  Es posible intentar recuperar una unidad que no deshabilita la seguridad correctamente incluso cuando se proporciona la clave de autenticación correcta. Para realizar esta operación, quite las unidades del sistema moverlas a Available, ejecute un borrado seguro en la unidad y vuelva a moverlas a Active.

- **DesconecttedClusterPair**

Una pareja de clústeres está desconectada o configurada incorrectamente. Compruebe la conectividad de red entre los clústeres.

- **DisconnectedRemoteNode**

  Un nodo remoto está desconectado o configurado incorrectamente. Compruebe la conectividad de red entre los nodos.

- **DesconectadoSnapMirrorEndpoint**

  Un extremo de SnapMirror remoto está desconectado o configurado incorrectamente. Compruebe la conectividad de red entre el clúster y el SnapMirrorEndpoint remoto.

- **Disponible**

  Hay una o más unidades disponibles en el clúster. En general, todos los clústeres deben tener todas las unidades añadidas, y ninguna debe estar en estado disponible. Si esta falla aparece de forma inesperada, comuníquese con el soporte de NetApp.

  Para resolver esta falla, añada las unidades disponibles al clúster de almacenamiento.

- **DriveFailed**

  El clúster devuelve esta falla cuando una o más unidades han fallado, lo cual indica una de las siguientes condiciones:

  - El administrador de unidades no puede acceder a la unidad.
  - El servicio de segmentos o bloques se ha producido un error demasiadas veces, probablemente debido a fallos de lectura o escritura de la unidad y no se puede reiniciar.
  - Falta la unidad.
  - No se puede acceder al servicio maestro del nodo (todas las unidades del nodo se consideran ausentes o con errores).
  - La unidad está bloqueada y no puede adquirirse la clave de autenticación de la unidad.
  - La unidad se bloqueó y la operación de desbloqueo falla. Para resolver este problema:
  - Compruebe la conectividad de red del nodo.
  - Sustituya la unidad.
  - Asegúrese de que la clave de autenticación esté disponible.

- **HealthdriveFault**

  Se produjo un error en la comprobación DEL estado INTELIGENTE de una unidad y, como resultado, se reducen las funciones de la unidad. Existe un nivel de gravedad crítico para esta falla:

  - Unidad con serie: <serial number> en ranura: <node slot> <drive slot> no superó la comprobación de estado general INTELIGENTE. Para resolver esta falla, reemplace la unidad.

- **DriveWeFault**

  La vida útil restante de una unidad cayó por debajo del umbral permitido, pero la unidad sigue funcionando.existen dos niveles de gravedad posibles para este fallo: Crucial y Advertencia:

  - Unidad con serie: <serial number> en ranura: <node slot> <drive slot> tiene niveles de desgaste críticos.

- Unidad con serie: <serial number> en ranura: <node slot> <drive slot> tiene bajas reservas de desgaste. Para resolver esta falla, reemplace la unidad cuanto antes.

- **DuplicateClusterMasterCandidates**

  Se detectó más de un candidato maestro de clúster de almacenamiento. Comuníquese con el soporte de NetApp para obtener ayuda.

- **EnableDriveSecurityFailed**

  El clúster se configura para requerir seguridad de unidades (cifrado en reposo), pero la seguridad de unidades no se pudo habilitar en al menos una unidad. Este fallo se registra con la gravedad "'Advertencia'".

  Para resolver esta falla, compruebe los detalles de la falla por el motivo por el que no se pudo habilitar la seguridad de la unidad. Los posibles motivos son:

  - No se pudo adquirir la clave de cifrado, investigue el problema de acceso a la clave o al servidor de claves externo.
  - Se produjo un error en la operación de habilitación en la unidad, para determinar si podría haberse adquirido una clave incorrecta. Si ninguno de estos son el motivo del fallo, es posible que sea necesario sustituir la unidad.

  Es posible intentar recuperar una unidad que no habilita la seguridad correctamente incluso cuando se proporciona la clave de autenticación correcta. Para realizar esta operación, quite las unidades del sistema moverlas a Available, ejecute un borrado seguro en la unidad y vuelva a moverlas a Active.

- * Ensembergraded*

  Se perdió la alimentación de energía o la conectividad de red en uno o varios de los nodos del conjunto.

  Para resolver esta falla, restaure la alimentación o la conectividad de red.

- **excepción**

  Una falla que no es de rutina. Estas fallas no se borran automáticamente de la cola de fallas. Comuníquese con el soporte de NetApp para obtener ayuda.

- **FailedSpaceTooFull**

  Un servicio de bloques no responde a las solicitudes de escritura de datos. Esto provoca que el servicio de segmentos se quede sin espacio para almacenar escrituras fallidas.

  Para resolver esto, restaure la funcionalidad de servicios de bloques de modo que las escrituras puedan continuar normalmente y que el espacio con fallas se vacíe en el servicio de segmentos.

- **FanSensor**

  Un sensor de ventilador presenta una falla o está ausente.

  Para resolver esta falla, reemplace cualquier hardware con errores.

- **FiberChannelAccessDegraded**

  Un nodo Fibre Channel no responde a otros nodos en el clúster de almacenamiento a través de su dirección IP de almacenamiento durante un período. En este estado, se considera que el nodo no

responde y se genera una falla en el clúster. Compruebe la conectividad de red.

- **FiberChannelAccessUnavailable**

  Ninguno de los nodos Fibre Channel responde. Se muestran los ID de los nodos. Compruebe la conectividad de red.

- **FiberChannelActiveIxL**

  El número de Nexus IXL se acerca al límite admitido de 8000 sesiones activas por nodo Fibre Channel.

  - El límite de mejores prácticas es de 5500.
  - El límite de advertencia es 7500.
  - El límite máximo (no forzado) es 8192. Para resolver esta falla, reduzca el número de Nexus IXL por debajo del límite de mejores prácticas de 5500.

- **FiberChannelConfig**

  Esta falla del clúster indica una de las siguientes condiciones:

  - Hay un puerto de Fibre Channel no esperado en una ranura PCI.
  - Hay un modelo de adaptador de bus de host de Fibre Channel no esperado.
  - Hay un problema con el firmware de un adaptador de bus de host de Fibre Channel.
  - Un puerto de Fibre Channel no está en línea.
  - Hay un problema persistente en la configuración de traspaso de Fibre Channel. Comuníquese con el soporte de NetApp para obtener ayuda.

- **FiberChannelIOPS**

  El número total de IOPS está cerca del límite de IOPS para los nodos Fibre Channel del clúster. Los límites son:

  - FC0025: Límite de 450 000 IOPS con un tamaño de bloque de 4 KB por nodo Fibre Channel.
  - FCN001: Límite de 625K OPS a un tamaño de bloque de 4K por nodo Fibre Channel. Para resolver esta falla, equilibre la carga en todos los nodos Fibre Channel disponibles.

- **FiberChannelStaticIxL**

  El número de Nexus IXL se acerca al límite admitido de 16000 sesiones estáticas por nodo Fibre Channel.

  - El límite de mejores prácticas es de 11000.
  - El límite de advertencia es 15000.
  - El límite máximo (obligatorio) es 16384. Para resolver esta falla, reduzca el número de Nexus IXL por debajo del límite de mejores prácticas de 11000.

- **FileSystemCapacidadLow**

  No hay espacio suficiente en uno de los sistemas de archivos.

  Para resolver esta falla, añada más capacidad al sistema de archivos.

- **FipsDrivesdiscordancia**

  Se insertó de forma física una unidad que no es FIPS en un nodo de almacenamiento compatible con

FIPS o se insertó de forma física una unidad FIPS en un nodo de almacenamiento que no es FIPS. Se genera un solo error por nodo y se enumera todas las unidades afectadas.

Para resolver esta falla, quite o sustituya la unidad o las unidades con discrepancias.

- **FipsDrivesOutOfCompliance**

  El sistema detectó que se deshabilitó el cifrado en reposo después de habilitar la función FIPS Drives. Esta falla también se genera cuando la función de unidades FIPS está habilitada y hay un nodo o una unidad no FIPS en el clúster de almacenamiento.

  Para resolver esta falla, habilite el cifrado en reposo o elimine el hardware que no es FIPS del clúster de almacenamiento.

