Documentación de software de SANtricity 11,80

SANtricity 11.8

NetApp
April 05, 2024

Tabla de contenidos

Documentación de software de SANtricity 11,80

Notas de la versión

Novedades en el sistema operativo SANtricity 11,80

En la siguiente tabla, se describen las nuevas funciones de SANtricity System Manager 11,8.

Nuevas funciones en la versión 11,80

Nueva función	Descripción
Exploración de paridad de volumen mejorada	El análisis de paridad de volúmenes ahora se puede iniciar como proceso en segundo plano mediante la API DE REST o la interfaz de línea de comandos. El análisis de paridad resultante se ejecutará en segundo plano siempre que sea necesario para completar la operación de análisis. Las operaciones de análisis sobrevivirán a los reinicios de la controladora y las operaciones de conmutación por error.
Compatibilidad con SAML para Unified Manager	Unified Manager ahora es compatible con SAML (lenguaje de marcado de aserción de seguridad). Una vez que SAML se habilita para Unified Manager, los usuarios deben usar la autenticación multifactor con el proveedor de identidades para poder interactuar con la interfaz de usuario. Tenga en cuenta que una vez que se habilita SAML en Unified Manager, la API DE REST no se puede usar sin pasar por el IdP para autenticar las solicitudes.
Función de configuración automática	Ahora admite la capacidad de establecer el parámetro de tamaño de bloque de volumen que se utilizará con la función Auto Configuration para la configuración inicial de la cabina. Esta función solo está disponible en la CLI como parámetro «blocksize».
Firma criptográfica del firmware de la controladora	El firmware de la controladora está firmado criptográficamente. Las firmas se comprueban durante la descarga inicial y en cada arranque de la controladora. No se espera ningún impacto sobre el usuario final. Las firmas están respaldadas por un certificado de validación extendida emitido por la CA.
Firma criptográfica del firmware de la unidad	El firmware de la unidad está firmado criptográficamente. Las firmas se comprueban durante la descarga inicial y están respaldadas por un certificado de validación extendida emitido por la CA. El contenido del firmware de la unidad ahora se entrega como archivo ZIP, que contiene el firmware no firmado más antiguo, así como el firmware nuevo firmado. El usuario debe seleccionar el archivo adecuado en función de la versión de lanzamiento del código que se esté ejecutando en el sistema de destino.

Nueva función	Descripción

Gestión de servidores de claves externos: Tamaño de clave de certificado	El nuevo tamaño de clave de certificado predeterminado es de 3072 bits (desde 2048). Se admiten tamaños de llave de hasta 4096 bits. Debe cambiarse un bit de NVSRAM para que admita los tamaños de claves no predeterminados.
	
	Los valores de selección de tamaño de clave son los siguientes:
	
	• EL VALOR PREDETERMINADO ES DE 15 0
	• LONGITUD 2048 = 1
	• LONGITUD 3072 = 2
	• LONGITUD 4096 = 3
	
	Para cambiar el tamaño de clave a 4096 mediante SMcli:
	
	`set controller[b] globalnvsrambyte[0xc0]=3;`
	`set controller[a] globalnvsrambyte[0xc0]=3;`
	
	Interrogue el tamaño de la clave:
	
	`show allcontrollers globalnvsrambyte[0xc0];`

Mejoras del pool de discos	Los pools de discos creados con controladoras que ejecutan 11,80 o superior serán pools *Version 1* en vez de pools *Version 0*. La operación de degradación está restringida cuando existe un pool de discos *Versión 1*. La versión de un pool de discos se puede identificar en el perfil de la cabina de almacenamiento.
System Manager y Unified Manager no se iniciarán a menos que se cumplan los requisitos mínimos del explorador	Se requiere una versión mínima del explorador para que se inicie System Manager o Unified Manager. Las siguientes son las versiones mínimas admitidas: • Firefox Versión mínima 80 • Chrome versión mínima 89 • Edge versión mínima 90 • Safari versión mínima 14
Compatibilidad con unidades SSD NVMe FIPS 140-3 TB	Ahora se admiten unidades SSD NVMe certificadas según NetApp, FIPS 140-3-2. Se identificarán correctamente como tales en el perfil de la cabina de almacenamiento y en System Manager.
Compatibilidad con caché de lectura de SSD en EF300 y EF600	La caché de lectura de SSD ahora se admite en las controladoras EF300 y EF600 si utilizan HDD con una ampliación SAS.

Nueva función	Descripción
Compatibilidad con iSCSI y mirroring remoto asíncrono de Fibre Channel en EF300 y EF600	El mirroring remoto asíncrono (ARVM) ahora se admite en las controladoras EF300 y EF600 con volúmenes basados en NVMe y SAS.
Admita EF300 y EF600 sin unidades en la bandeja base	Ahora se admiten las configuraciones de controladoras EF300 y EF600 sin unidades NVMe en el soporte base.
Puertos USB desactivados para todas las plataformas	Los puertos USB ahora están deshabilitados en todas las plataformas.

Notas de la versión

Las notas de la versión están disponibles fuera de este sitio. Se le pedirá que inicie sesión con sus credenciales del sitio de soporte de NetApp.

- "11,80 Notas de la versión"
- "Notas de la versión 11.70"
- "Notas de la versión 11.60"
- "Notas de la versión 11.50"

Manos a la obra

Información general del software SANtricity

Los sistemas E-Series incluyen el software SANtricity para el aprovisionamiento de almacenamiento y otras tareas.

En este sitio se describe cómo utilizar las siguientes interfaces de gestión de SANtricity:

- System Manager: Una interfaz basada en web que se utiliza para gestionar una cabina de almacenamiento individual en la red.
- Unified Manager: Interfaz basada en web que se utiliza para ver y gestionar todas las cabinas de almacenamiento de la red.

> Las cabinas de almacenamiento EF600 y EF300 no admiten el mirroring síncrono o los volúmenes finos.

System Manager de SANtricity

System Manager es un software de gestión basado en web integrado en cada controladora. Para acceder a la interfaz de usuario, apunte un explorador a la dirección IP de la controladora. Un asistente de configuración le ayuda a comenzar con la configuración del sistema.

System Manager ofrece diversas funciones de gestión como:

Rendimiento
Visualice hasta 30 días de datos de rendimiento, incluida la latencia de I/o, IOPS, utilización de CPU y rendimiento.
Almacenamiento
Aprovisione el almacenamiento mediante pools o grupos de volúmenes y cree cargas de trabajo de aplicaciones.
Protección de datos

Realice operaciones de backup y recuperación ante desastres mediante copias Snapshot, copias de volúmenes y mirroring remoto.
Hardware
Compruebe el estado de los componentes y realice algunas funciones relacionadas con esos componentes, como la asignación de unidades de repuesto.
Alertas
Notifique a los administradores sobre eventos importantes que se producen en la cabina de almacenamiento. Las alertas se pueden enviar por correo electrónico, capturas SNMP y syslog.
Administración de acceso
Configurar la autenticación de usuario que requiere que los usuarios inicien sesión en el sistema con credenciales asignadas.
Ajustes del sistema
Configure otras funciones de rendimiento del sistema, como la caché SSD y el equilibrio de carga automático.
Soporte
Ver datos de diagnóstico, gestionar actualizaciones y configurar AutoSupport, que supervisa el estado de una cabina de almacenamiento y envía mensajes automáticos al soporte técnico.

Unified Manager de SANtricity

Unified Manager es un software basado en web que se utiliza para gestionar todo el dominio. Desde una vista central puede ver el estado de todas las cabinas E-Series y EF-Series más recientes, como E2800, EF280,

EF300, E5700, EF570 Y EF600. También puede realizar operaciones en lote en cabinas de almacenamiento seleccionadas.

Unified Manager se encuentra instalado en un servidor de gestión junto con el proxy de servicios web. Para acceder a Unified Manager, se abre un explorador e introduce la URL que indica el servidor donde está instalado el proxy de servicios web.

Unified Manager ofrece varias funciones de gestión, como:

Descubra las matrices de almacenamiento
Busque y añada las cabinas de almacenamiento que desea gestionar en la red de la organización. Luego, es posible ver el estado de todas las cabinas de almacenamiento desde una sola página.
Lanzamiento
Abra una instancia de System Manager para realizar operaciones de gestión individuales en una determinada cabina de almacenamiento.
Importar configuración
Ejecute una importación en lote desde una cabina de almacenamiento a varias cabinas, incluida la configuración de las alertas, AutoSupport y servicios de directorio.
Mirroring
Configure las parejas reflejadas asíncronas o síncronas entre dos cabinas de almacenamiento.
Gestionar grupos
Organice las cabinas de almacenamiento en grupos para facilitar la gestión.

Centro de actualización
Actualice el software de sistema operativo SANtricity en varias cabinas de almacenamiento.
Certificados
Cree solicitudes de firma de certificados (CSR), importe certificados y gestione certificados existentes para varias cabinas de almacenamiento.
Administración de acceso
Configurar la autenticación de usuario que requiere que los usuarios inicien sesión en Unified Manager con credenciales asignadas.

Exploradores compatibles y sistemas operativos

El software SANtricity admite varios tipos de exploradores y sistemas operativos.

Exploradores

Se admiten los siguientes exploradores en las versiones mencionadas.

Navegador	Versión mínima
Google Chrome	89
Mozilla Firefox	80
Safari	14
Microsoft Edge	90

Para Unified Manager, el proxy de servicios web debe estar instalado y disponible para el explorador. Para obtener más información, consulte "Información general sobre el proxy de servicios web de SANtricity"

Sistemas operativos

Se admiten los sistemas operativos y las versiones siguientes.

De NetApp	Versión/arquitectura mínima
Red Hat Enterprise Linux (RHEL)	7.x, 8.x / 64 bits
SUSE Linux Enterprise Server (SLES)	12.x, 15.x / 64 bits
Oracle Linux (OL)	7.x, 8.x / 64 bits
Servidor Windows Server	2016, 2019, 2022 / 64 bits
Ubuntu	18.04, 20.04 / 64 bits

Configuración de System Manager

Acceda a System Manager

Para acceder a la interfaz de usuario de System Manager, debe dirigir un explorador a la dirección IP de la controladora. Un asistente de configuración le ayuda a comenzar con la configuración del sistema.

Antes de empezar

- Instale y configure el hardware, tal y como se describe en una de las guías de configuración exprés:
  - "Configuración exprés de Linux"
  - "Configuración exprés de VMware"
  - "Configuración exprés de Windows"
- Configure una estación de administración que cumpla con los siguientes requisitos:
  - Conectado a una red que es 1 Gbps o más rápido.
  - Conectados a la misma subred que los puertos de administración del almacenamiento.
  - Se utiliza como una estación independiente, en lugar de como un host (con conexión a I/o) que se utiliza para la gestión de datos.
  - Configuración para una gestión fuera de banda, en la que una estación de administración del almacenamiento envía comandos al sistema de almacenamiento a través de las conexiones Ethernet a la controladora.
  - Realice la configuración con un navegador compatible. Consulte "Exploradores compatibles y sistemas operativos".

Pasos

1. Desde el explorador, introduzca la siguiente URL: `https://<IPAddress>`

   `IPAddress` es la dirección de una de las controladoras de la cabina de almacenamiento.

   La primera vez que se abre System Manager en una cabina sin configurar, aparece el aviso Set

Administrator Password.

2. Introduzca la contraseña del administrador del sistema para la función admin en los campos Set Administrator Password y Confirm Password y, a continuación, haga clic en **Set Password**.

   Se iniciará el asistente de configuración la primera vez que inicie sesión.

3. Use el asistente de configuración para realizar las siguientes tareas:
   - **Verificar hardware (controladores y unidades)** — verificar el número de controladores y unidades en la matriz de almacenamiento. Asigne un nombre a la cabina.
   - **Verificar hosts y sistemas operativos** — verificar los tipos de host y sistema operativo a los que puede acceder la matriz de almacenamiento.
   - **Aceptar pools** — acepte la configuración de pool recomendada para el método de instalación rápida. Un pool es un grupo lógico de unidades.
   - **Configurar alertas** — permitir que System Manager reciba notificaciones automáticas cuando se produce un problema en la cabina de almacenamiento.
   - **Enable AutoSupport**: Supervise automáticamente el estado de la cabina de almacenamiento y envíe mensajes al soporte técnico.

Para obtener más información sobre el Asistente de configuración, consulte "Información general del asistente de configuración de".

Información general del asistente de configuración

Utilice el asistente de configuración para configurar la cabina de almacenamiento, incluido el hardware, los hosts, las aplicaciones, las cargas de trabajo, Pools, alertas y AutoSupport.

Configuración por primera vez

Cuando se abre por primera vez System Manager, aparece el asistente de configuración. El asistente de configuración le solicita que realice tareas de configuración básicas, como asignar un nombre a la cabina de almacenamiento, configurar los hosts, seleccionar aplicaciones y crear pools de almacenamiento.

> Antes de continuar con la configuración inicial, vaya al centro de actualización (menú:Soporte[Centro de actualización]) y asegúrese de que el software de sistema operativo SANtricity está actualizado. Si es necesario, actualice a la versión más reciente y actualice el explorador para continuar con la configuración. Para obtener más información, consulte "Información general del centro de actualización".

Si cancela el asistente, no podrá volver a ejecutarlo manualmente. El asistente se vuelve a ejecutar automáticamente cuando abre System Manager o actualiza el explorador y se cumple *al menos una* de las siguientes condiciones:

- No se detectan pools ni grupos de volúmenes.
- No se detectan cargas de trabajo.
- No hay notificaciones configuradas.

Terminología

El asistente de configuración usa los siguientes términos.

Duración	Descripción
Cliente más	Una aplicación es un programa de software como Microsoft SQL Server o Microsoft Exchange.
Alerta	Las alertas notifican a los administradores sobre eventos importantes que se producen en las cabinas de almacenamiento. Se pueden enviar por correo electrónico, capturas SNMP o syslog.
AutoSupport	La función AutoSupport supervisa el estado de una cabina de almacenamiento y envía mensajes automáticos al soporte técnico.
Hardware subyacente	El hardware del sistema de almacenamiento incluye las cabinas de almacenamiento, las controladoras y las unidades.
Host	Un host es un servidor que envía I/o a un volumen de una cabina de almacenamiento.
Objeto	Un objeto es cualquier componente de almacenamiento lógico o físico. Los objetos lógicos incluyen grupos de volúmenes, pools y volúmenes. Los objetos físicos abarcan la cabina de almacenamiento, las controladoras de las cabinas, los hosts y las unidades.
Piscina	Un pool es un conjunto de unidades que se agrupan en forma lógica. Se puede usar un pool para crear uno o más volúmenes accesibles para un host. (Se crean volúmenes desde un pool o un grupo de volúmenes).
Volumen	Un volumen es un contenedor en el cual las aplicaciones, las bases de datos y los sistemas de archivos almacenan datos. Es el componente lógico que se crea para que el host acceda al almacenamiento de la cabina de almacenamiento. Un volumen se crea a partir de la capacidad disponible de un pool o un grupo de volúmenes. Un volumen tiene una capacidad definida. Aunque es posible que un volumen conste de más de una unidad, un volumen aparece como un componente lógico para el host.
Grupo de volúmenes	Un grupo de volúmenes es un contenedor para volúmenes con características compartidas. Un grupo de volúmenes tiene una capacidad definida y un nivel de RAID. Se puede usar un grupo de volúmenes para crear uno o más volúmenes a los que se pueda acceder mediante un host. (Los volúmenes se crean a partir de un pool o un grupo de volúmenes).

Duración	Descripción
Carga de trabajo	Una carga de trabajo es un objeto de almacenamiento que admite una aplicación. Se pueden definir una o más cargas de trabajo o instancias por aplicación. En algunas aplicaciones, el sistema configura la carga de trabajo para contener volúmenes con características subyacentes similares. Estas características de volumen se optimizan según el tipo de aplicación que es compatible con la carga de trabajo. Por ejemplo, si crea una carga de trabajo que es compatible con la aplicación Microsoft SQL Server y, a continuación, crea volúmenes para esa carga de trabajo, las características de volumen subyacentes se optimizan para ser compatibles con Microsoft SQL Server.

Preguntas frecuentes

¿Qué sucede si no veo todos mis componentes de hardware?

Si no se ven todos los componentes de hardware en el cuadro de diálogo verificar hardware, es posible que una bandeja de unidades no esté conectada correctamente o que se haya instalado una bandeja incompatible en la cabina de almacenamiento.

Verifique que se hayan conectado correctamente todas las bandejas de unidades. Si no está seguro de cuáles bandejas de unidades son compatibles, póngase en contacto con el soporte técnico.

¿Qué sucede si no puedo ver todos mis hosts?

Si no se observan los hosts conectados, hay un error en la detección automática, los hosts están conectados incorrectamente o no hay hosts conectados actualmente.

Es posible configurar los hosts más adelante, después de completar la configuración. Es posible crear hosts de manera automática o manual de la siguiente manera:

- Si se instaló el agente de contexto de host (HCA) en los hosts, este inserta la información de configuración del host en la cabina de almacenamiento. System Manager configura automáticamente estos hosts y los muestra en el asistente de configuración inicial. (HCA no rige para los hosts NVMe over Fabrics).
- Es posible crear hosts manualmente y asociarlos con los identificadores de puerto de host adecuados en **Storage › hosts**. Los hosts que se han creado manualmente también aparecen en el asistente **Configuración inicial**.
- El objetivo y el host deben configurarse para el tipo de puerto de host (por ejemplo, iSCSI o NVMe over roce), y debe establecerse una sesión en el almacenamiento para que la detección automática funcione.

¿Cómo ayuda la identificación de aplicaciones a gestionar la cabina de almacenamiento?

Cuando se identifican aplicaciones, System Manager recomienda automáticamente una configuración de volumen que optimiza el almacenamiento según el tipo de aplicación.

La optimización de volúmenes por aplicación puede aumentar la eficiencia de las operaciones de almacenamiento de datos. Las características como el tipo de I/o, el tamaño de segmento, la propiedad de controladora y la caché de lectura y escritura se incluyen en la configuración de volumen. Además, es posible visualizar datos de rendimiento por aplicación y por carga de trabajo para evaluar la latencia, las I/o por segundo y los MIB/seg de aplicaciones y de sus cargas de trabajo asociadas.

¿Qué es una carga de trabajo?

Para algunas aplicaciones de la red, como SQL Server o Exchange, es posible definir una carga de trabajo que optimice el almacenamiento para esa aplicación.

Una carga de trabajo es un objeto de almacenamiento que admite una aplicación. Se pueden definir una o más cargas de trabajo o instancias por aplicación. En algunas aplicaciones, el sistema configura la carga de trabajo para contener volúmenes con características subyacentes similares. Estas características de volumen se optimizan según el tipo de aplicación que es compatible con la carga de trabajo. Por ejemplo, si crea una carga de trabajo que es compatible con la aplicación Microsoft SQL Server y, a continuación, crea volúmenes para esa carga de trabajo, las características de volumen subyacentes se optimizan para ser compatibles con Microsoft SQL Server.

Durante la creación de un volumen, el sistema indica que se deben responder preguntas acerca del uso de las cargas de trabajo. Por ejemplo, si se crean volúmenes para Microsoft Exchange, se consultará cuántos buzones se necesitan, cuáles son los requisitos de capacidad promedio del buzón y cuántas copias de la base de datos se desean. El sistema utiliza esta información para crear una configuración de volumen óptima para el usuario, que se puede editar en caso de ser necesario.

¿Cómo se configura el método de entrega para AutoSupport?

Para acceder a las tareas de configuración de los métodos de entrega de AutoSupport, vaya al menú:Soporte[Centro de soporte] y, a continuación, haga clic en la ficha **AutoSupport**.

Se admiten los siguientes protocolos: HTTPS, HTTP y SMTP.

¿Cómo saber si debe aceptarse la configuración de pool recomendada?

Si se acepta la configuración de pool recomendada depende de unos pocos factores.

Para determinar el tipo de almacenamiento que es mejor para sus requisitos, responda estas preguntas:

- ¿Prefiere varios pools de menor capacidad en lugar de pools con la mayor capacidad posible?
- ¿Prefiere grupos de volúmenes RAID en lugar de pools?
- ¿Prefiere aprovisionar manualmente las unidades en lugar de que le recomienden una configuración?

Si respondió afirmativamente a cualquiera de esas preguntas, considere rechazar la configuración de pool recomendada.

System Manager no detectó ningún host. ¿Qué debo hacer?

Si no se observan los hosts conectados, hay un error en la detección automática, los hosts están conectados incorrectamente o no hay hosts conectados actualmente.

Es posible configurar los hosts más adelante, después de completar la configuración. Es posible crear hosts de manera automática o manual de la siguiente manera:

- Si se instaló el agente de contexto de host (HCA) en los hosts, este inserta la información de configuración del host en la cabina de almacenamiento. System Manager configura automáticamente estos hosts y los muestra en el asistente **Configuración inicial**. (HCA no rige para los hosts NVMe over Fabrics).
- Es posible crear hosts manualmente y asociarlos con los identificadores de puerto de host adecuados en

Storage › hosts. Los hosts que se han creado manualmente también aparecen en el asistente **Configuración inicial**.

- El objetivo y el host deben configurarse para el tipo de puerto de host (por ejemplo, iSCSI o NVMe over roce), y debe establecerse una sesión en el almacenamiento para que la detección automática funcione.

Configuración de Unified Manager

Instale Unified Manager

Unified Manager se incluye en el proxy de servicios web, que es un servidor API RESTful instalado por separado en un sistema host para gestionar los sistemas de almacenamiento E-Series de NetApp.

Para instalar Web Services Proxy y Unified Manager, consulte las siguientes instrucciones en el centro de documentación de E-Series y SANtricity:

1. "Revise los requisitos de instalación y actualización"
2. "Descargue e instale el archivo Web Services Proxy"

Acceda a Unified Manager

Después de instalar el proxy de servicios web, puede acceder a Unified Manager para gestionar varios sistemas de almacenamiento en una interfaz web.

> Para ver los exploradores compatibles, consulte "Exploradores compatibles y sistemas operativos".

Pasos

1. Abra un explorador e introduzca la siguiente URL:

   ```
   http[s]://<server>:<port>/um
   ```

   En esta URL, `<server>` Representa la dirección IP o el FQDN del servidor donde está instalado el proxy de servicios web, y. `<port>` Representa el número de puerto de escucha (el número predeterminado es 8080 para HTTP y 8443 para HTTPS).

   Se abrirá la página de inicio de sesión en Unified Manager.

2. Si inicia sesión por primera vez, introduzca `admin` para el nombre de usuario, y después establecer y confirmar una contraseña para el usuario administrador.

   La contraseña puede tener hasta 30 caracteres.

Para obtener más información acerca de los usuarios y contraseñas, consulte "Cómo funciona Access Management".

Gestión de cabina única con System Manager 11,8

Interfaz principal

Información general de la interfaz de System Manager

System Manager es una interfaz basada en Web que permite gestionar una cabina de almacenamiento en una sola vista.

Página de inicio

La página Inicio ofrece una vista de consola para la gestión cotidiana de la cabina de almacenamiento. Cuando se inicia sesión en System Manager, la página Inicio es la primera pantalla que aparece.

La vista de consola incluye cuatro áreas de resumen que contienen información clave sobre el estado y la condición de la cabina de almacenamiento. Es posible encontrar más información en el área de resumen.

Zona	Descripción
Notificaciones	El área de notificaciones muestra notificaciones de problemas que indican el estado de la cabina de almacenamiento y sus componentes. Además, este portlet muestra alertas automatizadas que pueden ayudarle a resolver problemas antes de que afecten a otras áreas de su entorno de almacenamiento.
Rendimiento	El área de rendimiento permite comparar y contrastar el uso de recursos a lo largo del tiempo. Es posible ver las métricas de rendimiento de una cabina de almacenamiento relacionadas con el tiempo de respuesta (IOPS), las tasas de transferencia (MIB/s) y la cantidad de capacidad de procesamiento que se utiliza (CPU).
Capacidad	El área de capacidad muestra una vista de gráfico de la capacidad asignada, la capacidad de almacenamiento libre y la capacidad de almacenamiento sin asignar en la cabina de almacenamiento.
Jerarquía de almacenamiento	El área de jerarquía de almacenamiento ofrece una vista organizada de los distintos componentes de hardware y objetos de almacenamiento gestionados por la cabina de almacenamiento. Haga clic en la flecha desplegable para realizar una determinada acción en ese componente de hardware u objeto de almacenamiento.

Configuración de la interfaz

Puede cambiar las preferencias de presentación y otras configuraciones desde la interfaz principal.

Ajuste	Descripción
Preferencias de presentación	Cambie los valores de capacidad y el margen de tiempo del menú desplegable Preferencias de la esquina superior derecha de la interfaz.
Tiempos de espera de sesión	Configurar los tiempos de espera para que las sesiones inactivas de los usuarios se desconecten después de un periodo especificado.
Ayuda	Acceda a la documentación de la Ayuda y a otros recursos desde el menú desplegable de la esquina superior derecha de la interfaz.

Inicios de sesión y contraseñas de usuario

El usuario actual que ha iniciado sesión en el sistema se muestra en la esquina superior derecha de la interfaz.

Para obtener más información sobre usuarios y contraseñas, consulte:

- "Configure la protección con contraseña de administrador"
- "Cambiar contraseñas"

Ver los datos de rendimiento

Información general sobre rendimiento

La página rendimiento ofrece maneras sencillas para supervisar el rendimiento de la cabina de almacenamiento.

¿Qué puedo aprender de los datos de rendimiento?

Los gráficos y las tablas de rendimiento muestran datos de rendimiento casi en tiempo real, lo que ayuda a determinar si una cabina de almacenamiento está experimentando problemas. También puede guardar los datos de rendimiento para construir una vista histórica de una cabina de almacenamiento e identificar cuándo comenzó un problema o qué lo provocó.

Obtenga más información:

- "Gráficos de rendimiento y directrices"
- "Condiciones de rendimiento"

¿Cómo puedo ver los datos de rendimiento?

Los datos de rendimiento están disponibles en la página Inicio y en la página almacenamiento.

Obtenga más información:

- "Ver los datos de rendimiento gráficos"
- "Ver y guardar los datos de rendimiento tabulares"
- "Interpretar datos de rendimiento"

Gráficos de rendimiento y directrices

La página rendimiento ofrece gráficos y tablas de datos que permiten evaluar el rendimiento de la cabina de almacenamiento en varias áreas clave.

Las funciones de rendimiento permiten realizar estas tareas:

- Vea los datos de rendimiento casi en tiempo real para determinar si una cabina de almacenamiento está experimentando problemas.
- Exportar datos de rendimiento para construir una vista histórica de una cabina de almacenamiento e identificar cuándo comenzó un problema o qué lo provocó.
- Seleccionar los objetos, las métricas de rendimiento y el periodo que se desean visualizar.
- Comparar métricas.

Los datos de rendimiento se pueden ver en tres formatos:

- * Gráficos en tiempo real* — traza los datos de rendimiento de un gráfico casi en tiempo real.
- * Tabulaciones en tiempo casi real* — enumera los datos de rendimiento en una tabla en casi tiempo real.
- **Archivo CSV exportado** — permite guardar los datos de rendimiento tabulares en un archivo de valores separados por comas para su posterior visualización y análisis.

Características de los formatos de datos de rendimiento

Tipo de monitorización del rendimiento	Intervalo de muestreo	Duración de la hora mostrada	Número máximo de objetos visualizados	Capacidad para guardar datos
Gráficos en tiempo real, activos Gráficos en tiempo real, históricos	10 s (activo) 5 min (histórico) Los puntos de datos visualizados dependen del lapso seleccionado	El lapso predeterminado es 1 hora. Opciones: • 5 minutos • 1 hora • 8 horas • 1 día • 7 días • 30 días	5	No
Tabulaciones casi en tiempo real (vista de tabla)	10 segundos -1 horas	Valor más actual	Ilimitada	Sí
Archivo de valores separados por comas (CSV)	Depende del lapso seleccionado	Depende del lapso seleccionado	Ilimitada	Sí

Directrices para visualizar datos de rendimiento

- La recogida de datos de rendimiento siempre está activada. No existe una opción para desactivarla.
- Cada vez que transcurre un intervalo de muestreo, se consulta a la cabina de almacenamiento y se actualizan los datos.
- Para los datos gráficos, el lapso de 5 minutos admite una actualización de 10 segundos promediada cada 5 minutos. El resto de los lapsos se actualizan cada 5 minutos, promediado por el lapso seleccionado.
- Los datos de rendimiento en las vistas gráficas se actualizan en tiempo real. Los datos de rendimiento en las vista de tabla se actualizan casi en tiempo real.
- Si un objeto supervisado se modifica durante el lapso en que se recogen datos, es posible que ese objeto no tenga un conjunto de puntos de datos completo que abarque el lapso seleccionado. Por ejemplo, los conjuntos de volúmenes pueden cambiar a medida que los volúmenes se crean, eliminan, asignan o se anula su asignación; o bien mientras se añaden, eliminan o fallan unidades.

Terminología de rendimiento

Conozca la forma en que los términos de rendimiento se aplican a su cabina de almacenamiento.

Duración	Descripción
Cliente más	Una aplicación es un programa de software como SQL o Exchange.
CPU	CPU es la sigla en inglés para la unidad central de procesamiento. La CPU indica el porcentaje de capacidad de procesamiento de la cabina de almacenamiento que está en uso.
Host	Un host es un servidor que envía I/o a un volumen de una cabina de almacenamiento.
IOPS	IOPS es la sigla en inglés para las operaciones de I/o por segundo.
Latencia	La latencia es el intervalo de tiempo entre una solicitud, como un comando de lectura o escritura, y la respuesta del host o la cabina de almacenamiento.
LUN	Un número de unidad lógica (LUN) es el número asignado al espacio de dirección que utiliza un host para acceder a un volumen. El volumen se presenta al host como capacidad en forma de LUN. Cada host tiene su propio espacio de dirección de LUN. Por lo tanto, distintos hosts pueden utilizar el mismo LUN para acceder a diferentes volúmenes.
MIB	MIB es la contracción de mebibyte (mega binary byte). Un MIB es 220 o 1,048,576 bytes. Se compara con MB, que representa un valor sobre la base de 10. Un MB equivale a 1,024 bytes.

Duración	Descripción
Objeto	Un objeto es cualquier componente de almacenamiento lógico o físico. Los objetos lógicos incluyen grupos de volúmenes, pools y volúmenes. Los objetos físicos abarcan la cabina de almacenamiento, las controladoras de las cabinas, los hosts y las unidades.
Piscina	Un pool es un conjunto de unidades que se agrupan en forma lógica. Se puede usar un pool para crear uno o más volúmenes accesibles para un host. (Se crean volúmenes desde un pool o un grupo de volúmenes).
Lea	La lectura es la forma abreviada de "operación de lectura", lo que se produce cuando el host solicita datos de la cabina de almacenamiento.
Volumen	Un volumen es un contenedor en el cual las aplicaciones, las bases de datos y los sistemas de archivos almacenan datos. Es el componente lógico que se crea para que el host acceda al almacenamiento de la cabina de almacenamiento. Un volumen se crea a partir de la capacidad disponible de un pool o un grupo de volúmenes. Un volumen tiene una capacidad definida. Aunque es posible que un volumen conste de más de una unidad, un volumen aparece como un componente lógico para el host.
Nombre del volumen	Un nombre de volumen es una cadena de caracteres que se asignan al volumen cuando se crea. Se puede aceptar el nombre predeterminado o se puede proporcionar un nombre más descriptivo que indique el tipo de datos almacenados en el volumen.
Grupo de volúmenes	Un grupo de volúmenes es un contenedor para volúmenes con características compartidas. Un grupo de volúmenes tiene una capacidad definida y un nivel de RAID. Se puede usar un grupo de volúmenes para crear uno o más volúmenes a los que se pueda acceder mediante un host. (Los volúmenes se crean a partir de un pool o un grupo de volúmenes).
Carga de trabajo	Una carga de trabajo es un objeto de almacenamiento que admite una aplicación. Se pueden definir una o más cargas de trabajo o instancias por aplicación. En algunas aplicaciones, el sistema configura la carga de trabajo para contener volúmenes con características subyacentes similares. Estas características de volumen se optimizan según el tipo de aplicación que es compatible con la carga de trabajo. Por ejemplo, si crea una carga de trabajo que es compatible con la aplicación Microsoft SQL Server y, a continuación, crea volúmenes para esa carga de trabajo, las características de volumen subyacentes se optimizan para ser compatibles con Microsoft SQL Server.
Escritura	La escritura es la forma abreviada de "operación de escritura", cuando se envían datos desde el host hacia la cabina con fines de almacenamiento.

Ver los datos de rendimiento gráficos

Es posible ver datos gráficos de rendimiento para objetos lógicos, objetos físicos, aplicaciones y cargas de trabajo.

Acerca de esta tarea

Los gráficos de rendimiento muestran datos históricos, así como datos en directo que se capturan en el momento. Una línea vertical sobre el gráfico, con la etiqueta actualización en vivo, distingue entre datos históricos y datos en directo.

Vista de página de inicio

La página Inicio contiene un gráfico donde se muestra el rendimiento en la cabina de almacenamiento. Puede seleccionar métricas limitadas desde esta vista o puede hacer clic en **Ver detalles de rendimiento** para seleccionar todas las métricas disponibles.

Vista detallada

Los gráficos disponibles de la vista detallada de rendimiento se distribuyen en tres pestañas:

- **Vista lógica** — muestra los datos de rendimiento de objetos lógicos agrupados por grupos de volúmenes y agrupaciones. Los objetos lógicos incluyen grupos de volúmenes, pools y volúmenes.
- **Vista física** — muestra datos de rendimiento para el controlador, los canales de host, los canales de unidad y las unidades.
- **Aplicaciones y cargas de trabajo Ver** — muestra una lista de objetos lógicos (volúmenes) agrupados por los tipos de aplicación y cargas de trabajo que haya definido.

Pasos

1. Seleccione **Inicio**.
2. Para seleccionar una vista de la cabina de almacenamiento, haga clic en los botones IOPS, MIB/s o CPU.
3. Para ver más detalles, haga clic en **Ver detalles de rendimiento**.
4. Seleccione la ficha **Vista lógica**, **Vista física** o **Vista de aplicaciones y cargas de trabajo**.

   Según el tipo de objeto, aparecen diferentes gráficos en cada pestaña.

Pestañas de vista	Datos de rendimiento que se muestran para cada tipo de objeto
Vista lógica	• **Matriz de almacenamiento**: IOPS, MIB/s • * Pools*: Latencia, IOPS, MIB/s • **Grupos de volúmenes**: Latencia, IOPS, MIB/s • **Volúmenes**: Latencia, IOPS, MIB/s
Vista física	• **Controladoras**: IOPS, MIB/s, CPU, margen adicional • **Canales de host**: Latencia, IOPS, MIB/s, margen adicional • **Canales de unidad**: Latencia, IOPS, MIB/s • **Unidades**: Latencia, IOPS, MIB/s

Pestañas de vista	Datos de rendimiento que se muestran para cada tipo de objeto
Vista de aplicaciones y cargas de trabajo	• **Matriz de almacenamiento**: IOPS, MIB/s • **Aplicaciones**: Latencia, IOPS, MIB/s • **Cargas de trabajo**: Latencia, IOPS, MIB/s • **Volúmenes**: Latencia, IOPS, MIB/s

5. Utilice las opciones para ver los objetos y la información que necesita.

Opciones

Opciones para ver objetos	Descripción
Expanda un cajón para ver la lista de objetos.	*Cajones de navegación* contiene objetos de almacenamiento, tales como pools, grupos de volúmenes y unidades. Haga clic en el cajón para ver la lista de objetos del cajón.
Seleccione los objetos que desea ver.	Seleccione la casilla de comprobación a la izquierda de cada objeto para elegir los datos de rendimiento que desea ver.
Use filtros para buscar nombres de objeto o nombres parciales.	En la casilla de filtros, introduzca el nombre o un nombre parcial de los objetos para enumerar solo los objetos del cajón.
Haga clic en **Actualizar gráficos** después de seleccionar objetos.	Después de seleccionar objetos de los cajones, seleccione **Actualizar gráficos** para ver datos gráficos de los elementos seleccionados.
Ocultar o mostrar gráfico	Seleccione el título del gráfico para ocular o mostrar el gráfico.