- **FipsSelfTestFailure**

  El subsistema FIPS detectó un fallo durante la autoprueba.

  Comuníquese con el soporte de NetApp para obtener ayuda.

- **HardwareConfigdiscordancia**

  Esta falla del clúster indica una de las siguientes condiciones:

  - La configuración no coincide con la definición del nodo.
  - El tamaño de unidad para este tipo de nodo es incorrecto.
  - Se detectó una unidad no compatible. Un posible motivo es que la versión de elemento instalada no reconoce esta unidad. Recomienda actualizar el software Element en este nodo.
  - Hay un error de coincidencia en el firmware de la unidad.
  - El estado de capacidad de cifrado de la unidad no coincide con el nodo. Comuníquese con el soporte de NetApp para obtener ayuda.

- **IdPCertificateExpiración**

  El certificado SSL del proveedor de servicios del clúster para su uso con un proveedor de identidades (IDP) de terceros está a punto de expirar o ya ha caducado. Este fallo utiliza las siguientes gravedades en función de la urgencia:

Gravedad	Descripción
Advertencia	El certificado caduca dentro de los 30 días.
Error	El certificado caduca dentro de los 7 días.
Crítico	El certificado caduca en un plazo de 3 días o ya ha caducado.

  Para resolver esta falla, actualice el certificado SSL antes de que caduque. Utilice el método API UpdateIdpConfiguration con `refreshCertificateExpirationTime=true` Para proporcionar el certificado SSL actualizado.

- **InconstentBondModes**

Los modos de enlace en el dispositivo de VLAN no están presentes. Esta falla muestra el modo de enlace esperado y el modo de enlace actualmente en uso.

- **InconstentInterfaceConfiguration**

  La configuración de la interfaz es inconsistente.

  Para resolver esta falla, asegúrese de que las interfaces de nodos en el clúster de almacenamiento estén configuradas de manera consistente.

- * InconstentMtus*

  Esta falla del clúster indica una de las siguientes condiciones:

  - Bond1G mismatch: Se detectaron varias MTU inconsistentes en interfaces Bond1G.
  - Bond10G mismatch: Se detectaron varias MTU inconsistentes en interfaces Bond10G. Esta falla muestra los nodos en cuestión junto con el valor de MTU asociado.

- **InconstentRoutingRules**

  Las reglas de enrutamiento de esta interfaz son inconsistentes.

- * InconstentSubnetMasks*

  La máscara de red en el dispositivo de VLAN no coincide con la máscara de red registrada internamente para la VLAN. Esta falla muestra la máscara de red esperada y la máscara de red actualmente en uso.

- * IncorrectBondPortCount*

  El número de puertos de enlace es incorrecto.

- **InvalidConfigdFiberChannelNodeCount**

  Una de las dos conexiones de nodos Fibre Channel esperadas está degradada. Esta falla aparece cuando se conecta un solo nodo Fibre Channel.

  Para resolver esta falla, compruebe la conectividad de red y el cableado de red del clúster y compruebe los servicios con errores. Si no hay problemas de red o servicio, comuníquese con el soporte de NetApp para obtener el reemplazo de un nodo Fibre Channel.

- **IrqBalanceFailed**

  Se produjo una excepción al intentar balancear las interrupciones.

  Comuníquese con el soporte de NetApp para obtener ayuda.

- **KmipCertificateFault**
  - El certificado de la entidad de certificación raíz (CA) está cerca de su vencimiento.

    Para resolver este fallo, adquiera un nuevo certificado de la CA raíz con una fecha de caducidad de al menos 30 días y utilice ModifyKeyServerKmip para proporcionar el certificado de CA raíz actualizado.

  - El certificado de cliente está a punto de expirar.

    Para resolver esta falla, cree una nueva CSR con GetClientCertificateSigningRequest, asegúrese de

que la nueva fecha de caducidad se agota al menos 30 días y utilice ModifyKeyServerKmip para reemplazar el certificado de cliente KMIP que caduca con el nuevo certificado.

- El certificado de la entidad de certificación raíz (CA) ha caducado.

  Para resolver este fallo, adquiera un nuevo certificado de la CA raíz con una fecha de caducidad de al menos 30 días y utilice ModifyKeyServerKmip para proporcionar el certificado de CA raíz actualizado.

- El certificado de cliente ha caducado.

  Para resolver esta falla, cree una nueva CSR con GetClientCertificateSigningRequest, asegúrese de que la nueva fecha de caducidad se agota al menos 30 días y utilice ModifyKeyServerKmip para reemplazar el certificado de cliente KMIP caducado con el nuevo certificado.

- Error de certificado de entidad de certificación raíz (CA).

  Para resolver esta falla, compruebe que se proporcionó el certificado correcto y, si fuera necesario, vuelva a adquirir el certificado de la CA raíz. Utilice ModifyKeyServerKmip para instalar el certificado de cliente KMIP correcto.

- Error del certificado de cliente.

  Para resolver esta falla, compruebe que esté instalado el certificado de cliente KMIP correcto. La CA raíz del certificado de cliente debe instalarse en el EKS. Utilice ModifyKeyServerKmip para instalar el certificado de cliente KMIP correcto.

- **KmipServerFault**
  - Error de conexión

    Para resolver esta falla, compruebe que el servidor de claves externo esté vivo y sea posible acceder a él a través de la red. Utilice TestKeyServerKimp y TestKeyProviderKmip para probar su conexión.

  - Error de autenticación

    Para resolver esta falla, compruebe que se estén utilizando los certificados de cliente KMIP y de CA raíz correctos, y que coincidan las claves privadas y el certificado de cliente KMIP.

  - Error del servidor

    Para resolver esta falla, compruebe los detalles del error. Es posible que sea necesario solucionar los problemas en el servidor de claves externo según el error que se devuelve.

- **MemoryEccThreshold**

  Se ha detectado un gran número de errores ECC corregibles o no corregibles. Este fallo utiliza las siguientes gravedades en función de la urgencia:

Evento	Gravedad	Descripción
Un único módulo DIMM cErrorCount llega a cDimmcorrectableErrWarnThreshold.	Advertencia	Errores corregibles de memoria ECC por encima del umbral en DIMM: <Processor> <DIMM Slot>

Un único DIMM cErrorCount permanece por encima de cDimmcorrectableErrWarnThreshold hasta que el temporizador ciErrorFaultTimer caduca para el DIMM.	Error	Errores corregibles de memoria ECC por encima del umbral en DIMM: <Processor> <DIMM>
Un controlador de memoria informa cErrorCount encima de cMemCtlrcorrectableErrWarnThreshold y se especifica cMemCtlrcorrectableErrWarnDuration.	Advertencia	Errores corregibles de memoria ECC por encima del umbral en el controlador de memoria: <Processor> <Memory Controller>
Un controlador de memoria informa cErrorCount sobre cMemCtlrcorrectableErrWarnThreshold hasta que cErrorFaultTimer caduca para el controlador de memoria.	Error	Errores corregibles de memoria ECC por encima del umbral en DIMM: <Processor> <DIMM>
Un módulo DIMM único informa de un uErrorCount por encima de cero, pero inferior a cDimmUncorrectTaberreErrFaultThreshold.	Advertencia	Errores de memoria ECC no corregibles detectados en el módulo DIMM: <Processor> <DIMM Slot>
Un módulo DIMM único informa de un uErrorCount de al menos cmimUncorrecttableErrFaultThreshold.	Error	Errores de memoria ECC no corregibles detectados en el módulo DIMM: <Processor> <DIMM Slot>
Un controlador de memoria informa de un uErrorCount por encima de cero, pero menor que cMemctlenseUncorrecttableErrFaultThreshold.	Advertencia	Errores de memoria ECC no corregibles detectados en el controlador de memoria: <Processor> <Memory Controller>
Un controlador de memoria informa de un uErrorCount de al menos cMemctlrUncorrecttableErrFaultThreshold.	Error	Errores de memoria ECC no corregibles detectados en el controlador de memoria: <Processor> <Memory Controller>

Para resolver esta falla, comuníquese con el soporte de NetApp para obtener ayuda.

- **MemyUsageThreshold**

  El uso de memoria está por encima de lo normal. Este fallo utiliza las siguientes gravedades en función de la urgencia:

Consulte el encabezado **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 se ha consumido por completo.

Para resolver esta falla, comuníquese con el soporte de NetApp para obtener ayuda.

- **MetadataClusterFull**

  No hay suficiente espacio libre de almacenamiento de metadatos para admitir la pérdida de un solo nodo. Consulte el método API GetClusterFullThreshold para obtener detalles sobre los niveles de ocupación de los clústeres. Esta falla del clúster indica una de las siguientes condiciones:

  - Stage3Low (Advertencia): Se superó el umbral definido por el usuario. Ajuste la configuración del clúster lleno o añada más nodos.
  - Stage4Critical (error): No hay espacio suficiente para recuperar el sistema de un fallo de 1 nodo. No se permite la creación de volúmenes, snapshots y clones.
  - Stage5CompletelyConsumed (crítico)1; no se permiten escrituras ni nuevas conexiones iSCSI. Se mantendrán las conexiones iSCSI actuales. Las escrituras fallarán hasta que se añada más capacidad al clúster. Purgue o elimine datos o añada más nodos. Para resolver esta falla, purgue o elimine volúmenes o añada otro nodo de almacenamiento al clúster de almacenamiento.
- **MtuCheckFailure**

  Un dispositivo de red no tiene configurado el tamaño de MTU correcto.

  Para resolver esta falla, asegúrese de que todas las interfaces de red y puertos del switch tengan configuradas tramas gigantes (MTU de hasta 9000 bytes de tamaño).
- **NetworkConfig**

  Esta falla del clúster indica una de las siguientes condiciones:

  - No hay una interfaz esperada.
  - Hay una interfaz duplicada.
  - Una interfaz configurada está inactiva.
  - Se requiere reiniciar la red. Comuníquese con el soporte de NetApp para obtener ayuda.
- **NoAvailableVirtualNetworkIPAddresses**

  No hay direcciones de red virtual disponibles en el bloque de direcciones IP.

  - VirtualNetworkID # TAG(#) no tiene direcciones IP de almacenamiento disponibles. No es posible agregar nodos adicionales al clúster. Para resolver esta falla, añada más direcciones IP al bloque de direcciones de red virtual.

- **NodeHardwarFault (falla de interfaz de red <name> o el cable está desconectado)**

  Una interfaz de red está desconectada o el cable está desenchufado.

  Para resolver esta falla, compruebe la conectividad de red de los nodos.

- **NodeHardwarfault (el estado de capacidad de cifrado de la unidad coincide con el estado de capacidad de cifrado del nodo para la unidad en la ranura <node slot> <drive slot>)**

  Una unidad no coincide con las funcionalidades de cifrado del nodo de almacenamiento en el que se instala.

- **NodeHardwareFault (error de tamaño de unidad <drive type> <actual size> para la unidad en la ranura <node slot> <drive slot> para este tipo de nodo - <expected size> esperado)**

  Un nodo de almacenamiento contiene una unidad que tiene un tamaño incorrecto para este nodo.

- **NodeHardwareFault (unidad no compatible detectada en la ranura <node slot> <drive slot>; las estadísticas de la unidad y la información de estado no estarán disponibles)**

  Un nodo de almacenamiento contiene una unidad que no es compatible.

- **NodeHardwareFault (la unidad de la ranura <node slot> <drive slot> debe utilizar la versión de firmware <expected version>, pero utiliza la versión no compatible <actual version>)**

  Un nodo de almacenamiento contiene una unidad que ejecuta una versión de firmware no compatible.

- * NodeMaintenanceMode*

  Se ha colocado un nodo en modo de mantenimiento. Este fallo utiliza las siguientes gravedades en función de la urgencia:

Gravedad	Descripción
Advertencia	Indica que el nodo aún está en modo de mantenimiento.
Error	Indica que el modo de mantenimiento no se ha desactivado, lo más probable es que se deba a stabys activos o con errores.

  Para resolver esta falla, deshabilite el modo de mantenimiento una vez que finalice el mantenimiento. Si el fallo del nivel de error persiste, comuníquese con el soporte de NetApp para obtener ayuda.

- **NodeOffline**

  El software Element no puede comunicarse con el nodo especificado. Compruebe la conectividad de red.

- **NotUsingLACPBondMode**

  El modo de enlace LACP no está configurado.

  Para resolver esta falla, use el enlace LACP cuando se implementan nodos de almacenamiento; es posible que los clientes experimenten problemas de rendimiento si LACP no está habilitado y configurado

correctamente.

- **NtpServerUnalcanzable**

  El clúster de almacenamiento no puede comunicarse con los servidores NTP especificados.

  Para resolver esta falla, compruebe la configuración del servidor NTP, de la red y del firewall.

- **NtpTimeNotInSync**

  La diferencia entre el tiempo del clúster de almacenamiento y el tiempo del servidor NTP es demasiado amplia. El clúster de almacenamiento no puede corregir esta diferencia automáticamente.

  Para resolver esta falla, use los servidores NTP internos a la red en lugar de los que vienen predeterminados en la instalación. Si usa los servidores NTP internos y el problema persiste, comuníquese con el soporte de NetApp para obtener ayuda.

- **NvramDeviceStatus**

  Un dispositivo NVRAM presenta un error, está fallando o ya falló. Este fallo tiene las siguientes gravedades:

Gravedad	Descripción
Advertencia	El hardware ha detectado una advertencia. Esta condición puede ser transitoria, como una advertencia de temperatura. • NvmLifetimeerror • NvmLifetimeStatus • EnergySourceLifetimeStatus • EnergySourceTemperatureStatus • WarningThresholdExceeded
Error	El hardware ha detectado un error o estado crítico. El maestro de clústeres intenta quitar la unidad de segmentos de la operación (esto genera un evento de eliminación de la unidad). Si no hay servicios de segmentos secundarios disponibles, no se eliminará la unidad. Errores devueltos además de los errores de nivel de advertencia: • El punto de montaje del dispositivo NVRAM no existe. • La partición del dispositivo NVRAM no existe. • Existe una partición del dispositivo NVRAM, pero no está montada.

Crítico	El hardware ha detectado un error o estado crítico. El maestro de clústeres intenta quitar la unidad de segmentos de la operación (esto genera un evento de eliminación de la unidad). Si no hay servicios de segmentos secundarios disponibles, no se eliminará la unidad. • Persistente perdido • ArmStatusSaveNArmed • CsaveStatuserror

Sustituya cualquier hardware con fallos en el nodo. Si esto no se resuelve el problema, comuníquese con el soporte de NetApp para obtener ayuda.

- **PowerSupplyError**

  Esta falla del clúster indica una de las siguientes condiciones:

  - No hay un suministro de alimentación.
  - Se produjo un error de suministro de alimentación.
  - La entrada de un suministro de alimentación es nula o está fuera de rango. Para resolver esta falla, compruebe que se suministra alimentación redundante a todos los nodos. Comuníquese con el soporte de NetApp para obtener ayuda.

- **AprovisionadoSpaceTooFull**

  La capacidad general aprovisionada del clúster está demasiado llena.

  Para resolver esta falla, añada más espacio aprovisionado, o elimine y purgue los volúmenes.

- **RemoteRepAsyncDelayExceeded**

  Se superó la demora de replicación asíncrona configurada. Compruebe la conectividad de red entre clústeres.

- **RemoteRepClusterFull**

  Los volúmenes pusieron en pausa la replicación remota porque el clúster de almacenamiento de destino está demasiado lleno.

  Para resolver esta falla, libere un poco de espacio en el clúster de almacenamiento de destino.

- **RemoteRepSnapshotClusterFull**

  Los volúmenes pusieron en pausa la replicación remota de copias de Snapshot porque el clúster de almacenamiento de destino está demasiado lleno.

  Para resolver esta falla, libere un poco de espacio en el clúster de almacenamiento de destino.

- **RemoteRepSnapshotsExceedLimit**

  Los volúmenes pusieron en pausa la replicación remota de copias de Snapshot porque el volumen del clúster de almacenamiento de destino superó su límite de copias de Snapshot.

Para resolver esta falla, aumente el límite de snapshots en el clúster de almacenamiento de destino.