6. Según sea necesario, use las opciones adicionales para ver datos de rendimiento.

Opciones adicionales

Opción	Descripción
Plazo	Seleccione la cantidad de tiempo que desea ver (5 minutos, 1 hora, 8 horas, 1 día, 7 días, o 30 días). El valor predeterminado es 1 hora. Cargar datos de rendimiento para un lapso de 30 días puede llevar varios minutos. No salga de la página web, no actualice la página web ni cierre el explorador mientras se cargan los datos.
Detalles de punto de datos	Pase el cursor sobre el gráfico para ver métricas de un punto de datos en particular.
Barra de desplazamiento	Use la barra de desplazamiento debajo del gráfico para ver un plazo anterior o posterior.
Barra de zoom	Debajo del gráfico, arrastre los bordes de la barra de zoom para reducir un plazo. Cuanto más ancha sea la barra de zoom, menos granulares serán los detalles del gráfico. Para restablecer el gráfico, seleccione una de las opciones del plazo.
Arrastre y suelte	En el gráfico, arrastre el cursor de un momento específico a otro para expandir un plazo. Para restablecer el gráfico, seleccione una de las opciones del plazo.

Ver y guardar los datos de rendimiento tabulares

Es posible ver y guardar datos de gráficos de rendimiento en una tabla de resultados. Esto permite filtrar los datos que se desean ver.

Pasos

1. Desde cualquier gráfico de datos de rendimiento, haga clic en **Iniciar vista de tabla**.

   Se muestra una tabla con todos los datos de rendimiento de los objetos seleccionados.

2. Use el menú desplegable para la selección de objetos y el filtro, según sea necesario.
3. Haga clic en el botón **Mostrar/ocultar columnas** para seleccionar las columnas que desea incluir en la tabla.

   Es posible hacer clic en cada casilla de comprobación para seleccionar o anular la selección de un elemento.

4. Seleccione **Exportar** en la parte inferior de la pantalla para guardar la vista tabular en un archivo de valores separados por comas (CSV).

Aparece el cuadro de diálogo Exportar tabla, que indica el número de filas que se van a exportar y el formato de archivo de la exportación (valores separados por comas o formato CSV).

5. Haga clic en **Exportar** para continuar con la descarga o haga clic en **Cancelar**.

   En función de la configuración del explorador, el archivo se guarda o se le solicita que elija un nombre y una ubicación para el archivo.

   El formato predeterminado del nombre de archivo es `performanceStatistics-yyyy-mm-dd_hh-mm-ss.csv`, que incluye la fecha y la hora en que se exportó el archivo.

Interpretar datos de rendimiento

Los datos de rendimiento pueden guiarlo para ajustar el rendimiento de la cabina de almacenamiento.

Cuando se interpretan datos de rendimiento, es necesario tener en cuenta que varios factores afectan al rendimiento de la cabina de almacenamiento. En la siguiente tabla, se describen los principales aspectos que se deben tener en cuenta.

Datos de rendimiento	Implicancias para el ajuste del rendimiento
Latencia (milisegundos o ms)	Supervise la actividad de I/o de un objeto específico. Identifique potencialmente objetos que son cuellos de botella: • Si un grupo de volúmenes se comparte entre varios volúmenes, es posible que los volúmenes individuales necesiten sus propios grupos de volúmenes para mejorar el rendimiento secuencial de las unidades y reducir la latencia. • Con los pools, se introducen latencias más grandes y es posible que existan cargas de trabajo desparejas entre unidades, por lo que los valores de latencia serán menos significativos y, por lo general, más altos. • Tipo de unidad y latencia por influencia de la velocidad. Con las operaciones de I/o aleatorias, los discos que giran más rápido pasan menos tiempo moviendo elementos hacia y desde diferentes lugares del disco. • Una cantidad muy reducida de unidades genera una cantidad mayor de comandos en la cola y un periodo más largo para que la unidad los procese, lo que aumenta la latencia general del sistema. • Las operaciones de I/o más grandes tienen una mayor latencia debido al tiempo adicional que supone la transferencia de datos. • Una latencia más alta puede indicar que el patrón de I/o es de naturaleza aleatoria. Las unidades con I/o aleatorias tendrán una mayor latencia que las que tienen flujos secuenciales. • Una disparidad de latencia entre unidades o volúmenes de un grupo de volúmenes común puede indicar una unidad lenta.

Datos de rendimiento	Implicancias para el ajuste del rendimiento
IOPS	Entre los factores que afectan a las operaciones de entrada/salida por segundo (IOPS o IO/s) se encuentran los siguientes: • Patrón de acceso (aleatorio o secuencial) • Tamaño de I/O. • Nivel de RAID • Tamaño del bloque de caché • Si el almacenamiento en caché de lectura está habilitado • Si el almacenamiento en caché de escritura está habilitado • Captura previa de lectura de caché dinámica • Tamaño de los segmentos • La cantidad de unidades en los grupos de volúmenes o la cabina de almacenamiento Cuanto más alta es la tasa de aciertos en caché, mayor será la tasa de I/O. Se experimentan tasas más altas de I/o con el almacenamiento en caché de escritura habilitado que con esta opción deshabilitada. Al decidir si habilitar el almacenamiento en caché de escritura para un volumen individual, observe las IOPS actuales y las IOPS máximas. Las tasas deberían ser más altas para los patrones de I/o secuenciales que para los patrones de I/o aleatorios. Más allá del patrón de I/o, habilite el almacenamiento en caché de escritura para maximizar la tasa de I/o y reducir el tiempo de respuesta de la aplicación. Pueden verse mejoras de rendimiento provocadas por el cambio de tamaño de segmentos en las estadísticas de IOPS de un volumen. Experimente para determinar el tamaño de segmento óptimo o utilice el tamaño del sistema de archivos o el tamaño de bloques de la base de datos.
MIB/s	Las tasas de transferencia o rendimiento están determinadas por el tamaño de I/o y la tasa de I/o de la aplicación. Por lo general, las solicitudes de I/o de aplicaciones pequeñas provocan tasas de transferencia más bajas, pero ofrecen una tasa de I/o más rápida y un tiempo de respuesta más corto. Con las solicitudes de I/o de aplicaciones más grandes, es posible obtener tasas de rendimiento más altas. Comprender los patrones de I/o típicos de una aplicación puede ayudar a determinar las tasas de transferencia de I/o máximas para una cabina de almacenamiento específica.

Datos de rendimiento	Implicancias para el ajuste del rendimiento
CPU	Este valor es un porcentaje de la capacidad de procesamiento que se está utilizando. Es posible que note una disparidad en el uso de CPU con los mismos tipos de objetos. Por ejemplo, el uso de CPU de una controladora es pesado o aumenta con el transcurso del tiempo, mientras que el de otra controladora es más liviano o más estable. En este caso, se recomienda cambiar la propiedad de la controladora de uno o varios volúmenes a la controladora con el porcentaje de CPU más bajo. Puede ser conveniente supervisar el uso de CPU en toda la cabina de almacenamiento. Si el uso de CPU sigue subiendo con el tiempo y el rendimiento de las aplicaciones disminuye, es posible que deba añadir más cabinas de almacenamiento. Al añadir cabinas de almacenamiento a su empresa, puede seguir satisfaciendo necesidades de aplicaciones a un nivel de rendimiento aceptable.
Margen adicional	El margen adicional se refiere a la funcionalidad de rendimiento restante de las controladoras, los canales del host de las controladoras y los canales de la unidad de las controladoras. Este valor se expresa como porcentaje, y expresa la brecha entre el máximo rendimiento posible que estos objetos pueden ofrecer y los niveles de rendimiento actuales. • Para las controladoras, el margen adicional es un porcentaje de las IOPS máximas posibles. • Para los canales, el margen adicional es un porcentaje del rendimiento o MIB/s máximo El rendimiento de lectura, el rendimiento de escritura y el rendimiento bidireccional se incluyen en el cálculo.

Ver la jerarquía de almacenamiento

La jerarquía de almacenamiento en la interfaz principal ofrece una vista organizada de los distintos componentes de hardware y objetos de almacenamiento gestionados por la cabina de almacenamiento.

Para ver la jerarquía de almacenamiento, vaya a la página Inicio y haga clic en la flecha desplegable de un componente de la cabina de almacenamiento u objeto de almacenamiento. Una cabina de almacenamiento está compuesta por un conjunto de componentes físicos y lógicos.

Componentes físicos

En esta tabla, se describen los componentes físicos de una cabina de almacenamiento.

Componente	Descripción
Controladora	Una controladora consta de una placa, un firmware y un software. Controla las unidades e implementa las funciones de System Manager.

Componente	Descripción
Bandeja	Una bandeja es un compartimento que se instala en un armario o rack. Incluye componentes de hardware para la cabina de almacenamiento. Existen dos tipos de bandejas: Una bandeja de controladoras y una de unidades. La bandeja de controladoras incluye controladoras y unidades. Una bandeja de unidades incluye módulos de I/o (IOM) y unidades. Si la cabina de almacenamiento contiene tipos de medios o de interfaz diferentes, se muestra una bandeja de unidades para cada tipo de unidad.
Unidad	Una unidad es un dispositivo mecánico electromagnético o un dispositivo de memoria de estado sólido que proporciona medios de almacenamiento físico para datos.
Host	Un host es un servidor que envía I/o a un volumen de una cabina de almacenamiento.
Adaptador de bus de host (HBA)	Un adaptador de bus de host (HBA) es una placa que se encuentra en un host y tiene uno o más puertos de host.
Puerto de host	Un puerto de host es un puerto en un adaptador de bus de host (HBA) que facilita la conexión física a una controladora y se usa en operaciones de I/O.
Cliente de gestión	Un cliente de gestión es el equipo donde se instala un explorador para acceder a System Manager.

Componentes lógicos

Las unidades de la cabina de almacenamiento proporcionan capacidad de almacenamiento físico para los datos. System Manager se utiliza para configurar la capacidad física en los componentes lógicos, como pools, grupos de volúmenes y volúmenes. Estos componentes son las herramientas que se utilizan para configurar, almacenar, mantener y conservar datos en la cabina de almacenamiento. En esta tabla, se describen los componentes lógicos de una cabina de almacenamiento.

Componente	Descripción
Piscina	Un pool es un conjunto de unidades que se agrupan en forma lógica. Se puede usar un pool para crear uno o más volúmenes accesibles para un host. (Se crean volúmenes desde un pool o un grupo de volúmenes).
Grupo de volúmenes	Un grupo de volúmenes es un contenedor para volúmenes con características compartidas. Un grupo de volúmenes tiene una capacidad definida y un nivel de RAID. Se puede usar un grupo de volúmenes para crear uno o más volúmenes a los que se pueda acceder mediante un host. (Los volúmenes se crean a partir de un pool o un grupo de volúmenes).

Componente	Descripción
Volumen	Un volumen es un contenedor en el cual las aplicaciones, las bases de datos y los sistemas de archivos almacenan datos. Es el componente lógico que se crea para que el host acceda al almacenamiento de la cabina de almacenamiento.
Número de unidad lógica (LUN)	Un número de unidad lógica (LUN) es el número asignado al espacio de dirección que utiliza un host para acceder a un volumen. El volumen se presenta al host como capacidad en forma de LUN. Cada host tiene su propio espacio de dirección de LUN. Por lo tanto, distintos hosts pueden utilizar el mismo LUN para acceder a diferentes volúmenes.

Gestione la configuración de la interfaz

Administrar la protección con contraseña

Debe configurar la cabina de almacenamiento con contraseñas para protegerla del acceso no autorizado.

Configurar y cambiar contraseñas

Cuando inicia System Manager por primera vez, se le solicita que establezca una contraseña de administrador. Cualquier usuario que tenga la contraseña de administrador puede realizar cambios de configuración en la cabina de almacenamiento, por ejemplo, añadir, cambiar o quitar objetos o la configuración. Para establecer la contraseña de administrador durante el inicio inicial, consulte "Acceda a System Manager".

Por razones de seguridad, puede intentar introducir una contraseña solo cinco veces antes de que la cabina de almacenamiento quede bloqueada. En este estado, la cabina de almacenamiento rechaza cualquier nuevo intento de introducir una contraseña. Se deben esperar 10 minutos para que la cabina de almacenamiento se restablezca y pueda volver a introducir una contraseña.

Además de la contraseña de administrador, la cabina de almacenamiento incluye perfiles de usuario predefinidos con uno o varios roles asignados. Para obtener más información, consulte "Permisos para roles asignados". Los perfiles de usuario y las asignaciones no pueden cambiarse. Solo las contraseñas pueden modificarse. Si desea cambiar la contraseña de administrador u otras contraseñas de usuario, consulte "Cambiar contraseñas".

Vuelva a introducir contraseñas después de tiempos de espera de la sesión

El sistema solicita la contraseña una sola vez durante una misma sesión de gestión. Sin embargo, una sesión finaliza a los 30 minutos de inactividad; después de ese período, deberá introducir la contraseña otra vez. Si otro usuario que esté gestionando la misma cabina de almacenamiento desde otro cliente de gestión cambia la contraseña mientras su sesión está en progreso, se le solicitará una contraseña la próxima vez que intente realizar una operación de configuración o de vista.

Es posible ajustar el tiempo de espera de la sesión, o bien directamente pueden deshabilitarse los tiempos de espera de sesión. Consulte "Gestionar los tiempos de espera de sesión".

Quite las unidades o la protección con contraseña

Si quita unidades protegidas con contraseña o desea deshabilitar la protección con contraseña, debe tener en cuenta lo siguiente:

- **Si quita unidades con protección por contraseña** — la contraseña se almacena en un área reservada de cada unidad de la matriz de almacenamiento. Si se quitan todas las unidades de la cabina de almacenamiento, la contraseña ya no funciona. Para corregir esta situación, se debe volver a instalar una de las unidades originales en la cabina de almacenamiento.
- **Si desea eliminar la protección con contraseña** — Si ya no desea que los comandos estén protegidos con contraseña, introduzca la contraseña de administrador actual y deje los cuadros de texto de la nueva contraseña en blanco.

> Si se ejecutan comandos de configuración en una cabina de almacenamiento, se pueden producir daños graves, incluso la pérdida de datos. Por este motivo, siempre debe configurar una contraseña de administrador para la cabina de almacenamiento. Use una contraseña de administrador de al menos 15 caracteres alfanuméricos para reforzar la seguridad.

Establezca unidades predeterminadas para los valores de capacidad

System Manager puede mostrar los valores de capacidad en gibibytes (GIB) o tebibytes (TIB).

Las preferencias se almacenan en un almacenamiento local del explorador para que todos los usuarios puedan tener su propia configuración.

Pasos

1. Seleccione MENU:Preferencias[establecer preferencias].
2. Haga clic en el botón de opción gibibytes* o tebibytes* y confirme que desea ejecutar la operación.

   Consulte la siguiente tabla para ver las abreviaturas y los valores.

Abreviatura	Valor
GIB	1,024 3 bytes
TIB	1,024 4 bytes

Establecer el plazo predeterminado para los gráficos de rendimiento

Es posible cambiar el plazo predeterminado que se muestra en los gráficos de rendimiento.

Acerca de esta tarea

Los gráficos de rendimiento que se muestran en la página Inicio y la página rendimiento indican inicialmente el plazo de 1 hora. Las preferencias se almacenan en un almacenamiento local del explorador para que todos los usuarios puedan tener su propia configuración.

Pasos

1. Seleccione MENU:Preferencias[establecer preferencias].

2. En la lista desplegable, seleccione **5 minutos**, **1 hora**, **8 horas**, **1 día** o **7 días**, y confirme que desea llevar a cabo la operación.

Configure el banner de inicio de sesión

Puede crear un banner de inicio de sesión que se presente a los usuarios antes de que puedan establecer sesiones en System Manager. El banner puede incluir un aviso de asesoría y un mensaje de consentimiento.

Acerca de esta tarea

Al crear un banner, este aparece antes de la pantalla de inicio de sesión en un cuadro de diálogo.

Pasos

1. Seleccione MENU:Settings[System].
2. En la sección General, seleccione **Configurar banner de inicio de sesión**.

   Se abre el cuadro de diálogo Configurar banner de inicio de sesión.

3. Introduzca el texto que desea que aparezca en el banner de inicio de sesión.

   No use formato HTML ni otras etiquetas de marcado.

4. Haga clic en **Guardar**.

Resultados

La próxima vez que los usuarios inicien sesión en System Manager, el texto se abrirá en un cuadro de diálogo. Los usuarios deben hacer clic en **Aceptar** para continuar con la pantalla de inicio de sesión.

Gestionar los tiempos de espera de sesión

Es posible configurar los tiempos de espera en System Manager para que las sesiones inactivas de los usuarios se desconecten después de un periodo especificado.

Acerca de esta tarea

De manera predeterminada, el tiempo de espera de sesión para System Manager es de 30 minutos. Es posible ajustar el tiempo, o bien directamente pueden deshabilitarse los tiempos de espera de sesión.

Si se configura Access Management con las funcionalidades del lenguaje de marcado de aserción de seguridad (SAML) integradas en la cabina, es posible que se agote el tiempo de espera de sesión cuando la sesión SSO del usuario alcance su límite máximo. Esto puede ocurrir antes del tiempo de espera de sesión de System Manager.

Pasos

1. Seleccione MENU:Settings[System].
2. En la sección General, seleccione **Habilitar/deshabilitar tiempo de espera de la sesión**.

   Se abre el cuadro de diálogo Habilitar/deshabilitar tiempo de espera de la sesión.

3. Utilice los controles de desplazamiento para aumentar o disminuir el tiempo en minutos.

   El tiempo de espera mínimo que puede configurarse para System Manager es de 15 minutos.

Para desactivar los tiempos de espera de sesiones, anule la selección de la casilla de verificación **establecer el lapso…**.

4. Haga clic en **Guardar**.

Gestionar notificaciones

Información general sobre notificaciones de problemas

System Manager utiliza iconos y otros métodos para notificar los problemas en la cabina de almacenamiento.

Iconos

System Manager utiliza estos iconos para indicar el estado de la cabina de almacenamiento y sus componentes.

.	Descripción
	Óptimo
	No óptimo o con error
	Se requiere atención o corrección
	Precaución

System Manager muestra estos iconos en diversas ubicaciones.

- En el área Notifications de la página Inicio, se muestra el icono de error y un mensaje.
- En el área de navegación, se muestra el icono de error con el icono de la página Home.
- En la página componentes, se muestra el icono de error en el gráfico de unidades y controladoras.

Alertas y LED

Además, System Manager notifica los problemas de otras maneras.

- System Manager envía notificaciones SNMP o mensajes de error por correo electrónico.
- Se encienden los indicadores LED de acción de servicio requerida en el hardware.

Al recibir una notificación de un problema, utilice Recovery Guru como ayuda para corregir el problema. Cuando sea necesario, utilice la documentación del hardware con los pasos de recuperación para reemplazar componentes con errores.

Ver y actuar durante operaciones en curso

Para ver y actuar durante operaciones de ejecución prolongada, use la página Operaciones en curso.

Acerca de esta tarea

Para cada operación enumerada en la página Operations, se muestran un porcentaje de finalización y el tiempo restante estimado para completar la operación. En algunos casos, es posible detener una operación o colocarla en una prioridad superior o inferior. También es posible borrar una operación de copia de volumen de la lista.

Pasos

1. En la página Inicio, seleccione **Mostrar operaciones en curso**.

   Aparece la página Operaciones en curso.

2. Si lo desea, use los enlaces de la columna acciones para detener o cambiar la prioridad de una operación.

   > Lea todo el texto de advertencia proporcionado en los cuadros de diálogo, en particular cuando detiene una operación.

   Es posible detener una operación de copia de volumen o cambiar su prioridad.

3. Una vez completada la operación de copia de volumen, puede seleccionar **Borrar** para eliminarla de la lista.

   En la parte superior de la página Inicio, cuando una operación se completa, se muestran un mensaje informativo y un icono amarillo con una llave inglesa. Este mensaje incluye un enlace que permite borrar la operación de la página Operaciones en curso.

Algunas de las operaciones que aparecen en la página Operaciones en curso son las siguientes:

Funcionamiento	Posible estado de la operación	Acciones que se pueden realizar
Copia de volumen	Completado	Claro
Copia de volumen	En curso	• Cambiar prioridad • Pare
Copia de volumen	Pendiente	Claro
Copia de volumen	Error	• Claro • Volver a copiar
Copia de volumen	Detenido	• Claro • Volver a copiar
Volume create (solo volúmenes de pool estáticos de más de 64 TIB)	En curso	*none*
Volume delete (solo volúmenes de pool estáticos de más de 64 TIB)	En curso	*none*

Funcionamiento	Posible estado de la operación	Acciones que se pueden realizar
Sincronización inicial del grupo de reflejos asíncronos	En curso	Suspender
Sincronización inicial del grupo de reflejos asíncronos	Suspendida	Reanudar
Mirroring sincrónico	En curso	Suspender
Mirroring sincrónico	Suspendida	Reanudar
Reversión de la imagen Snapshot	En curso	Cancelar
Reversión de la imagen Snapshot	Pendiente	Cancelar
Reversión de la imagen Snapshot	En pausa	• Cancelar • Reanudar
Evacuación de la unidad	En curso	Cancelar (depende del tipo de evacuación de la unidad)
Añadir capacidad a un pool o grupo de volúmenes	En curso	*none*
Cambiar el nivel de RAID de un volumen	En curso	*none*
Reducir la capacidad de un pool	En curso	*none*
Recuperación de volúmenes finos	En curso	*none*
Comprobar el tiempo restante en una operación de formato de disponibilidad instantánea (IAF) para los volúmenes del pool	En curso	*none*
Comprobar la redundancia de datos de un grupo de volúmenes	En curso	*none*
Desfragmentar un grupo de volúmenes	En curso	*none*
Inicializar un volumen	En curso	*none*
Aumente la capacidad de un volumen	En curso	*none*

Funcionamiento	Posible estado de la operación	Acciones que se pueden realizar
Cambiar el tamaño de los segmentos de un volumen	En curso	*none*
Copia de unidad	En curso	*none*
Reconstrucción de los datos	En curso	*none*
Copia posterior	En curso	*none*
Borrado de unidad	En curso	*none*
Importación de almacenamiento remoto	En curso	• Cambiar prioridad • Pare
Importación de almacenamiento remoto	Detenido	• Reanudar • Desconectar
Importación de almacenamiento remoto	Error	• Reanudar • Desconectar
Importación de almacenamiento remoto	Completado	Desconectar

Recuperarse de problemas mediante Recovery Guru

Recovery Guru es un componente de System Manager para diagnosticar problemas en la cabina de almacenamiento y recomendar procedimientos de recuperación para corregir los problemas.

Pasos

1. Seleccione **Inicio**.
2. Haga clic en el enlace con la etiqueta **recuperar de *n* problemas** en la parte superior central de la ventana.

   Se muestra el cuadro de diálogo Recovery Guru.

3. Seleccione el primer problema detallado en la lista de resumen y siga las instrucciones del procedimiento de recuperación para corregir el problema. Cuando sea necesario, siga las instrucciones de reemplazo para reemplazar componentes con errores. Repita este paso con cada problema de la lista.

   Una cabina de almacenamiento puede presentar varios problemas relacionados. En este caso, el orden en que se corrijan los problemas puede afectar el resultado. Seleccione y corrija los problemas en el orden en que se detallan en la lista de resumen.

   Si un contenedor de suministro de alimentación presenta varios errores, estos se agrupan y se muestran como un solo problema en la lista de resumen. Si un contenedor de ventilador presenta varios errores,

estos también se muestran como un solo problema.

4. Para asegurarse de que el procedimiento de recuperación se ha realizado correctamente, haga clic en **Volver a comprobar**.

   Si seleccionó un problema de un grupo de reflejos asíncronos o un miembro de un grupo de reflejos asíncronos, primero haga clic en **Borrar** para borrar el error de la controladora y luego haga clic en **Volver a comprobar** para eliminar el evento de Recovery Guru.

   Una vez corregidos todos los problemas, el icono de la cabina de almacenamiento de atención requerida se convertirá en el icono óptimo. En algunos problemas, se muestra un icono de corrección mientras existe una operación, como la reconstrucción, en curso.

5. **Opcional:** para guardar la información de Recovery Guru en un archivo, haga clic en el icono **Guardar**.

   El archivo se guarda en la carpeta de descargas del explorador con el nombre `recovery-guru-failure-yyyy-mm-dd-hh-mm-ss-mmm.html`.

6. Para imprimir la información de Recovery Guru, haga clic en el icono **Imprimir**.

Preguntas frecuentes

¿Qué exploradores son compatibles?

En System Manager se admiten las siguientes versiones de exploradores.

Navegador	Versión mínima
Google Chrome	89
Mozilla Firefox	80
Safari	14
Microsoft Edge	90

¿Cuáles son los métodos abreviados de teclado?

Es posible navegar por System Manager usando solo el teclado.

Navegación general

Acción	Método abreviado de teclado
Moverse al elemento siguiente.	Pestaña
Moverse al elemento anterior.	Mayús + lengüeta
Seleccionar un elemento.	Introduzca

Acción	Método abreviado de teclado
Lista desplegable: Moverse al elemento siguiente o anterior.	Flecha arriba o abajo
Casilla de verificación: Seleccione un elemento.	Barra espaciadora
Botones de opción: Cambiar entre elementos.	Flecha arriba o abajo
Texto expansible: Expandir o contraer un elemento.	Introduzca

Navegación por tablas

Acción	Método abreviado de teclado
Seleccionar una fila.	Tabulador para seleccionar una fila, luego presionar Intro
Desplazarse hacia arriba o hacia abajo.	Flecha abajo/arriba o Av Pág/Re Pág
Cambiar el orden de selección de una columna.	Tabulador para seleccionar el encabezado de una columna, luego presionar Intro

Navegación por calendario

Acción	Método abreviado de teclado
Moverse al mes anterior.	Re Pág
Moverse al mes siguiente.	AV Pág
Moverse al año anterior.	Control + Re Pág
Moverse al año siguiente.	Control + Av Pág
Abrir el seleccionador de fechas, si estuviera cerrado.	Control + Inicio
Moverse al mes actual.	Control/comando + Inicio
Moverse al día anterior.	Control/comando + izquierda
Moverse al día siguiente.	Control/comando + derecha
Moverse a la semana anterior.	Control/comando + Arriba
Moverse a la semana siguiente.	Control/comando + abajo

Acción	Método abreviado de teclado
Seleccionar la fecha deseada.	Introduzca
Cerrar el seleccionador de fecha y borrar la fecha.	Control/comando + fin
Cerrar el seleccionador de fecha sin seleccionar nada.	Escape

¿Cómo se relacionan las estadísticas de rendimiento de volúmenes individuales con el total?

Las estadísticas de pools y grupos de volúmenes se calculan sumando todos los volúmenes, incluidos los volúmenes de capacidad reservada.

El sistema de almacenamiento utiliza la capacidad reservada internamente con el fin de admitir volúmenes finos, Snapshot y mirroring asíncrono; esta capacidad no es visible para hosts de I/O. En consecuencia, es posible que las estadísticas de pools, controladoras y cabinas de almacenamiento no sean iguales a la suma de los volúmenes visibles.

Sin embargo, para las estadísticas de aplicaciones y cargas de trabajo, solo se suman los volúmenes visibles.

¿Por qué los datos se muestran como cero en los gráficos y la tabla?

Cuando se muestra un cero en un punto de datos en los gráficos y la tabla, significa que no hay actividad de I/o del objeto en ese momento específico. Esta situación podría ocurrir porque el host no inicia operaciones de I/o en ese objeto, o podría haber un problema con el objeto en sí.

La visualización de los datos históricos del objeto sigue disponible. Los gráficos y la tabla mostrarán datos distintos a cero una vez que comience la actividad de I/o del objeto.

En la tabla siguiente, se enumeran los motivos más comunes por los cuales un valor de punto de datos puede ser cero en cualquier objeto dado.

Tipo de objeto de nivel de cabina	Motivo por el que los datos se muestran como cero
Volumen	• El volumen no tenía asignación de host.
Grupo de volúmenes	• El grupo de volúmenes se está importando. • El grupo de volúmenes no contiene un volumen asignado a un host, el grupo de volúmenes ***y*** no contiene ninguna capacidad reservada.
Unidad	• Falló la unidad. • Se quitó la unidad. • La unidad está en estado desconocido.

Tipo de objeto de nivel de cabina	Motivo por el que los datos se muestran como cero
Controladora	• La controladora está sin conexión. • Falló la controladora. • Se quitó la controladora. • La controladora está en estado desconocido.
Cabina de almacenamiento	• La cabina de almacenamiento no contiene volúmenes.

¿Qué se muestra en el gráfico de latencia?

En el gráfico latencia, se proporcionan estadísticas de latencia, en milisegundos (ms), de volúmenes, grupos de volúmenes, pools, aplicaciones y cargas de trabajo. Este gráfico se muestra en las pestañas Logical View, Physical View y Vista de aplicaciones y cargas de trabajo.

La latencia se refiere a cualquier demora que ocurre mientras se leen o se escriben datos. Pase el cursor por un punto del gráfico para ver los siguientes valores, en milisegundos (ms), de ese momento específico:

- Tiempo de lectura.
- Tiempo de escritura.
- Tamaño de I/o promedio.

¿Qué se muestra en el gráfico de IOPS?

En el gráfico IOPS, se muestran estadísticas para operaciones de entrada/salida por segundo. En la página Inicio, este gráfico muestra estadísticas de la cabina de almacenamiento. En las pestañas Logical View, Physical View y Vista de aplicaciones y cargas de trabajo del icono rendimiento, este gráfico muestra estadísticas de la cabina de almacenamiento, los volúmenes, los grupos de volúmenes, los pools, las aplicaciones, y cargas de trabajo.

IOPS es la abreviatura en inglés de operaciones *entrada/salida (I/o) por segundo*. Pase el cursor por un punto del gráfico para ver los siguientes valores de ese momento específico:

- Cantidad de operaciones de lectura.
- Cantidad de operaciones de escritura.
- Total de operaciones de lectura y escritura combinadas.

¿Qué se muestra en el gráfico de MIB/s?

El gráfico MIB/s muestra las estadísticas de velocidad de transferencia en mebibytes por segundo. En la página Inicio, este gráfico muestra estadísticas de la cabina de almacenamiento. En las pestañas Logical View, Physical View y Vista de aplicaciones y cargas de trabajo del icono rendimiento, este gráfico muestra estadísticas de la cabina

de almacenamiento, los volúmenes, los grupos de volúmenes, los pools, las aplicaciones, y cargas de trabajo.

MIB/s es la abreviatura de *mebibytes por segundo* o 1,048,576 bytes por segundo. Pase el cursor por un punto del gráfico para ver los siguientes valores de ese momento específico:

- La cantidad de datos leídos.
- La cantidad de datos escritos.
- La cantidad total de datos de lectura y escritura combinados.

¿Qué se muestra en el gráfico de CPU?

En el gráfico de la CPU, se muestran las estadísticas de capacidad de procesamiento de cada controladora (controladora A y controladora B). CPU es la abreviatura en inglés de *central processing unit*. En la página Inicio, este gráfico muestra estadísticas de la cabina de almacenamiento. En la pestaña Vista física del icono rendimiento, este gráfico muestra estadísticas de la cabina de almacenamiento y las unidades.

En el gráfico de la CPU, se muestra el porcentaje de la capacidad de procesamiento de la CPU que se usa para operaciones de la cabina. Aun cuando no se produzcan operaciones de I/o externas, es posible que el porcentaje de utilización de CPU no sea cero, debido a que el sistema operativo de almacenamiento podría estar realizando operaciones en segundo plano y supervisión. Pase el cursor por un punto del gráfico para ver un porcentaje de la funcionalidad de procesamiento que se está utilizando en ese momento específico.

¿Qué se muestra en el gráfico de margen adicional?

El gráfico margen adicional se relaciona con la funcionalidad de rendimiento restante de las controladoras de la cabina de almacenamiento. Este gráfico está visible en la página Inicio y en la pestaña Vista física del icono rendimiento.

En el gráfico margen adicional, se muestra la funcionalidad de rendimiento restante de los objetos físicos del sistema de almacenamiento. Pase el cursor por un punto del gráfico para ver los porcentajes de funcionalidad de IOPS y MIB/s restante para la controladora A y la controladora B.

¿Dónde puedo obtener más información sobre las preferencias de presentación?

Para obtener información acerca de las opciones de visualización disponibles:

- Para seguir leyendo acerca de las unidades predeterminadas para la visualización de valores de capacidad, consulte "Establezca unidades predeterminadas para los valores de capacidad".
- Para seguir leyendo acerca del tiempo predeterminado para visualizar los gráficos de rendimiento, consulte "Establecer el plazo predeterminado para los gráficos de rendimiento".

Pools y grupos de volúmenes

Información general sobre pools y grupos de volúmenes

Es posible crear capacidad de almacenamiento lógico a partir de un subconjunto de unidades sin asignar en la cabina de almacenamiento. Esta capacidad lógica puede

adoptar la forma de un pool o un grupo de volúmenes, según las necesidades del entorno.

¿Qué son los pools y los grupos de volúmenes?

Un *pool* es un conjunto de unidades agrupadas lógicamente. Un *volume group* es un contenedor para volúmenes con características compartidas. Se puede usar un pool o un grupo de volúmenes para crear volúmenes accesibles para un host.

Obtenga más información:

- "Cómo funcionan los pools y los grupos de volúmenes"
- "Terminología de capacidad"
- "Decidir si se utilizará un pool y un grupo de volúmenes"

¿Cómo se crean pools?

Es posible permitir que System Manager cree pools automáticamente cuando detecta capacidad sin asignar en una cabina de almacenamiento. Como alternativa, cuando la creación automática no puede determinar la mejor configuración, puede crear pools manualmente desde el menú:almacenamiento[Pools y grupos de volúmenes].

Obtenga más información:

- "Creación de pools automática versus manual"
- "Crear un pool automáticamente"
- "Crear un pool manualmente"
- "Añadir capacidad a un pool o grupo de volúmenes"

¿Cómo se crean los grupos de volúmenes?

Es posible crear grupos de volúmenes desde el menú:almacenamiento[Pools y grupos de volúmenes].

Obtenga más información:

- "Cree un grupo de volúmenes"
- "Añadir capacidad a un pool o grupo de volúmenes"

Información relacionada

Más información sobre conceptos relacionados con los pools y los grupos de volúmenes:

- "Cómo funciona la capacidad reservada"
- "Cómo funciona caché SSD"

Conceptos

Cómo funcionan los pools y los grupos de volúmenes

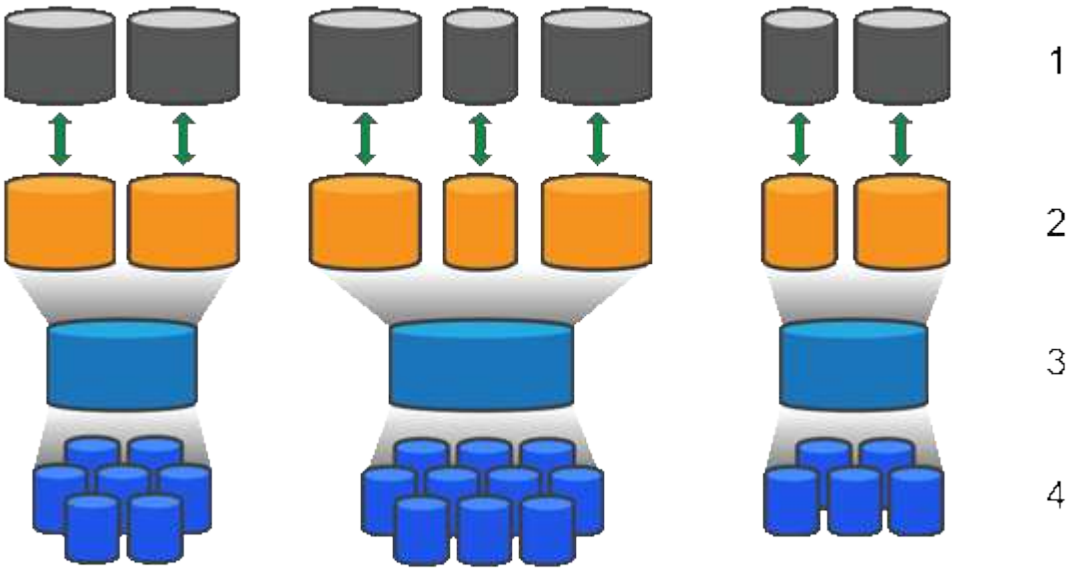
Para aprovisionar almacenamiento, es posible crear un pool o un grupo de volúmenes

que contendrá las unidades de disco duro (HDD) o los discos de estado sólido (SSD) que se desean usar en la cabina de almacenamiento.