- * Error de Acción de Ugenera*

  Ocurrió un error en la ejecución de una o más actividades programadas.

  La falla se borra si la actividad programada se vuelve a ejecutar, esta vez, correctamente, si la actividad programada se elimina o si la actividad se pone en pausa y luego se reanuda.

- **SensorReadingFailed**

  La autoprueba de la controladora de gestión de placa base (BMC) produjo un error o un sensor no pudo comunicarse con la BMC.

  Comuníquese con el soporte de NetApp para obtener ayuda.

- **ServiceNotRunning**

  Un servicio requerido no está en ejecución.

  Comuníquese con el soporte de NetApp para obtener ayuda.

- **SliceServiceTooFull**

  Un servicio de segmentos tiene asignada muy poca capacidad aprovisionada.

  Para resolver esta falla, añada más capacidad aprovisionada.

- **SliceServiceUnhealthy**

  El sistema detectó que un servicio de segmentos está en estado incorrecto y lo decomisiona automáticamente.

  - Gravedad = Advertencia: No se realiza ninguna acción. Este período de aviso caducará en 6 minutos.
  - Gravedad = error: El sistema decomisiona automáticamente los datos y vuelve a replicar los datos en otras unidades en buen estado. Compruebe si existen problemas de conectividad de red y errores de hardware. Si se han producido errores en componentes de hardware específicos, habrá otros errores. El fallo se borrará cuando se pueda acceder al servicio de cortes o cuando se haya retirado el servicio.

- **SshEnabled**

  El servicio SSH está habilitado en uno o más nodos del clúster de almacenamiento.

  Para resolver esta falla, deshabilite el servicio SSH en los nodos correspondientes o comuníquese con el soporte de NetApp para obtener ayuda.

- **SslCertificateExpiración**

  El certificado SSL asociado con este nodo está cerca de su vencimiento o ha caducado. Este fallo utiliza las siguientes gravedades en función de la urgencia:

Gravedad	Descripción
Advertencia	El certificado caduca dentro de los 30 días.

Error	El certificado caduca dentro de los 7 días.
Crítico	El certificado caduca en un plazo de 3 días o ya ha caducado.

Para resolver esta falla, reemplace el certificado SSL por uno nuevo. Si es necesario, comuníquese con el soporte de NetApp para obtener ayuda.

- **StrandedCapacity**

  Un solo nodo representa más de la mitad de la capacidad de un clúster de almacenamiento.

  Para mantener la redundancia de datos, el sistema reduce la capacidad del nodo más grande de manera que parte de su capacidad de bloque se quede sin utilizar (no se utiliza).

  Para resolver esta falla, añada más unidades a los nodos de almacenamiento existentes o añada nodos de almacenamiento al clúster.

- **Sensor de temperatura**

  Un sensor de temperatura informa de temperaturas más altas que las normales. Esta falla puede activarse en conjunto con fallas de tipo powerSupplyError o fanSensor.

  Para resolver esta falla, compruebe que el flujo de aire no esté obstruido cerca del clúster de almacenamiento. Si es necesario, comuníquese con el soporte de NetApp para obtener ayuda.

- **actualización**

  Hay una actualización en curso desde hace más de 24 horas.

  Para resolver esta falla, reanude la actualización o comuníquese con el soporte de NetApp para obtener ayuda.

- **UnresponveService**

  Un servicio ha dejado de responder.

  Comuníquese con el soporte de NetApp para obtener ayuda.

- **VirtualNetworkConfig**

  Esta falla del clúster indica una de las siguientes condiciones:

  - No hay una interfaz presente.
  - La interfaz tiene un espacio de nombres incorrecto.
  - Hay una máscara de red incorrecta.
  - Hay una dirección IP incorrecta.
  - Una interfaz no está en funcionamiento.
  - Hay una interfaz superflua en un nodo. Comuníquese con el soporte de NetApp para obtener ayuda.

- **VolumesDegraded**

Los volúmenes secundarios aún se están replicando y sincronizando. El mensaje se borra al finalizar la sincronización.

- **VolumesOffline**

  Uno o más volúmenes del clúster de almacenamiento están fuera de línea. El fallo **volumeDegraded** también estará presente.

  Comuníquese con el soporte de NetApp para obtener ayuda.

Ver la actividad de rendimiento del nodo

La actividad de rendimiento de cada nodo se puede ver en formato de gráfico. Esta información proporciona estadísticas en tiempo real para las operaciones de I/o de lectura/escritura por segundo (IOPS) de CPU y en cada unidad del nodo. El gráfico de uso se actualiza cada cinco segundos y el gráfico de estadísticas de unidad se actualiza cada diez segundos.

1. Haga clic en **Cluster** > **Nodes**.
2. Haga clic en **acciones** para el nodo que desea ver.
3. Haga clic en **Ver detalles**.

Puede ver momentos específicos en los gráficos de líneas y barras colocando el cursor sobre la línea o la barra.

Ver el rendimiento del volumen

Puede ver información detallada del 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 puede usar filtros de la información según determinados criterios.

Puede 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 elige Never, se deshabilita la actualización automática de página.

Puede volver a activar la actualización automática haciendo clic en **Activar la actualización automática**.

1. En la interfaz de usuario de Element, seleccione **Reporting** > **Volume Performance**.
2. En la lista de volúmenes, haga clic en el icono Actions de un volumen.
3. Haga clic en **Ver detalles**.

   Aparecerá una bandeja en la parte inferior de la página 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 y gráficos de rendimiento del volumen.

Obtenga más información

Detalles de rendimiento de volumen

Detalles de rendimiento de volumen

Las estadísticas de rendimiento de los volúmenes se pueden ver en la página Volume Performance de la pestaña Reporting en la interfaz de usuario de Element.

La lista siguiente describe los detalles que tienen a su disposición:

- **ID**

  El ID que genera el sistema para el volumen.

- **Nombre**

  El nombre que se le dio al volumen cuando se creó.

- **Cuenta**

  El nombre de la cuenta asignada al volumen.

- **Grupos de acceso**

  El nombre del grupo o los grupos de acceso de volúmenes a los que pertenece el volumen.

- **Utilización de volumen**

  Un valor de porcentaje que describe la cantidad del volumen que está usando el cliente.

  Los posibles valores son los siguientes:

  - 0 = el cliente no usa el volumen
  - 100 = el cliente usa el máximo
  - >100 = el cliente está utilizando la ráfaga

- **IOPS total**

  El número total de IOPS (lectura y escritura) que se está ejecutando en el volumen.

- **Leer IOPS**

  El número total de IOPS de lectura que se está ejecutando en el volumen.

- **Escribir IOPS**

  El número total de IOPS de escritura que se está ejecutando en el volumen.

- **Rendimiento total**

  La cantidad total de rendimiento (lectura y escritura) que se está ejecutando en el volumen.

- **Rendimiento de lectura**

La cantidad total de rendimiento de lectura que se está ejecutando en el volumen.

- **Grabación**

  La cantidad total de rendimiento de escritura que se está ejecutando en el volumen.

- **Latencia total**

  El tiempo medio, en microsegundos, para completar operaciones de lectura y escritura en un volumen.

- **Latencia de lectura**

  El tiempo medio, en microsegundos, para completar operaciones de lectura del volumen en los últimos 500 milisegundos.

- **Latencia de escritura**

  El tiempo medio, en microsegundos, para completar operaciones de escritura a un volumen en los últimos 500 milisegundos.

- **Profundidad de cola**

  Número de operaciones de lectura y escritura pendientes en el volumen.

- **Tamaño medio de E/S**

  Tamaño promedio en bytes de I/o reciente en el volumen en los últimos 500 milisegundos.

Ver sesiones iSCSI

Es posible ver las sesiones iSCSI que están conectadas al clúster. Puede filtrar la información para que incluya solo las sesiones que desea.

1. En la interfaz de usuario de Element, seleccione **Reporting** > **iSCSI Sessions**.
2. Para ver los campos de criterios de filtro, haga clic en **filtro**.

Obtenga más información

Detalles de la sesión iSCSI

Detalles de la sesión iSCSI

Es posible ver información sobre las sesiones iSCSI que están conectadas al clúster.