El hardware físico se aprovisiona en componentes lógicos para que los datos puedan organizarse y recuperarse fácilmente. Se admiten dos tipos de agrupamientos:

- Piscinas
- Grupos de volúmenes RAID

Los pools y los grupos de volúmenes son las unidades de almacenamiento de nivel superior en una cabina de almacenamiento: Separan la capacidad de las unidades en divisiones gestionables. Dentro de estas divisiones lógicas se encuentran los volúmenes individuales o LUN, donde se almacenan los datos. En la siguiente figura, se ilustra este concepto.



Hacia esta 1 LUN de host; hacia estos 2 volúmenes; grupos o pools de volúmenes de 3; hacia estas 4 unidades de disco duro o SSD de software

Cuando se implementa un sistema de almacenamiento, el primer paso es presentar la capacidad disponible de las unidades a los distintos hosts mediante:

- Creación de pools o grupos de volúmenes con capacidad suficiente
- Adición de la cantidad de unidades requerida para satisfacer los requisitos de rendimiento del pool o grupo de volúmenes
- Selección del nivel adecuado de protección RAID (si se usan grupos de volúmenes) para satisfacer requisitos comerciales específicos

Es posible tener pools o grupos de volúmenes en el mismo sistema de almacenamiento, pero una unidad no puede formar parte de más de un pool o grupo de volúmenes. Los volúmenes que se presentan a los hosts para I/o se crean a continuación, con el espacio del pool o grupo de volúmenes.

Piscinas

Los pools están diseñados para añadir unidades de disco duro físicas a un gran espacio de almacenamiento y proporcionar protección RAID. Un pool crea muchos conjuntos RAID virtuales de la cantidad de unidades totales asignadas al pool y reparte los datos de manera uniforme entre todas las unidades participantes. Si se pierde o se añade una unidad, System Manager vuelve a equilibrar dinámicamente los datos entre todas las

unidades activas.

Los pools funcionan como otro nivel de RAID y virtualizan la arquitectura RAID subyacente para optimizar el rendimiento y la flexibilidad cuando se realizan tareas de reconstrucción, ampliación de unidades y gestión de pérdida de unidades. System Manager establece automáticamente el nivel de RAID en 6 con una configuración de 8+2 (ocho discos de datos más dos discos de paridad).

Emparejamiento de unidades

Es posible seleccionar HDD o SSD para usar en pools; sin embargo, como sucede con los grupos de volúmenes, todas las unidades del pool deben usar la misma tecnología. Los controladores seleccionan automáticamente las unidades que deben incluirse; por lo tanto, debe asegurarse de contar con la cantidad suficiente de unidades para la tecnología seleccionada.

Gestión de unidades con error

Los pools tienen una capacidad mínima de 11 discos; sin embargo, se reserva la capacidad equivalente a una unidad para capacidad de reserva en caso de fallo de unidad. Esta capacidad de reserva se denomina «capacidad de conservación».

Cuando se crean pools, se conserva una cierta capacidad para uso de emergencia. Esta capacidad se expresa en términos de una cantidad de unidades en System Manager, pero la implementación real se reparte entre todo el pool de unidades. La cantidad predeterminada de capacidad que se conserva se basa en la cantidad de unidades del pool.

Después de crear el pool, es posible cambiar el valor de capacidad de conservación a más o menos capacidad, o incluso configurarlo para que no exista capacidad de conservación (valor equivalente a 0 unidades). La cantidad máxima de capacidad que puede conservarse (expresada como cantidad de unidades) es 10, pero la capacidad que está disponible puede ser menor, según la cantidad total de unidades en el pool.

Grupos de volúmenes

Los grupos de volúmenes definen de qué forma se asigna la capacidad a los volúmenes en el sistema de almacenamiento. Las unidades de disco se organizan en grupos y volúmenes RAID entre las unidades en un grupo RAID. Por lo tanto, las opciones de configuración de grupos de volúmenes identifican qué unidades forman parte del grupo y qué nivel de RAID se utiliza.

Cuando se crea un grupo de volúmenes, las controladoras seleccionan automáticamente las unidades que se incluirán en el grupo. Debe seleccionar manualmente el nivel de RAID para el grupo. La capacidad del grupo de volúmenes es la cantidad total de unidades seleccionadas multiplicadas por su capacidad.

Emparejamiento de unidades

Debe emparejar las unidades del grupo de volúmenes según el tamaño y el rendimiento. Si existen unidades pequeñas y grandes en el grupo de volúmenes, se reconocen todas las unidades con el tamaño de capacidad menor. Si existen unidades lentas y rápidas en el grupo de volúmenes, se reconocen todas las unidades con la velocidad menor. Estos factores afectan al rendimiento y a la capacidad general del sistema de almacenamiento.

No puede combinar tecnologías de unidad distintas (unidades de disco duro y unidades SSD). RAID 3, 5 y 6 se limitan a un máximo de 30 unidades. RAID 1 y RAID 10 utilizan mirroring y, en consecuencia, estos grupos de volúmenes tienen una cantidad uniforme de discos.

Gestión de unidades con error

Los grupos de volúmenes utilizan unidades de repuesto como reserva en caso de fallos en los volúmenes RAID 1/10, RAID 3, RAID 5 o RAID 6 incluidos en un grupo de volúmenes. Una unidad de repuesto no contiene datos y añade otro nivel de redundancia a una cabina de almacenamiento.

Si se produce un error en una unidad de la cabina de almacenamiento, la unidad de repuesto automáticamente sustituye a la unidad con error sin necesidad de realizar un cambio físico. Si la unidad de repuesto está disponible cuando se produce un error en una unidad, la controladora utiliza datos de redundancia para reconstruir los datos de la unidad con error en la unidad de repuesto.

Terminología de capacidad

Conozca la forma en que los términos de capacidad se aplican a su cabina de almacenamiento.

Objetos de almacenamiento

La siguiente terminología describe los diferentes tipos de objetos de almacenamiento que pueden interactuar con la cabina de almacenamiento.

Objeto de almacenamiento	Descripción
Host	Un host es un servidor que envía I/o a un volumen de una cabina de almacenamiento.
LUN	Un número de unidad lógica (LUN) es el número asignado al espacio de dirección que utiliza un host para acceder a un volumen. El volumen se presenta al host como capacidad en forma de LUN. Cada host tiene su propio espacio de dirección de LUN. Por lo tanto, distintos hosts pueden utilizar el mismo LUN para acceder a diferentes volúmenes.
Grupo de coherencia de reflejos	Un grupo de coherencia de reflejos es un contenedor para una o más parejas reflejadas. Para las operaciones de mirroring asíncrono, se debe crear un grupo de coherencia de reflejos.
Pareja de volúmenes reflejados	Una pareja reflejada comprende dos volúmenes: Un volumen primario y uno secundario.
Piscina	Un pool es un conjunto de unidades que se agrupan en forma lógica. Se puede usar un pool para crear uno o más volúmenes accesibles para un host. (Se crean volúmenes desde un pool o un grupo de volúmenes).
Grupo de coherencia Snapshot	Un grupo de coherencia Snapshot es una recogida de volúmenes que se tratan como una entidad única cuando se crea una imagen Snapshot. Cada uno de estos volúmenes tiene su propia imagen Snapshot, pero todas las imágenes se crean en el mismo momento específico.

Objeto de almacenamiento	Descripción
Grupo Snapshot	Un grupo Snapshot es una recogida de imágenes Snapshot de un volumen base único.
Volumen Snapshot	Un volumen Snapshot permite que el host acceda a los datos de la imagen Snapshot. El volumen Snapshot tiene su propia capacidad reservada que almacena cualquier modificación del volumen base sin afectar a la imagen Snapshot original.
Volumen	Un volumen es un contenedor en el cual las aplicaciones, las bases de datos y los sistemas de archivos almacenan datos. Es el componente lógico que se crea para que el host acceda al almacenamiento de la cabina de almacenamiento.
Grupo de volúmenes	Un grupo de volúmenes es un contenedor para volúmenes con características compartidas. Un grupo de volúmenes tiene una capacidad definida y un nivel de RAID. Se puede usar un grupo de volúmenes para crear uno o más volúmenes a los que se pueda acceder mediante un host. (Los volúmenes se crean a partir de un pool o un grupo de volúmenes).

Capacidad de almacenamiento

La siguiente terminología describe los diferentes tipos de capacidad que se utilizan en la cabina de almacenamiento.

Tipo de capacidad	Descripción
Capacidad asignada	La capacidad asignada es la capacidad física asignada de las unidades en un pool o grupo de volúmenes. Se utiliza la capacidad asignada para crear volúmenes y para operaciones de servicios de copia.
Capacidad libre	La capacidad libre es la capacidad disponible en un pool o grupo de volúmenes que todavía no se asignó a la creación de un volumen ni las operaciones de servicio de copia y objetos de almacenamiento.
Capacidad de pool o grupo de volúmenes	La capacidad de pool, volumen o grupo de volúmenes es la capacidad de una cabina de almacenamiento que se asignó a un pool o un grupo de volúmenes. Esta capacidad se usa para crear volúmenes y atender las diversas necesidades de capacidad de las operaciones de servicios de copia y objetos de almacenamiento.
Capacidad inutilizable en pool	La capacidad inutilizable del pool es el espacio del pool que no se puede usar debido al desequilibrio de los tamaños de las unidades.
Capacidad de conservación	La capacidad de conservación es la cantidad de capacidad (cantidad de unidades) que se reserva en un pool para admitir fallos de unidad potenciales.

Tipo de capacidad	Descripción
Capacidad notificada	La capacidad notificada es la capacidad que se informa al host y a la que el host puede acceder.
Capacidad reservada	La capacidad reservada es la capacidad física asignada que se usa para cualquier operación de servicio de copia y objeto de almacenamiento. El host no puede leerla directamente.
Caché SSD	La caché SSD es un conjunto de unidades de disco de estado sólido (SSD) que se agrupan lógicamente en la cabina de almacenamiento. La función SSD Cache almacena en caché los datos a los que se accede con más frecuencia (datos "activos") en las unidades SSD de menor latencia para acelerar dinámicamente las cargas de trabajo de la aplicación.
Capacidad sin asignar	La capacidad sin asignar es el espacio de una cabina de almacenamiento que **no** se asignó a un pool o a un grupo de volúmenes.
Capacidad escrita	La capacidad escrita es la cantidad que se escribió de la capacidad reservada asignada para volúmenes finos.

Decidir si se utilizará un pool y un grupo de volúmenes

Es posible crear volúmenes a través de un pool o de un grupo de volúmenes. La mejor selección depende principalmente de los requisitos de almacenamiento clave, como la carga de trabajo de I/o esperada, los requisitos de rendimiento y los requisitos de protección de datos.

Motivos para elegir un pool o un grupo de volúmenes

Elegir una piscina

- Si necesita recompilaciones de la unidad más rápidas y gestión de almacenamiento simplificada, requiere volúmenes finos y/o posee una carga de trabajo altamente aleatoria.
- Si desea distribuir los datos para cada volumen de manera aleatoria en una serie de unidades que componen el pool.

  No es posible configurar o cambiar el nivel de RAID de los pools ni los volúmenes en los pools. Los pools utilizan RAID nivel 6.

Elija un grupo de volúmenes

- Si necesita el máximo ancho de banda del sistema, la capacidad para modificar la configuración de almacenamiento y una carga de trabajo altamente secuencial.
- Si desea distribuir datos en las unidades según un nivel de RAID. Es posible especificar el nivel de RAID al crear el grupo de volúmenes.
- Si desea escribir los datos para cada volumen secuencialmente a través del conjunto de unidades que componen el grupo de volúmenes.

Debido a que los pools pueden coexistir con los grupos de volúmenes, una cabina de almacenamiento puede incluir tanto pools como grupos de volúmenes.

Diferencias de funciones entre pools y grupos de volúmenes

En la siguiente tabla, se incluye una comparación entre grupos de volúmenes y pools.

Uso	Piscina	Grupo de volúmenes
Carga de trabajo aleatoria	Mejor	Muy bien
Carga de trabajo secuencial	Muy bien	Mejor
Tiempo de recompilación de la unidad	Rápido	Más lento
Rendimiento (modo óptimo)	Bueno: Ideal para carga de trabajo aleatoria de bloques pequeños	Bueno: Ideal para carga de trabajo secuencial de bloques grandes
Rendimiento (modo de recompilación de la unidad)	Mejor: Generalmente mejor que RAID 6	Degradado: Caída de rendimiento de hasta el 40 %
Fallos de unidad múltiples	Mayor protección de datos: Recompilaciones priorizadas y más rápidas	Menor protección de datos: Recompilaciones más lentas, mayor riesgo de pérdida de datos
Agregar unidades	Más rápido: Añadir al pool sobre la marcha	Más lento: Requiere una operación de expansión de capacidad dinámica
Compatibilidad con volúmenes finos	Sí	No
Compatibilidad con discos de estado sólido (SSD)	Sí	Sí
Administración simplificada	Sí: No es necesario asignar piezas de repuesto ni configurar RAID	No: Es necesario asignar piezas de repuesto y configurar RAID
Rendimiento ajustable	No	Sí

Comparación funcional de pools y grupos de volúmenes

La función y el objetivo de un pool y un grupo de volúmenes son los mismos. Ambos objetos son un conjunto de unidades agrupadas lógicamente en una cabina de almacenamiento, y se usan para crear volúmenes a los que puede acceder un host.

En la siguiente tabla, se ofrece información para ayudar a decidir si un pool o un grupo de volúmenes es lo que mejor se adapta a sus necesidades de almacenamiento.

Función	Piscina	Grupo de volúmenes
Compatibilidad con diferentes niveles de RAID	No Siempre RAID 6 en System Manager.	Sí. RAID 0, 1, 10, 5 y 6 disponibles.
Compatibilidad con volúmenes finos	Sí	No
Compatibilidad con cifrado de disco completo (FDE)	Sí	Sí
Compatibilidad con Data Assurance (DA)	Sí	Sí
Compatibilidad con protección contra pérdida de bandeja	Sí	Sí
Compatibilidad con protección contra pérdida de cajón	Sí	Sí
Compatibilidad con velocidades de unidad mixtas	Se recomienda que sea la misma, pero no es obligatorio. La unidad más lenta determina la velocidad de todas las unidades.	Se recomienda que sea la misma, pero no es obligatorio. La unidad más lenta determina la velocidad de todas las unidades.
Compatible con capacidad de unidad mixta	Se recomienda que sea la misma, pero no es obligatorio. La unidad más pequeña determina la capacidad de todas las unidades.	Se recomienda que sea la misma, pero no es obligatorio. La unidad más pequeña determina la capacidad de todas las unidades.
Número mínimo de unidades	11	Depende del nivel de RAID. RAID 0 necesita 1. RAID 1 o 10 necesita 2 (requiere un número par). El mínimo para RAID 5 es 3. El mínimo para RAID 6 es 5.
Número máximo de unidades	Hasta el límite máximo para la cabina de almacenamiento	RAID 1 y 10: Hasta el límite máximo de la cabina de almacenamiento - RAID 5, 6 unidades
Es posible elegir unidades individuales al crear un volumen	No	Sí
Es posible especificar el tamaño de los segmentos al crear un volumen	Sí. Compatibilidad con 128 K.	Sí

Función	Piscina	Grupo de volúmenes
Es posible especificar las características de I/o al crear un volumen	No	Sí. Es compatible con sistema de archivos, base de datos, multimedia y opciones personalizadas.
Protección ante fallos de unidad	Utiliza la capacidad de conservación en cada unidad del pool para que la reconstrucción sea más rápida.	Utiliza una unidad de repuesto. La reconstrucción está limitada por las IOPS de la unidad.
Advertencia cuando se llega al límite de capacidad	Sí. Es posible configurar una alerta cuando la capacidad utilizada llega a un porcentaje de la capacidad máxima.	No
Compatibilidad con migración a otra cabina de almacenamiento	No Requiere migrar a un grupo de volúmenes en primer lugar.	Sí
Tamaño de segmentos dinámico (DSS)	No	Sí
Es posible cambiar el nivel de RAID	No	Sí
Ampliación de volumen (aumentar capacidad)	Sí	Sí
Ampliación de capacidad (añadir capacidad)	Sí	Sí
Reducción de capacidad	Sí	No

Los tipos de unidades mixtas (HDD, SSD) no son compatibles con pools o grupos de volúmenes.

Creación de pools automática versus manual

Es posible crear pools de manera automática o manual para permitir el agrupamiento del almacenamiento físico para luego asignarlo dinámicamente según sea necesario. Cuando se crea un pool, es posible añadir unidades físicas.

Creación automática

La creación de pools automática se inicia cuando System Manager detecta capacidad sin asignar en una cabina de almacenamiento. Cuando se detecta capacidad sin asignar, System Manager solicita automáticamente crear uno o varios pools, añadir la capacidad sin asignar a un pool existente, o ambas opciones.

La creación de pools automática se produce cuando se cumple alguna de estas condiciones:

- La cabina de almacenamiento no contiene pools y existen unidades similares suficientes para crear un pool nuevo.
- Se añaden nuevas unidades a una cabina de almacenamiento que contiene al menos un pool.

Cada unidad en un pool debe ser del mismo tipo (unidad de disco duro o unidad de estado sólido) y tener una capacidad similar. System Manager solicita al usuario que complete las siguientes tareas:

- Cree un solo pool si existe una cantidad suficiente de unidades de esos tipos.
- Cree varios pools si la capacidad sin asignar consta de diferentes tipos de unidades.
- Añada las unidades a un pool existente si ya existe un pool definido en la cabina de almacenamiento, y añada nuevas unidades del mismo tipo al pool.
- Añada las unidades del mismo tipo al pool existente y use los otros tipos de unidades para crear distintos pools si las unidades nuevas son de distinto tipo.

Creación manual

Quizás sea conveniente crear un pool manualmente cuando la creación automática no puede determinar cuál es la mejor configuración. Esta situación puede ocurrir por uno de los siguientes motivos:

- Las unidades nuevas pueden añadirse potencialmente a varios pools.
- Uno o varios de los candidatos de pool nuevos pueden usar protección contra pérdida de bandeja o protección contra pérdida de cajón.
- Uno o varios de los candidatos a pool existentes no pueden mantener su estatus de protección contra pérdida de bandeja o protección contra pérdida de cajón.

También es posible que desee crear un pool manualmente si tiene varias aplicaciones en la cabina de almacenamiento y no quiere que compitan por los mismos recursos de la unidad. En este caso, puede considerarse la creación manual de un pool más pequeño para una o varias de aplicaciones. Puede asignar solo uno o dos volúmenes en lugar de asignar la carga de trabajo a un pool más grande que tiene varios volúmenes en los cuales se pueden distribuir los datos. La creación manual de un pool individual dedicado a la carga de trabajo de una aplicación específica puede permitir que las operaciones de cabina de almacenamiento sean más rápidas y con menos contención.

Configurar el almacenamiento

Crear un pool automáticamente

La creación de un pool se inicia automáticamente cuando System Manager detecta unidades sin asignar en la cabina de almacenamiento. Es posible usar la creación automática de pools para configurar fácilmente todas las unidades sin asignar en la cabina de almacenamiento en un pool y añadir unidades a pools existentes.

Antes de empezar

Para abrir el cuadro de diálogo Configuración automática del pool se debe presentar alguna de estas condiciones:

- Se detectó al menos una unidad sin asignar que se puede añadir a un pool existente con tipos de unidades similares.

- Se detectaron once (11) o más unidades sin asignar que se pueden usar para crear un pool nuevo (si no se pueden añadir al pool existente debido a que los tipos de unidad son distintos).

Acerca de esta tarea

Se debe recordar lo siguiente:

- Si se añaden unidades a una cabina de almacenamiento, System Manager automáticamente detecta las unidades y solicita la creación de un pool único o varios pools según el tipo de unidad y la configuración actual.
- Si se definieron pools previamente, System Manager automáticamente ofrece la opción de añadir las unidades compatibles a un pool existente. Si se añaden unidades nuevas a un pool existente, System Manager automáticamente redistribuye los datos conforme a la capacidad nueva, que ahora incluye las unidades nuevas que se añadieron.
- Al configurar una cabina de almacenamiento EF600 o EF300, asegúrese de que cada controladora tenga acceso a un número igual de unidades en las primeras 12 ranuras y un número igual de unidades en las últimas 12 ranuras. Esta configuración ayuda a las controladoras a usar ambos autobuses PCIe de la unidad de forma más eficaz.

Se puede abrir el cuadro de diálogo Configuración automática del pool mediante cualquiera de los siguientes métodos:

- Si se detecta capacidad sin asignar, se muestra la recomendación Configuración automática del pool en el área notificación de la página Inicio. Haga clic en **Ver configuración automática del pool** para abrir el cuadro de diálogo.
- También se puede abrir el cuadro de diálogo Configuración automática del pool en la página Pools y grupos de volúmenes, como se describe en la siguiente tarea.

Pasos

1. Seleccione MENU:almacenamiento[Pools y grupos de volúmenes].
2. Seleccione MENU:More[Iniciar configuración automática del pool].

   En la tabla de resultados, se muestra una lista de los pools nuevos, los pools existentes con unidades añadidas o ambos. El nombre de un pool nuevo es, de forma predeterminada, un número secuencial.

   System Manager realiza las siguientes tareas:

   - Crea un pool único si hay una cantidad suficiente de unidades del mismo tipo (HDD o SSD) y con capacidad similar.
   - Crea varios pools si la capacidad sin asignar consta de diferentes tipos de unidades.
   - Añade las unidades a un pool existente si ya hay un pool definido en la cabina de almacenamiento y si se añaden unidades nuevas del mismo tipo al pool.
   - Añade las unidades del mismo tipo al pool existente y usa los otros tipos de unidades para crear distintos pools si las unidades nuevas son de distinto tipo.
3. Para cambiar el nombre de una nueva agrupación, haga clic en el icono **Editar** (el lápiz).
4. Para ver las características adicionales del pool, sitúe el cursor sobre el icono **Detalles** (la página) o toque el icono.

   Se muestra información acerca del tipo de unidad, la función de seguridad, la funcionalidad Data Assurance (DA), la protección contra pérdida de bandeja y la protección contra pérdida de cajón.

Para las cabinas de almacenamiento EF600 y EF300, también se muestran las configuraciones para el aprovisionamiento de recursos y los tamaños de bloque de volúmenes.

5. Haga clic en **Aceptar**.

Crear un pool manualmente

Se puede crear un pool manualmente (desde un conjunto de candidatos) si la función Pool Auto Configuration no ofrece un pool que satisfaga las necesidades.

Un pool proporciona la capacidad de almacenamiento lógico necesaria desde la cual se pueden crear volúmenes individuales que se pueden utilizar para alojar las aplicaciones.

Antes de empezar

- Se deben tener al menos 11 unidades con el mismo tipo de unidad (HDD o SSD).
- La protección contra pérdida de bandeja requiere que las unidades que componen el pool se coloquen al menos en seis bandejas de unidades distintas y que no haya más de dos unidades en una única bandeja de unidades.
- La protección contra pérdida de cajón requiere que las unidades que componen el pool se coloquen al menos en cinco cajones diferentes y que el pool tenga la misma cantidad de bandejas de unidades en cada cajón.
- Al configurar una cabina de almacenamiento EF600 o EF300, asegúrese de que cada controladora tenga acceso a un número igual de unidades en las primeras 12 ranuras y un número igual de unidades en las últimas 12 ranuras. Esta configuración ayuda a las controladoras a usar ambos autobuses PCIe de la unidad de forma más eficaz. Actualmente, System Manager permite seleccionar unidades en la función Avanzada al crear un grupo de volúmenes. Para la creación de un pool, se recomienda usar todas las unidades de la cabina de almacenamiento.

Pasos

1. Seleccione MENU:almacenamiento[Pools y grupos de volúmenes].
2. Haga clic en MENU:Create[Pool].

   Se muestra el cuadro de diálogo Crear un pool.

3. Escriba un nombre para el pool.
4. **Opcional:** Si tiene más de un tipo de unidad en la matriz de almacenamiento, seleccione el tipo de unidad que desea utilizar.

   En la tabla de resultados, se muestra una lista de todos los pools posibles que se pueden crear.

5. Seleccione el candidato de pool que desea utilizar en función de las siguientes características y, a continuación, haga clic en **Crear**.

Característica	Uso
Capacidad libre	Muestra la capacidad libre del candidato de pool en GIB. Seleccione un candidato de pool con la capacidad que necesita el almacenamiento de la aplicación. La capacidad de conservación (reserva) también se distribuye en todo el pool y no forma parte de la cantidad de capacidad libre.

Característica	Uso
Unidades totales	Indica la cantidad de unidades disponibles en el candidato de pool. System Manager reserva automáticamente tantas unidades como sea posible para la capacidad de conservación (por cada seis unidades de un pool, System Manager reserva una unidad para la capacidad de conservación). Cuando se produce un fallo de unidad, la capacidad de conservación se usa para contener los datos reconstruidos.
Tamaño de bloque de unidad (solo EF300 y EF600)	Muestra el tamaño de bloque (tamaño de sector) que las unidades del pool pueden escribir. Los valores pueden incluir: • 512 — tamaño del sector de 512 bytes. • 4K: Tamaño del sector de 4,096 bytes.
Compatible con la función de seguridad	Indica si este candidato de pool se compone íntegramente de unidades compatibles con la función de seguridad, que pueden ser de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS). • Se puede proteger el pool con Drive Security, pero todas las unidades deben ser compatibles con la función de seguridad para poder usar esta función. • Si desea crear un pool solo para FDE, busque **Sí - FDE** en la columna compatible con la función de seguridad. Si desea crear un pool sólo para FIPS, busque **Sí - FIPS** o **Sí - FIPS (mixta)**. "Mixto" indica una combinación de unidades de 140-2 y 140-3 niveles. Si usa una mezcla de estos niveles, tenga en cuenta que la piscina entonces operará al nivel más bajo de seguridad (140-2). • Se puede crear un pool compuesto por unidades compatibles o no con la función de seguridad, o que tengan una combinación de niveles de seguridad. Si alguna de las unidades del pool no es compatible con la función de seguridad, no se podrá establecer la seguridad del pool.
Habilitar seguridad?	Ofrece la opción de habilitar la función Drive Security con unidades que sean compatibles con la función de seguridad. Si el pool es compatible con la función de seguridad y se creó una clave de seguridad, se podrá habilitar la seguridad al seleccionar la casilla de comprobación. La única manera de quitar Drive Security después de haberse habilitado es eliminar el pool y borrar las unidades.

Característica	Uso
Compatible con DA	Indica si está disponible la función Data Assurance (DA) para este candidato de pool. DA comprueba y corrige los errores que se pueden producir durante la transferencia de datos a través de las controladoras hasta las unidades. DA está habilitada si todas las unidades son compatibles con DA. LA función DA se puede deshabilitar después de crear el volumen. Para ello, seleccione menú:almacenamiento[volúmenes > Ver/editar configuración > Avanzada > Deshabilitar permanentemente la garantía de datos]. Si ESTÁ deshabilitada EN un volumen, no puede volver a habilitarse.
Capacidad de aprovisionamiento de recursos (solo EF300 y EF600)	Muestra si el aprovisionamiento de recursos está disponible para este candidato de pool. El aprovisionamiento de recursos es una función disponible en las cabinas de almacenamiento EF300 y EF600, lo que permite poner en uso los volúmenes de inmediato sin proceso de inicialización en segundo plano.
Protección contra pérdida de bandeja	Indica si la protección contra pérdida de bandeja está disponible. La protección contra pérdida de bandeja garantiza la accesibilidad a los datos de los volúmenes de un pool en caso de que se produzca una pérdida total de comunicación con una única bandeja de unidades.
Protección contra pérdida de cajón	Muestra si la protección contra pérdida de cajón está disponible, que solo se ofrece si se utiliza una bandeja de unidades que contiene cajones. La protección contra pérdida de cajón garantiza la accesibilidad a los datos de los volúmenes de un pool en caso de que se produzca una pérdida total de comunicación con un cajón único de una bandeja de unidades.
Tamaños de bloque de volumen compatibles (solo EF300 y EF600)	Muestra los tamaños de bloque que se pueden crear para los volúmenes del pool: • 512n — 512 bytes nativos. • 512e — emulado 512 bytes. • 4K — 4,096 bytes.

Cree un grupo de volúmenes

Es posible usar un grupo de volúmenes para crear uno o varios volúmenes a los que el host puede acceder. Un grupo de volúmenes es un contenedor para volúmenes con características compartidas, como nivel de RAID y capacidad.

Con unidades de mayor capacidad y la capacidad para distribuir volúmenes en controladoras, crear más de un volumen por grupo de volúmenes es una buena manera de utilizar la capacidad de almacenamiento y proteger los datos.

Antes de empezar

Revise estas directrices para poder crear un grupo de volúmenes:

- Se necesita al menos una unidad sin asignar.
- Existen límites en la cantidad de unidades que se pueden tener en un único grupo de volúmenes. Estos límites varían según el nivel de RAID.
- Para habilitar la protección de bandeja/cajón, debe crear un grupo de volúmenes que utilice unidades ubicadas en al menos tres bandejas o cajones, a menos que utilice RAID 1, donde dos bandejas/cajones es el valor mínimo.
- Si tiene una cabina de almacenamiento EF600 o EF300 y piensa crear un grupo de volúmenes manualmente, asegúrese de que cada controladora tenga acceso a un mismo número de unidades en las primeras 12 ranuras y un mismo número de unidades en las últimas 12 ranuras. Esta configuración ayuda a las controladoras a usar ambos autobuses PCIe de la unidad de forma más eficaz. Actualmente, System Manager permite seleccionar unidades en la función Avanzada al crear un grupo de volúmenes.
- Revise de qué manera la selección del nivel de RAID afecta a la capacidad resultante del grupo de volúmenes:
  - Si selecciona RAID 1, debe añadir dos unidades al mismo tiempo para asegurarse de que se haya seleccionado una pareja reflejada. Las operaciones de mirroring y segmentación (denominada RAID 10 o RAID 1+0) se logran cuando se seleccionan cuatro o más unidades.
  - Si selecciona RAID 5, debe añadir un mínimo de tres unidades para crear el grupo de volúmenes.
  - Si selecciona RAID 6, debe añadir un mínimo de cinco unidades para crear el grupo de volúmenes.

Pasos

1. Seleccione MENU:almacenamiento[Pools y grupos de volúmenes].
2. Haga clic en MENU:Create[Grupo de volúmenes].

   Se muestra el cuadro de diálogo Crear un grupo de volúmenes.

3. Escriba un nombre para el grupo de volúmenes.
4. Seleccione el nivel de RAID que mejor cumpla sus requisitos de almacenamiento y protección de datos.

   Aparece la tabla de candidatos del grupo de volúmenes, donde se muestran solo los candidatos compatibles con el nivel de RAID seleccionado.

5. **Opcional:** Si tiene más de un tipo de unidad en la matriz de almacenamiento, seleccione el tipo de unidad que desea utilizar.

   Aparece la tabla de candidatos del grupo de volúmenes, donde se muestran solo los candidatos compatibles con el tipo de unidad y el nivel de RAID seleccionados.

6. **Opcional:** puede seleccionar el método automático o el método manual para definir las unidades que se utilizarán en el grupo de volúmenes. El método automático es la selección predeterminada.

   Para seleccionar unidades manualmente, haga clic en el enlace **selección manual de unidades (avanzada)**. Al hacer clic en esta opción, cambia a **Seleccionar automáticamente unidades (avanzadas)**.

   El método manual permite seleccionar las unidades específicas que componen el grupo de volúmenes. Es posible seleccionar unidades sin asignar específicas para obtener la capacidad requerida. Si la cabina de almacenamiento contiene unidades con tipos de medios diferentes o tipos de interfaces diferentes, es posible seleccionar solo la capacidad sin configurar de un solo tipo de unidad para crear el grupo de volúmenes.

Solo los expertos que entienden la redundancia de unidades y las configuraciones de unidades óptimas deben usar el método manual.

7. Según las características de la unidad que se muestran, seleccione las unidades que desea usar en el grupo de volúmenes y, a continuación, haga clic en **Crear**.

   Las características de la unidad que se muestran dependen de si se seleccionó el método automático o el método manual.

Características de unidades del método Automatic

Característica	Uso
Capacidad libre	Muestra la capacidad disponible en GIB. Seleccione un candidato de grupo de volúmenes con capacidad para las necesidades de almacenamiento de la aplicación.
Unidades totales	Muestra la cantidad de unidades disponibles para este grupo de volúmenes. Seleccione un candidato de grupo de volúmenes con la cantidad de unidades que desea.
Tamaño de bloque de unidad (solo EF300 y EF600)	Muestra el tamaño de bloque (tamaño de sector) que las unidades del grupo pueden escribir. Los valores pueden incluir: • 512 — tamaño del sector de 512 bytes. • 4K: Tamaño del sector de 4,096 bytes.
Compatible con la función de seguridad	Indica si este candidato de grupo de volúmenes está compuesto enteramente por unidades compatibles con la función de seguridad, que pueden ser unidades de cifrado de disco completo (FDE) o unidades de estándar de procesamiento de información federal (FIPS). • Es posible proteger un grupo de volúmenes con Drive Security, pero todas las unidades deben ser compatibles con la función de seguridad para usar esa función. • Si desea crear un grupo de volúmenes solo con FDE, busque **Sí - FDE** en la columna compatible con la función de seguridad. Si desea crear un grupo de volúmenes solo con FIPS, busque **Sí - FIPS** o **Sí - FIPS (mixta)**. "Mixto" indica una combinación de unidades de 140-2 y 140-3 niveles. Si usa una combinación de estos niveles, tenga en cuenta que el grupo de volúmenes luego funcionará con el nivel de seguridad más bajo (140-2). • Puede crear un grupo de volúmenes compuesto por unidades que sean compatibles con la función de seguridad o no, o que presenten una combinación de niveles de seguridad. Si las unidades del grupo de volúmenes incluyen unidades que no son compatibles con la función de seguridad, el grupo de volúmenes no podrá ser seguro.
Habilitar seguridad?	Ofrece la opción de habilitar la función Drive Security con unidades que sean compatibles con la función de seguridad. Si el grupo de volúmenes es compatible con la función de seguridad y se configuró una clave de seguridad, seleccione la casilla de comprobación para habilitar Drive Security. La única manera de eliminar Drive Security después de habilitarla es eliminar el grupo de volúmenes y borrar las unidades.