En la lista siguiente se describe la información que se puede encontrar acerca de las sesiones iSCSI:

- **Nodo**

  El nodo que aloja la partición de metadatos principal del volumen.

- **Cuenta**

  El nombre de la cuenta a la que pertenece el volumen. Si el valor está vacío, se muestra un guion (-).

- **Volumen**

  El nombre del volumen identificado en el nodo.

- **ID de volumen**

  El ID del volumen asociado con el IQN de destino.

- **ID de iniciador**

  Un ID que genera el sistema para el iniciador.

- **Alias del iniciador**

  Un nombre opcional para el iniciador que facilite encontrar el iniciador cuando la lista es larga.

- **IP de Initator**

  La dirección IP del extremo que inicia la sesión.

- **IQN del iniciador**

  El IQN del extremo que inicia la sesión.

- **IP de destino**

  La dirección IP del nodo donde se aloja el volumen.

- **IQN objetivo**

  El IQN del volumen.

- **Creado el**

  La fecha en la que se estableció la sesión.

Consulte las sesiones Fibre Channel

Es posible ver las sesiones Fibre Channel (FC) que están conectadas al clúster. Puede filtrar la información para que incluya únicamente las conexiones que desea que aparezcan en la ventana.

1. En la interfaz de usuario de Element, seleccione **Reporting** > **FC Sessions**.
2. Para ver los campos de criterios de filtro, haga clic en **filtro**.

Obtenga más información

Detalles de la sesión Fibre Channel

Detalles de la sesión Fibre Channel

Se proporciona información sobre las sesiones activas de Fibre Channel (FC) que están conectadas al clúster.

En la lista siguiente se describe la información que puede encontrar acerca de las sesiones FC conectadas al clúster:

- **ID de nodo**

  El nodo que aloja la sesión de la conexión.

- **Nombre de nodo**

  El nombre del nodo que genera el sistema.

- **ID de iniciador**

  Un ID que genera el sistema para el iniciador.

- **WWPN del iniciador**

  El nombre de puerto que se inicia a nivel mundial.

- **Alias del iniciador**

  Un nombre opcional para el iniciador que facilite encontrar el iniciador cuando la lista es larga.

- **WWPN de destino**

  El nombre de puerto objetivo a nivel mundial.

- **Grupo de acceso por volumen**

  El nombre del grupo de acceso de volúmenes al que pertenece la sesión.

- **ID de grupo de acceso de volumen**

  El ID que genera el sistema para el grupo de acceso.

Solucione problemas de unidades

Una unidad de estado sólido (SSD) con fallos se puede sustituir con una unidad de reemplazo. Las unidades SSD de los nodos de almacenamiento SolidFire se pueden intercambiar en caliente. Si sospecha que una unidad SSD puede tener errores, póngase en contacto con el soporte de NetApp para verificar el error y le guiaremos por el procedimiento de resolución de problemas adecuado. El soporte de NetApp también trabaja con usted para obtener una unidad de reemplazo de acuerdo con su acuerdo de nivel de servicio.

Cómo se puede cambiar en este caso esto significa que es posible quitar una unidad con error de un nodo activo y reemplazarla por una nueva unidad SSD de NetApp. No se recomienda quitar unidades sin errores en un clúster activo.

Debe mantener las piezas de repuesto que sugiere el soporte de NetApp para poder sustituir inmediatamente la unidad si falla.

Para realizar pruebas, si simula un error en una unidad al extraer una unidad de un nodo, debe esperar 30 segundos para poder insertar la unidad de nuevo en la ranura.

Si una unidad falla, Double Helix redistribuye los datos de la unidad por los nodos que permanecen en el clúster. Varios fallos de unidad en el mismo nodo no suponen un problema, ya que el software Element protege frente a dos copias de datos que residen en el mismo nodo. Una unidad con errores produce los siguientes eventos:

- Los datos se migran fuera de la unidad.
- La capacidad general del clúster se reduce según la capacidad de la unidad.
- La protección de datos Double Helix garantiza que haya dos copias válidas de los datos.

Los sistemas de almacenamiento de SolidFire no permiten que se elimine una unidad si esto provoca que haya una cantidad insuficiente de almacenamiento para migrar los datos.

Si quiere más información

- Quite las unidades con errores del clúster
- Solución de problemas básica de unidades MDSS
- Quite las unidades MDSS
- "Reemplazar unidades para nodos de almacenamiento SolidFire"
- "Reemplazar unidades para nodos de almacenamiento serie H600S"
- "Información de hardware H410S y H610S"
- "Información sobre hardware de SF-Series"

Quite las unidades con errores del clúster

El sistema SolidFire pone una unidad en estado de error cuando el sistema de autodiagnóstico de la unidad indica al nodo que se ha producido un error o cuando la comunicación con la unidad se detiene durante cinco minutos y medio o más. El sistema muestra una lista de las unidades con errores. Debe quitar una unidad con error de la lista de unidades con errores en el software NetApp Element.

Las unidades de la lista **Alertas** aparecen como **blockServiceUnhealthy** cuando un nodo está desconectado. Cuando se reinicia 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 siguen mostrándose como unidades activas en el clúster.

1. En la interfaz de usuario de Element, seleccione **Cluster** > **Drives**.
2. Haga clic en **error** para ver la lista de unidades con errores.
3. Anote el número de ranura de la unidad con error.

   Esta información se necesita para localizar la unidad con error en el chasis.

4. Quite las unidades con errores mediante uno de los siguientes métodos:

Opción	Pasos

Para quitar unidades individuales	a. Haga clic en **acciones** para la unidad que desea quitar. b. Haga clic en **Quitar**.
Para quitar varias unidades	a. Seleccione todas las unidades que desee quitar y haga clic en **acciones masivas**. b. Haga clic en **Quitar**.

Solución de problemas básica de unidades MDSS

Puede recuperar las unidades de metadatos (o de segmentos) si se vuelven a añadir al clúster en el caso de que se produzca un error en una o en ambas unidades de metadatos. Puede llevar a cabo la operación de recuperación en la interfaz de usuario de NetApp Element si la función MDSS ya está habilitada en el nodo.

Si se produce un error en una de las unidades de metadatos de un nodo o en las dos, el servicio de segmentos se cerrará y se realizarán backups de los datos de ambas unidades en distintas unidades del nodo.

En los siguientes escenarios se describen posibles escenarios de fallos y se ofrecen recomendaciones básicas para corregir el problema:

Error en la unidad de segmentos del sistema

- En este caso, la ranura 2 se verifica y vuelve a un estado available.
- La unidad de segmentos del sistema se debe volver a rellenar antes de que el servicio de segmentos vuelva a conectarse.
- Debe sustituir la unidad de segmentos del sistema cuando esta esté disponible, añada la unidad y la unidad de la ranura 2 a la vez.

No es posible añadir la unidad de la ranura 2 por sí misma como una unidad de metadatos. Debe volver a añadir al nodo ambas unidades a la vez.

Error en la ranura 2

- En este escenario, la unidad de segmentos del sistema se verifica y vuelve a un estado available.
- Debe reemplazar la ranura 2 con una unidad de repuesto y, cuando la ranura 2 esté disponible, añada la unidad de segmentos del sistema y la unidad de la ranura 2 al mismo tiempo.

Se produce un error en la unidad de segmentos del sistema y en la ranura 2

- Debe reemplazar la unidad de segmentos del sistema y la ranura 2 con una unidad de repuesto. Cuando las dos unidades estén disponibles, añada la unidad de segmentos del sistema y la unidad de la ranura 2 al mismo tiempo.

Orden de las operaciones

- Reemplace la unidad de hardware en la que se haya producido el error con una unidad de repuesto (reemplace ambas unidades en caso de que las dos tengan errores).

- Vuelva a añadir las unidades al clúster cuando se hayan rellenado de nuevo y estén en el estado available.

Verificar operaciones

- Verifique que las unidades de la ranura 0 (o internas) y la ranura 2 se hayan identificado como unidades de metadatos en la lista de unidades activas.
- Compruebe que el equilibrado de todos los segmentos se ha completado (no hay más mensajes del tipo moving slices en el registro de eventos durante al menos 30 minutos).

Si quiere más información

Añada unidades MDSS

Añada unidades MDSS

Es posible añadir una segunda unidad de metadatos en un nodo de SolidFire de si se convierte la unidad de bloques de la ranura 2 en una unidad de segmentos. Para ello, debe habilitar la función del servicio de segmentos de varias unidades (MDSS). Para habilitar esta función, debe ponerse en contacto con el soporte de NetApp.

Para que una unidad de segmentos tenga el estado available, puede que deba reemplazar una unidad con errores por una unidad nueva o de repuesto. Debe añadir la unidad de segmentos del sistema al mismo tiempo que añade la unidad para la ranura 2. Si intenta añadir solo la unidad de segmentos de la ranura 2 o añadirla antes de la unidad de segmentos del sistema, el sistema mostrará un error.

1. Haga clic en **Cluster** > **Drives**.
2. Haga clic en **disponible** para ver la lista de unidades disponibles.
3. Seleccione las unidades de segmentos que desea añadir.
4. Haga clic en **acciones masivas**.
5. Haga clic en **Agregar**.
6. Confirme en la ficha **Active Drives** que las unidades se han añadido.

Quite las unidades MDSS

Es posible quitar las unidades del servicio de segmentos de varias unidades (MDSS). Este procedimiento solo se aplica si el nodo tiene varias unidades de segmentos.

> Si se produce un error en la unidad de segmentos del sistema y en la unidad de ranura 2, el sistema cerrará los servicios de segmentos y quitará las unidades. Si no se produce ningún error y quita las unidades, tendrá que quitar ambas unidades a la vez.

1. Haga clic en **Cluster** > **Drives**.
2. En la ficha unidades **disponibles** , haga clic en la casilla de verificación correspondiente a las unidades de segmentos que se van a eliminar.
3. Haga clic en **acciones masivas**.
4. Haga clic en **Quitar**.
5. Confirme la acción.

Solucione los problemas de los nodos

Los nodos se pueden quitar de un clúster cuando requieren mantenimiento o se deben sustituir. Debe usar la API o la interfaz de usuario de NetApp Element para quitar los nodos antes de desconectarlos.

A continuación, se ofrece una descripción general del procedimiento para quitar nodos de almacenamiento:

- Compruebe que haya suficiente capacidad en el clúster para crear una copia de los datos en el nodo.
- Quite las unidades del clúster mediante la interfaz de usuario o el método API RemoveDrives.

  Esto provoca que el sistema migre los datos desde las unidades del nodo a otras unidades en el clúster. El tiempo que se tarda en realizar este proceso depende de la cantidad de datos que haya que migrar.

- Quite el nodo del clúster.

Tenga en cuenta las siguientes consideraciones antes de apagar o encender un nodo:

- La desconexión de nodos y clústeres implica riesgos si no se realiza correctamente.

  La desconexión de un nodo se debe hacer bajo la supervisión del soporte de NetApp.

- Si un nodo ha estado desconectado más de 5.5 minutos en alguna condición de apagado, la protección de datos de Double Helix comienza la tarea de escritura de bloques replicados sencillos 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 con errores.
- Para reiniciar o desconectar correctamente un nodo, puede usar el comando de API Shutdown.
- Si un nodo está sin actividad o desconectado, debe ponerse en contacto con el soporte de NetApp antes de volver a conectarlo.
- Una vez que el nodo se ha conectado de nuevo, debe volver a añadir las unidades al clúster, en función de la cantidad de tiempo que ha estado fuera de servicio.

Si quiere más información

"Reemplazar un chasis SolidFire con fallos"

"Reemplazar un nodo serie H600S con fallos"

Apague un clúster

Realice el siguiente procedimiento para desconectar un clúster completo.

Pasos

1. (Opcional) comuníquese con el soporte de NetApp para obtener ayuda en la realización de los pasos preliminares.
2. Verifique que todas las operaciones de I/o se hayan detenido.
3. Desconecte todas las sesiones de iSCSI:
   a. Acceda a la dirección IP virtual de gestión (MVIP) en el clúster para abrir la interfaz de usuario de Element.
   b. Revise los nodos que aparecen en la lista Nodes.

c. Ejecute el método API Shutdown especificando la opción halt en cada ID de nodo del clúster.

Cuando reinicia el clúster, debe seguir algunos pasos para verificar que todos los nodos entran en línea:

1. Compruebe que todas las gravedad crítica y. `volumesOffline` se resolvieron errores del clúster.
2. Espere de 10 a 15 minutos para que el clúster se asiente.
3. Empiece a poner los hosts a acceder a los datos.

Si desea permitir más tiempo al encender los nodos y verificar que su estado sea después del mantenimiento, póngase en contacto con el soporte técnico para obtener ayuda con la demora de la sincronización de datos para evitar la sincronización innecesaria de bandejas.

Obtenga más información

"Cómo apagar y encender correctamente un clúster de almacenamiento SolidFire/HCI de NetApp"

Trabaje con utilidades por nodo para los nodos de almacenamiento

Puede usar 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 proporcionan suficiente información para la solución de problemas. Las utilidades por nodo proporcionan información y herramientas específicas que pueden ayudarle a solucionar problemas de red entre los nodos o con el nodo de gestión.

Obtenga más información

- Acceda a la configuración por nodo con la interfaz de usuario por nodo
- Los detalles de la configuración de red de la interfaz de usuario por nodo
- Detalles de la configuración de clúster de la interfaz de usuario por nodo
- Ejecute las pruebas del sistema usando la interfaz de usuario por nodo
- Ejecute las utilidades del sistema con la interfaz de usuario por nodo

Acceda a la configuración por nodo con la interfaz de usuario por nodo

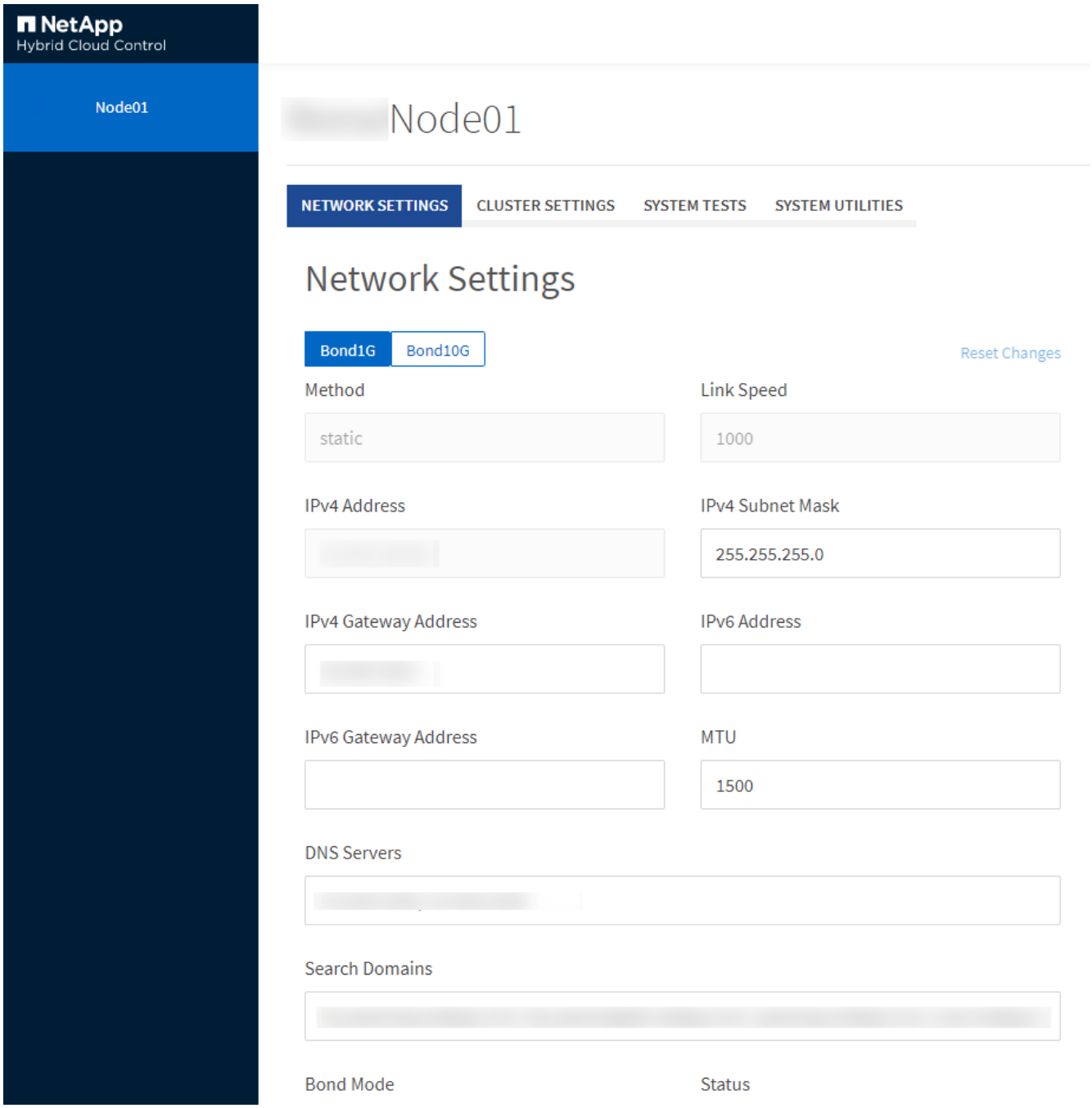
Tras introducir la IP y la autenticación del nodo de gestión, puede acceder a los ajustes de red, los ajustes del clúster y las pruebas y las utilidades del sistema en la interfaz de usuario por nodo de gestión.