Característica	Uso
Compatible con DA	Indica si Data Assurance (DA) está disponible para el grupo. La garantía de datos (DA) comprueba y corrige los errores que se pueden producir durante la transferencia de datos a través de las controladoras hasta las unidades. Si desea usar DA, seleccione un grupo de volúmenes con capacidad DA. (Para unidades compatibles con DA, LA función DA se habilita automáticamente en los volúmenes creados en el pool). Un grupo de volúmenes puede contener unidades con o sin capacidad DA, pero todas las unidades deben poseer capacidad DA para que pueda usarse esta función.
Capacidad de aprovisionamiento de recursos (solo EF300 y EF600)	Muestra si el aprovisionamiento de recursos está disponible para este grupo. El aprovisionamiento de recursos es una función disponible en las cabinas de almacenamiento EF300 y EF600, lo que permite poner en uso los volúmenes de inmediato sin proceso de inicialización en segundo plano.
Protección contra pérdida de bandeja	Indica si la protección contra pérdida de bandeja está disponible. La protección contra pérdida de bandeja garantiza accesibilidad a los datos en los volúmenes de un grupo de volúmenes si se produce una pérdida total de comunicación con una bandeja.
Protección contra pérdida de cajón	Muestra si la protección contra pérdida de cajón está disponible, que solo se ofrece si se utiliza una bandeja de unidades que contiene cajones. La protección contra pérdida de cajón garantiza accesibilidad a los datos en los volúmenes de un grupo de volúmenes si se produce una pérdida total de comunicación con un solo cajón en una bandeja de unidades.
Tamaños de bloque de volumen compatibles (solo EF300 y EF600)	Muestra los tamaños de bloque que se pueden crear para los volúmenes del grupo: • 512n — 512 bytes nativos. • 512e — emulado 512 bytes. • 4K — 4,096 bytes.

Características de unidades del método Manual

Característica	Uso
Tipo de medios	Indica el tipo de medio. Se admiten los siguientes tipos de medios: • Unidad de disco duro • Unidad de estado sólido (SSD) Un grupo de volúmenes debe contener unidades de un mismo tipo de medio (todos discos SSD o todas unidades de disco duro). Un grupo de volúmenes no puede contener una combinación de tipos de medios o tipos de interfaces.
Tamaño de bloque de unidad (solo EF300 y EF600)	Muestra el tamaño de bloque (tamaño de sector) que las unidades del grupo pueden escribir. Los valores pueden incluir: • 512 — tamaño del sector de 512 bytes. • 4K: Tamaño del sector de 4,096 bytes.
Capacidad de unidad	Indica la capacidad de la unidad. • Siempre que sea posible, seleccione unidades con una capacidad igual a la de las unidades actuales en el grupo de volúmenes. • Si debe añadir unidades sin asignar con una capacidad menor, tenga en cuenta que se reducirá la capacidad utilizable de cada unidad actual en el grupo de volúmenes. Por lo tanto, la capacidad de las unidades es la misma en todo el grupo de volúmenes. • Si debe añadir unidades sin asignar con una capacidad mayor, tenga en cuenta que se reducirá la capacidad utilizable de las unidades sin asignar que añada para que coincida con las capacidades actuales de las unidades en el grupo de volúmenes.
Soporte	Indica la ubicación del soporte de la unidad.
Ranura	Indica la ubicación de la ranura de la unidad.
Velocidad (RPM)	Indica la velocidad de la unidad.
Tamaño de sector lógico	Indica el tamaño y el formato del sector.

Característica	Uso
Compatible con la función de seguridad	Indica si este candidato de grupo de volúmenes está compuesto enteramente por unidades compatibles con la función de seguridad, que pueden ser unidades de cifrado de disco completo (FDE) o unidades de estándar de procesamiento de información federal (FIPS). • Es posible proteger un grupo de volúmenes con Drive Security, pero todas las unidades deben ser compatibles con la función de seguridad para usar esa función. • Si desea crear un grupo de volúmenes solo con FDE, busque **Sí - FDE** en la columna compatible con la función de seguridad. Si desea crear un grupo de volúmenes solo con FIPS, busque **Sí - FIPS** o **Sí - FIPS (mixta)**. "Mixto" indica una combinación de unidades de 140-2 y 140-3 niveles. Si usa una combinación de estos niveles, tenga en cuenta que el grupo de volúmenes luego funcionará con el nivel de seguridad más bajo (140-2). • Puede crear un grupo de volúmenes compuesto por unidades que sean compatibles con la función de seguridad o no, o que presenten una combinación de niveles de seguridad. Si las unidades del grupo de volúmenes incluyen unidades que no son compatibles con la función de seguridad, el grupo de volúmenes no podrá ser seguro.
Compatible con DA	Indica si Data Assurance (DA) está disponible para el grupo. La garantía de datos (DA) comprueba y corrige los errores que se pueden producir durante la comunicación de los datos a través de las controladoras hasta las unidades. Si desea usar DA, seleccione un grupo de volúmenes con capacidad DA. (Para unidades compatibles con DA, LA función DA se habilita automáticamente en los volúmenes creados en el pool). Un grupo de volúmenes puede contener unidades con o sin capacidad DA, pero todas las unidades deben poseer capacidad DA para que pueda usarse esta función.
Tamaños de bloque de volumen compatibles (solo EF300 y EF600)	Muestra los tamaños de bloque que se pueden crear para los volúmenes del grupo: • 512n — 512 bytes nativos. • 512e — emulado 512 bytes. • 4K — 4,096 bytes.
Capacidad de aprovisionamiento de recursos (solo EF300 y EF600)	Muestra si el aprovisionamiento de recursos está disponible para este grupo. El aprovisionamiento de recursos es una función disponible en las cabinas de almacenamiento EF300 y EF600, lo que permite poner en uso los volúmenes de inmediato sin proceso de inicialización en segundo plano.

Añadir capacidad a un pool o grupo de volúmenes

Es posible añadir unidades para expandir la capacidad de un pool o un grupo de volúmenes existente.

Con la ampliación, se incluye capacidad libre adicional al pool o grupo de volúmenes. Se puede utilizar esta capacidad libre para crear volúmenes adicionales. Es posible acceder a los datos de los volúmenes durante esta operación.

Antes de empezar

- Las unidades deben estar en el estado óptima.
- Las unidades deben ser del mismo tipo (unidad de disco duro o unidad de estado sólido).
- El pool o el grupo de volúmenes deben estar en el estado óptima.
- La cantidad máxima de volúmenes permitidos en un grupo de volúmenes es de 256.
- La cantidad máxima de volúmenes permitidos en un pool depende del modelo del sistema de almacenamiento:
  - 2,048 volúmenes (series EF600 y E5700)
  - 1,024 volúmenes (EF300)
  - 512 volúmenes (serie E2800)
- Si todas las unidades del pool o grupo de volúmenes son compatibles con la función de seguridad, añada únicamente unidades compatibles con la función de seguridad para continuar usando las habilidades de cifrado de ese tipo de unidades.

  Las unidades compatibles con la función de seguridad pueden ser unidades de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS).

Acerca de esta tarea

En los pools, es posible añadir 60 unidades al mismo tiempo como máximo. En los grupos de volúmenes, es posible añadir 2 unidades al mismo tiempo como máximo. Si necesita añadir más unidades que la cantidad máxima, repita el procedimiento. (Un pool no puede contener más unidades que el límite máximo de un sistema de almacenamiento.)

> Al añadir unidades, es posible que sea necesario aumentar la capacidad de conservación. Se recomienda aumentar la capacidad reservada después de una operación de ampliación.

> Evite el uso de unidades compatibles con la función Data Assurance (DA) para añadir capacidad a un pool o un grupo de volúmenes no compatibles con DA. El pool o el grupo de volúmenes no podrán aprovechar las funcionalidades de las unidades compatibles con DA. Contemple la posibilidad de usar unidades no compatibles con DA en esta situación.

Pasos

1. Seleccione MENU:almacenamiento[Pools y grupos de volúmenes].
2. Seleccione el pool o el grupo de volúmenes a los que desea añadir unidades y haga clic en **Añadir capacidad**.

   Se muestra el cuadro de diálogo Añadir capacidad. Solo se muestran las unidades sin asignar que son compatibles con el pool o el grupo de volúmenes.

3. En **Seleccione las unidades para añadir capacidad…**, seleccione una o varias unidades que desea añadir al pool o grupo de volúmenes existente.

   El firmware de la controladora ordena las unidades sin asignar de modo que las mejores opciones se enumeren primero. La capacidad libre total añadida al pool o grupo de volúmenes se muestra debajo de la lista en **capacidad total seleccionada**.

Detalles del campo

Campo	Descripción
Bandeja	Indica la ubicación de la bandeja de la unidad.
Bahía	Indica la ubicación de la bahía de la unidad.
Capacidad (GIB)	Indica la capacidad de la unidad. • Siempre que sea posible, seleccione unidades con una capacidad igual a la de las unidades actuales en el pool o el grupo de volúmenes. • Si debe añadir unidades sin asignar con una capacidad menor, tenga en cuenta que se reducirá la capacidad utilizable de cada unidad actual en el pool o el grupo de volúmenes. Por lo tanto, la capacidad de las unidades es la misma en todo el pool o grupo de volúmenes. • Si debe añadir unidades sin asignar con una capacidad mayor, tenga en cuenta que se reducirá la capacidad utilizable de las unidades sin asignar que añada para que coincida con las capacidades actuales de las unidades en el pool o el grupo de volúmenes.
Compatible con la función de seguridad	Indica si la unidad es compatible con la función de seguridad. • Para proteger el pool o el grupo de volúmenes con la función Drive Security, todas las unidades deben ser compatibles con la función de seguridad. • Es posible crear un pool o un grupo de volúmenes con una combinación de unidades compatibles y no compatibles con la función de seguridad, pero la función Drive Security no puede estar habilitada. • Un pool o un grupo de volúmenes con todas unidades compatibles con la función de seguridad no pueden aceptar una unidad no compatible con la función de seguridad para realizar reservas o expansión, aunque no esté en uso la funcionalidad de cifrado. • Las unidades que se notifican como compatibles con la función de seguridad pueden ser unidades de cifrado de disco completo (FDE) o unidades de estándar de procesamiento de información federal (FIPS). • Una unidad FIPS puede ser de nivel 140-2 o 140-3, con el nivel 140-3 como mayor nivel de seguridad. Si se selecciona una combinación de unidades de 140-2 y 140-3 niveles, el pool o el grupo de volúmenes luego se operará al nivel de seguridad menor (140-2).

Campo	Descripción
Compatible con DA	Indica si la unidad es compatible con la función Data Assurance (DA). • No se recomienda el uso de unidades compatibles con la función Data Assurance (DA) para añadir capacidad a un pool o un grupo de volúmenes compatibles con DA. El pool o el grupo de volúmenes ya no tendrán funcionalidades DE DA y no será posible habilitar DA en los volúmenes recién creados dentro del pool o grupo de volúmenes. • No se recomienda el uso de unidades compatibles con la función Data Assurance (DA) para añadir capacidad a un pool o un grupo de volúmenes no compatibles con DA, ya que el pool o el grupo de volúmenes no podrán aprovechar las funcionalidades de las unidades compatible con DA (los atributos de las unidades no coincidirán). Contemple la posibilidad de usar unidades que no sean compatibles con DA en esta situación.
Compatible con DULBE	Indica si la unidad tiene la opción de error de bloque lógico no escrito o desasignado (DULBE). DULBE es una opción en las unidades NVMe con la que la cabina de almacenamiento EF300 o EF600 puede admitir volúmenes con aprovisionamiento de recursos.

4. Haga clic en **Agregar**.

   Si desea añadir unidades a un pool o grupo de volúmenes, se muestra un cuadro de diálogo de confirmación al seleccionar una unidad por la que el pool o el grupo de volúmenes ya no tendrá uno o varios de los siguientes atributos:

   - Protección contra pérdida de bandeja
   - Protección contra pérdida de cajón
   - Funcionalidad de cifrado de disco completo
   - Funcionalidad de garantía de datos
   - Funcionalidad DULBE
5. Para continuar, haga clic en **Sí**; de lo contrario, haga clic en **Cancelar**.

Resultados

Después de añadir las unidades sin asignar a un pool o grupo de volúmenes, se redistribuyen los datos de cada volumen del pool o del grupo de volúmenes para incluir las unidades adicionales.

Gestionar el almacenamiento

Compruebe la redundancia de un volumen

Con ayuda del soporte técnico o según indique Recovery Guru, puede comprobar la redundancia de un volumen en un pool o grupo de volúmenes para determinar si los datos de ese volumen son consistentes.

Los datos de redundancia se utilizan para reconstruir información rápidamente en una unidad de reemplazo si

falla una de las unidades de un pool o grupo de volúmenes.

Antes de empezar

- El estado del pool o del grupo de volúmenes debe ser óptimo.
- El pool o grupo de volúmenes no debe tener operaciones de modificación del volumen en curso.
- Es posible verificar la redundancia en cualquier nivel de RAID excepto en RAID 0, ya que RAID 0 no tiene redundancia de datos.

> Compruebe la redundancia del volumen solamente cuando Recovery Guru le indique hacerlo y con la ayuda del soporte técnico.

Acerca de esta tarea

Es posible realizar esta comprobación solo en un pool o grupo de volúmenes a la vez. Una comprobación de redundancia de un volumen realiza las acciones siguientes:

- Analiza los bloques de datos en un volumen RAID 3, un volumen RAID 5 o un volumen RAID 6, y verifica la información de redundancia de cada bloque. (RAID 3 solo puede asignarse a grupos de volúmenes con interfaz de línea de comandos.)
- Compara los bloques de datos en unidades reflejadas RAID 1.
- Devuelve errores de redundancia si el firmware de la controladora determina que los datos no coinciden.

> Si se ejecuta de inmediato una comprobación de redundancia en el mismo pool o grupo de volúmenes, se puede generar un error. Para evitar este problema, espere de uno a dos minutos antes de ejecutar otra comprobación de redundancia en el mismo pool o grupo de volúmenes.

Pasos

1. Seleccione MENU:almacenamiento[Pools y grupos de volúmenes].
2. Seleccione menú:tareas no comunes[comprobar redundancia de volumen].

   Se muestra el cuadro de diálogo comprobar redundancia.

3. Seleccione los volúmenes que desea verificar y después escriba `check` para confirmar que desea llevar a cabo esta operación.
4. Haga clic en **Comprobación**.

   Comienza la operación de comprobación de redundancia del volumen. Los volúmenes del pool o grupo de volúmenes se analizan secuencialmente, comenzando por la parte superior de la tabla en el cuadro de diálogo. Estas acciones ocurren a medida que se analiza cada volumen:

   - Se selecciona el volumen en la tabla de volúmenes.
   - El estado de la comprobación de redundancia se muestra en la columna **Estado**.
   - La comprobación se detiene en cada error de medios o de paridad detectado, y después informa ese error.

Más acerca del estado de la comprobación de redundancia

Estado	Descripción
Pendiente	Este es el primer volumen que se analizará, y no ha hecho clic en Inicio para comenzar la comprobación de redundancia. o. La operación de comprobación de redundancia se lleva a cabo en otros volúmenes del pool o grupo de volúmenes.
Comprobando	El volumen está sometido a la comprobación de redundancia.
Superada	El volumen superó la comprobación de redundancia. No se detectaron faltas de coincidencia en la información sobre redundancia.
Error	El volumen no superó la comprobación de redundancia. Se detectaron faltas de coincidencia en la información sobre redundancia.
Error de medios	Los medios de la unidad presentan defectos y son ilegibles. Siga las instrucciones que se señalan en Recovery Guru.
Error de paridad	La paridad no es lo que debería ser en una cierta porción de los datos. Un error de paridad es potencialmente grave y puede producir la pérdida permanente de los datos.

5. Haga clic en **hecho** después de comprobar el último volumen del pool o grupo de volúmenes.

Elimine un pool o grupo de volúmenes

Es posible eliminar un pool o un grupo de volúmenes para crear más capacidad sin asignar, que puede volver a configurarse para satisfacer necesidades de almacenamiento de aplicaciones.

Antes de empezar

- Previamente, es necesario realizar backup de los datos en todos los volúmenes del pool o grupo de volúmenes.
- Detuvo todas las operaciones de entrada/salida (I/o).
- Desmontó todos los sistemas de archivos de los volúmenes.
- Previamente, deben haberse eliminado todas las relaciones de reflejo en el pool o el grupo de volúmenes.
- Detuvo todas las operaciones de copia de volumen en curso para el pool o el grupo de volúmenes.
- El pool o el grupo de volúmenes no participan en una operación de mirroring asíncrono.
- Las unidades en el grupo de volúmenes no tienen una reserva persistente.

Pasos

1. Seleccione MENU:almacenamiento[Pools y grupos de volúmenes].
2. Seleccione un pool o un grupo de volúmenes de la lista.

   Solo puede seleccionar un pool o un grupo de volúmenes a la vez. Desplácese hacia abajo por la lista para ver pools o grupos de volúmenes adicionales.

3. Seleccione menú:tareas no comunes[Eliminar] y confirme.

Resultados

System Manager realiza lo siguiente:

- Elimina todos los datos en el pool o grupo de volúmenes.
- Elimina todas las unidades en el pool o grupo de volúmenes.
- Desasigna las unidades asociadas, lo que permite reutilizarlas en pools o grupos de volúmenes nuevos o existentes.

Consolidar la capacidad libre de un grupo de volúmenes

Utilice la opción consolidar capacidad libre para consolidar las extensiones libres existentes de un grupo de volúmenes seleccionado. Con esta acción, se pueden crear volúmenes adicionales de la cantidad máxima de capacidad libre de un grupo de volúmenes.

Antes de empezar

- El grupo de volúmenes debe contener al menos un área de capacidad libre.
- Todos los volúmenes del grupo de volúmenes deben estar en línea y con el estado óptima.
- No debe haber operaciones de modificación de volúmenes en curso, por ejemplo, cambio del tamaño de segmento de un volumen.

Acerca de esta tarea

No se puede cancelar la operación una vez iniciada. Se puede acceder a los datos durante la operación de consolidación.

Para abrir el cuadro de diálogo consolidar capacidad libre, se puede utilizar cualquiera de los siguientes métodos:

- Si se detecta al menos un área de capacidad libre para un grupo de volúmenes, se muestra la recomendación de que se debe consolidar la capacidad libre en la página Inicio del área notificación. Haga clic en el enlace **consolidar capacidad libre** para abrir el cuadro de diálogo.
- También se puede abrir el cuadro de diálogo consolidar capacidad libre en la página Pools y grupos de volúmenes, como se describe en la siguiente tarea.

Más información acerca de las áreas de capacidad libre

Un área de capacidad libre es la capacidad libre que puede surgir después de eliminar un volumen o por no utilizar toda la capacidad libre disponible durante la creación de un volumen. Cuando se crea un volumen en un grupo de volúmenes que tiene una o más áreas de capacidad libre, la capacidad del volumen se limita al área de capacidad libre más grande de ese grupo de volúmenes. Por ejemplo, si un grupo de volúmenes tiene una capacidad libre total de 15 GIB y el área de capacidad libre más grande es 10 GIB, el volumen más grande que se puede crear es de 10 GIB.

Se puede consolidar la capacidad libre de un grupo de volúmenes para mejorar el rendimiento de escritura. La capacidad libre del grupo de volúmenes se fragmentará con el tiempo a medida que el host escribe, modifica y elimina archivos. A la larga, la capacidad disponible ya no estará ubicada en un único bloque contiguo, sino que estará distribuida en pequeños fragmentos del grupo de volúmenes. Esto aumenta la fragmentación del archivo, ya que el host debe escribir archivos nuevos en forma de fragmentos para poder ubicarlos en los rangos disponibles de los clústeres libres.

Cuando se consolida la capacidad libre de un grupo de volúmenes seleccionado, se observa que mejora el rendimiento del sistema de archivos cada vez que el host escribe en archivos nuevos. El proceso de consolidación también ayuda a evitar que se fragmenten archivos nuevos en el futuro.

Pasos

1. Seleccione MENU:almacenamiento[Pools y grupos de volúmenes].
2. Seleccione el grupo de volúmenes que tenga la capacidad libre que se desea consolidar y, luego, seleccione menú:tareas no comunes[consolidar la capacidad libre del grupo de volúmenes].

   Se muestra el cuadro de diálogo consolidar capacidad libre.

3. Tipo `consolidate` para confirmar que desea llevar a cabo esta operación.
4. Haga clic en **consolidar**.

   System Manager comienza a consolidar (desfragmentar) las áreas de capacidad libre del grupo de volúmenes en una cantidad contigua para las tareas subsiguientes de configuración del almacenamiento.

Después de terminar

Seleccione MENU:Inicio[Ver operaciones en curso] para ver el progreso de la operación Consolidate Free Capacity. Es posible que esta operación demore y que afecte el rendimiento del sistema.

Exportar/importar grupos de volúmenes

La migración de grupos de volúmenes permite exportar un grupo de volúmenes de forma tal que se lo pueda importar a otra cabina de almacenamiento.

La función Export/Import no se admite en la interfaz de usuario de SANtricity System Manager. Deben usar la interfaz de línea de comandos (CLI) para exportar o importar un grupo de volúmenes a otra cabina de almacenamiento.

Encender las luces localizadoras en un pool, un grupo de volúmenes o la caché SSD

Se pueden localizar las unidades para identificar físicamente todas las unidades que conforman una caché SSD, un pool o un grupo de volúmenes seleccionado. En cada unidad, se enciende un indicador LED en la caché SSD, el pool o el grupo de volúmenes

seleccionado.

Pasos

1. Seleccione MENU:almacenamiento[Pools y grupos de volúmenes].
2. Seleccione el pool, el grupo de volúmenes o la caché SSD que desea localizar y, a continuación, haga clic en **more › encender las luces de localización**.

   Se muestra un cuadro de diálogo que indica que las luces de las unidades que conforman la caché SSD, el pool o el grupo de volúmenes seleccionado están encendidas.

3. Una vez que haya localizado correctamente las unidades, haga clic en **Apagar**.

Quite capacidad de un pool o una caché SSD

Es posible quitar unidades para reducir la capacidad de un pool o una caché SSD existente.

Una vez eliminadas las unidades, se redistribuirán los datos de cada volumen del pool o de la caché SSD a las unidades restantes. Las unidades eliminadas se mostrarán como sin asignar y su capacidad se volverá parte de la capacidad libre total de la cabina de almacenamiento.

Acerca de esta tarea

Siga estas directrices al quitar capacidad:

- No puede quitar la última unidad de una caché SSD sin antes eliminar la caché SSD.
- No se puede reducir la cantidad de unidades en un pool a menos de 11.
- Es posible eliminar un máximo de 12 unidades al mismo tiempo. Si necesita quitar más de 12 unidades, repita el procedimiento.
- No puede quitar unidades si no dispone de capacidad libre suficiente en el pool o la caché SSD para contener los datos cuando esos datos se redistribuyan a las unidades restantes del pool o de la caché SSD.

Conozca el posible impacto en el rendimiento

- Cuando se quitan unidades de un pool o una caché SSD, es posible que se reduzca el rendimiento del volumen.
- Cuando se quita capacidad de un pool o una caché SSD, no se consume capacidad de conservación. Sin embargo, es posible que la capacidad de conservación se reduzca según la cantidad de unidades que queden en el pool o la caché SSD.

Conozca el impacto sobre las unidades compatibles con la función de seguridad

- Si se quita la última unidad no compatible con la función de seguridad, el pool solo contendrá unidades compatibles con la función de seguridad. En esta situación, se ofrece la opción de habilitar la seguridad para el pool.
- Si se quita la última unidad que no es compatible con la función Data Assurance (DA), el pool solo contendrá unidades compatibles con DA.

> Todos los volúmenes nuevos que se creen en el pool serán compatibles con DA. Si desea que los volúmenes existentes sean compatibles con DA, debe eliminar y volver a crear los volúmenes.

Pasos

1. Seleccione MENU:almacenamiento[Pools y grupos de volúmenes].
2. Seleccione el pool o la caché SSD y haga clic en menú:más[Quitar capacidad].

   Se muestra el cuadro de diálogo Eliminar capacidad.

3. Seleccione una o varias unidades de la lista.

   A medida que seleccione o anule la selección de unidades en la lista, se actualizará el campo **capacidad total seleccionada**. Este campo muestra la capacidad total del pool o de la caché SSD que se obtendrá al quitar las unidades seleccionadas.

4. Haga clic en **Quitar** y confirme que desea quitar las unidades.

   La capacidad recién reducida del pool o de la caché SSD se reflejará en la vista Pools y grupos de volúmenes.

Modifique la configuración del pool y del grupo

Cambiar la configuración de un pool

La configuración de un pool se puede editar, incluido el nombre, las alertas de capacidad, las prioridades de modificación y la capacidad de conservación.

Acerca de esta tarea

En esta tarea, se describe cómo cambiar la configuración de un pool.

> No es posible cambiar el nivel de RAID de un pool mediante la interfaz de System Manager. System Manager configura automáticamente los pools como RAID 6.

Pasos

1. Seleccione MENU:almacenamiento[Pools y grupos de volúmenes].
2. Seleccione el pool que desea editar y, a continuación, haga clic en **Ver/editar configuración**.

   Se muestra el cuadro de diálogo Configuración del pool.

3. Seleccione la ficha **Configuración** y, a continuación, edite la configuración del pool según corresponda.

Detalles del campo

Ajuste	Descripción
Nombre	El nombre del pool proporcionado por el usuario se puede modificar. Es necesario especificar un nombre para el pool.
Alertas de capacidad	Las notificaciones de alerta se pueden enviar cuando la capacidad libre de un pool alcanza o supera un umbral especificado. Cuando los datos almacenados en el pool superan el umbral especificado, System Manager envía un mensaje y otorga tiempo para añadir más espacio de almacenamiento o eliminar los objetos que no son necesarios. Las alertas se muestran en el área Notificaciones de la consola y se pueden enviar del servidor a los administradores por correo electrónico y mensajes de captura SNMP. Se pueden definir las siguientes alertas sobre capacidad: • **Alerta crítica** — esta alerta crítica le avisa cuando la capacidad libre en el pool alcanza o supera el umbral especificado. Se deben usar los controles de desplazamiento para ajustar el porcentaje del umbral. Seleccione la casilla de comprobación para deshabilitar esta notificación. • **Alerta temprana** — esta alerta anticipada le notifica cuando la capacidad libre en un pool está alcanzando un umbral especificado. Se deben usar los controles de desplazamiento para ajustar el porcentaje del umbral. Seleccione la casilla de comprobación para deshabilitar esta notificación.

Ajuste	Descripción
Prioridades de modificación	Se pueden especificar niveles de prioridad para las operaciones de modificación en un pool con respecto al rendimiento del sistema. Si se le otorga una mayor prioridad a las operaciones de modificación de un pool, se agiliza el tiempo de finalización de la operación, pero puede ralentizar el rendimiento de I/o del host. Si se otorga una prioridad, las operaciones tardan más tiempo, pero el rendimiento de I/o del host se ve menos afectado. Se puede elegir entre cinco niveles de prioridad: Mínimo, bajo, medio, alto y máximo. Cuanto más alto sea el nivel de prioridad, mayor será el impacto sobre las operaciones de I/o del host y el rendimiento del sistema. • **Prioridad de reconstrucción crítica** — esta barra deslizante determina la prioridad de una operación de reconstrucción de datos cuando múltiples fallos de unidad dan lugar a una condición en la que algunos datos no tienen redundancia y un fallo de unidad adicional puede resultar en la pérdida de datos. • **Prioridad de reconstrucción degradada** — esta barra deslizante determina la prioridad de la operación de reconstrucción de datos cuando se ha producido un fallo de unidad, pero los datos siguen teniendo redundancia y un fallo de unidad adicional no provoca la pérdida de datos. • **Prioridad de operación en segundo plano** — esta barra deslizante determina la prioridad de las operaciones en segundo plano del pool que ocurren mientras el pool está en estado óptimo. Entre estas operaciones se incluyen la expansión dinámica de volúmenes (DVE), el formato de disponibilidad instantánea (IAF) y la migración de datos a una unidad reemplazada o añadida.

Ajuste	Descripción
Capacidad de conservación ("capacidad de optimización" para EF600 o EF300)	**Capacidad de conservación** — se puede definir la cantidad de unidades para determinar la capacidad que se reserva en el pool para admitir posibles fallos de unidad. Cuando se produce un fallo de unidad, la capacidad de conservación se usa para contener los datos reconstruidos. Los pools utilizan la capacidad de conservación durante el proceso de reconstrucción de datos en lugar de las unidades de repuesto, que se utilizan en los grupos de volúmenes. Use los controles de desplazamiento para ajustar la cantidad de unidades. La capacidad de conservación del pool aparece junto al cuadro de desplazamiento en función de la cantidad de unidades. Tenga en cuenta la siguiente información acerca de la capacidad de conservación. • Debido a que la capacidad de conservación se sustrae de la capacidad libre total de un pool, la cantidad de capacidad que se reserva afecta a la cantidad de capacidad libre disponible para crear volúmenes. Si se especifica el valor 0 para la capacidad de conservación, se utiliza toda la capacidad libre del pool para la creación del volumen. • Si se disminuye la capacidad de conservación, aumenta la capacidad que se puede usar para los volúmenes del pool. **Capacidad de optimización adicional** (sólo cabinas EF600 y EF300): Cuando se crea un pool, se genera una capacidad de optimización recomendada que proporciona un equilibrio entre la capacidad disponible frente al rendimiento y la vida útil de la unidad. Puede ajustar este equilibrio moviendo el control deslizante a la derecha para mejorar el rendimiento y el deterioro de la unidad a expensas de la capacidad disponible aumentada, o bien moviéndolo a la izquierda para aumentar la capacidad disponible a costa de un mejor rendimiento y de la vida útil de la unidad. Las unidades SSD tendrán una mayor vida útil y mejor rendimiento de escritura máximo cuando una parte de su capacidad no está asignada. Para las unidades asociadas con un pool, la capacidad sin asignar consta de la capacidad de conservación de un pool, la capacidad libre (capacidad que no utilizan los volúmenes) y una parte de la capacidad utilizable se diferencia como capacidad de optimización adicional. La capacidad de optimización adicional garantiza un nivel mínimo de capacidad de optimización mediante la reducción de la capacidad utilizable, y, como tal, no está disponible para la creación de volúmenes.

4. Haga clic en **Guardar**.

Cambiar la configuración de un grupo de volúmenes

Es posible editar la configuración de un grupo de volúmenes, incluido el nombre y el nivel de RAID.

Antes de empezar

Si va a cambiar el nivel de RAID para acomodar las necesidades de rendimiento de las aplicaciones que acceden al grupo de volúmenes, asegúrese de cumplir los siguientes requisitos previos:

- El grupo de volúmenes debe tener el estado óptima.
- Se debe contar con suficiente capacidad en el grupo de volúmenes como para convertir al nivel de RAID nuevo.

Pasos

1. Seleccione MENU:almacenamiento[Pools y grupos de volúmenes].
2. Seleccione el grupo de volúmenes que desea editar y haga clic en **Ver/editar configuración**.

   Se muestra el cuadro de diálogo Configuración del grupo de volúmenes.

3. Seleccione la ficha **Configuración** y, a continuación, edite la configuración del grupo de volúmenes según corresponda.

Detalles del campo

Ajuste	Descripción
Nombre	Es posible modificar el nombre del grupo de volúmenes provisto por el usuario. Es necesario especificar un nombre para el grupo de volúmenes.
Nivel de RAID	Seleccione el nuevo nivel de RAID en el menú desplegable. • **RAID 0 striping** — ofrece alto rendimiento, pero no proporciona ninguna redundancia de datos. Si una unidad única falla en el grupo de volúmenes, todos los volúmenes asociados fallarán y se perderán todos los datos. Un grupo RAID de segmentación combina dos o más unidades en una unidad lógica grande. • **RAID 1 mirroring** — ofrece un alto rendimiento y la mejor disponibilidad de datos, y es adecuado para el almacenamiento de datos confidenciales a nivel corporativo o personal. Para proteger los datos, crea reflejos del contenido de una unidad en una segunda unidad en la pareja reflejada. Proporciona protección en caso de fallo de una unidad única. • **RAID 10 striping/mirror** — proporciona una combinación de RAID 0 (segmentación) y RAID 1 (duplicación), y se logra cuando se seleccionan cuatro o más unidades. RAID 10 es adecuado para aplicaciones transaccionales de alto volumen, como una base de datos, que requieren alto rendimiento y tolerancia a fallos. • **RAID 5** — óptimo para entornos multiusuario (como almacenamiento de bases de datos o sistemas de archivos) donde el tamaño típico de E/S es pequeño y hay una alta proporción de actividad de lectura. • **RAID 6**: Óptimo para entornos que requieren protección contra redundancia más allá de RAID 5, pero que no requieren un alto rendimiento de escritura. RAID 3 solo se puede asignar a grupos de volúmenes con interfaz de línea de comandos (CLI). Cuando cambia el nivel de RAID, no es posible cancelar esta operación una vez iniciada. Durante el cambio, los datos seguirán estando disponibles.

Ajuste	Descripción
Capacidad de optimización (solo cabinas EF600)	Cuando se crea un grupo de volúmenes, se genera una capacidad de optimización recomendada que ofrece un equilibrio entre la capacidad disponible y el rendimiento y la vida útil de la unidad. Puede ajustar este equilibrio moviendo el control deslizante a la derecha para mejorar el rendimiento y el deterioro de la unidad a expensas de la capacidad disponible aumentada, o bien moviéndolo a la izquierda para aumentar la capacidad disponible a costa de un mejor rendimiento y de la vida útil de la unidad. Las unidades SSD tendrán una mayor vida útil y mejor rendimiento de escritura máximo cuando una parte de su capacidad no está asignada. Para las unidades asociadas con un grupo de volúmenes, la capacidad sin asignar consta de la capacidad libre de un grupo (capacidad que no usan los volúmenes) y una parte de la capacidad utilizable asignada como capacidad de optimización adicional. La capacidad de optimización adicional garantiza un nivel mínimo de capacidad de optimización mediante la reducción de la capacidad utilizable, y, como tal, no está disponible para la creación de volúmenes.

4. Haga clic en **Guardar**.

   Se muestra un cuadro de diálogo de confirmación si se reduce la capacidad, se pierde la redundancia de volumen o se pierde la protección contra pérdida de bandeja/cajón como resultado del cambio de nivel de RAID. Seleccione **Sí** para continuar; de lo contrario, haga clic en **no**.

Resultados

Si cambia el nivel de RAID de un grupo de volúmenes, System Manager cambia los niveles de RAID de todos los volúmenes que componen el grupo de volúmenes. Es posible que el rendimiento se vea levemente afectado durante la operación.

Habilitar o deshabilitar el aprovisionamiento de recursos en pools y grupos de volúmenes existentes

Para cualquier unidad compatible con DULBE, puede habilitar o deshabilitar el aprovisionamiento de recursos en los volúmenes existentes en un pool o grupo de volúmenes.

El aprovisionamiento de recursos es una función disponible en las cabinas de almacenamiento EF300 y EF600, lo que permite poner en uso los volúmenes de inmediato sin proceso de inicialización en segundo plano. Todos los bloques de unidades asignados al volumen no se asignan (desasignan), es posible mejorar la vida útil de las unidades de estado sólido y aumentar el rendimiento de escritura máximo.

De forma predeterminada, el aprovisionamiento de recursos está habilitado en sistemas donde las unidades admiten DULBE. No es necesario habilitar el aprovisionamiento de recursos a menos que se haya deshabilitado anteriormente.

Antes de empezar

- Debe tener una cabina de almacenamiento EF300 o EF600.
- Debe tener grupos de volúmenes SSD o pools, donde todas las unidades admiten la funcionalidad de recuperación de error de bloque lógico no escrito o desasignado (DULBE). De lo contrario, la opción de

aprovisionamiento de recursos no está disponible.

Acerca de esta tarea

Cuando se habilita el aprovisionamiento de recursos para los grupos de volúmenes y pools existentes, se cambian todos los volúmenes en el pool o grupo de volúmenes seleccionado para permitir que se reasignen los bloques. Este proceso podría implicar una operación en segundo plano para garantizar una asignación consistente con la granularidad UNMAP. Esta operación no desasignar ningún espacio. Una vez que se completa la operación en segundo plano, el sistema operativo necesita desasignar los bloques no utilizados para crear espacio libre.

Cuando se deshabilita el aprovisionamiento de recursos para los grupos de volúmenes o pools existentes, una operación en segundo plano reescribe todos los bloques lógicos en cada volumen. Los datos existentes no se modifican. Las escrituras asignarán o aprovisionarán los bloques en las unidades asociadas con el grupo de volúmenes o pool.

> Para los nuevos grupos de volúmenes y pools, puede habilitar o deshabilitar el aprovisionamiento de recursos en el menú:Configuración[sistema > Configuración adicional > Habilitar/deshabilitar volúmenes aprovisionados con recursos].

Pasos

1. Seleccione MENU:almacenamiento[Pools y grupos de volúmenes].
2. Seleccione un pool o un grupo de volúmenes de la lista.

   Solo puede seleccionar un pool o un grupo de volúmenes a la vez. Desplácese hacia abajo por la lista para ver pools o grupos de volúmenes adicionales.

3. Seleccione **tareas no comunes** y, a continuación, **Activar aprovisionamiento de recursos** o **Desactivar aprovisionamiento de recursos**.
4. Confirme la operación en el cuadro de diálogo.

> **Si vuelve a habilitar DULBE** — después de que finalice la operación en segundo plano, es posible que deba reiniciar el host para que detecte los cambios de configuración DULBE y, a continuación, volver a montar todos los sistemas de archivos.

Habilitar o deshabilitar el aprovisionamiento de recursos para nuevos grupos de volúmenes o pools

Si anteriormente deshabilitó la función predeterminada para el aprovisionamiento de recursos, puede volver a habilitarla para todos los grupos de volúmenes SSD o pools nuevos que cree. También puede desactivar de nuevo el ajuste.

El aprovisionamiento de recursos es una función disponible en las cabinas de almacenamiento EF300 y EF600, lo que permite poner en uso los volúmenes de inmediato sin proceso de inicialización en segundo plano. Todos los bloques de unidades asignados al volumen no se asignan (desasignan), es posible mejorar la vida útil de las unidades de estado sólido y aumentar el rendimiento de escritura máximo.

> De forma predeterminada, el aprovisionamiento de recursos está habilitado en sistemas donde las unidades admiten DULBE.

Antes de empezar

- Debe tener una cabina de almacenamiento EF300 o EF600.

- Debe tener grupos de volúmenes SSD o pools, donde todas las unidades admiten la funcionalidad de recuperación de error de bloque lógico no escrito o desasignado (DULBE).

Acerca de esta tarea

Cuando se vuelve a habilitar el aprovisionamiento de recursos para nuevos grupos de volúmenes o pools, solo se ven afectados los grupos de volúmenes y pools recién creados. Todos los grupos de volúmenes y pools existentes con el aprovisionamiento de recursos habilitado permanecerán sin cambios.

Pasos

1. Seleccione MENU:Settings[System].
2. Desplácese hasta **Configuración adicional** y, a continuación, haga clic en **Habilitar/deshabilitar volúmenes aprovisionados mediante recursos**.

   La descripción de la configuración indica si el aprovisionamiento de recursos está activado o desactivado.

3. Confirme la operación en el cuadro de diálogo.

Resultados

La habilitación o deshabilitación del aprovisionamiento de recursos afecta únicamente a los pools de SSD o los grupos de volúmenes nuevos que se creen. Los pools o grupos de volúmenes existentes no cambian.

Habilite la seguridad para un pool o un grupo de volúmenes

Es posible habilitar Drive Security para un pool o grupo de volúmenes con el fin de evitar el acceso no autorizado a los datos en las unidades contenidas en un pool o un grupo de volúmenes. El acceso de lectura y escritura para las unidades solo está disponible a través de una controladora que está configurada con una clave de seguridad.

Antes de empezar

- Se debe habilitar la función Drive Security.
- Debe crearse una clave de seguridad.
- El pool o el grupo de volúmenes deben estar en el estado óptima.
- Todas las unidades del pool o grupo de volúmenes deben ser unidades compatibles con la función de seguridad.

Acerca de esta tarea

Si desea usar Drive Security, seleccione un pool o un grupo de volúmenes compatibles con la función de seguridad. Un pool o un grupo de volúmenes pueden contener tanto una unidad compatible con la función de seguridad como una que no lo sea, pero todas las unidades deben ser compatibles con la función de seguridad para usar la funcionalidad de cifrado.

Después de habilitar la seguridad, solo es posible deshabilitarla si se elimina el pool o el grupo de volúmenes y, a continuación, se borran las unidades.

Pasos

1. Seleccione MENU:almacenamiento[Pools y grupos de volúmenes].
2. Seleccione el pool o el grupo de volúmenes en donde desea habilitar la seguridad y, a continuación, haga clic en **more › Habilitar seguridad**.

   Se muestra el cuadro de diálogo Confirmar Habilitar seguridad.

3. Confirme que desea habilitar la seguridad para el pool o el grupo de volúmenes seleccionados y, a continuación, haga clic en **Activar**.

Gestione la caché SSD

Cómo funciona caché SSD

La función SSD Cache es una solución basada en la controladora que almacena en la caché los datos de acceso más frecuente (los datos "activos") en unidades de estado sólido (SSD) de latencia más baja para acelerar dinámicamente el rendimiento del sistema. La caché SSD se usa exclusivamente para las lecturas del host.

Caché SSD versus caché primaria

La caché SSD es una caché secundaria para usar con la caché primaria en la memoria dinámica de acceso aleatorio (DRAM) de la controladora.

La caché SSD opera de manera diferente a la caché primaria:

- Para la caché primaria, cada operación de I/o debe preparar datos a través de la caché para realizar la operación.

  En la caché primaria, los datos se almacenan en DRAM después de la lectura en el host.

- La caché SSD se utiliza solo si es conveniente para colocar los datos en la caché a fin de mejorar el rendimiento del sistema general.

  En la caché SSD, se copian datos de volúmenes y se almacenan en dos volúmenes de RAID internos (uno por controladora) que se crean automáticamente al crear una caché SSD.

Los volúmenes RAID internos se usan para fines de procesamiento de la caché interna. No puede accederse a estos volúmenes desde la interfaz de usuario y no aparecen en ella. Sin embargo, estos dos volúmenes cuentan para la cantidad total de volúmenes permitidos en la cabina de almacenamiento.

Cómo se utiliza la caché SSD

El almacenamiento en caché inteligente coloca los datos en una unidad de latencia baja para agilizar las respuestas a solicitudes futuras de esos datos. Si un programa solicita datos que están en la caché (lo que se denomina «acierto en caché»), la unidad de menor latencia puede satisfacer esta transacción. De lo contrario, se produce una «'omisión de caché'» y deberá accederse a los datos desde la unidad original, más lenta. Cuantos más aciertos en caché se produzcan, mejor será el rendimiento general.

Cuando un programa host accede a las unidades de la cabina de almacenamiento, los datos se almacenan en la caché SSD. Cuando el programa host vuelve a acceder a los mismos datos, se lee desde la caché SSD y no desde las unidades de disco duro. Los datos de acceso común se almacenan en la caché SSD. Solo se accede a los discos duros cuando no pueden leerse los datos desde la caché SSD.

La caché SSD se utiliza solo cuando es conveniente para colocar los datos en la caché a fin de mejorar el rendimiento del sistema general.

Cuando la CPU necesita procesar datos de lectura, sigue estos pasos:

1. Comprueba la caché de DRAM.

2. Si no los encuentra en la caché de DRAM, revisa la caché SSD.
3. Si no los encuentra en la caché SSD, los obtiene del disco duro. Si los datos se consideran valiosos para estar en la caché, los copia en caché SSD.

Mejor rendimiento

Copiar los datos a los que accede con más frecuencia (puntos críticos) en la caché SSD permite un funcionamiento más eficaz del disco duro, menor latencia y velocidades aceleradas de lectura y escritura. El uso de unidades SSD de alto rendimiento para almacenar en la caché datos de unidades de disco duro mejora el rendimiento de I/o y los tiempos de respuesta.

Se utilizan mecanismos de I/o de volúmenes simples para transferir datos desde y hacia la caché SSD. Después de almacenar datos en la caché y en la unidad SSD, las lecturas posteriores de esos datos se realizan en la caché SSD, por lo que se elimina la necesidad de acceder al volumen de la unidad de disco duro.

Caché SSD y la función Drive Security

Para usar la caché SSD en un volumen que también utiliza Drive Security (es decir, con la función de seguridad habilitada), las funcionalidades de Drive Security del volumen y de la caché SSD deben coincidir. Si no coinciden, el volumen no tendrá la función de seguridad habilitada.

Implemente caché SSD

Para implementar la caché SSD, haga lo siguiente:

1. Cree la caché SSD.
2. Asocie la caché SSD con los volúmenes para los que desea implementar el almacenamiento en caché de lectura de SSD.

> Cualquier volumen asignado para utilizar una caché SSD de una controladora no es elegible para una transferencia de equilibrio de carga automática.

Restricciones de la caché SSD

Obtenga información acerca de las restricciones en el uso de la caché SSD en una cabina de almacenamiento.

Restricciones

- Cualquier volumen asignado para utilizar una caché SSD de una controladora no es elegible para una transferencia de equilibrio de carga automática.
- Actualmente, solo se admite una caché SSD por cabina de almacenamiento.
- La capacidad máxima que se puede utilizar de caché SSD en una cabina de almacenamiento es 8 TB.
- Las imágenes Snapshot no admiten la función SSD Cache.
- Si importa o exporta volúmenes que tienen habilitada o deshabilitada la función SSD Cache, los datos en caché no se importan ni se exportan.
- No puede quitar la última unidad de una caché SSD sin antes eliminar la caché SSD.

Restricciones con Drive Security

- Solo es posible habilitar la seguridad en la caché SSD cuando se crea la caché SSD. No se puede habilitar la seguridad posteriormente como en un volumen.
- Si se combinan unidades compatibles y no compatibles con la función de seguridad en la caché SSD, no se puede habilitar Drive Security en estas unidades.
- Los volúmenes con la función de seguridad habilitada deben tener una caché SSD que se encuentre habilitada para la función de seguridad.

Cree una caché SSD

Para acelerar de manera dinámica el rendimiento del sistema, se puede usar la función SSD Cache para almacenar en caché los datos a los que se accede con mayor frecuencia (datos "activos") en unidades de estado sólido (SSD) de menor latencia. La caché SSD se usa exclusivamente para las lecturas del host.

Antes de empezar

La cabina de almacenamiento debe tener algunas unidades SSD.

Acerca de esta tarea

Para la creación de una caché SSD nueva, es posible usar una unidad única o varias unidades. Debido a que la caché de lectura se encuentra en la cabina de almacenamiento, todas las aplicaciones que utilizan la cabina de almacenamiento comparten el almacenamiento en caché. Una vez seleccionados los volúmenes que se desean almacenar en caché, el almacenamiento en caché se realiza de forma automática y dinámica.

Siga estas directrices al crear una caché SSD.

- Puede habilitar la función de seguridad en la caché SSD solo en el momento de la creación, no después.
- Solo se admite una caché SSD por cabina de almacenamiento.
- Si solo un volumen tiene la caché SSD habilitada, toda la caché SSD se asignará a la controladora que pertenece a ese volumen.
- La capacidad máxima de la caché SSD utilizable de una cabina de almacenamiento depende de la capacidad de la caché primaria de la controladora.
- Las imágenes Snapshot no admiten la función SSD Cache.
- Si importa o exporta volúmenes que tienen habilitada o deshabilitada la función SSD Cache, los datos en caché no se importan ni se exportan.
- Cualquier volumen asignado para utilizar una caché SSD de una controladora no es elegible para una transferencia de equilibrio de carga automática.
- Si los volúmenes asociados tienen la función de seguridad habilitada, cree una caché SSD con la función de seguridad habilitada.

Pasos

1. Seleccione MENU:almacenamiento[Pools y grupos de volúmenes].
2. Haga clic en menú:Crear[caché SSD].

   Se muestra el cuadro de diálogo Crear caché SSD.

3. Escriba un nombre para la caché SSD.

4. Seleccione el candidato de caché SSD que desea usar según las siguientes características.

Característica	Uso
Capacidad	Muestra la capacidad disponible en GIB. Seleccione la capacidad que necesita el almacenamiento de la aplicación. La capacidad máxima de la caché SSD depende de la capacidad de caché primaria de la controladora. Si se asigna más de la cantidad máxima a la caché SSD, no se podrá utilizar la capacidad excedente. La capacidad de la caché SSD se debe incluir en la capacidad total asignada.
Unidades totales	Indica la cantidad de unidades disponibles en esta caché SSD. Seleccione el candidato de SSD que tenga la cantidad de unidades que desea.
Compatible con la función de seguridad	Indica si este candidato de caché SSD se compone íntegramente de unidades compatibles con la función de seguridad, que pueden ser de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS). Si desea crear una caché SSD con la función de seguridad habilitada, busque **Sí - FDE** o **Sí - FIPS** en la columna compatible con la función de seguridad.
Habilitar seguridad?	Ofrece la opción de habilitar la función Drive Security con unidades que sean compatibles con la función de seguridad. Si desea crear una caché SSD con la función de seguridad habilitada, marque la casilla de comprobación Habilitar seguridad. Una vez que habilitada, la seguridad no se puede deshabilitar. Puede habilitar la función de seguridad en la caché SSD solo en el momento de la creación, no después.
Compatible con DA	Indica si está disponible la función Data Assurance (DA) para este candidato de caché SSD. La garantía de datos (DA) comprueba y corrige los errores que se pueden producir durante la transferencia de datos a través de las controladoras hasta las unidades. Si desea usar DA, seleccione un candidato de caché SSD que sea compatible con ESTA función. Esta opción solo está disponible si está habilitada la función DA. Una caché SSD puede contener unidades que son compatibles con DA o que no lo son, pero todas las unidades deben ser compatibles con DA para poder usar ESTA función.

5. Asocie la caché SSD con los volúmenes para los que desea implementar el almacenamiento en caché de lectura de SSD. Para activar caché SSD en volúmenes compatibles de inmediato, active la casilla de verificación **Activar caché SSD en volúmenes compatibles existentes asignados a hosts**.

   Los volúmenes son compatibles si comparten las mismas funcionalidades Drive Security y DA.

6. Haga clic en **Crear**.

Cambiar la configuración de la caché SSD

Es posible editar el nombre de la caché SSD y visualizar el estado, las capacidades máxima y actual, el estado de las funciones Drive Security y Garantía de datos, y los volúmenes y las unidades asociadas.

Pasos

1. Seleccione MENU:almacenamiento[Pools y grupos de volúmenes].
2. Seleccione la caché SSD que desea editar y, a continuación, haga clic en **Ver/editar configuración**.

   Se muestra el cuadro de diálogo Configuración de caché SSD.

3. Revise o edite la configuración de la caché SSD según corresponda.

Detalles del campo

Ajuste	Descripción
Nombre	Muestra el nombre de la caché SSD, que se puede modificar. El nombre de la caché SSD es obligatorio.
Características	Muestra el estado de la caché SSD. Los Estados posibles incluyen los siguientes: • Óptimo • Desconocido • Degradado • Con errores (Un estado fallido genera un evento MEL crítico). • Suspendida
Capacidades	Muestra la capacidad actual y la capacidad máxima permitida de la caché SSD. La capacidad máxima permitida de la caché SSD depende del tamaño de la caché primaria de la controladora: • Hasta 1 GIB • 1 GIB a 2 GIB • 2 GIB a 4 GIB • Más de 4 GIB
Seguridad y DA	Muestra el estado de Drive Security y Garantía de datos de la caché SSD. • **Compatible con la función de seguridad** — indica si la caché SSD está compuesta íntegramente por unidades compatibles con la función de seguridad. Una unidad compatible con la función de seguridad es una unidad de autocifrado que puede proteger los datos contra el acceso no autorizado. • **Secure-enabled** — indica si la seguridad está habilitada en la caché SSD. • **Compatible con DA**: Indica si la caché SSD está compuesta íntegramente por unidades compatibles con DA. Una unidad compatible con DA puede comprobar la existencia de errores que pueden producirse durante la comunicación de los datos entre el host y la cabina de almacenamiento, y corregirlos.
Objetos asociados	Muestra los volúmenes y las unidades asociados con la caché SSD.

4. Haga clic en **Guardar**.

Ver estadísticas de la caché SSD

Es posible ver estadísticas de la caché SSD, como lecturas, escrituras, aciertos en caché, porcentaje de asignación de caché, y el porcentaje de utilización de la caché.

Las estadísticas nominales, que son un subconjunto de estadísticas detalladas, se muestran en el cuadro de diálogo Ver estadísticas de la caché SSD. Es posible ver estadísticas detalladas de la caché SSD solo cuando se exportan todas las estadísticas de SSD a un `.csv` archivo.

Al revisar e interpretar las estadísticas, tenga en cuenta que algunas interpretaciones provienen del análisis de una combinación de estadísticas.

Pasos

1. Seleccione MENU:almacenamiento[Pools y grupos de volúmenes].
2. Seleccione la caché SSD para la cual desea ver estadísticas y haga clic en menú:más[Ver estadísticas de la caché SSD].

   Se muestra el cuadro de diálogo Ver estadísticas de la caché SSD, donde se proporcionan las estadísticas nominales de la caché SSD seleccionada.

Detalles del campo

Configuración	Descripción
Lecturas	Se muestra el número total de lecturas del host de los volúmenes con la función de caché SSD habilitada. Cuanto más alto sea el ratio de lecturas a escrituras, mejor será el funcionamiento de la caché.
Escrituras	El número total de escrituras del host en los volúmenes con la función de caché SSD habilitada. Cuanto más alto sea el ratio de lecturas a escrituras, mejor será el funcionamiento de la caché.
Aciertos en caché	Se muestra el número de aciertos en caché.
Aciertos en caché	Se muestra el porcentaje de aciertos en caché. Este número deriva de los aciertos en caché/(lecturas + escrituras). El porcentaje de aciertos en caché debe ser mayor que 50 % para un funcionamiento eficaz de la caché SSD.
Asignación en caché	Se muestra el porcentaje de almacenamiento de la caché SSD asignado, expresado como un porcentaje del almacenamiento de la caché SSD que está disponible para esta controladora y deriva de los bytes asignados/bytes disponibles.
Uso de caché	Se muestra el porcentaje de almacenamiento de la caché SSD que contiene datos de volúmenes habilitados, expresado como un porcentaje del almacenamiento de la caché SSD asignado. Esta cantidad representa la utilización o la densidad de la caché SSD. Derivado de bytes asignados/bytes disponibles.
Exportar todo	Exporta todas las estadísticas de la caché SSD a un formato CSV. El archivo exportado contiene todas las estadísticas disponibles de la caché SSD (tanto nominales como detalladas).

3. Haga clic en **Cancelar** para cerrar el cuadro de diálogo.

Gestione la capacidad reservada

Cómo funciona la capacidad reservada

La capacidad reservada se crea automáticamente cuando se proporcionan operaciones de servicio de copia, como operaciones Snapshot o mirroring asíncrono, para los volúmenes.

El objetivo de la capacidad reservada es almacenar cambios de datos en estos volúmenes en caso de que algo salga mal. Al igual que los volúmenes, la capacidad reservada se crea a partir de pools o grupos de volúmenes.

Copiar objetos de servicio que utilizan capacidad reservada

La capacidad reservada es el mecanismo de almacenamiento subyacente que utilizan estos objetos de servicio de copia:

- Grupos Snapshot
- Volúmenes Snapshot de lectura/escritura
- Volúmenes miembro de grupo de coherencia
- Volúmenes de parejas reflejadas

Cuando se crean o se expanden estos objetos de servicio de copia, es necesario crear capacidad reservada nueva desde un pool o grupo de volúmenes. En general, la capacidad reservada constituye el 40 % del volumen base para operaciones Snapshot y el 20 % del volumen base para operaciones de mirroring asíncrono. No obstante, la capacidad reservada varía, según la cantidad de cambios en los datos originales.

Volúmenes finos y capacidad reservada

Para un volumen fino, si se alcanzó la capacidad máxima informada de 256 TIB, no se puede aumentar la capacidad. Asegúrese de que la capacidad reservada del volumen fino esté configurada con un tamaño más grande que la capacidad máxima informada. (Un volumen fino siempre es de aprovisionamiento fino; esto significa que la capacidad se asigna a medida que se escriben los datos en el volumen.)

Si crea capacidad reservada con un volumen fino en un pool, repase las acciones y los resultados de capacidad reservada siguientes:

- Si falla la capacidad reservada de un volumen fino, el propio volumen fino no podrá hacer la transición automática hacia el estado con errores. Sin embargo, debido a que todas las operaciones de I/o de un volumen fino requieren acceso al volumen de capacidad reservada, las operaciones de I/o siempre generarán la devolución de una comprobación de condición al host solicitante. Si puede resolverse el problema subyacente del volumen de capacidad reservada, este regresa al estado óptima y el volumen fino vuelve a funcionar.
- Si utiliza un volumen fino existente para completar una pareja reflejada asíncrona, ese volumen fino se vuelve a inicializar con un nuevo volumen de capacidad reservada. Durante el proceso de sincronización inicial, solo se transfieren los bloques aprovisionados en el lado primario.

Alertas de capacidad

El objeto del servicio de copia tiene un umbral de advertencia y alerta de capacidad configurable, además de una respuesta configurable cuando la capacidad reservada está llena.

Cuando la capacidad reservada de un volumen de objeto de servicio de copia está cerca del punto de llenado, se envía una alerta al usuario. De manera predeterminada, esta alerta se envía cuando el volumen de capacidad reservada está lleno en un 75 %; sin embargo, puede ajustar este punto de alerta hacia arriba o hacia abajo si es necesario. Si recibe esta alerta, es posible aumentar la capacidad del volumen de capacidad reservada en ese momento. Cada objeto de servicio de copia puede configurarse de manera independiente en este aspecto.

Volúmenes huérfanos de capacidad reservada

Un volumen huérfano de capacidad reservada es un volumen que ya no almacena datos para operaciones de servicio de copia porque se eliminó su objeto de servicio de copia asociado. Cuando se eliminó el objeto de servicio de copia, su volumen de capacidad reservada también debió haberse eliminado. Sin embargo, el volumen de capacidad reservada no pudo eliminarse.

Como ningún host puede acceder a los volúmenes huérfanos de capacidad reservada, estos son candidatos a la recuperación. Elimine manualmente el volumen huérfano de capacidad reservada para poder usar su capacidad en otras operaciones.

System Manager envía alertas sobre los volúmenes huérfanos de capacidad reservada con el mensaje "reclamar capacidad no utilizada" en el área Notifications de la página Inicio. Puede hacer clic en **reclamar capacidad no utilizada** para mostrar el cuadro de diálogo reclamar capacidad no utilizada, donde puede eliminar el volumen huérfano de capacidad reservada.

Características de la capacidad reservada

- La capacidad asignada a la capacidad reservada debe considerarse durante la creación de volúmenes, con el fin de conservar suficiente capacidad libre.
- La capacidad reservada puede ser menor que el volumen base (el tamaño mínimo es de 8 MIB).
- Los metadatos consumen parte del espacio, pero es muy poco (192 KiB). Por eso, no debe tomarse en cuenta para determinar el tamaño del volumen de capacidad reservada.
- La capacidad reservada no puede leerse ni escribirse directamente desde un host.
- La capacidad reservada existe para cada volumen Snapshot de lectura/escritura, grupo Snapshot, volumen miembro de grupos de coherencia y volumen de parejas reflejadas.

Aumente la capacidad reservada

Es posible aumentar la capacidad reservada, que es la capacidad asignada físicamente para cualquier operación de servicio de copia en un objeto de almacenamiento.

Para las operaciones Snapshot, generalmente representa el 40 % del volumen base; para las operaciones de mirroring asíncrono, generalmente se trata del 20 % del volumen base. En términos generales, se aumenta la capacidad reservada cuando se recibe una advertencia de que la capacidad reservada del objeto de almacenamiento se está llenando.

Antes de empezar

- El volumen en el pool o el grupo de volúmenes debe tener el estado óptima y no debe estar en ningún estado de modificación.
- Debe existir capacidad libre en el pool o grupo de volúmenes que desea usar para aumentar la capacidad.

  Si no hay capacidad libre en ningún pool o grupo de volúmenes, es posible añadir capacidad sin asignar en forma de unidades no utilizadas a un pool o un grupo de volúmenes.

Acerca de esta tarea

Es posible aumentar la capacidad reservada solo en incrementos de 8 GIB para los siguientes objetos de almacenamiento:

- Grupo Snapshot
- Volumen Snapshot
- Volumen miembro del grupo de coherencia
- Volumen de pareja reflejada

Use un porcentaje alto si considera que el volumen primario se someterá a muchos cambios o si la vida útil de una operación de servicio de copia será muy prolongada.

No es posible aumentar la capacidad reservada para un volumen Snapshot de solo lectura. Solo los volúmenes Snapshot que son de lectura y escritura requieren capacidad reservada.

Pasos

1. Seleccione MENU:almacenamiento[Pools y grupos de volúmenes].
2. Seleccione la pestaña **capacidad reservada**.
3. Seleccione el objeto de almacenamiento para el que desea aumentar la capacidad reservada y haga clic en **aumentar capacidad**.

   Se muestra el cuadro de diálogo aumentar la capacidad reservada.

4. Utilice el cuadro de desplazamiento para ajustar el porcentaje de capacidad.

   Si no hay capacidad libre en el pool o el grupo de volúmenes que contiene el objeto de almacenamiento seleccionado y la cabina de almacenamiento posee capacidad sin asignar, es posible crear un nuevo pool o grupo de volúmenes. Puede volver a intentar esta operación con la nueva capacidad libre en ese pool o grupo de volúmenes.

5. Haga clic en **aumentar**.

Resultados

System Manager realiza lo siguiente:

- Aumenta la capacidad reservada del objeto de almacenamiento.
- Muestra la capacidad reservada recientemente añadida.

Reduzca la capacidad reservada

Puede utilizar la opción disminuir capacidad para reducir la capacidad reservada de los siguientes objetos de almacenamiento: Grupo Snapshot, volumen Snapshot y volumen miembro de grupo de coherencia. Puede reducir la capacidad reservada solo en las cantidades que utilizó para aumentarla.

Antes de empezar

- El objeto de almacenamiento debe contener más de un volumen de capacidad reservada.
- El objeto de almacenamiento no debe ser un volumen de pareja reflejado.
- Si el objeto de almacenamiento es un volumen Snapshot, debe estar deshabilitado.
- Si el objeto de almacenamiento es un grupo Snapshot, no debe contener ninguna imagen Snapshot asociada.

Acerca de esta tarea

Revise las siguientes directrices:

- Es posible eliminar volúmenes de capacidad reservada solo en el orden inverso en que se añadieron.
- No es posible reducir la capacidad reservada de un volumen Snapshot de solo lectura, ya que no tiene ninguna capacidad reservada asociada. Solo los volúmenes Snapshot que son de lectura y escritura requieren capacidad reservada.

Pasos

1. Seleccione MENU:almacenamiento[Pools y grupos de volúmenes].
2. Haga clic en la pestaña **capacidad reservada**.
3. Seleccione el objeto de almacenamiento para el que desea reducir la capacidad reservada y haga clic en **disminuir capacidad**.

   Se muestra el cuadro de diálogo disminuir capacidad reservada.

4. Seleccione la cantidad de capacidad en que desea reducir la capacidad reservada y haga clic en **disminuir**.

Resultados

System Manager realiza lo siguiente:

- Actualiza la capacidad del objeto de almacenamiento.
- Muestra la capacidad reservada recientemente actualizada para el objeto de almacenamiento.
- Cuando reduce la capacidad de un volumen Snapshot, System Manager hace una transición automática del volumen Snapshot al estado deshabilitado. Esto significa que el volumen Snapshot no está asociado a una imagen Snapshot y, en consecuencia, no puede asignarse a un host para I/O.

Cambiar la configuración de capacidad reservada para un grupo Snapshot

Es posible modificar la configuración de un grupo Snapshot y cambiarle el nombre, la configuración de eliminación automática, la cantidad máxima de imágenes Snapshot permitidas, el punto de porcentaje en el que System Manager envía una alerta de capacidad reservada, o bien la política que debe utilizarse cuando la capacidad reservada alcanza el porcentaje máximo definido.

Durante la creación de un grupo Snapshot, se crea capacidad reservada para almacenar los datos de todas las imágenes Snapshot que contiene el grupo.

Pasos

1. Seleccione MENU:almacenamiento[Pools y grupos de volúmenes].
2. Haga clic en la pestaña **capacidad reservada**.
3. Seleccione el grupo de instantáneas que desea editar y, a continuación, haga clic en **Ver/editar configuración**.

   Se muestra el cuadro de diálogo Configuración del grupo Snapshot.

4. Cambie la configuración del grupo Snapshot según sea necesario.

Detalles del campo

Ajuste	Descripción
Ajustes del grupo Snapshot	Nombre
El nombre del grupo Snapshot. Es necesario indicar un nombre para el grupo Snapshot.	Eliminación automática
Un ajuste para mantener la cantidad total de imágenes Snapshot del grupo en un valor igual o inferior al máximo establecido por el usuario. Cuando esta opción está habilitada, System Manager elimina automáticamente la imagen Snapshot más antigua del grupo cada vez que se crea una imagen Snapshot nueva, a fin de poder cumplir con la cantidad máxima de imágenes Snapshot permitidas en el grupo.	Límite de la imagen Snapshot
Un valor configurable para especificar la cantidad máxima de imágenes Snapshot permitidas en un grupo.	Programación Snapshot
En caso afirmativo, se establece una programación para crear Snapshot automáticamente.	**Ajustes de capacidad reservada**

Ajuste	Descripción
Enviarme una alerta cuando…	Use el cuadro de desplazamiento para ajustar el punto de porcentaje en el que System Manager envía una notificación de alerta cuando la capacidad reservada de un grupo Snapshot está casi completa. Cuando la capacidad reservada del grupo Snapshot supera el umbral especificado, System Manager envía una alerta que otorga tiempo para aumentar la capacidad reservada o eliminar los objetos innecesarios.
Política para capacidad reservada completa	Se puede seleccionar una de las siguientes políticas: • **Purgar la imagen Snapshot más antigua** — System Manager purga automáticamente la imagen Snapshot más antigua del grupo Snapshot, lo que libera la capacidad reservada de la imagen Snapshot para su reutilización dentro del grupo. • **Rechazar escrituras en volumen base**: Cuando la capacidad reservada alcanza el porcentaje máximo definido, System Manager rechaza toda solicitud de escritura de I/o en el volumen base que activó el acceso a la capacidad reservada.
Objetos asociados	Volumen base
El nombre del volumen base utilizado para el grupo. Un volumen base es el origen desde el cual se crea una imagen Snapshot. Puede ser un volumen grueso o fino y, por lo general, se asigna a un host. El volumen base puede residir en un grupo de volúmenes o un pool de discos.	Imágenes Snapshot

5. Haga clic en **Guardar** para aplicar los cambios a la configuración del grupo de instantáneas.

Cambiar la configuración de capacidad reservada para un volumen Snapshot

Puede cambiar la configuración de un volumen Snapshot a fin de ajustar el punto de porcentaje en el que el sistema envía una notificación de alerta cuando la capacidad reservada de un volumen Snapshot está casi completa.

Pasos

1. Seleccione MENU:almacenamiento[Pools y grupos de volúmenes].
2. Haga clic en la pestaña **capacidad reservada**.
3. Seleccione el volumen de instantánea que desea editar y, a continuación, haga clic en **Ver/editar**

configuración.

Se muestra el cuadro de diálogo Configuración de capacidad reservada de volumen Snapshot.

4. Cambie la configuración de la capacidad reservada para el volumen Snapshot, según sea necesario.

Detalles del campo

Ajuste	Descripción
Enviarme una alerta cuando…	Use el cuadro de desplazamiento para ajustar el punto de porcentaje en el que el sistema envía una alerta cuando la capacidad reservada para un volumen asociado está casi completa. Cuando la capacidad reservada para el volumen Snapshot supera el umbral específico, el sistema envía una alerta que da tiempo a aumentar la capacidad reservada o eliminar los objetos innecesarios.

5. Haga clic en **Guardar** para aplicar los cambios en la configuración de capacidad reservada del volumen Snapshot.

Cambiar la configuración de la capacidad reservada para un volumen miembro del grupo de coherencia

Es posible cambiar la configuración de un volumen miembro del grupo de coherencia para ajustar el punto de porcentaje en el que System Manager envía una notificación de alerta cuando la capacidad reservada de un volumen miembro está casi completa y para cambiar la política que debe utilizarse cuando la capacidad reservada alcanza su máximo definido porcentaje.

Acerca de esta tarea

Al cambiar la configuración de la capacidad reservada de un volumen miembro individual, también se cambia la configuración de capacidad reservada de todos los volúmenes miembro asociados con un grupo de coherencia.

Pasos

1. Seleccione MENU:almacenamiento[Pools y grupos de volúmenes].
2. Haga clic en la pestaña **capacidad reservada**.
3. Seleccione el volumen miembro del grupo de coherencia que desea editar y, a continuación, haga clic en **Ver/editar configuración**.

   Se muestra el cuadro de diálogo Configuración de capacidad reservada de volumen miembro.

4. Cambie la configuración de la capacidad reservada del volumen miembro, según corresponda.

Detalles del campo

Ajuste	Descripción
Enviarme una alerta cuando…	Use el cuadro de desplazamiento para ajustar el punto de porcentaje en el que System Manager envía una notificación de alerta cuando la capacidad reservada de un volumen miembro está casi completa. Cuando la capacidad reservada del volumen miembro supera el umbral especificado, System Manager envía una alerta que otorga tiempo para aumentar la capacidad reservada o eliminar los objetos innecesarios. Si se cambia la configuración de alerta de un volumen miembro, se cambiará la de los volúmenes miembro *All* que pertenecen al mismo grupo de coherencia.
Política para capacidad reservada completa	Se puede seleccionar una de las siguientes políticas: • **Purgar la imagen Snapshot más antigua** — System Manager purga automáticamente la imagen Snapshot más antigua del grupo de coherencia, lo que libera la capacidad reservada del miembro para su reutilización dentro del grupo. • **Rechazar escrituras en volumen base**: Cuando la capacidad reservada alcanza el porcentaje máximo definido, System Manager rechaza toda solicitud de escritura de I/o en el volumen base que activó el acceso a la capacidad reservada.

5. Haga clic en **Guardar** para aplicar los cambios.

Resultados

System Manager modifica la configuración de la capacidad reservada del volumen miembro, como también la configuración de la capacidad reservada de todos los volúmenes miembro del grupo de coherencia.

Cambie la configuración de capacidad reservada para un volumen de parejas reflejadas

Puede cambiar la configuración del volumen de una pareja reflejada a fin de ajustar el punto de porcentaje en el que System Manager envía una notificación de alerta cuando la capacidad reservada para una pareja reflejada está casi completa.

Pasos

1. Seleccione MENU:almacenamiento[Pools y grupos de volúmenes].
2. Seleccione la pestaña **capacidad reservada**.
3. Seleccione el volumen de la pareja reflejada que desea editar y, a continuación, haga clic en **Ver/editar configuración**.

   Se muestra el cuadro de diálogo Configuración de capacidad reservada de volumen de pareja reflejada.

4. Cambie la configuración de la capacidad reservada para el volumen de la pareja reflejada, según sea necesario.

Detalles del campo

Ajuste	Descripción
Enviarme una alerta cuando…	Use el cuadro de desplazamiento para ajustar el punto de porcentaje en el que System Manager envía una notificación de alerta cuando la capacidad reservada de una pareja reflejada está casi completa. Cuando la capacidad reservada de la pareja reflejada supera el umbral especificado, System Manager envía una alerta que otorga tiempo para aumentar la capacidad reservada. Si se cambia la configuración de alertas de una pareja reflejada, se modifica la configuración de alertas de todas las parejas reflejadas que pertenecen al mismo grupo de coherencia reflejado.

5. Haga clic en **Guardar** para aplicar los cambios.

Cancelar una imagen Snapshot pendiente

Es posible cancelar una imagen Snapshot pendiente antes de que se complete. Las Snapshot se ejecutan de forma asíncrona y el estado de la Snapshot es pendiente hasta que se completa. La imagen Snapshot se completa tan pronto como se completa la operación de sincronización.

Acerca de esta tarea

Una imagen Snapshot muestra el estado pendiente debido a las siguientes condiciones simultáneas:

- El volumen base de un grupo Snapshot o uno o varios volúmenes miembro de un grupo de coherencia que contiene esta imagen Snapshot son miembros de un grupo de reflejos asíncronos.
- Los volúmenes se encuentran en una operación de sincronización de mirroring asíncrono.