Si desea modificar la configuración de un nodo en un estado Active que forme parte de un clúster, debe iniciar sesión como usuario de administrador de clúster.

Debe configurar o modificar un nodo por vez. Debe asegurarse de que la configuración de red especificada tenga el efecto deseado y que la red sea estable y se ejecute correctamente antes de hacer modificaciones en otro nodo.

1. Abra la interfaz de usuario por nodo mediante uno de los siguientes métodos:

- Introduzca la dirección IP de administración seguida de :442 en una ventana del navegador e inicie sesión con un nombre de usuario y una contraseña de administrador.
- En la interfaz de usuario de Element, seleccione **Cluster** > **Nodes** y haga clic en el enlace de la dirección IP de administración correspondiente al nodo que desea configurar o modificar. En la ventana del navegador que se abre, puede editar la configuración del nodo.



Los detalles de la configuración de red de la interfaz de usuario por nodo

Es posible cambiar la configuración de red del nodo de almacenamiento para dar al nodo un nuevo conjunto de atributos de red.

Puede ver la configuración de red para un nodo de almacenamiento en la página **Configuración de red** cuando inicia sesión en el nodo (https://<node IP>:442/hcc/node/network-settings). Puede seleccionar las opciones **Bond1G** (administración) o **Bond10G** (almacenamiento). En la lista siguiente se describe la

configuración que se puede modificar cuando el estado de un nodo de almacenamiento es Available, Pending o Active:

- **Método**

  El método que se utiliza para configurar la interfaz. Métodos posibles:

  - Loopback: Se utiliza para definir la interfaz de bucle invertido de IPv4.
  - Manual: Se utiliza para definir interfaces para las que no se realiza ninguna configuración de forma predeterminada.
  - dhcp: Se utiliza para obtener una dirección IP a través de DHCP.
  - Static: Se utiliza para definir interfaces Ethernet con direcciones IPv4 asignadas de forma estática.

- **Velocidad de enlace**

  La velocidad negociada por la NIC virtual.

- **Dirección IPv4**

  La dirección IPv4 de la red eth0.

- **Máscara de subred IPv4**

  Las subdivisiones de dirección de la red IPv4.

- **Dirección de puerta de enlace IPv4**

  La dirección de red del enrutador para enviar paquetes fuera de la red local.

- **Dirección IPv6**

  La dirección IPv6 de la red eth0.

- **Dirección de puerta de enlace IPv6**

  La dirección de red del enrutador para enviar paquetes fuera de la red local.

- **MTU**

  Tamaño de paquete más grande que un protocolo de red puede transmitir. Debe ser mayor o igual que 1500. Si se añade un segundo NIC de almacenamiento, el valor debería ser 9000.

- **Servidores DNS**

  La interfaz de red que se utiliza para la comunicación del clúster.

- **Buscar dominios**

  La búsqueda de direcciones MAC adicionales que hay disponibles en el sistema.

- **Modo Bond**

  Puede ser uno de los siguientes modos:

  - ActivePassive (predeterminado)

- ALB
- LACP

- **Estado**

  Los posibles valores son los siguientes:

  - UpAndRunning
  - Abajo
  - Arriba

- **Etiqueta de red virtual**

  La etiqueta asignada cuando se creó la red virtual.

- **Rutas**

  Las rutas estáticas para especificar hosts o redes a través de la interfaz asociada que se ha configurado para que usen las rutas.

Detalles de la configuración de clúster de 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.

En la siguiente lista se describe la configuración del clúster para un nodo de almacenamiento que se indica en la página **Configuración de clúster** de la interfaz de usuario por nodo (https://<node IP>:442/hcc/node/cluster-settings).

- **Rol**

  El rol que tiene el nodo en el clúster. Los posibles valores son los siguientes:

  - Storage: Nodo de almacenamiento o Fibre Channel.
  - Management: Se trata de un nodo de gestión.

- **Nombre de host**

  El nombre del nodo.

- **Cluster**

  El nombre del clúster.

- **Composición de grupo**

  El estado del nodo. Los posibles valores son los siguientes:

  - Available: El nodo no tienen ningún nombre de clúster asociado y aún no forma parte de un clúster.
  - Pending: Se ha configurado el nodo y se puede añadir a un clúster designado. No es necesario autenticarse para acceder al nodo.
  - PendingActive: El sistema está instalando el software compatible en el nodo. Cuando finalice, el nodo se moverá al estado Active.

- Active: El nodo participa en un clúster. Es necesario autenticarse para modificar el nodo.

- **Versión**

  La versión del software Element que se ejecuta en el nodo.

- **Ensemble**

  Los nodos que forman parte del conjunto de base de datos.

- **ID de nodo**

  El ID asignado cuando se añade un nodo al clúster.

- **Interfaz de clúster**

  La interfaz de red que se utiliza para la comunicación del clúster.

- **Interfaz de administración**

  La interfaz de red de gestión. De forma predeterminada es Bond1G, pero también puede usar Bond10G.

- **Interfaz de almacenamiento**

  La interfaz de red de almacenamiento que usa Bond10G.

- **Capacidad de cifrado**

  Indica si el nodo admite el cifrado de unidad o no.

Ejecute las pruebas del sistema usando la interfaz de usuario por nodo

Es posible probar los cambios en los ajustes de red después de confirmar los cambios en la configuración de red. Es posible ejecutar las pruebas para garantizar que el nodo de almacenamiento sea estable y que se pueda conectar sin ningún problema.

Inició sesión en la interfaz de usuario por nodo del nodo de almacenamiento.

1. Haga clic en **pruebas del sistema**.
2. Haga clic en **Ejecutar prueba** junto a la prueba que desea ejecutar o seleccione **Ejecutar todas las pruebas**.

   La ejecución de todas las operaciones de prueba puede llevar bastante tiempo y solo se debe realizar según lo indique el soporte de NetApp.

   - **Comprobar Ensemble** conectado

     Prueba y verifica la conectividad con un conjunto de bases de datos. De forma predeterminada, la prueba utiliza el conjunto para el clúster con el que está asociado el nodo. Como alternativa, puede proporcionar un conjunto diferente para probar la conectividad.

   - **Test Connect Mvip**

     Hace ping en la dirección IP virtual de gestión especificada (MVIP) y, a continuación, ejecuta una

llamada API sencilla a la MVIP para verificar la conectividad. De manera predeterminada, la prueba utiliza la MVIP para el clúster con el que está asociado el nodo.

- **Test Connect SVIP**

  Hace ping en la dirección IP virtual de almacenamiento especificada (SVIP) mediante los paquetes del protocolo de mensajes de control de Internet (ICMP) que coinciden con el tamaño de unidad de transmisión máxima (MTU) establecido en el adaptador de red. Se conecta entonces con la SVIP como un iniciador iSCSI. De forma predeterminada, la prueba utiliza la SVIP para el clúster con el que está asociado el nodo.