Pasos

1. Seleccione MENU:almacenamiento[Pools y grupos de volúmenes].
2. Haga clic en la pestaña **capacidad reservada**.
3. Seleccione el grupo Snapshot en el que desea cancelar una imagen Snapshot pendiente y haga clic en menú:tareas no comunes[Cancelar imagen Snapshot pendiente].
4. Haga clic en **Sí** para confirmar que desea cancelar la imagen Snapshot pendiente.

Eliminar grupo Snapshot

El grupo Snapshot se elimina cuando desea eliminar de forma permanente los datos y quitarlos del sistema. Si se elimina un grupo Snapshot, se reclama la capacidad reservada para volver a utilizarla en el pool o el grupo de volúmenes.

Acerca de esta tarea

Cuando se elimina un grupo Snapshot, también se eliminan todas las imágenes Snapshot en el grupo.

Pasos

1. Seleccione MENU:almacenamiento[Pools y grupos de volúmenes].
2. Haga clic en la pestaña **capacidad reservada**.
3. Seleccione el grupo Snapshot que desea eliminar y haga clic en menú:tareas no comunes[Eliminar grupo Snapshot].

   Se muestra el cuadro de diálogo Confirmar eliminación de grupo Snapshot.

4. Tipo `delete` para confirmar.

Resultados

System Manager realiza lo siguiente:

- Elimina todas las imágenes Snapshot asociadas con el grupo Snapshot.
- Deshabilita cualquier volumen Snapshot asociado con las imágenes del grupo Snapshot.
- Elimina la capacidad reservada que existe en el grupo Snapshot.

Preguntas frecuentes

¿Qué es un grupo de volúmenes?

Un grupo de volúmenes es un contenedor para volúmenes con características compartidas. Un grupo de volúmenes tiene una capacidad definida y un nivel de RAID. Se puede usar un grupo de volúmenes para crear uno o más volúmenes a los que se pueda acceder mediante un host. (Los volúmenes se crean a partir de un pool o un grupo de volúmenes).

¿Qué es un pool?

Un pool es un conjunto de unidades que se agrupan en forma lógica. Se puede usar un pool para crear uno o más volúmenes accesibles para un host. (Se crean volúmenes desde un pool o un grupo de volúmenes).

Los pools pueden eliminar la necesidad de que los administradores supervisen el uso de cada host para determinar cuándo es posible que se queden sin espacio de almacenamiento y evitar la interrupción del servicio convencional para ajustar el tamaño del disco. Cuando un pool se está por agotar, se pueden añadir unidades adicionales al pool sin producir interrupciones, y el aumento de la capacidad es transparente para el host.

Con los pools, los datos se redistribuyen automáticamente para mantener el equilibrio. Al distribuir la información de paridad y la capacidad de reserva en el pool, cada unidad del pool se puede usar para recompilar una unidad con error. Este enfoque no utiliza unidades de repuesto dedicadas, sino que reserva capacidad de conservación (repuesto) en el pool. En caso de que falle una unidad, los segmentos de otras unidades se leen para volver a crear los datos. Posteriormente, se selecciona una unidad nueva para escribir cada segmento que estaba en la unidad con error con el fin de mantener la distribución de los datos en las unidades.

¿Qué es la capacidad reservada?

La capacidad reservada es la capacidad físicamente asignada para almacenar datos de

objetos de servicio de copia, como imágenes Snapshot volúmenes miembro del grupo de coherencia y volúmenes de parejas reflejadas.

El volumen de capacidad reservada asociado con una operación de servicio de copia reside en un pool o grupo de volúmenes. Se crea la capacidad reservada ya sea desde un pool o grupo de volúmenes.

¿Qué es la seguridad FDE/FIPS?

La seguridad FDE/FIPS hace referencia a unidades compatibles con la función de seguridad que cifran datos durante las escrituras y los descifran durante las lecturas mediante una clave de cifrado única. Estas unidades compatibles con la función de seguridad evitan el acceso no autorizado a los datos en una unidad que se quita físicamente de la cabina de almacenamiento.

Las unidades compatibles con la función de seguridad pueden ser unidades de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS). Las unidades FIPS se sometieron a pruebas de certificación.

> Para los volúmenes que requieren compatibilidad FIPS, se deben utilizar solo unidades FIPS. Si se mezclan unidades FIPS y FDE en un grupo de volúmenes o un pool, todas las unidades se tratarán como unidades FDE. Además, no se puede agregar una unidad FDE ni utilizarse como reserva en un pool o grupo de volúmenes FIPS.

¿Qué es una comprobación de redundancia?

Una comprobación de redundancia determina si los datos de un volumen en un pool o grupo de volúmenes son consistentes. Los datos de redundancia se utilizan para reconstruir información rápidamente en una unidad de reemplazo si falla una de las unidades de un pool o grupo de volúmenes.

Es posible realizar esta comprobación solo en un pool o grupo de volúmenes a la vez. Una comprobación de redundancia de un volumen realiza las acciones siguientes:

- Escanea los bloques de datos en un volumen RAID 3, un volumen RAID 5 o un volumen RAID 6 y, a continuación, comprueba la información de redundancia de cada bloque. (RAID 3 solo puede asignarse a grupos de volúmenes con interfaz de línea de comandos.)
- Compara los bloques de datos en unidades reflejadas RAID 1.
- Devuelve errores de redundancia si el firmware de la controladora determina que los datos no son consistentes.

> Si se ejecuta de inmediato una comprobación de redundancia en el mismo pool o grupo de volúmenes, se puede generar un error. Para evitar este problema, espere de uno a dos minutos antes de ejecutar otra comprobación de redundancia en el mismo pool o grupo de volúmenes.

¿Cuáles son las diferencias entre los pools y los grupos de volúmenes?

Un pool es similar a un grupo de volúmenes, con las siguientes diferencias.

- Los datos de un pool se almacenan al azar en todas las unidades del pool, a diferencia de los datos de un grupo de volúmenes, que se almacenan en el mismo conjunto de unidades.

- Un pool tiene menos degradación del rendimiento cuando falla una unidad, y demora menos tiempo para reconstruirse.
- Un pool tiene capacidad de conservación incorporada; por consiguiente, no requiere unidades de repuesto dedicadas.
- Un pool permite agrupar un gran número de unidades.
- Un pool no necesita un nivel de RAID específico.

¿Por qué debería configurar manualmente un pool?

Los ejemplos siguientes describen por qué se configuraría un pool de forma manual.

- Si tiene varias aplicaciones en la cabina de almacenamiento y no quiere que compitan por los mismos recursos de la unidad, puede considerar la creación manual de un pool más pequeño para una o varias de las aplicaciones.

  Puede asignar solo uno o dos volúmenes en lugar de asignar la carga de trabajo a un pool más grande que tiene varios volúmenes en los cuales se pueden distribuir los datos. La creación manual de un pool individual dedicado a la carga de trabajo de una aplicación específica puede permitir que las operaciones de cabina de almacenamiento sean más rápidas y con menos contención.

  Para crear manualmente un pool: Seleccione **almacenamiento** y, a continuación, seleccione **Pools y grupos de volúmenes**. En la pestaña toda la capacidad, haga clic en **Create › Pool**.

- Si hay varios pools del mismo tipo de unidad, se muestra un mensaje que indica que System Manager no puede recomendar automáticamente las unidades para un pool. Sin embargo, es posible añadir manualmente las unidades a un pool existente.

  Para añadir unidades manualmente a un pool existente: En la página Pools y grupos de volúmenes, seleccione el pool y haga clic en **Añadir capacidad**.

¿Por qué son importantes las alertas de capacidad?

Las alertas de capacidad indican cuándo añadir unidades a un pool. Un pool necesita capacidad libre suficiente para realizar correctamente las operaciones de la cabina de almacenamiento. Es posible evitar interrupciones en estas operaciones si se configura System Manager para que envíe alertas cuando la capacidad libre de un pool alcanza o supera un porcentaje especificado.

Este porcentaje se establece cuando se crea un pool mediante la opción **Configuración automática del pool** o la opción **Crear pool**. Si elige la opción automática, la configuración predeterminada determina automáticamente cuándo recibirá notificaciones de alerta. Si elige la opción de creación manual del pool, puede determinar la configuración de notificaciones de alerta, o bien, si lo prefiere, puede aceptar los ajustes predeterminados. Puede modificar esta configuración posteriormente en MENU:Settings[Alerts].

> Cuando la capacidad libre en el pool alcance el porcentaje especificado, se enviará una notificación de alerta con el método especificado en la configuración de alertas.

¿Por qué no puedo aumentar mi capacidad de conservación?

Si se crearon volúmenes en toda la capacidad utilizable disponible, es posible que no se

pueda aumentar la capacidad de conservación.

La capacidad de conservación es la cantidad de capacidad (número de unidades) reservada en un pool para dar soporte a fallos de unidad potenciales. Cuando se crea un pool, el sistema reserva automáticamente una cantidad predeterminada de capacidad de conservación según el número de unidades del pool. Si creó volúmenes en toda la capacidad utilizable disponible, no puede aumentar la capacidad de conservación sin agregar capacidad al pool, ya sea sumando unidades o eliminando volúmenes.

Puede cambiar la capacidad de conservación de **Pools y grupos de volúmenes**. Seleccione el pool que desea editar. Haga clic en **Ver/editar configuración** y, a continuación, seleccione la ficha **Configuración**.

> La capacidad de conservación se especifica como el número de unidades, a pesar de que la capacidad de conservación real se distribuya en las unidades del pool.

¿Existe un límite para la cantidad de unidades que pueden eliminarse de un pool?

System Manager establece límites en cuanto a la cantidad de unidades que pueden eliminarse de un pool.

- No se puede reducir la cantidad de unidades en un pool a menos de 11.
- No se pueden eliminar unidades si no hay suficiente capacidad libre en el pool para contener los datos de las unidades eliminadas cuando esos datos se redistribuyen a las unidades restantes del pool.
- Es posible eliminar un máximo de 60 unidades al mismo tiempo. Si selecciona más de 60, se deshabilitará la opción Quitar unidades. Si necesita eliminar más de 60 unidades, repita la operación Quitar unidades.

¿Qué tipos de medios son compatibles para una unidad?

Los siguientes tipos de medios son compatibles: Unidad de disco duro (HDD) y disco de estado sólido (SSD).

¿Por qué no se muestran algunas unidades?

En el cuadro de diálogo Añadir capacidad, no todas las unidades se encuentran disponibles para añadir capacidad a un pool o grupo de volúmenes existente.

Las unidades no serán elegibles por cualquiera de los motivos siguientes:

- Una unidad debe estar sin asignar y no debe tener la función de seguridad habilitada. Las unidades que son parte de otro pool, de otro grupo de volúmenes o que están configuradas como pieza de repuesto no son elegibles. Si una unidad está sin asignar, pero tiene la función de seguridad habilitada, se debe eliminar manualmente esa unidad para que sea elegible.
- Una unidad que se encuentra en un estado distinto a Optimal no es elegible.
- Si una unidad tiene muy poca capacidad, no es elegible.
- El tipo de medios de la unidad debe coincidir dentro de un pool o grupo de volúmenes. No puede mezclar lo siguiente:
  - Unidades de disco duro (HDD) con discos de estado sólido (SSD)
  - NVMe con unidades SAS
  - Unidades con tamaños de bloques de volúmenes de 512 bytes y 4 KiB

- Si todas las unidades de un pool o un grupo de volúmenes son compatibles con la función de seguridad, las unidades no compatibles con la función de seguridad no se enumeran.
- Si un pool o grupo de volúmenes contiene todas unidades compatibles con el estándar de procesamiento de información federal (FIPS), las unidades no compatibles con FIPS no se enumeran.
- Si un pool o grupo de volúmenes contiene todas unidades compatibles con la función Garantía de datos (DA) y al menos un volumen del pool o grupo de volúmenes tiene habilitada la función DA, una unidad que no sea compatible con DA no es elegible, por lo que no puede añadirse a ese pool o grupo de volúmenes. Sin embargo, si ningún volumen tiene la función DA habilitada en el pool o grupo de volúmenes, una unidad que no sea compatible con LA función DA puede añadirse a ese pool o grupo de volúmenes. Si decide combinar estas unidades, tenga en cuenta que no podrá crear ningún volumen con la función DA habilitada.

Es posible aumentar la capacidad de la cabina de almacenamiento con la adición de unidades nuevas o la eliminación de pools o grupos de volúmenes.

¿Cómo se mantiene la protección contra pérdida de bandeja/cajón?

Para mantener la protección contra pérdida de bandeja/cajón para un pool o un grupo de volúmenes, use los criterios especificados en la siguiente tabla.

Nivel	Criterios para la protección contra pérdida de bandeja/cajón	Cantidad mínima de bandejas/cajones requeridos
Piscina	Para las bandejas, el pool no debe contener más de dos unidades en una sola bandeja. Para los cajones, el pool debe incluir la misma cantidad de unidades en cada uno de ellos.	6 para bandejas 5 para cajones
RAID 6	El grupo de volúmenes no contiene más de dos unidades por bandeja o cajón.	3
RAID 3 o RAID 5	Cada unidad del grupo de volúmenes está ubicada en una bandeja o un cajón por separado.	3
RAID 1	Cada unidad de una pareja reflejada debe ubicarse en una bandeja o un cajón por separado.	2
RAID 0	No se puede lograr la protección contra pérdida de bandeja/cajón.	No aplicable

La protección contra pérdida de bandeja/cajón no se mantiene si una unidad ya tuvo fallos en el pool o el grupo de volúmenes. En este caso, la pérdida de acceso a la bandeja o el cajón de unidades y, en consecuencia, a otra unidad en el pool o el grupo de volúmenes provoca la pérdida de datos.

¿Cuál es el posicionamiento de unidad óptimo para pools y grupos de volúmenes?

Al crear pools y grupos de volúmenes, asegúrese de equilibrar la selección de unidades entre las ranuras de unidades superior e inferior.

Para las controladoras EF600 y EF300, las ranuras de unidad 0-11 están conectadas a un puente PCI, mientras que las ranuras 12-23 están conectadas a un puente PCI diferente. Para obtener un rendimiento óptimo, se debe equilibrar la selección de unidades para incluir una cantidad prácticamente igual de unidades en las ranuras superior e inferior. Este posicionamiento garantiza que sus volúmenes no alcanzan el límite de ancho de banda antes de lo necesario.

¿Cuál es el nivel de RAID óptimo para cada aplicación?

Para maximizar el rendimiento de un grupo de volúmenes, se debe seleccionar el nivel de RAID adecuado. Es posible determinar el nivel de RAID apropiado si se conocen los porcentajes de escritura y lectura de las aplicaciones que acceden al grupo de volúmenes. Utilice la página rendimiento para obtener estos porcentajes.

Niveles de RAID y rendimiento de la aplicación

RAID se basa en una serie de configuraciones, denominadas *niveles*, para determinar cómo los datos de redundancia y usuario se escriben en las unidades y se recuperan de ellas. Cada nivel de RAID proporciona diferentes funciones de rendimiento. Las aplicaciones con un porcentaje alto de lectura tendrán un buen rendimiento con volúmenes RAID 5 o RAID 6 debido al rendimiento de lectura destacado de las configuraciones RAID 5 y RAID 6.

Las aplicaciones con un porcentaje bajo de lectura (de escritura intensiva) no rinden tan bien con volúmenes RAID 5 o RAID 6. El rendimiento degradado resulta de la forma en que una controladora escribe los datos y los datos de redundancia en las unidades de un grupo de volúmenes RAID 5 o RAID 6.

Seleccione un nivel de RAID según la información siguiente.

RAID 0

- **Descripción**
  - No redundante, modo de segmentación.
- **Cómo funciona**
  - RAID 0 segmenta los datos en todas las unidades del grupo de volúmenes.
- **Funciones de protección de datos**
  - RAID 0 no se recomienda para necesidades de alta disponibilidad. RAID 0 es más adecuado para datos no cruciales.
  - Si una unidad única falla en el grupo de volúmenes, todos los volúmenes asociados fallarán y se perderán todos los datos.
- **Requisitos del número de la unidad**

- Se requiere un mínimo de una unidad para el nivel de RAID 0.
- Los grupos de volúmenes de RAID 0 pueden tener más de 30 unidades.
- Es posible crear un grupo de volúmenes que incluya todas las unidades en la cabina de almacenamiento.

RAID 1 o RAID 10

- **Descripción**
  - Modo de segmentación/reflejo.
- **Cómo funciona**
  - RAID 1 utiliza las operaciones de mirroring de discos para escribir datos en dos discos duplicados en simultáneo.
  - RAID 10 utiliza la segmentación de unidades para segmentar los datos de un conjunto de parejas de unidades reflejadas.
- **Funciones de protección de datos**
  - RAID 1 y RAID 10 ofrecen alto rendimiento y la mejor disponibilidad de datos.
  - RAID 1 y RAID 10 utilizan las operaciones de mirroring de unidades para realizar una copia exacta de una unidad en otra.
  - Si una de las unidades de una pareja de unidades falla, la cabina de almacenamiento puede cambiar instantáneamente a la otra sin perder datos o servicios.
  - Un fallo de unidad única provoca el estado degradado de los volúmenes asociados. La unidad reflejo permite acceder a los datos.
  - Un fallo de la pareja de unidades en un grupo de volúmenes provoca el fallo de todos los volúmenes asociados, y podría ocurrir una pérdida de datos.
- **Requisitos del número de la unidad**
  - Se requiere un mínimo de dos unidades para RAID 1: Una unidad para los datos de usuario y una unidad para los datos reflejados.
  - Si se seleccionan cuatro o más unidades, RAID 10 se configura automáticamente en el grupo de volúmenes: Dos unidades para los datos de usuario y dos unidades para los datos reflejados.
  - El grupo de volúmenes debe tener un número par de unidades. Si no se cuenta con un número par de unidades y quedan algunas sin asignar, vaya a **Pools y grupos de volúmenes** para añadir unidades adicionales al grupo de volúmenes y vuelva a intentar la operación.
  - Los grupos de volúmenes de RAID 1 y RAID 10 pueden tener más de 30 unidades. Se puede crear un grupo de volúmenes que incluya todas las unidades de la cabina de almacenamiento.

RAID 5

- **Descripción**
  - Modo de I/o elevado.
- **Cómo funciona**
  - Los datos de usuario y la información redundante (paridad) se segmentan en las unidades.
  - Se utiliza la capacidad equivalente de una unidad para la información redundante.
- **Funciones de protección de datos**
  - Si una unidad única falla en un grupo de volúmenes RAID 5, todos los volúmenes asociados se

degradan. La información redundante permite que aún pueda accederse a los datos.
    - Si dos o más unidades fallan en un grupo de volúmenes RAID 5, todos los volúmenes asociados fallarán y se perderán todos los datos.
- **Requisitos del número de la unidad**
    - Se debe contar con un mínimo de tres unidades en el grupo de volúmenes.
    - Por lo general, el grupo de volúmenes tiene un límite máximo de 30 unidades.

RAID 6

- **Descripción**
    - Modo de I/o elevado.
- **Cómo funciona**
    - Los datos de usuario y la información redundante (doble paridad) se segmentan en las unidades.
    - Se utiliza la capacidad equivalente de dos unidades para la información redundante.
- **Funciones de protección de datos**
    - Si una o dos unidades fallan en un grupo de volúmenes RAID 6, todos los volúmenes asociados se degradarán, pero la información redundante permitirá que aún pueda accederse a los datos.
    - Si tres o más unidades fallan en un grupo de volúmenes RAID 6, todos los volúmenes asociados fallarán y se perderán todos los datos.
- **Requisitos del número de la unidad**
    - Se debe contar con un mínimo de cinco unidades en el grupo de volúmenes.
    - Por lo general, el grupo de volúmenes tiene un límite máximo de 30 unidades.

> No es posible cambiar el nivel de RAID de un pool. La interfaz de usuario configura automáticamente los pools como RAID 6.

Niveles de RAID y protección de datos

RAID 1, RAID 5 y RAID 6 escriben los datos de redundancia en los medios de la unidad para la tolerancia a fallos. Los datos de redundancia pueden ser una copia de los datos (reflejados) o un código de corrección de error derivado de los datos. Es posible utilizar los datos de redundancia para reconstruir información rápidamente en una unidad de reemplazo si se produce un error en una unidad.

Se configura un nivel de RAID único en un grupo de volúmenes único. Todos los datos de redundancia de ese grupo de volúmenes se almacenan en el grupo de volúmenes. La capacidad del grupo de volúmenes es la capacidad agregada de las unidades miembro menos la capacidad reservada para los datos de redundancia. La cantidad de capacidad necesaria para la redundancia depende del nivel de RAID utilizado.

¿Qué es la garantía de datos?

La garantía de datos (DA) implementa el estándar de información de protección (PI) T10, con el cual se comprueban y corrigen los errores que se pueden producir durante la transferencia de datos a través de la ruta de I/o con el fin de aumentar la integridad de los datos.

El uso típico de la función Garantía de datos es revisar la porción de la ruta de I/o entre las controladoras y las unidades. Las funcionalidades DE DA se presentan a nivel del pool y grupo de volúmenes.

Si esta función está habilitada, la cabina de almacenamiento añade códigos de comprobación de errores (también conocidos como comprobaciones de redundancia cíclicas o CRC) a cada bloque de datos del volumen. Una vez movido un bloque de datos, la cabina de almacenamiento utiliza estos códigos de CRC para determinar si se produjeron errores durante la transmisión. Los datos posiblemente dañados no se escriben en el disco ni se vuelven a transferir al host. Si desea usar la función DA, seleccione un pool o grupo de volúmenes compatible con DA al crear un volumen nuevo (busque la opción "Sí" junto a "DA" en la tabla de candidatos de pools y grupos de volúmenes).

Asegúrese de asignar estos volúmenes con la función DA habilitada a un host que utilice una interfaz de I/o compatible con DA. Las interfaces de I/o compatibles con DA son Fibre Channel, SAS, iSCSI over TCP/IP, NVMe/FC, NVMe/IB, NVME/roce e Iser over InfiniBand (extensiones iSCSI para RDMA/IB). SRP over InfiniBand no es compatible con DA.

¿Qué significa ser compatible con la función de seguridad (Drive Security)?

Drive Security es una función que evita el acceso no autorizado a datos almacenados en unidades con la función de seguridad habilitada cuando la unidad se quita de la cabina de almacenamiento. Estas unidades pueden ser unidades de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS).

¿Qué debo saber acerca del aumento de la capacidad reservada?

Por lo general, se debe aumentar la capacidad cuando se recibe una advertencia que indica que la capacidad reservada corre el peligro de completarse. Es posible aumentar la capacidad reservada únicamente en incrementos de 8 GIB.

- Debe tener suficiente capacidad libre en el pool o el grupo de volúmenes para poder realizar una expansión si es necesario.

  Si no hay capacidad libre en ningún pool o grupo de volúmenes, es posible añadir capacidad sin asignar en forma de unidades no utilizadas a un pool o un grupo de volúmenes.

- El volumen en el pool o el grupo de volúmenes debe tener el estado óptima y no debe estar en ningún estado de modificación.
- Debe existir capacidad libre en el pool o grupo de volúmenes que desea usar para aumentar la capacidad.
- No es posible aumentar la capacidad reservada para un volumen Snapshot de solo lectura. Solo los volúmenes Snapshot que son de lectura y escritura requieren capacidad reservada.

Para las operaciones Snapshot, la capacidad reservada generalmente es el 40 % del volumen base. Para las operaciones de mirroring asíncrono, generalmente es el 20 % del volumen base. Use un porcentaje más alto si cree que el volumen base se someterá a muchos cambios, o si la expectativa de duración estimada de una operación de servicio de copia de un objeto de almacenamiento será muy larga.

¿Por qué no puedo elegir otra cantidad para disminuirla?

Es posible reducir la capacidad reservada solo en la cantidad que se utilizó para aumentarla. La capacidad reservada de los volúmenes miembro puede quitarse solo en el orden inverso al que se añadió.

No es posible reducir la capacidad reservada de un objeto de almacenamiento si se da alguna de las condiciones siguientes:

- Si el objeto de almacenamiento es un volumen de pareja reflejada.
- Si el objeto de almacenamiento contiene solo un volumen para la capacidad reservada. El objeto de almacenamiento debe contener al menos dos volúmenes para la capacidad reservada.
- Si el objeto de almacenamiento es un volumen Snapshot deshabilitado.
- Si el objeto de almacenamiento contiene una o más imágenes Snapshot asociadas.

Solo se pueden quitar volúmenes de capacidad reservada en el orden inverso al que se añadieron.

No es posible reducir la capacidad reservada de un volumen Snapshot de solo lectura, ya que no tiene ninguna capacidad reservada asociada. Solo los volúmenes Snapshot que son de lectura y escritura requieren capacidad reservada.

¿Por qué necesito capacidad reservada para cada volumen miembro?

Cada volumen miembro de un grupo de coherencia Snapshot debe tener su propia capacidad reservada para guardar cualquier modificación que realice la aplicación host en el volumen base sin afectar a la imagen Snapshot de referencia del grupo de coherencia. La capacidad reservada proporciona a la aplicación host el acceso de escritura a una copia de los datos contenidos en el volumen miembro designado como de lectura/escritura.

Los hosts no tienen acceso de lectura o escritura de forma directa a una imagen Snapshot del grupo de coherencia. En cambio, la imagen Snapshot se utiliza para guardar solo los datos capturados desde el volumen base.

Durante la creación de un volumen Snapshot de grupo de coherencia designado como de lectura/escritura, System Manager crea una capacidad reservada para cada volumen miembro del grupo de coherencia. Esta capacidad reservada proporciona a la aplicación host el acceso de escritura a una copia de los datos contenidos en la imagen Snapshot del grupo de coherencia.

¿Cómo se visualizan y se interpretan todas las estadísticas de caché SSD?

Es posible visualizar estadísticas nominales y detalladas para la caché SSD. Las estadísticas nominales son un subconjunto de las estadísticas detalladas.

Las estadísticas detalladas se pueden visualizar solo cuando se exportan todas las estadísticas de SSD a un `.csv` archivo. Al revisar e interpretar las estadísticas, tenga en cuenta que algunas interpretaciones provienen del análisis de una combinación de estadísticas.

Estadísticas nominales

Para ver las estadísticas de caché SSD, seleccione MENU:almacenamiento[Pools y grupos de volúmenes]. Seleccione la caché SSD sobre la cual desea ver estadísticas y, a continuación, seleccione MENU:más[Ver estadísticas]. Las estadísticas nominales se muestran en el cuadro de diálogo Ver estadísticas de la caché SSD.

En la siguiente lista, se incluyen estadísticas nominales, que son un subconjunto de las estadísticas detalladas.

Estadística nominal	Descripción
Lecturas/escrituras	La cantidad total de lecturas de host o escrituras de host en los volúmenes con la función de caché SSD habilitada. Compare las lecturas en relación con las escrituras. Las lecturas deben ser mayores que las escrituras para un funcionamiento eficaz de la caché SSD. Cuando mayor sea la proporción de lecturas con respecto a las escrituras, mejor será el funcionamiento de la caché.
Aciertos en caché	El número de aciertos en caché.
Aciertos en caché (%)	Se deriva de los aciertos en caché/(lecturas + escrituras). El porcentaje de aciertos en caché debe ser mayor que 50 % para un funcionamiento eficaz de la caché SSD. Una cifra pequeña puede indicar varias cuestiones: • El ratio de lecturas respecto de escrituras es demasiado pequeño • Las lecturas no se repiten • La capacidad de la caché es demasiado baja
Asignación en caché (%)	La cantidad de almacenamiento de la caché SSD que se asigna, expresada como un porcentaje del almacenamiento de la caché SSD que está disponible para esta controladora. Derivado de bytes asignados/bytes disponibles. El porcentaje de asignación de la caché normalmente se muestra como 100 %. Si este número es menor que 100 %, significa que la caché no se preparó o que la capacidad de la caché SSD es mayor que la de todos los datos a los que se intenta acceder. En el último caso, una menor capacidad de caché SSD podría ofrecer el mismo nivel de rendimiento. Es preciso tener en cuenta que esto no indica que los datos en caché se colocaron en la caché SSD; simplemente es un paso de preparación antes de que los datos puedan colocarse en la caché SSD.
Uso de caché (%)	La cantidad de almacenamiento en la caché SSD que contiene datos de volúmenes habilitados, expresado como un porcentaje del almacenamiento de la caché SSD que se asigna. Este valor representa la utilización o la densidad de la caché SSD derivada de los bytes de datos de usuario/bytes asignados. El porcentaje de utilización de la caché normalmente es inferior al 100 %, puede que sea mucho menor. Esta cifra muestra el porcentaje de capacidad de la caché SSD que se llena con datos de caché. Esta cifra es menor que 100 %, ya que cada unidad de asignación de caché SSD, el bloque de caché SSD, se divide en unidades más pequeñas denominadas subbloques, que se llenan de manera bastante independiente. Por lo general, una cifra más alta es mejor, pero las mejoras de rendimiento pueden ser significativas incluso con una cifra menor.

Estadística detallada

Las estadísticas detalladas consisten en las estadísticas normales más las estadísticas adicionales. Estas estadísticas adicionales se guardan junto con las estadísticas nominales; pero, a diferencia de las estadísticas nominales, no se muestran en el cuadro de diálogo Ver estadísticas de la caché SSD. Es posible ver las estadísticas detalladas solo después de exportar las estadísticas a `.csv` archivo.

Al ver la `.csv` file, tenga en cuenta que las estadísticas detalladas se enumeran después de las estadísticas nominales:

Estadística detallada	Descripción
Bloques de lectura	La cantidad de bloques en lecturas de host.
Bloques de escritura	La cantidad de bloques en escrituras de host.
Bloques de acierto completo	La cantidad de bloques en aciertos en caché. Los bloques de acierto completo indican la cantidad de bloques que se leyeron completamente de la caché SSD. La caché SSD solo ofrece beneficios en cuanto al rendimiento de las operaciones que son aciertos en caché completos.
Aciertos parciales	La cantidad de lecturas de host, donde al menos un bloque, pero no todos los bloques, se encontraban en la caché SSD. Un acierto parcial es una caché SSD **omisión** donde las lecturas se satisficieron desde el volumen base.
Aciertos parciales - bloques	La cantidad de bloques en aciertos parciales. Los aciertos en caché parciales y los bloques de acierto en caché resultan de una operación que solo tiene una porción de sus datos en la caché SSD. En este caso, la operación debe obtener los datos del volumen de la unidad de disco duro (HDD) almacenado en caché. La caché SSD no ofrece beneficios de rendimiento para este tipo de acierto. Si el número de bloques de acierto en caché parcial es mayor que los bloques de acierto en caché completo, se podría mejorar el rendimiento con un tipo de característica de I/o diferente (sistema de archivos, base de datos o servidor web). Se espera que haya una cifra mayor de aciertos y omisiones en caché en una comparación con los aciertos en caché cuando se está preparando la caché SSD.
Pérdidas	La cantidad de lecturas de host, donde ninguno de los bloques se encontraba en la caché SSD. Una omisión de caché SSD se produce cuando las lecturas se satisficieron desde el volumen base. Se espera que haya una cifra mayor de aciertos y omisiones en caché en una comparación con los aciertos en caché cuando se está preparando la caché SSD.
Pérdidas - bloques	La cantidad de bloques en omisiones.
Completar acciones (Lecturas de host)	La cantidad de lecturas de host donde se copiaron datos desde el volumen base hacia la caché SSD.
Completar acciones(Lecturas de host) - bloques	La cantidad de bloques en acciones de llenado (lecturas de host).
Completar acciones (Escrituras de host)	La cantidad de escrituras de host donde se copiaron datos desde el volumen base hacia la caché SSD. El número de completar acciones (Escrituras de host) puede ser cero para la opción de la configuración de caché que no llena la caché debido a una operación de I/o de escritura.

Estadística detallada	Descripción
Completar acciones(Escrituras de host) - bloques	La cantidad de bloques en acciones de llenado (escrituras de host).
Invalidar acciones	La cantidad de veces que se invalidaron o se eliminaron datos de la caché SSD. Se realiza una operación de invalidación de caché para cada solicitud de escritura de host, cada solicitud de lectura de host con acceso forzado a la unidad (FUA), cada solicitud de verificación, y también en otras circunstancias.
Reciclar acciones	La cantidad de veces que el bloque de caché SSD se reutilizó para otro volumen base y/u otro rango de direcciones de bloque lógico (LBA). Para una operación efectiva de la caché, la cantidad de reciclados debe ser reducida comparada con la cifra sumada de operaciones de lectura y escritura. Si la cantidad de acciones de reciclado está cerca de la cifra sumada de lecturas y escrituras, se está produciendo una hiperpaginación de la caché SSD. Es necesario aumentar la capacidad de caché o la carga de trabajo no es favorable para usar con la caché SSD.
Bytes disponibles	La cantidad de bytes disponibles en la caché SSD que puede utilizar esta controladora.
Bytes asignados	La cantidad de bytes que asignó esta controladora desde la caché SSD. Los bytes asignados de la caché SSD pueden estar vacíos o contener datos de volúmenes base.
Bytes de datos de usuario	La cantidad de bytes asignados en la caché SSD que contienen datos de volúmenes base. Los bytes disponibles, los bytes asignados y los bytes de datos de usuario se usan para computar el porcentaje de asignación de caché y el porcentaje de utilización de caché.

¿Qué es la capacidad de optimización para pools?

Las unidades SSD tendrán una mayor vida útil y mejor rendimiento de escritura máximo cuando una parte de su capacidad no está asignada.

Para las unidades asociadas con un pool, la capacidad sin asignar consta de la capacidad de conservación de un pool, la capacidad libre (capacidad que no utilizan los volúmenes) y una parte de la capacidad utilizable se diferencia como capacidad de optimización adicional. La capacidad de optimización adicional garantiza un nivel mínimo de capacidad de optimización mediante la reducción de la capacidad utilizable, y, como tal, no está disponible para la creación de volúmenes.

Cuando se crea un pool, se genera una capacidad de optimización recomendada que ofrece un equilibrio del rendimiento, la vida útil de la unidad y la capacidad disponible. El control deslizante capacidad de optimización adicional ubicado en el cuadro de diálogo Configuración del pool permite ajustar la capacidad de optimización del pool. El ajuste del control deslizante proporciona un mejor rendimiento y una mayor vida útil de la unidad cuando se descuenta la capacidad disponible, o bien capacidad disponible adicional, costa del rendimiento y la vida útil de la unidad.

El control deslizante de capacidad de optimización adicional solo está disponible para los sistemas de almacenamiento EF600 y EF300.

¿Qué es la capacidad de optimización de los grupos de volúmenes?

Las unidades SSD tendrán una mayor vida útil y mejor rendimiento de escritura máximo cuando una parte de su capacidad no está asignada.

Para las unidades asociadas con un grupo de volúmenes, la capacidad sin asignar consta de la capacidad libre de un grupo de volúmenes (capacidad que no usan los volúmenes) y una parte del conjunto de capacidad utilizable como capacidad de optimización. La capacidad de optimización adicional garantiza un nivel mínimo de capacidad de optimización mediante la reducción de la capacidad utilizable, y, como tal, no está disponible para la creación de volúmenes.

Cuando se crea un grupo de volúmenes, se genera una capacidad de optimización recomendada que ofrece un equilibrio entre rendimiento, vida útil de la unidad y capacidad disponible. El control deslizante capacidad de optimización adicional en el cuadro de diálogo Configuración del grupo de volúmenes permite ajustar la capacidad de optimización de un grupo de volúmenes. El ajuste del control deslizante proporciona un mejor rendimiento y una mayor vida útil de la unidad cuando se descuenta la capacidad disponible, o bien capacidad disponible adicional, costa del rendimiento y la vida útil de la unidad.

El control deslizante de capacidad de optimización adicional solo está disponible para los sistemas de almacenamiento EF600 y EF300.

¿Qué permite el aprovisionamiento de recursos?

El aprovisionamiento de recursos es una función disponible en las cabinas de almacenamiento EF300 y EF600, lo que permite poner en uso los volúmenes de inmediato sin proceso de inicialización en segundo plano.

Un volumen aprovisionado por recursos es un volumen grueso de un grupo de volúmenes SSD o pool, donde se asigna capacidad de la unidad (asignada al volumen) cuando se crea el volumen, pero los bloques de unidades no se asignan (anula la asignación). En comparación, en un volumen grueso tradicional, todos los bloques de unidades se asignan o se asignan durante una operación de inicialización de volúmenes en segundo plano para inicializar los campos de información de protección de Data Assurance y para hacer que la paridad de datos y RAID sea coherente en cada franja de RAID. Con un volumen aprovisionado, no existe una inicialización en segundo plano vinculada al tiempo. En su lugar, cada franja RAID se inicializa con la primera escritura en un bloque de volumen en la franja.

Los volúmenes aprovisionados mediante recursos solo se admiten en los grupos de volúmenes SSD y pools, donde todas las unidades del grupo o pool admiten la funcionalidad de recuperación de error de bloque lógico no escrito o desasignado (DULBE). Cuando se crea un volumen aprovisionado por recursos, todos los bloques de unidades asignados al volumen se desasignan (desasignan). Asimismo, los hosts pueden desasignar bloques lógicos del volumen mediante el comando Gestión de conjuntos de datos de NVMe o el comando SCSI Unmap. Si se desasignan bloques, es posible mejorar la vida útil de las unidades de estado sólido y aumentar el rendimiento de escritura máximo. La mejora varía en función del modelo y la capacidad de cada unidad.

¿Qué debo saber acerca de la función de volúmenes aprovisionados mediante recursos?

El aprovisionamiento de recursos es una función disponible en las cabinas de almacenamiento EF300 y EF600, lo que permite poner en uso los volúmenes de

inmediato sin proceso de inicialización en segundo plano.

Un volumen aprovisionado por recursos es un volumen grueso de un grupo de volúmenes SSD o pool, donde se asigna capacidad de la unidad (asignada al volumen) cuando se crea el volumen, pero los bloques de unidades no se asignan (anula la asignación). En comparación, en un volumen grueso tradicional, todos los bloques de unidades se asignan o se asignan durante una operación de inicialización de volúmenes en segundo plano para inicializar los campos de información de protección de Data Assurance y para hacer que la paridad de datos y RAID sea coherente en cada franja de RAID. Con un volumen aprovisionado, no existe una inicialización en segundo plano vinculada al tiempo. En su lugar, cada franja RAID se inicializa con la primera escritura en un bloque de volumen en la franja.

Los volúmenes aprovisionados mediante recursos solo se admiten en los grupos de volúmenes SSD y pools, donde todas las unidades del grupo o pool admiten la funcionalidad de recuperación de error de bloque lógico no escrito o desasignado (DULBE). Cuando se crea un volumen aprovisionado por recursos, todos los bloques de unidades asignados al volumen se desasignan (desasignan). Asimismo, los hosts pueden desasignar bloques lógicos del volumen mediante el comando Gestión de conjuntos de datos de NVMe o el comando SCSI Unmap. Si se desasignan bloques, es posible mejorar la vida útil de las unidades de estado sólido y aumentar el rendimiento de escritura máximo. La mejora varía en función del modelo y la capacidad de cada unidad.

El aprovisionamiento de recursos está habilitado de forma predeterminada en sistemas donde las unidades admiten DULBE. Puede desactivar esa configuración predeterminada en **Pools y grupos de volúmenes**.

Volúmenes y cargas de trabajo

Información general de los volúmenes y las cargas de trabajo

Es posible crear un volumen como contenedor en el cual las aplicaciones, las bases de datos y los sistemas de archivos almacenan datos. Al crear un volumen, también se debe seleccionar una carga de trabajo para personalizar la configuración de la cabina de almacenamiento para una aplicación específica.

¿Qué son los volúmenes y las cargas de trabajo?

A *volume* es el componente lógico creado con capacidad específica al que debe acceder el host. Aunque es posible que un volumen conste de más de una unidad, un volumen aparece como un componente lógico para el host. Una vez definido un volumen, puede añadirlo a una carga de trabajo. Un *Workload* es un objeto de almacenamiento que admite una aplicación, como SQL Server o Exchange, que se puede utilizar para optimizar el almacenamiento para esa aplicación.

Obtenga más información:

- "Cómo funcionan los volúmenes"
- "Cómo funcionan las cargas de trabajo"
- "Terminología de volúmenes"
- "La forma en que se asigna la capacidad a los volúmenes"
- "Acciones que se pueden realizar en volúmenes"

¿Cómo crea volúmenes y cargas de trabajo?

En primer lugar, debe crear una carga de trabajo. Vaya a MENU:Storage[Volumes] y abra un asistente que le guiará por los pasos. A continuación, se crea un volumen a partir de la capacidad disponible en un pool o un grupo de volúmenes y, luego, se asigna la carga de trabajo que se creó.

Obtenga más información:

- "Flujo de trabajo para crear volúmenes"
- "Crear cargas de trabajo"
- "Cree volúmenes"
- "Añadir volúmenes a la carga de trabajo"

Información relacionada

Más información acerca de conceptos relacionados con los volúmenes:

- "Integridad y seguridad de los datos para volúmenes"
- "Caché SSD y volúmenes"
- "Supervisión de volúmenes finos"

Conceptos

Cómo funcionan los volúmenes

Los volúmenes son contenedores de datos que gestionan y organizan el espacio de almacenamiento en la cabina de almacenamiento.

Es posible crear volúmenes a partir de la capacidad de almacenamiento disponible en la cabina de almacenamiento, y organizar y usar los recursos del sistema con facilidad. Este concepto es similar a usar carpetas o directorios en un equipo para organizar archivos con el fin de simplificar y agilizar el acceso.

Los volúmenes son la única capa de datos visible para los hosts. En un entorno SAN, los volúmenes se asignan a números de unidad lógica (LUN), que son visibles para los hosts. Los LUN conservan los datos de usuario a los que se puede acceder mediante uno o varios de los protocolos de acceso de host compatibles con la cabina de almacenamiento, incluidos FC, iSCSI y SAS.

Tipos de volúmenes que se pueden crear a partir de pools y grupos de volúmenes

Los volúmenes extraen su capacidad de pools o grupos de volúmenes. Es posible crear los siguientes tipos de volúmenes a partir de los pools o los grupos de volúmenes existentes en la cabina de almacenamiento.

- * A partir de pools* — puede crear volúmenes de un pool como volúmenes *completamente aprovisionados (gruesos)* o volúmenes *con Thin-Provisioning (finos).*

  > La interfaz de System Manager no proporciona ninguna opción para crear volúmenes finos. Si se desea crear volúmenes finos, se debe usar la interfaz de línea de comandos (CLI).

- **A partir de grupos de volúmenes** — puede crear volúmenes a partir de un grupo de volúmenes sólo como *volúmenes* completamente aprovisionados (gruesos).

Los volúmenes gruesos y finos extraen capacidad de la cabina de almacenamiento de diferentes formas:

- La capacidad para un volumen grueso se asigna cuando se crea el volumen.
- La capacidad para un volumen fino se asigna como datos cuando se escribe en el volumen.

El thin provisioning ayuda a evitar que se desperdicie capacidad asignada y permite que las empresas ahorren en costos iniciales de almacenamiento. Sin embargo, el aprovisionamiento completo ofrece la ventaja de una menor latencia, porque todo el almacenamiento se asigna de una vez cuando se crean los volúmenes gruesos.

Los sistemas de almacenamiento EF600 y EF300 no admiten thin provisioning.

Características de volúmenes

Cada volumen de un pool o grupo de volúmenes puede tener sus propias características individuales según los tipos de datos se almacenarán en el volumen. Algunas de esas características son:

- **Tamaño de segmento** — un segmento es la cantidad de datos en kilobytes (KiB) que se almacenan en una unidad antes de que la matriz de almacenamiento pase a la siguiente unidad de la franja (grupo RAID). El tamaño del segmento es igual o menor que la capacidad del grupo de volúmenes. El tamaño del segmento es fijo y no se puede cambiar para los pools.
- **Capacidad** — se crea un volumen a partir de la capacidad libre disponible en un pool o grupo de volúmenes. Para poder crear un volumen, el pool o el grupo de volúmenes ya deben existir y debe haber suficiente capacidad libre para crear el volumen.
- **Propiedad de controlador** — todas las matrices de almacenamiento pueden tener uno o dos controladores. En una configuración de controladora única, una sola controladora gestiona la carga de trabajo del volumen. En una configuración de controladora doble, un volumen tendrá una controladora preferida (A o B) que «'es propietaria'» del volumen. En una configuración de controladora doble, la propiedad del volumen se ajusta automáticamente mediante la función Automatic Load Balancing para corregir cualquier problema con el equilibrio de carga cuando las cargas de trabajo cambian según la controladora. La función Automatic Load Balancing proporciona equilibrio de cargas de trabajo de I/o automatizado y garantiza que el tráfico de I/o entrante desde los hosts se gestione de manera dinámica y se equilibre entre ambas controladoras.
- **Asignación de volumen** — puede dar acceso de host a un volumen ya sea al crear el volumen o posteriormente. El acceso a todos los hosts se gestiona mediante un número de unidad lógica (LUN). Los hosts detectan LUN que, a su vez, se asignan a volúmenes. Si va a asignar un volumen a varios hosts, use software de clustering para asegurarse de que el volumen esté disponible para todos los hosts.

  El tipo de host puede tener límites específicos en lo que respecta a la cantidad de volúmenes a los que puede acceder el host. Tenga presente este límite cuando cree volúmenes que utilizará un host en particular.

- **Nombre descriptivo** — se puede nombrar un volumen cualquiera que sea su nombre, pero se recomienda que el nombre sea descriptivo.

Durante la creación de volúmenes, se asigna capacidad a cada volumen y se otorga un nombre, un tamaño de segmento (únicamente grupos de volúmenes), una propiedad de controladora y una asignación de volumen a host al volumen. Los datos de volumen se cargan de manera equilibrada y automática en las controladoras, según sea necesario.

Cómo funcionan las cargas de trabajo

Al crear un volumen, se debe seleccionar una carga de trabajo para personalizar la configuración de la cabina de almacenamiento para una aplicación específica.

Una carga de trabajo es un objeto de almacenamiento que admite una aplicación. Se pueden definir una o más cargas de trabajo o instancias por aplicación. En algunas aplicaciones, el sistema configura la carga de trabajo para contener volúmenes con características subyacentes similares. Estas características de volumen se optimizan según el tipo de aplicación que es compatible con la carga de trabajo. Por ejemplo, si crea una carga de trabajo que es compatible con la aplicación Microsoft SQL Server y, a continuación, crea volúmenes para esa carga de trabajo, las características de volumen subyacentes se optimizan para ser compatibles con Microsoft SQL Server.

Durante la creación de un volumen, el sistema indica que se deben responder preguntas acerca del uso de las cargas de trabajo. Por ejemplo, si se crean volúmenes para Microsoft Exchange, se consultará cuántos buzones se necesitan, cuáles son los requisitos de capacidad promedio del buzón y cuántas copias de la base de datos se desean. El sistema utiliza esta información para crear una configuración de volumen óptima para el usuario, que se puede editar en caso de ser necesario. De manera opcional, es posible omitir este paso en la secuencia de creación de volúmenes.

Tipos de cargas de trabajo

Es posible crear dos tipos de cargas de trabajo: Específicas para una aplicación y de otro tipo.

- **Específico de la aplicación**. Cuando se crean volúmenes con una carga de trabajo específica de la aplicación, el sistema puede recomendar una configuración de volumen optimizada para minimizar la contención entre las operaciones de I/o de la carga de trabajo de la aplicación y demás tráfico de la instancia de la aplicación. Las características del volumen, como tipo de I/o, tamaño de segmentos, propiedad de la controladora, y caché de lectura y escritura, se recomiendan y se optimizan automáticamente para las cargas de trabajo que se crean para los siguientes tipos de aplicaciones.
  - Microsoft® SQL Server™
  - Microsoft® Exchange Server™
  - Aplicaciones de videovigilancia
  - VMware ESXi™ (para volúmenes que se usarán con Virtual Machine File System)

    Se puede revisar la configuración de volumen recomendada y editar, añadir o eliminar volúmenes y características recomendados por el sistema mediante el cuadro de diálogo Añadir/editar volúmenes.

- **Otros** (o aplicaciones sin compatibilidad con la creación de volúmenes específicos). Otras cargas de trabajo utilizan una configuración de volumen que debe especificar manualmente cuando desea crear una carga de trabajo no asociada con una aplicación específica, o si el sistema no posee la optimización integrada para la aplicación que piensa utilizar en la cabina de almacenamiento. Debe especificar manualmente la configuración del volumen en el cuadro de diálogo Añadir/editar volúmenes.

Vistas de aplicaciones y cargas de trabajo

Para ver aplicaciones y cargas de trabajo, ejecute System Manager de SANtricity. Desde esa interfaz, es posible ver la información asociada a una carga de trabajo específica de la aplicación de dos maneras diferentes:

- Es posible seleccionar la pestaña **aplicaciones y cargas de trabajo** en el icono volúmenes para ver los volúmenes de la cabina de almacenamiento agrupados por carga de trabajo, además del tipo de aplicación con la que está asociada la carga de trabajo.
- Puede seleccionar la pestaña **aplicaciones y cargas de trabajo** en el icono rendimiento para ver métricas de rendimiento (latencia, IOPS y MB) de objetos lógicos. Los objetos se agrupan por aplicación y carga de trabajo asociada. Al recoger estos datos de rendimiento en intervalos regulares, se pueden establecer mediciones de referencia y analizar tendencias, que pueden ayudar a investigar problemas relacionados con el rendimiento de I/O.

Terminología de volúmenes

Conozca la forma en que los términos de volúmenes se aplican a su cabina de almacenamiento.

Todos los tipos de volúmenes

Duración	Descripción
Capacidad asignada	Se utiliza la capacidad asignada para crear volúmenes y para operaciones de servicios de copia. La capacidad asignada y la capacidad notificada son iguales en los volúmenes gruesos, pero son diferentes en los volúmenes finos. En el caso de un volumen grueso, el espacio físicamente asignado es igual al espacio que se informa en el host. En un volumen fino, la capacidad notificada es la capacidad que se notifica a los hosts, mientras que la capacidad asignada es la cantidad de espacio de la unidad asignado para la escritura de datos.
Cliente más	Una aplicación es un software, como SQL Server o Exchange. Se definen una o más cargas de trabajo que sean compatibles con cada aplicación. En algunas aplicaciones, el sistema recomienda automáticamente una configuración de volumen que optimice el almacenamiento. Las características como el tipo de I/o, el tamaño de segmento, la propiedad de controladora y la caché de lectura y escritura se incluyen en la configuración de volumen.
Capacidad	La capacidad es la cantidad de datos que se pueden almacenar en un volumen.
Propiedad de la controladora	La propiedad de controladora define la controladora que se designa como propietaria o primaria, la controladora del volumen. Un volumen puede tener un controlador preferido (A o B) que "'posea'" el volumen. La propiedad del volumen se ajusta automáticamente con la función Automatic Load Balancing para corregir cualquier problema de equilibrio de carga cuando las cargas de trabajo cambian entre las controladoras. La función Automatic Load Balancing proporciona equilibrio de cargas de trabajo de I/o automatizado y garantiza que el tráfico de I/o entrante desde los hosts se gestione de manera dinámica y se equilibre entre ambas controladoras.
Captura previa de lectura de caché dinámica	La captura previa de lectura de la caché dinámica permite a la controladora copiar otros bloques de datos secuenciales en la caché mientras lee bloques de datos de una unidad en la caché. Ese almacenamiento en caché aumenta la posibilidad de que se puedan cumplir futuras solicitudes de datos de la caché. La captura previa de lectura de la caché dinámica es importante para las aplicaciones multimedia que utilizan I/o secuencial La cantidad y la velocidad de las capturas previas de los datos en la caché se ajustan automáticamente según la velocidad y el tamaño de solicitud de las lecturas del host. El acceso aleatorio no provoca la captura previa de los datos en la caché. Esta función no se aplica cuando el almacenamiento en caché de lectura está deshabilitado. En el caso de volumen fino, la captura previa de la lectura de caché dinámica siempre está deshabilitada y no se puede modificar.

Duración	Descripción
Área de capacidad libre	Un área de capacidad libre es la capacidad libre que puede surgir después de eliminar un volumen o por no utilizar toda la capacidad libre disponible durante la creación de un volumen. Cuando se crea un volumen en un grupo de volúmenes que tiene una o más áreas de capacidad libre, la capacidad del volumen se limita al área de capacidad libre más grande de ese grupo de volúmenes. Por ejemplo, si un grupo de volúmenes tiene una capacidad libre total de 15 GIB y el área de capacidad libre más grande es 10 GIB, el volumen más grande que se puede crear es de 10 GIB. Al consolidar la capacidad libre, se pueden crear volúmenes adicionales de la cantidad máxima de capacidad libre de un grupo de volúmenes.
Host	Un host es un servidor que envía I/o a un volumen de una cabina de almacenamiento.
Clúster de hosts	Un clúster de hosts es un grupo de hosts. Se crea un clúster de hosts para facilitar la asignación de los mismos volúmenes en varios hosts.
Unidad de repuesto	Las unidades de repuesto solo son compatibles con los grupos de volúmenes. La unidad de repuesto no contiene datos y queda en espera en caso de que se produzca un error en una unidad de los volúmenes RAID 1, RAID 3, RAID 5 o RAID 6 que se encuentran en un grupo de volúmenes. La unidad de repuesto añade otro nivel de redundancia a la cabina de almacenamiento.
LUN	Un número de unidad lógica (LUN) es el número asignado al espacio de dirección que utiliza un host para acceder a un volumen. El volumen se presenta al host como capacidad en forma de LUN. Cada host tiene su propio espacio de dirección de LUN. Por lo tanto, distintos hosts pueden utilizar el mismo LUN para acceder a diferentes volúmenes.
Análisis de medios	Un análisis de medios proporciona un método para detectar errores de medios en la unidad antes de que se detecten durante operaciones de lectura o escritura normales en las unidades. El análisis de medios se realiza como una operación en segundo plano y analiza todos los datos y la información de redundancia en los volúmenes de usuario definidos.
Espacio de nombres	Un espacio de nombres es almacenamiento NVM que se formateó para el acceso en bloque. Es análogo a una unidad lógica en SCSI, que se relaciona con un volumen en la cabina de almacenamiento.
Piscina	Un pool es un conjunto de unidades que se agrupan en forma lógica. Se puede usar un pool para crear uno o más volúmenes accesibles para un host. (Se crean volúmenes desde un pool o un grupo de volúmenes).

Duración	Descripción
Capacidad de pool o grupo de volúmenes	La capacidad de pool, volumen o grupo de volúmenes es la capacidad de una cabina de almacenamiento que se asignó a un pool o un grupo de volúmenes. Esta capacidad se usa para crear volúmenes y atender las diversas necesidades de capacidad de las operaciones de servicios de copia y objetos de almacenamiento.
Caché de lectura	La caché de lectura es un búfer que almacena datos que se leyeron de las unidades. Es posible que los datos de una operación de lectura ya deban estar en la caché debido a una operación anterior, por lo tanto, no es necesario acceder a las unidades. Los datos se conservan en la caché de lectura hasta que esta se vacía.
Capacidad notificada	La capacidad notificada es la capacidad que se informa al host y a la que el host puede acceder. La capacidad notificada y la capacidad asignada son iguales en los volúmenes gruesos, pero son diferentes en los volúmenes finos. En el caso de un volumen grueso, el espacio físicamente asignado es igual al espacio que se informa en el host. En un volumen fino, la capacidad notificada es la capacidad que se notifica a los hosts, mientras que la capacidad asignada es la cantidad de espacio de la unidad asignado para la escritura de datos.
Tamaño de los segmentos	Un segmento es la cantidad de datos en kilobytes (KiB) que se almacenan en una unidad antes de que la cabina de almacenamiento pase a la unidad siguiente en la franja (grupo RAID). El tamaño del segmento es igual o menor que la capacidad del grupo de volúmenes. El tamaño del segmento es fijo y no se puede cambiar para los pools.
Segmentación	La segmentación es una manera de almacenar datos en la cabina de almacenamiento. La segmentación divide el flujo de datos en bloques de un determinado tamaño (denominado "tamaño de bloque") y luego escribe esos bloques en las unidades uno por uno. Esta manera de almacenamiento de datos se usa para distribuir y almacenar datos en varias unidades físicas. La segmentación es un sinónimo de RAID 0 y distribuye los datos en todas las unidades de un grupo RAID sin paridad.
Volumen	Un volumen es un contenedor en el cual las aplicaciones, las bases de datos y los sistemas de archivos almacenan datos. Es el componente lógico que se crea para que el host acceda al almacenamiento de la cabina de almacenamiento.
Asignación de volúmenes	La asignación de volumen es cómo se asignan los LUN de host a un volumen.
Nombre del volumen	Un nombre de volumen es una cadena de caracteres que se asignan al volumen cuando se crea. Se puede aceptar el nombre predeterminado o se puede proporcionar un nombre más descriptivo que indique el tipo de datos almacenados en el volumen.

Duración	Descripción
Grupo de volúmenes	Un grupo de volúmenes es un contenedor para volúmenes con características compartidas. Un grupo de volúmenes tiene una capacidad definida y un nivel de RAID. Se puede usar un grupo de volúmenes para crear uno o más volúmenes a los que se pueda acceder mediante un host. (Los volúmenes se crean a partir de un pool o un grupo de volúmenes).
Carga de trabajo	Una carga de trabajo es un objeto de almacenamiento que admite una aplicación. Se pueden definir una o más cargas de trabajo o instancias por aplicación. En algunas aplicaciones, el sistema configura la carga de trabajo para contener volúmenes con características subyacentes similares. Estas características de volumen se optimizan según el tipo de aplicación que es compatible con la carga de trabajo. Por ejemplo, si crea una carga de trabajo que es compatible con la aplicación Microsoft SQL Server y, a continuación, crea volúmenes para esa carga de trabajo, las características de volumen subyacentes se optimizan para ser compatibles con Microsoft SQL Server.
Caché de escritura	La caché de escritura es un búfer que almacena datos del host que todavía no se escribieron en las unidades. Los datos permanecen en la caché de escritura hasta que se escriben en las unidades. El almacenamiento en caché de escritura puede aumentar el rendimiento de I/O.
Almacenamiento en caché de escritura con mirroring	El almacenamiento en caché de escritura con mirroring se produce cuando los datos escritos en la memoria caché de una controladora también se escriben en la memoria caché de otra controladora. Por lo tanto, si una controladora falla, la otra puede completar todas las operaciones de escritura pendientes. El mirroring de la caché de escritura está disponible solo si el almacenamiento en caché de escritura está habilitado y existen dos controladoras. El almacenamiento en caché de escritura con mirroring es la configuración predeterminada cuando se crea un volumen.
Almacenamiento en caché de escritura sin baterías	La configuración de almacenamiento en caché de escritura sin baterías permite que el almacenamiento en caché de escritura continúe incluso si las baterías faltan, fallan, están completamente descargadas o no están totalmente cargadas. Por lo general, no se recomienda elegir el almacenamiento en caché de escritura sin baterías porque se pueden perder los datos en caso de interrupción del suministro eléctrico. Comúnmente, la controladora desactiva en forma temporal el almacenamiento en caché de escritura hasta que se cargan las baterías o se reemplaza una batería con errores.

Específico de volúmenes finos

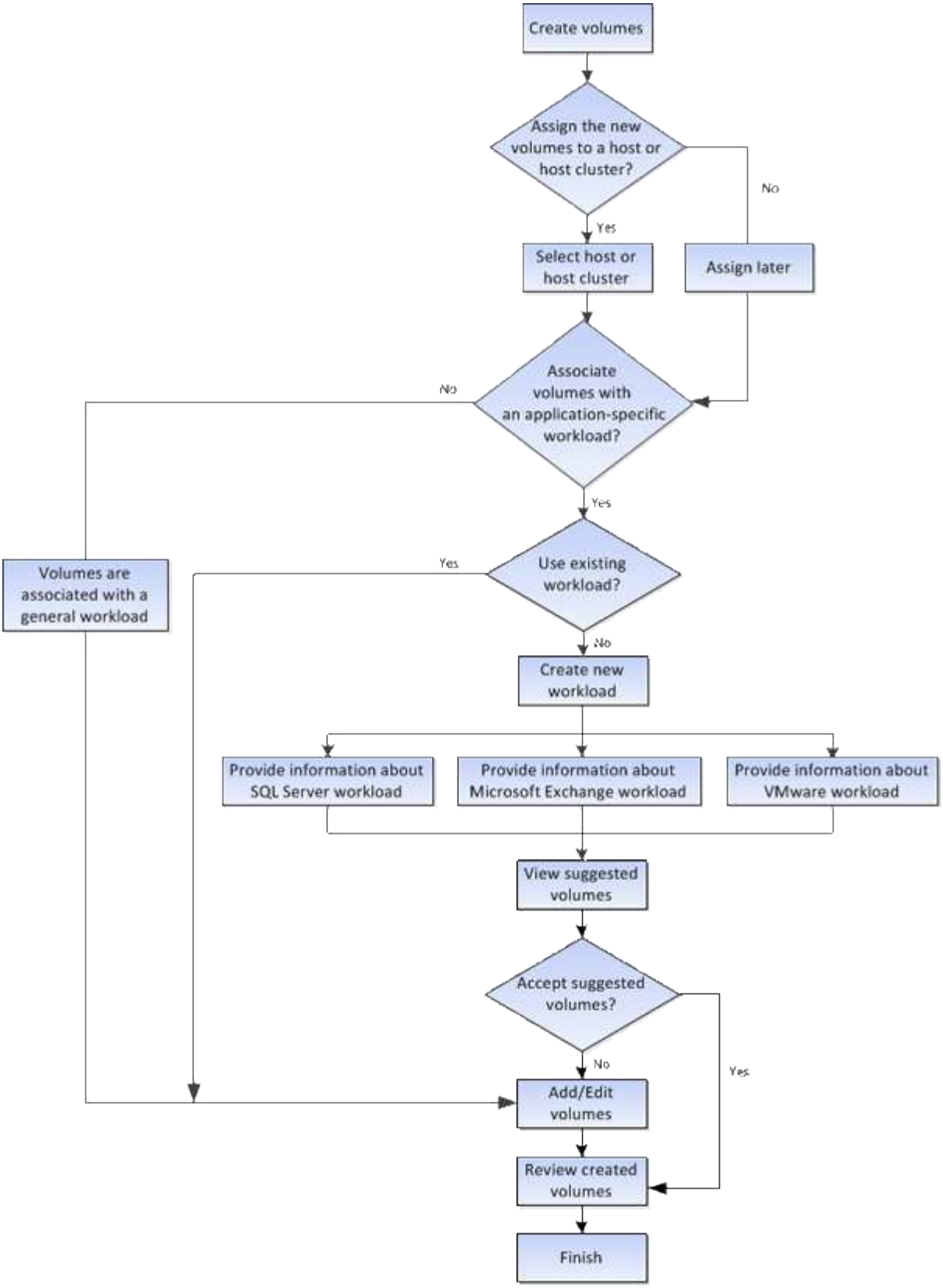
System Manager no proporciona ninguna opción para crear volúmenes finos. Si se desea crear volúmenes finos, se debe usar la interfaz de línea de comandos (CLI).

Los volúmenes finos no están disponibles en los sistemas de almacenamiento EF600 o EF300.

Duración	Descripción
Límite de capacidad asignada	El límite de la capacidad asignada equivale a cuánto puede aumentar la capacidad física asignada para un volumen fino.
Capacidad escrita	La capacidad escrita es la cantidad que se escribió de la capacidad reservada asignada para volúmenes finos.
Umbral de advertencia	Se puede definir una alerta de umbral de advertencia que indique cuándo la capacidad asignada para un volumen fino alcanza la totalidad del porcentaje (el umbral de advertencia).

Flujo de trabajo para crear volúmenes

En System Manager, se pueden crear volúmenes mediante los pasos siguientes.



Integridad y seguridad de los datos para volúmenes

Es posible habilitar volúmenes para que usen las funciones Data Assurance (DA) y Drive Security. Estas funciones se presentan en los niveles de pool y grupo de volúmenes.

Garantía de datos

La garantía de datos (DA) implementa el estándar de información de protección (PI) T10, con el cual se comprueban y corrigen los errores que se pueden producir durante la transferencia de datos a través de la ruta de I/o con el fin de aumentar la integridad de los datos. El uso típico de la función Garantía de datos es revisar la porción de la ruta de I/o entre las controladoras y las unidades. Las funcionalidades DE DA se presentan a nivel del pool y grupo de volúmenes.

Si esta función está habilitada, la cabina de almacenamiento añade códigos de comprobación de errores (también conocidos como comprobaciones de redundancia cíclicas o CRC) a cada bloque de datos del volumen. Una vez movido un bloque de datos, la cabina de almacenamiento utiliza estos códigos de CRC para determinar si se produjeron errores durante la transmisión. Los datos posiblemente dañados no se escriben en el disco ni se vuelven a transferir al host. Si desea usar la función DA, seleccione un pool o grupo de volúmenes compatible con DA al crear un volumen nuevo (busque la opción "Sí" junto a "DA" en la tabla de candidatos de pools y grupos de volúmenes).

Drive Security

Drive Security es una función que evita el acceso no autorizado a datos almacenados en unidades con la función de seguridad habilitada cuando la unidad se quita de la cabina de almacenamiento. Estas unidades pueden ser unidades de cifrado de disco completo (FDE) o unidades certificadas para cumplir con el estándar de procesamiento de información federal 140-2 de nivel 2 (unidades FIPS).

Cómo funciona Drive Security en el nivel de unidad

Una unidad compatible con la función de seguridad, FDE o FIPS, cifra los datos durante la escritura y descifra los datos durante la lectura. Estas operaciones de cifrado y descifrado no afectan al rendimiento ni al flujo de trabajo del usuario. Cada unidad tiene su propia clave de cifrado, que jamás puede transferirse de la unidad.

Cómo funciona Drive Security en el nivel de volumen

Al crear un pool o un grupo de volúmenes desde unidades compatibles con la función de seguridad, también es posible habilitar Drive Security para estos pools o grupos de volúmenes. La opción Drive Security permite que las unidades y los pools y los grupos de volúmenes asociados tengan la función de seguridad-*enabled*. Un pool o un grupo de volúmenes pueden contener tanto una unidad compatible con la función de seguridad como una que no lo sea, pero todas las unidades deben ser compatibles con la función de seguridad para usar la funcionalidad de cifrado.

Cómo implementar Drive Security

Para implementar Drive Security, siga estos pasos.

1. Equipe la cabina de almacenamiento con unidades compatibles con la función de seguridad, ya sea con unidades FDE o FIPS. (Para los volúmenes que requieren compatibilidad con FIPS, debe utilizar únicamente unidades FIPS. Si se mezclan unidades FIPS y FDE en un grupo de volúmenes o un pool, todas las unidades se tratarán como unidades FDE. Además, una unidad FDE no puede añadirse a ni usarse como pieza de repuesto en un grupo de volúmenes o un pool completamente FIPS.)
2. Cree una clave de seguridad, que es una cadena de caracteres compartida por la controladora y las unidades para acceso de lectura/escritura. Es posible crear una clave interna desde la memoria persistente de la controladora o una clave externa desde un servidor de gestión de claves. Para la gestión de claves externas, debe establecerse una autenticación con el servidor de gestión de claves.
3. Habilite Drive Security para pools y grupos de volúmenes:
    - Cree un pool o grupo de volúmenes (busque **Sí** en la columna **compatible con la función de seguridad** de la tabla candidatos).

- Seleccione un pool o grupo de volúmenes cuando cree un volumen nuevo (busque **Sí** junto a **compatible con la función de seguridad** en la tabla de candidatos de pools y grupos de volúmenes).

  Con la función Drive Security, se crea una clave de seguridad que se comparte entre las unidades con la función de seguridad habilitada y las controladoras en una cabina de almacenamiento. Siempre que se encienden y se apagan las unidades, las unidades con la función de seguridad habilitada cambian al estado Security Locked hasta que la controladora aplica la clave de seguridad.

Caché SSD y volúmenes

Es posible añadir un volumen a la caché SSD como una manera de aumentar el rendimiento de solo lectura. La caché SSD se compone de un conjunto de unidades de disco de estado sólido (SSD) agrupadas de forma lógica en la cabina de almacenamiento.

Volúmenes

Se utilizan mecanismos de I/o de volúmenes simples para transferir datos desde y hacia la caché SSD. Después de almacenar datos en la caché y en la unidad SSD, las lecturas posteriores de esos datos se realizan en la caché SSD, por lo que se elimina la necesidad de acceder al volumen de la unidad de disco duro.

La caché SSD es una caché secundaria para usar con la caché primaria en la memoria dinámica de acceso aleatorio (DRAM) de la controladora.

- En la caché primaria, los datos se almacenan en DRAM después de la lectura en el host.
- En la caché SSD, se copian datos de volúmenes y se almacenan en dos volúmenes de RAID internos (uno por controladora) que se crean automáticamente al crear una caché SSD.

Los volúmenes RAID internos se usan para fines de procesamiento de la caché interna. No puede accederse a estos volúmenes desde la interfaz de usuario y no aparecen en ella. Sin embargo, estos dos volúmenes cuentan para la cantidad total de volúmenes permitidos en la cabina de almacenamiento.

> Cualquier volumen asignado para utilizar una caché SSD de una controladora no es elegible para una transferencia de equilibrio de carga automática.

Función Drive Security

Para usar la caché SSD en un volumen que también utiliza Drive Security (es decir, con la función de seguridad habilitada), las funcionalidades de Drive Security del volumen y de la caché SSD deben coincidir. Si no coinciden, el volumen no tendrá la función de seguridad habilitada.

Acciones que se pueden realizar en volúmenes

Se pueden realizar varias acciones distintas en un volumen: Aumentar la capacidad, eliminar, copiar, inicializar, redistribuir, cambio de propiedad, cambio de la configuración de la caché y cambio de configuración de análisis de medios.

Aumente la capacidad

Es posible expandir la capacidad de un volumen de dos maneras:

- Usar la capacidad libre que está disponible en el pool o el grupo de volúmenes.

  Si desea añadir capacidad al volumen, seleccione MENU:almacenamiento[Pools y grupos de volúmenes > Añadir capacidad].

- Añadir capacidad sin asignar (en la forma de unidades sin utilizar) en el pool o el grupo de volúmenes del volumen. Use esta opción cuando no existe capacidad libre en el pool o el grupo de volúmenes.

  Si desea añadir capacidad sin asignar al pool o grupo de volúmenes, seleccione menú:almacenamiento[Pools y grupos de volúmenes > Añadir capacidad].

  Si no hay capacidad libre disponible en el pool o el grupo de volúmenes, no es posible aumentar la capacidad del volumen. Debe aumentar el tamaño del pool o grupo de volúmenes en primer lugar o eliminar volúmenes sin usar.

Después de expandir la capacidad del volumen, debe aumentar manualmente el tamaño del sistema de archivos para que coincidan. La forma de hacerlo depende del sistema de archivos utilizado. Para obtener detalles, compruebe la documentación del sistema operativo del host.

Eliminar

Por lo general, debe eliminar volúmenes si se crearon con los parámetros o la capacidad equivocados, ya no satisfacen las necesidades de configuración del almacenamiento o son imágenes Snapshot que ya no se necesitan para backup o prueba de aplicaciones. Al eliminar un volumen, aumenta la capacidad libre en el pool o el grupo de volúmenes.

Al eliminar volúmenes, se pierden todos los datos que contienen. Al eliminar un volumen, también se eliminan todas las imágenes Snapshot asociadas, las planificaciones y los volúmenes Snapshot, y se eliminan todas las relaciones de mirroring.

Copiar

Cuando se copian volúmenes, se crea una copia de un momento específico de dos volúmenes distintos, el volumen de origen y el volumen objetivo, en la misma cabina de almacenamiento. Si desea copiar volúmenes, seleccione MENU:almacenamiento[volúmenes > Servicios de copia > Copiar volumen].