- **Configuración del hardware de prueba**

  Prueba 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 se ejecuten correctamente. Es lo mismo que las pruebas de fábrica.

  Esta prueba consume muchos recursos y solo se debe ejecutar si lo solicita el soporte de NetApp.

- **Probar conectividad local**

  Prueba la conectividad con todos los otros nodos del clúster haciendo ping en la IP de clúster (CIP) en cada nodo. Esta prueba solo se mostrará en un nodo si el nodo forma parte de un clúster activo.

- **Probar grupo de localización**

  Valida que el nodo pueda localizar el clúster especificado en la configuración del clúster.

- **Probar configuración de red**

  Verifica que la configuración de red que se ha establecido coincide con la configuración de red que se está usando en el sistema. Esta prueba no se realiza con la intención de detectar errores en el hardware cuando un nodo participa de forma activa en un clúster.

- **Probar ping**

  Hace ping en una lista de hosts determinada o, si no se especifica ninguna, crea de forma dinámica una lista de todos los nodos registrados en el clúster y hace ping en cada uno de ellos para establecer una conectividad sencilla.

- **Probar la conectividad remota**

  Prueba la conectividad con todos los nodos de clústeres emparejados de forma remota haciendo ping en la IP de clúster (CIP) en cada nodo. Esta prueba solo se mostrará en un nodo si el nodo forma parte de un clúster activo.

Ejecute las utilidades del sistema con la interfaz de usuario por nodo

Se puede usar la interfaz de usuario por nodo para el nodo de almacenamiento a fin de crear o eliminar paquetes de soporte, restablecer la configuración de las unidades y reiniciar los servicios de red o de clúster.

Inició sesión en la interfaz de usuario por nodo del nodo de almacenamiento.

1. Haga clic en **Utilidades del sistema**.
2. Haga clic en el botón de la utilidad del sistema que desea ejecutar.
   - **Alimentación de control**

     Reinicia, apaga o enciende el nodo.

     > Esta operación provoca la pérdida temporal de conectividad de red.

     Especifique los siguientes parámetros:

     - Acción: Las opciones incluyen reinicio y parada (apagado).
     - Retraso en el reactivación: En cualquier momento adicional antes de que el nodo vuelva a estar online.
   - **Recopilar registros de nodos**

     Crea un paquete de soporte en el directorio /tmp/bundles del nodo.

     Especifique los siguientes parámetros:

     - Bundle Name: Nombre único para cada paquete de soporte creado. Si no se proporciona ningún nombre, "supportBundle" y el nombre de nodo se utilizan como nombre de archivo.
     - Extra args: Este parámetro se alimenta con el script sf_make_support_bundle. Este parámetro solo se debe usar si lo solicita el soporte de NetApp.
     - Timeout Sec: Especifique el número de segundos que se deben esperar para cada respuesta ping individual.
   - **Borrar registros de nodos**

     Elimina todos los paquetes de soporte actuales del nodo que se crearon con **Crear paquete de soporte de clúster** o el método API CreateSupportBundle.
   - **Restablecer las unidades**

     Inicializa las unidades y quita todos los datos que residen en ese momento en la unidad. Es posible reutilizar la unidad en un nodo existente o en un nodo actualizado.

     Especifique el siguiente parámetro:

     - Unidades: Lista de nombres de dispositivos (no driveID) que se van a 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.
   - **Restablecer nodo**

     Restablece un nodo a la configuración de fábrica. Todos los datos se quitan, pero la configuración de red del nodo se conserva durante esta operación. Los nodos solo se pueden restablecer si no se han asignado a un clúster y en estado disponible.

Cuando utiliza esta opción, se eliminan del nodo todos los datos, paquetes (actualizaciones de software), configuraciones y archivos de registro.

- **Reinicie Networking**

  Reinicia todos los servicios de red de un nodo.

  Esta operación puede provocar la pérdida temporal de conectividad de red.

- **Reinicie Servicios**

  Reinicia los servicios del software Element en un nodo.

  Esta operación puede provocar una interrupción temporal del servicio de los nodos. Debe realizar esta operación solo cuando lo indique el soporte de NetApp.

  Especifique los siguientes parámetros:

  - Servicio: Nombre del servicio que se va a reiniciar.
  - Acción: Acción a realizar en el servicio. Las opciones incluyen inicio, parada y reinicio.

Trabaje con el nodo de gestión

Es posible usar el nodo de gestión (mNode) para actualizar los servicios del sistema, gestionar 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 solución de problemas.

Como práctica recomendada, solo asocie un nodo de gestión a una instancia de VMware vCenter y evite definir los mismos recursos de almacenamiento y computación o instancias de vCenter en varios nodos de gestión.

Consulte "documentación del nodo de gestión" si quiere más información.

Comprender los niveles de llenado de clústeres

El clúster que ejecuta el software Element genera errores de clúster para advertir al administrador de almacenamiento cuándo se está quedando sin capacidad el clúster. Hay tres niveles de ocupación del clúster, cada uno de los cuales se muestra en la interfaz de usuario de NetApp Element: Warning, error y Critical.

El sistema usa el código de error BlockClusterFull para informar sobre el nivel de ocupación del almacenamiento en bloque de clúster. Puede ver los niveles de gravedad de ocupación del clúster en la pestaña Alerts 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 que puede configurar el cliente y que aparece cuando la capacidad de

bloques del clúster se acerca al nivel de gravedad de error. De forma predeterminada, este nivel se establece en el tres % por debajo del nivel de error y se puede ajustar a través de la interfaz de usuario y la API de Element. Debe añadir más capacidad o liberar capacidad Lo antes posible..

- **Error**

  Cuando el clúster presenta este estado, si se pierde un nodo, no habrá suficiente capacidad en el clúster para reconstruir la protección de datos de Double Helix. La creación de los volúmenes, los clones y las snapshots se bloquea cuando el clúster está en este estado. No es un estado seguro y no se recomienda para ningún clúster. Debe añadir más capacidad o liberar capacidad de inmediato.

- **Crítico**

  Este error crítico se ha producido porque se ha consumido el 100 % del clúster. Se trata de un estado de solo lectura y no se puede realizar ninguna conexión iSCSI nueva con el clúster. Cuando se alcanza este estado, debe liberar capacidad o añadir más de inmediato.

El sistema utiliza el código de error MetadataClusterFull para informar sobre la ocupación del almacenamiento de metadatos del clúster. Puede ver la ocupación del almacenamiento de metadatos del clúster en la sección Cluster Capacity en la página Overview de la pestaña Reporting en la interfaz de usuario de Element.

En la siguiente lista, se incluye información acerca de los niveles de gravedad de MetadataClusterFull:

- **Advertencia**

  Se trata de una advertencia que puede configurar el cliente y que aparece cuando la capacidad de datos de metadatos del clúster se acerca al nivel de gravedad de error. De forma predeterminada, este nivel se establece en el tres por ciento por debajo del nivel de error y se puede ajustar a través de la API de Element. Debe añadir más capacidad o liberar capacidad Lo antes posible..

- **Error**

  Cuando el clúster presenta este estado, si se pierde un nodo, no habrá suficiente capacidad en el clúster para reconstruir la protección de datos de Double Helix. La creación de los volúmenes, los clones y las snapshots se bloquea cuando el clúster está en este estado. No es un estado seguro y no se recomienda para ningún clúster. Debe añadir más capacidad o liberar capacidad de inmediato.

- **Crítico**

  Este error crítico se ha producido porque se ha consumido el 100 % del clúster. Se trata de un estado de solo lectura y no se puede realizar ninguna conexión iSCSI nueva con el clúster. Cuando se alcanza este estado, debe liberar capacidad o añadir más de inmediato.

Lo siguiente se aplica a los umbrales de clúster de dos nodos:

- El error de ocupación de metadatos está un 20% por debajo de crítico.
- El error de ocupación de los bloques es 1 unidad de bloque (incluida la capacidad desaprovechada) que se encuentra por debajo de la crucial. Esto significa que vale de dos unidades de bloque la capacidad por debajo de la crítica.