Inicializar

Al inicializar un volumen, se borran todos los datos del volumen. Un volumen se inicializa automáticamente cuando se crea por primera vez. Sin embargo, es posible que Recovery Guru recomiende inicializar manualmente un volumen para la recuperación de ciertas condiciones de fallo. Cuando se inicializa un volumen, este conserva su configuración de WWN, asignaciones de hosts, capacidad asignada y capacidad reservada. También conserva la misma configuración de Data Assurance (DA) y de seguridad.

Si desea inicializar volúmenes, seleccione MENU:Storage[Volumes > más > Initialize Volumes].

Redistribuir

Es posible redistribuir volúmenes para moverlos nuevamente a sus propietarios de controladoras preferidos. Por lo general, los controladores multivía mueven volúmenes de su propietario de controladora preferido cuando se produce un problema en la ruta de datos entre el host y la cabina de almacenamiento.

La mayoría de los controladores multivía intentan acceder a cada volumen en una ruta a su propietario de controladora preferido. Sin embargo, si esta ruta preferida no está disponible, el controlador multivía en el host conmuta al nodo de respaldo a una ruta alternativa. Esta conmutación al nodo de respaldo puede provocar

que la propiedad del volumen cambie a la controladora alternativa. Después de resolver la condición que provocó la conmutación al nodo de respaldo, es posible que algunos hosts muevan automáticamente la propiedad del volumen nuevamente al propietario de la controladora preferido; sin embargo, en algunos casos es posible que deba redistribuir manualmente los volúmenes.

Si desea redistribuir volúmenes, seleccione menú:almacenamiento[volúmenes > más > redistribuir volúmenes].

Cambiar la propiedad de un volumen

Al cambiar la propiedad de un volumen, se cambia la propiedad de la controladora preferida del volumen. El propietario de la controladora preferida de un volumen se muestra en una lista en el menú:almacenamiento[volúmenes > Ver/editar configuración > pestaña avanzada].

Si desea cambiar la propiedad de un volumen, seleccione menú:almacenamiento[volúmenes > más > Cambiar propiedad].

Mirroring y propiedad de volumen

Si el volumen primario de la pareja reflejada pertenece a la controladora A, el volumen secundario también pertenecerá a la controladora A en la cabina De almacenamiento remota. Al cambiar el propietario del volumen primario, se modificará automáticamente el propietario del volumen secundario para garantizar que los dos volúmenes pertenezcan a la misma controladora. Los cambios de propiedad actuales en el lado primario se propagan automáticamente a los cambios de propiedad correspondientes en el lado secundario.

Si un grupo de coherencia de reflejos contiene un volumen secundario local y se cambia la propiedad de la controladora, el volumen secundario automáticamente se vuelve a transferir a su propietario de controladora original en la primera operación de escritura. No puede cambiar la propiedad del controlador de un volumen secundario mediante la opción **Cambiar propiedad**.

Copia de volumen y propiedad de volumen

Durante una operación de copia de volumen, la misma controladora debe ser la propietaria del volumen de origen y del volumen objetivo. A veces, ambos volúmenes no tienen la misma controladora preferida cuando se inicia la operación de copia de volumen. Por lo tanto, la propiedad del volumen objetivo se transfiere automáticamente a la controladora preferida del volumen de origen. Cuando la copia de volumen se completa o se detiene, la propiedad del volumen objetivo se restaura a su controladora preferida.

Si la propiedad del volumen de origen se cambia durante la operación de copia de volumen, la propiedad del volumen objetivo también se cambia. En determinados entornos de sistema operativo, es posible que sea necesario volver a configurar el controlador de host multivía para poder utilizar la ruta de I/O. (Algunos controladores multivía requieren una edición para reconocer la ruta de I/O. Consulte la documentación de su controlador para obtener más información.)

Cambiar configuración de caché

La memoria caché es un área de almacenamiento volátil temporal (RAM) en la controladora que tiene un tiempo de acceso menor que los medios con unidades. Con el uso de la memoria caché, es posible aumentar el rendimiento general de las operaciones de I/o por las siguientes razones:

- Los datos solicitados desde el host para una lectura pueden estar ya en la caché debido a una operación anterior. Esto elimina la necesidad de acceder a la unidad.
- Los datos de escritura se escriben primero en la caché. Esto permite que la aplicación avance sin esperar que los datos se escriban en la unidad.

Seleccione **Storage › Volumes › more › Change cache settings** para cambiar las siguientes opciones de configuración de caché:

- **Caché de lectura y escritura** — la caché de lectura es un búfer que almacena datos que se han leído desde las unidades. Es posible que los datos de una operación de lectura ya deban estar en la caché debido a una operación anterior, por lo tanto, no es necesario acceder a las unidades. Los datos se conservan en la caché de lectura hasta que esta se vacía.

  La caché de escritura es un búfer que almacena datos del host que todavía no se escribieron en las unidades. Los datos permanecen en la caché de escritura hasta que se escriben en las unidades. El almacenamiento en caché de escritura puede aumentar el rendimiento de I/O.

- **Almacenamiento en caché de escritura con duplicación** — el almacenamiento en caché de escritura con duplicación se produce cuando los datos escritos en la memoria caché de un controlador también se escriben en la memoria caché del otro controlador. Por lo tanto, si una controladora falla, la otra puede completar todas las operaciones de escritura pendientes. El mirroring de la caché de escritura está disponible solo si el almacenamiento en caché de escritura está habilitado y existen dos controladoras. El almacenamiento en caché de escritura con mirroring es la configuración predeterminada cuando se crea un volumen.
- **Almacenamiento en caché de escritura sin baterías** — la configuración de almacenamiento en caché de escritura sin baterías permite que el almacenamiento en caché de escritura continúe incluso cuando las baterías faltan, fallan, están completamente descargadas o no están totalmente cargadas. Por lo general, no se recomienda elegir el almacenamiento en caché de escritura sin baterías porque se pueden perder los datos en caso de interrupción del suministro eléctrico. Comúnmente, la controladora desactiva en forma temporal el almacenamiento en caché de escritura hasta que se cargan las baterías o se reemplaza una batería con errores.

  Esta configuración solo está disponible si se habilita el almacenamiento en caché de escritura. Esta configuración no está disponible para volúmenes finos.

- **Captura previa de caché de lectura dinámica**: La captura previa de lectura de caché dinámica permite a la controladora copiar otros bloques de datos secuenciales en la caché mientras lee bloques de datos de una unidad en la caché. Ese almacenamiento en caché aumenta la posibilidad de que se puedan cumplir futuras solicitudes de datos de la caché. La captura previa de lectura de la caché dinámica es importante para las aplicaciones multimedia que utilizan I/o secuencial La cantidad y la velocidad de las capturas previas de los datos en la caché se ajustan automáticamente según la velocidad y el tamaño de solicitud de las lecturas del host. El acceso aleatorio no provoca la captura previa de los datos en la caché. Esta función no se aplica cuando el almacenamiento en caché de lectura está deshabilitado.

  En el caso de volumen fino, la captura previa de la lectura de caché dinámica siempre está deshabilitada y no se puede modificar.

Cambiar configuración de análisis de medios

En los análisis de medios, se detectan y reparan errores de medios en bloques de discos que las aplicaciones leen con poca frecuencia. Este análisis puede evitar la pérdida de datos si se producen errores en otras unidades del pool o grupo de volúmenes a medida que se reconstruyen los datos de las unidades con error mediante información de redundancia y datos de otras unidades del pool o grupo de volúmenes.

Los análisis de medios se ejecutan continuamente a una tasa constante sobre la base de la capacidad que se analizará y la duración del análisis. Una tarea que se ejecuta en segundo plano de mayor prioridad puede suspender temporalmente los análisis que se ejecutan en segundo plano (por ejemplo, una reconstrucción), pero se reanudan a la misma velocidad constante.

Es posible habilitar y establecer la duración de la ejecución del análisis de medios. Para ello, seleccione MENU:almacenamiento[volúmenes > más > Cambiar configuración de análisis de medios].

Un volumen solo se analiza cuando está habilitada la opción de análisis de medios para la cabina de almacenamiento y para ese volumen. Si también se habilita la verificación de redundancia para ese volumen, la información de redundancia del volumen se verifica para ver si coincide con los datos, siempre y cuando el volumen tenga redundancia. El análisis de medios con verificación de redundancia está habilitado de forma predeterminada para cada volumen cuando se crea.

Si se encuentra un error de medio irrecuperable durante el análisis, los datos se repararán usando la información de redundancia, si está disponible. Por ejemplo, la información de redundancia está disponible en volúmenes RAID 5 óptimos o en volúmenes RAID 6 que son óptimos o que solo tienen una sola unidad con fallos. Si el error irrecuperable no puede repararse mediante el uso de la información de redundancia, el bloque de datos se añade al registro de sectores ilegibles. Tanto los errores de medios que pueden corregirse como los que no pueden corregirse se informan en el registro de eventos.

Si se encuentra una incoherencia entre los datos y la información de redundancia en la verificación de redundancia, se informa en el registro de eventos.

La forma en que se asigna la capacidad a los volúmenes

Las unidades de la cabina de almacenamiento proporcionan capacidad de almacenamiento físico para los datos. Antes de comenzar a almacenar datos, es necesario configurar la capacidad asignada a los componentes lógicos conocidos como pools o grupos de volúmenes. Estos objetos de almacenamiento se utilizan para configurar, almacenar, mantener y conservar los datos en la cabina de almacenamiento.

Usar la capacidad para crear y expandir volúmenes

Es posible crear volúmenes a partir de la capacidad sin asignar o de la capacidad libre en un pool o grupo de volúmenes.

- Cuando se crea un volumen a partir de capacidad sin asignar, es posible crear un pool o grupo de volúmenes y el volumen al mismo tiempo.
- Cuando se crea un volumen a partir de capacidad libre, se crea un volumen adicional en un pool o grupo de volúmenes existente.

Después de expandir la capacidad del volumen, debe aumentar manualmente el tamaño del sistema de archivos para que coincidan. La forma de hacerlo depende del sistema de archivos utilizado. Para obtener detalles, compruebe la documentación del sistema operativo del host.

Tipos de capacidad para volúmenes gruesos y volúmenes finos

Es posible crear volúmenes gruesos o finos. La capacidad notificada y la capacidad asignada son iguales en los volúmenes gruesos, pero son diferentes en los volúmenes finos.

- En un volumen grueso, la capacidad notificada del volumen es igual a la cantidad de capacidad de almacenamiento físico asignada. Se debe presentar la cantidad de capacidad de almacenamiento físico completa. El espacio asignado físicamente es igual al espacio que se notifica al host.

  Normalmente, la capacidad notificada de un volumen grueso se establece como la capacidad máxima hasta la que se cree que el volumen se extenderá. Los volúmenes gruesos brindan un rendimiento alto y previsible para las aplicaciones. Esto se debe principalmente a que toda la capacidad del usuario se reserva y se asigna en la creación.

- En un volumen fino, la capacidad notificada es la capacidad que se notifica a los hosts, mientras que la capacidad asignada es la cantidad de espacio de la unidad asignado para la escritura de datos.

  La capacidad notificada puede ser mayor que la capacidad asignada en la cabina de almacenamiento. Es posible ajustar el tamaño de los volúmenes finos para acomodar el crecimiento sin considerar los activos disponibles actuales.

> System Manager de SANtricity no proporciona ninguna opción para crear volúmenes finos. Si se desea crear volúmenes finos, se debe usar la interfaz de línea de comandos (CLI).

Límites de capacidad para volúmenes gruesos

La capacidad mínima para un volumen grueso es 1 MIB y la capacidad máxima se determina en función de la cantidad de unidades en el pool o el grupo de volúmenes y su capacidad.

Al aumentar la capacidad notificada para un volumen grueso, tenga en cuenta las siguientes directrices:

- Puede especificar hasta tres espacios decimales (por ejemplo, 65 65.375 GIB).
- La capacidad debe ser menor (o igual) que el máximo disponible en el grupo de volúmenes.

  Al crear un volumen, se asigna previamente algo de capacidad adicional para la migración del tamaño de segmentos dinámico (DSS). La migración DSS es una función del software que permite cambiar el tamaño de los segmentos de un volumen.

- Algunos sistemas operativos host admiten volúmenes de más de 2 TIB (el sistema operativo host determina la capacidad notificada máxima). De hecho, algunos sistemas operativos host admiten volúmenes de hasta 128 TIB. Consulte la documentación del sistema operativo host para obtener más detalles.

Límites de capacidad para volúmenes finos

Es posible crear volúmenes finos con una gran capacidad notificada y una capacidad asignada relativamente pequeña, lo que es positivo para la eficiencia y la utilización del almacenamiento. Los volúmenes finos simplifican la administración del almacenamiento, ya que permiten aumentar la capacidad asignada a medida que las necesidades de las aplicaciones cambian, sin interrumpir la aplicación, lo que mejora la utilización del almacenamiento.

Además de capacidad notificada y capacidad asignada, los volúmenes finos pueden contener capacidad escrita. La capacidad escrita es la cantidad que se escribió de la capacidad reservada asignada para volúmenes finos.

En la siguiente tabla, se enumeran los límites de capacidad para un volumen fino.

Tipo de capacidad	Tamaño mínimo	Tamaño máximo
Informada	32 MIB	256 TIB
Asignada	4 MIB	64 TIB

Para un volumen fino, si se alcanzó la capacidad máxima informada de 256 TIB, no se puede aumentar la capacidad. Asegúrese de que la capacidad reservada del volumen fino esté configurada con un tamaño más grande que la capacidad máxima informada.

El sistema expande automáticamente la capacidad asignada de acuerdo con el límite de capacidad establecido. El límite de capacidad establecido permite limitar el crecimiento automático del volumen fino por debajo de la capacidad notificada. Cuando la cantidad de datos escritos se acerca a la capacidad asignada, es posible cambiar el límite de capacidad establecido.

Para modificar el límite de capacidad asignada, seleccione MENU:almacenamiento[volúmenes > pestaña Supervisión de volumen fino > Cambiar límite].

Como System Manager no asigna toda la capacidad al crear un volumen fino, la capacidad libre en el pool puede ser insuficiente. El espacio insuficiente puede bloquear las escrituras en el pool, no solo para los volúmenes finos, sino también para otras operaciones en las que se requiere capacidad del pool (por ejemplo, imágenes Snapshot o volúmenes Snapshot). No obstante, es posible realizar operaciones de lectura desde el pool. En esta situación, puede recibir una advertencia de umbral de alerta.

Supervisión de volúmenes finos

El espacio de los volúmenes finos se puede supervisar, y se pueden generar alertas adecuadas para evitar condiciones de falta de capacidad.

Los entornos con Thin-Provisioning pueden asignar más espacio lógico del almacenamiento físico subyacente que tienen. Se puede seleccionar menú:almacenamiento[volúmenes > Supervisión de volumen fino] para supervisar el crecimiento de los volúmenes finos antes de que alcancen el límite máximo de la capacidad asignada.

La vista Supervisión de volumen fino se puede usar para llevar a cabo las siguientes acciones:

- Definir el límite que restringe la capacidad asignada a la que un volumen fino se puede expandir automáticamente
- Establecer el porcentaje en el que se envía una alerta (umbral de advertencia superado) al área Notificaciones de la página Inicio cuando un volumen fino está cerca del límite máximo de capacidad asignada

Para aumentar la capacidad de un volumen fino, se debe aumentar su capacidad notificada.

> System Manager no proporciona ninguna opción para crear volúmenes finos. Si se desea crear volúmenes finos, se debe usar la interfaz de línea de comandos (CLI).

> Los volúmenes finos no están disponibles en los sistemas de almacenamiento EF600 o EF300.

Comparación entre volúmenes gruesos y volúmenes finos

Un volumen grueso siempre se aprovisiona en su totalidad, lo cual significa que toda la capacidad se asigna cuando se crea el volumen. Un volumen fino siempre se aprovisiona en medida reducida, lo cual significa que la capacidad se asigna a medida que los datos se escriben en el volumen.

> System Manager no proporciona ninguna opción para crear volúmenes finos. Si se desea crear volúmenes finos, se debe usar la interfaz de línea de comandos (CLI).

Tipo de volumen	Descripción
Volúmenes gruesos	• Los volúmenes gruesos se crean desde un pool o grupo de volúmenes. • En el caso de los volúmenes gruesos, se proporciona anticipadamente una gran cantidad de espacio de almacenamiento previendo las futuras necesidades de almacenamiento. • Los volúmenes gruesos se crean con todo el tamaño del volumen asignado previamente en el almacenamiento físico, en el momento en que se crea el volumen. La asignación previa implica que crear un volumen de 100 GIB consume en realidad 100 GIB de capacidad asignada en las unidades. Sin embargo, el espacio puede quedar sin utilizar y producir la subutilización de la capacidad de almacenamiento. • Al crear volúmenes gruesos, es necesario tener en cuenta que no se debe sobreasignar capacidad para un único volumen. Sobreasignar capacidad para un único volumen puede consumir rápidamente todo el almacenamiento físico del sistema. • Recuerde que la capacidad de almacenamiento también es necesaria para los servicios de copia (imágenes Snapshot, volúmenes Snapshot, copias de volúmenes y operaciones de mirroring asíncrono). Por lo tanto, no asigne toda la capacidad a los volúmenes gruesos. El espacio insuficiente puede bloquear la escritura en el pool o en el grupo de volúmenes. Si esta situación se presenta, recibirá una alerta por alcanzar el umbral de capacidad libre.
Volúmenes finos	• Los volúmenes finos se crean únicamente desde un pool, no desde un grupo de volúmenes. • Los volúmenes finos deben ser RAID 6. • Los volúmenes finos no están disponibles en los sistemas de almacenamiento EF600 o EF300. • Debe usar la CLI para crear volúmenes finos. • A diferencia de los volúmenes gruesos, el espacio necesario para los volúmenes finos no se asigna durante la creación, pero se otorga, bajo demanda, en un momento posterior. • Un volumen fino permite sobreasignar su tamaño. Es decir, se puede asignar un tamaño de LUN que sea mayor que el tamaño del volumen. A continuación se puede expandir el volumen según sea conveniente (si es necesario, se pueden añadir unidades en el proceso) sin expandir el tamaño del LUN y, por lo tanto, sin desconectar a los usuarios. • Se puede usar una reclamación de espacio de bloques de thin provisioning (UNMAP) para reclamar bloques de un volumen de Thin-Provisioning en la cabina de almacenamiento a través del comando SCSI UNMAP emitido por el host. Una cabina de almacenamiento que admite thin provisioning puede cambiar el propósito del espacio reclamado para satisfacer las solicitudes de asignación de algún otro volumen de thin provisioning dentro de la misma cabina de almacenamiento, lo cual permite emitir un mejor informe del consumo de espacio en disco y un uso más eficiente de los recursos.

Restricciones de los volúmenes finos

Los volúmenes finos admiten todas las mismas operaciones que los volúmenes gruesos, con las siguientes excepciones:

- No se puede cambiar el tamaño de los segmentos de un volumen fino.
- No se puede habilitar la comprobación de redundancia de lectura previa de un volumen fino.
- No se puede usar un volumen fino como volumen objetivo en la operación Copy Volume.
- Es posible modificar el límite de la capacidad asignada de un volumen fino y el umbral de advertencia solamente en el lado primario de una pareja reflejada asíncrona. Todos los cambios realizados en esos parámetros en el lado primario se propagan automáticamente al lado secundario.

Configurar el almacenamiento

Crear cargas de trabajo

Es posible crear cargas de trabajo para cualquier tipo de aplicación.

Acerca de esta tarea

Una carga de trabajo es un objeto de almacenamiento que admite una aplicación. Se pueden definir una o más cargas de trabajo o instancias por aplicación. En algunas aplicaciones, el sistema configura la carga de trabajo para contener volúmenes con características subyacentes similares. Estas características de volumen se optimizan según el tipo de aplicación que es compatible con la carga de trabajo. Por ejemplo, si crea una carga de trabajo que es compatible con la aplicación Microsoft SQL Server y, a continuación, crea volúmenes para esa carga de trabajo, las características de volumen subyacentes se optimizan para ser compatibles con Microsoft SQL Server.

System Manager recomienda una configuración de volumen optimizada solo para los siguientes tipos de aplicaciones:

- Microsoft® SQL Server™
- Microsoft® Exchange Server™
- Videovigilancia
- VMware ESXi ™ (para volúmenes que se usarán con el sistema de archivos de máquinas virtuales)

Tenga en cuenta estas directrices:

- _Cuando se usa una carga de trabajo específica para una aplicación, el sistema recomienda una configuración de volumen optimizada para minimizar la contención entre las operaciones de I/o de la carga de trabajo de la aplicación y otro tráfico de la instancia de la aplicación. Es posible revisar la configuración de volumen recomendada y luego editar, añadir o eliminar los volúmenes y las características recomendados por el sistema mediante el cuadro de diálogo Añadir/editar volúmenes.
- *Cuando utilice otros tipos de aplicación*, especifique manualmente la configuración de volumen con el cuadro de diálogo Añadir/editar volúmenes.

Pasos

1. Seleccione MENU:Storage[Volumes].
2. Seleccione MENU:Create[Workload].

   Se muestra el cuadro de diálogo Crear carga de trabajo de la aplicación.

3. Utilice la lista desplegable para seleccionar el tipo de aplicación para la que desea crear la carga de trabajo y luego escriba el nombre de la carga de trabajo.
4. Haga clic en **Crear**.

Después de terminar

Está listo para añadir capacidad de almacenamiento a la carga de trabajo creada. Utilice la opción **Crear volumen** para crear uno o varios volúmenes para una aplicación y para asignar cantidades específicas de capacidad a cada volumen.

Cree volúmenes

Se crean volúmenes para añadir capacidad de almacenamiento a una carga de trabajo específica de la aplicación y para que los volúmenes creados sean visibles para un host o clúster de hosts específicos. Además, la secuencia de creación de volúmenes ofrece las opciones de asignar cantidades específicas de capacidad a cada volumen que desea crear.

Acerca de esta tarea

La mayoría de los tipos de aplicaciones adoptan la configuración de volúmenes definida por el usuario en forma predeterminada. Algunos tipos de aplicaciones tienen una configuración inteligente aplicada al crear el volumen. Por ejemplo, si se crean volúmenes para la aplicación Microsoft Exchange, se consultará cuántos buzones se necesitan, cuáles son los requisitos de capacidad promedio del buzón y cuántas copias de la base de datos se desean. System Manager utiliza esta información para crear una configuración de volumen óptima para el usuario, que se puede editar en caso de ser necesario.

El proceso para crear un volumen es un procedimiento de varios pasos.

Paso 1: Seleccionar el host para un volumen

Se crean volúmenes para añadir capacidad de almacenamiento a una carga de trabajo específica de la aplicación y para que los volúmenes creados sean visibles para un host o clúster de hosts específicos. Además, la secuencia de creación de volúmenes ofrece las opciones de asignar cantidades específicas de capacidad a cada volumen que desea crear.

Antes de empezar

- Existen hosts o clústeres de hosts válidos en el icono hosts.
- Se definieron identificadores de puertos de host para el host.
- Para poder crear un volumen con la función DA habilitada, la conexión de host que se planea usar debe admitir DA. Si alguna de las conexiones de host de las controladoras de la cabina de almacenamiento no admite DA, los hosts asociados no podrán acceder a los datos de los volúmenes con la función DA habilitada.

Acerca de esta tarea

Tenga en cuenta estas directrices al asignar volúmenes:

- El sistema operativo de un host puede tener límites específicos acerca de la cantidad de volúmenes a los que puede acceder el host. Tenga presente este límite cuando cree volúmenes que utilizará un host en particular.
- Puede definir una asignación para cada volumen de la cabina de almacenamiento.
- Los volúmenes asignados se comparten entre controladoras de la cabina de almacenamiento.

- El host o un clúster de hosts no pueden usar el mismo número de unidad lógica (LUN) dos veces para acceder a un volumen. Se debe usar un LUN único.
- Si desea acelerar el proceso para crear volúmenes, puede omitir el paso de asignación de host para que los volúmenes recién creados se inicialicen sin conexión.

> Se producirá un error al asignar un volumen a un host si se intenta asignar un volumen a un clúster de hosts que produce un conflicto con una asignación establecida para un host en los clústeres de hosts.

Pasos

1. Seleccione MENU:Storage[Volumes].
2. Seleccione MENU:Create[Volume].

   Se muestra el cuadro de diálogo Crear volúmenes.

3. De la lista desplegable, seleccione el host o el clúster de hosts específicos a los que desea asignar volúmenes o elija asignar el host o el clúster de hosts más adelante.
4. Para continuar con la secuencia de creación de volúmenes para el host o clúster de hosts seleccionados, haga clic en **Siguiente**, y vaya a. Paso 2: Seleccionar una carga de trabajo para un volumen.

   Se muestra el cuadro de diálogo Seleccionar carga de trabajo.

Paso 2: Seleccionar una carga de trabajo para un volumen

Seleccione una carga de trabajo a fin de personalizar la configuración de la cabina de almacenamiento para una aplicación específica, por ejemplo, Microsoft SQL Server, Microsoft Exchange, aplicaciones de videovigilancia o VMware. Puede seleccionar "otra aplicación" si la aplicación que pretende usar de esta cabina de almacenamiento no aparece en la lista.

Acerca de esta tarea

En esta tarea, se describe cómo crear volúmenes para una carga de trabajo existente.

- *Cuando se crean volúmenes con una carga de trabajo específica de la aplicación*, el sistema puede recomendar una configuración de volumen optimizada para minimizar la contención entre las operaciones de I/o de la carga de trabajo de la aplicación y demás tráfico de la instancia de la aplicación. Se puede revisar la configuración de volumen recomendada y editar, añadir o eliminar volúmenes y características recomendados por el sistema mediante el cuadro de diálogo Añadir/editar volúmenes.
- *Cuando se crean volúmenes mediante "Other"* aplicaciones (o aplicaciones que no admiten la creación de un volumen específico), se debe especificar manualmente la configuración del volumen con el cuadro de diálogo Añadir/editar volúmenes.

Pasos

1. Debe realizar una de las siguientes acciones:
   - Seleccione la opción **Crear volúmenes para una carga de trabajo existente** para crear volúmenes para una carga de trabajo existente.
   - Seleccione la opción **Crear una carga de trabajo nueva** para definir una carga de trabajo nueva para una aplicación compatible o para "otras" aplicaciones.
     - De la lista desplegable, seleccione el nombre de la aplicación para la cual desea crear la carga de trabajo nueva.

Seleccione una de las entradas que figuran como "Other", si la aplicación que pretende usar en esta cabina de almacenamiento no aparece en la lista.

- Introduzca el nombre de la carga de trabajo que desea crear.

2. Haga clic en **Siguiente**.
3. Si la carga de trabajo está asociada con un tipo de aplicación admitida, introduzca la información solicitada, de lo contrario, vaya a. Paso 3: Añadir o editar volúmenes.

Paso 3: Añadir o editar volúmenes

System Manager puede sugerir una configuración de volumen según la aplicación o la carga de trabajo seleccionadas. Esta configuración de volumen se optimiza según el tipo de aplicación que admite la carga de trabajo. Se puede aceptar la configuración de volumen recomendada o se puede editar, según sea necesario. Si seleccionó la opción "Other" para aplicaciones, debe especificar manualmente los volúmenes y las características que desea crear.

Antes de empezar

- Los pools o los grupos de volúmenes deben tener suficiente capacidad libre.
- La cantidad máxima de volúmenes permitidos en un grupo de volúmenes es de 256.
- La cantidad máxima de volúmenes permitidos en un pool depende del modelo del sistema de almacenamiento:
  - 2,048 volúmenes (series EF600 y E5700)
  - 1,024 volúmenes (EF300)
  - 512 volúmenes (serie E2800)
- Para crear un volumen que tenga habilitada la función Garantía de datos (DA), la conexión de host que se planea usar debe admitir DA.

  Seleccionar un pool o un grupo de volúmenes que sea compatible con la función de seguridad

  Si desea crear un volumen con la función DA habilitada, seleccione un pool o un grupo de volúmenes que sea compatible con DA (asegúrese de **Sí** junto a "DA" en la tabla de candidatos de pools y grupos de volúmenes).

  Las funcionalidades DE DA se presentan a nivel del pool y grupo de volúmenes de System Manager. La protección DE DA comprueba y corrige los errores que se pueden producir durante la transferencia de datos a través de las controladoras hasta las unidades. Al seleccionar un pool o un grupo de volúmenes compatibles con DA para el volumen nuevo, se garantizan la detección y la corrección de cualquier error.

  Si alguna de las conexiones de host de las controladoras de la cabina de almacenamiento no admite DA, los hosts asociados no podrán acceder a los datos de los volúmenes con la función DA habilitada.

- Para crear un volumen con la función de seguridad habilitada, se debe crear una clave de seguridad para la cabina de almacenamiento.

Seleccionar un pool o un grupo de volúmenes que sea compatible con la función de seguridad

Si desea crear un volumen con la función de seguridad habilitada, seleccione un pool o un grupo de volúmenes que sean compatibles con la función de seguridad (asegúrese de que **Sí** junto a "compatible con la función de seguridad" en la tabla de candidatos de pools y grupos de volúmenes).

Las funcionalidades de seguridad de la unidad se presentan a nivel del pool y grupo de volúmenes de System Manager. Las unidades que son compatibles con la función de seguridad evitan el acceso no autorizado a los datos de una unidad que se quita físicamente de la cabina de almacenamiento. Una unidad con la función de seguridad habilitada cifra los datos durante la escritura y descifra los datos durante las lecturas mediante una *clave de cifrado* única.

Un pool o un grupo de volúmenes pueden contener tanto una unidad compatible con la función de seguridad como una que no lo sea, pero todas las unidades deben ser compatibles con la función de seguridad para usar la funcionalidad de cifrado.

- Para crear un volumen aprovisionado por recursos, todas las unidades deben ser unidades NVMe con la opción error de bloque lógico no escrito o desasignado (DULBE).

Acerca de esta tarea

Se crean volúmenes desde los pools o los grupos de volúmenes. El cuadro de diálogo Añadir/editar volúmenes muestra todos los pools y grupos de volúmenes elegibles de la cabina de almacenamiento. Para cada pool o grupo de volúmenes elegible, se muestran la cantidad de unidades y la capacidad libre total disponibles.

Para algunas cargas de trabajo específicas de la aplicación, cada pool o grupo de volúmenes elegible muestra la capacidad propuesta según la configuración de volumen sugerido y muestra también la capacidad libre restante en GIB. Para otras cargas de trabajo, la capacidad propuesta aparece a medida que se añaden volúmenes a un pool o un grupo de volúmenes y se especifica la cantidad informada.

Pasos

1. Elija una de estas acciones según si seleccionó otra carga de trabajo específica de la aplicación o la siguiente:
    - **Otros** — haga clic en **Añadir nuevo volumen** en cada pool o grupo de volúmenes que desee utilizar para crear uno o más volúmenes.

Detalles del campo

Campo	Descripción
Nombre del volumen	System Manager asigna un nombre predeterminado a un volumen durante la secuencia de creación de volúmenes. Se puede aceptar el nombre predeterminado o se puede proporcionar un nombre más descriptivo que indique el tipo de datos almacenados en el volumen.
Capacidad notificada	Defina la capacidad del volumen nuevo y las unidades de capacidad que desea usar (MIB, GIB o TIB). Para los volúmenes gruesos, la capacidad mínima es 1 MIB y la capacidad máxima se determina mediante la cantidad y la capacidad de las unidades del pool o del grupo de volúmenes. Recuerde que la capacidad de almacenamiento también es necesaria para los servicios de copia (imágenes Snapshot, volúmenes Snapshot, copias de volúmenes y reflejos remotos), por lo tanto, no asigne toda la capacidad a los volúmenes estándar. La capacidad de un pool se asigna en incrementos de 4 GIB o 8 GIB, según el tipo de unidad. Se asigna cualquier capacidad que no sea múltiplo de 4 o 8 GIB, pero no se puede usar. Para asegurarse de que toda la capacidad se pueda usar, especifique la capacidad en incrementos de 4 GIB o 8 GIB. Si hubiese capacidad que no puede usar, la única manera de recuperarla es aumentar la capacidad del volumen.
Tamaño de bloque de volumen (solo EF300 y EF600)	Muestra los tamaños de bloque que se pueden crear para el volumen: • 512 — 512 bytes • 4K — 4,096 bytes

Campo	Descripción
Tamaño del segmento	Muestra la configuración del ajuste de tamaño de segmentos, que solo aparece para los volúmenes de un grupo de volúmenes. Se puede cambiar el tamaño del segmento para optimizar el rendimiento. **Transiciones de tamaño de segmento permitidas** — System Manager determina las transiciones de tamaño de segmento permitidas. Los tamaños de segmento que no son transiciones adecuadas para el tamaño de segmento actual no están disponibles en la lista desplegable. Las transiciones permitidas, por lo general, son el doble o la mitad del tamaño de segmento actual. Por ejemplo, si el tamaño de segmento del volumen actual es 32 KiB, se permite un tamaño de segmento de volumen nuevo de 16 KiB o 64 KiB. **Volúmenes con caché SSD** habilitada — se puede especificar un tamaño de segmento de 4 KiB para volúmenes con caché SSD habilitada. Asegúrese de seleccionar el tamaño de segmento 4 KiB solo para los volúmenes con la función SSD Cache habilitada que controlan operaciones de I/o en bloques pequeños (por ejemplo, tamaños de bloques de I/o de 16 KiB o menos). El rendimiento podría verse afectado si selecciona 4 KiB para el tamaño de segmento en los volúmenes con la función SSD Cache habilitada que controlan operaciones secuenciales de bloques grandes. **Cantidad de tiempo para cambiar el tamaño del segmento** — la cantidad de tiempo para cambiar el tamaño del segmento de un volumen depende de estas variables: • La carga de I/o desde el host • La prioridad de modificación del volumen • La cantidad de unidades del grupo de volúmenes • La cantidad de canales de unidades • La potencia de procesamiento de las controladoras de la cabina de almacenamiento Si cambia el tamaño de segmento de un volumen, el rendimiento de I/o se ve afectado, pero los datos siguen disponibles.
Compatible con la función de seguridad	**Sí** aparece junto a "compatible con la función de seguridad" solo si las unidades del pool o grupo de volúmenes son compatibles con la función de seguridad. Drive Security evita el acceso no autorizado a los datos de una unidad que se quita físicamente de la cabina de almacenamiento. Esta opción solo está disponible si la función Drive Security está habilitada y hay una clave de seguridad configurada para la cabina de almacenamiento. Un pool o un grupo de volúmenes pueden contener tanto una unidad compatible con la función de seguridad como una que no lo sea, pero todas las unidades deben ser compatibles con la función de seguridad para usar la funcionalidad de cifrado.

Campo	Descripción
DA	**Sí** aparece junto a "DA" solo si las unidades del pool o grupo de volúmenes admiten Data Assurance (DA). DA mejora la integridad de los datos en todo el sistema de almacenamiento. DA permite que la cabina de almacenamiento compruebe y corrija los errores que se pueden producir durante la transferencia de datos a través de las controladoras hasta las unidades. El uso DE DA en el volumen nuevo garantiza la detección de cualquier error.
Recurso aprovisionado (solo EF300 y EF600)	**Sí** aparece junto a "recurso aprovisionado" sólo si las unidades admiten esta opción. El aprovisionamiento de recursos es una función disponible en las cabinas de almacenamiento EF300 y EF600, lo que permite poner en uso los volúmenes de inmediato sin proceso de inicialización en segundo plano.

- **Carga de trabajo específica de la aplicación** — haga clic en **Siguiente** para aceptar los volúmenes y las características recomendados por el sistema para la carga de trabajo seleccionada, o haga clic en **Editar volúmenes** para cambiar, añadir o eliminar los volúmenes y las características recomendados por el sistema para la carga de trabajo seleccionada.

Detalles del campo

Campo	Descripción
Nombre del volumen	System Manager asigna un nombre predeterminado a un volumen durante la secuencia de creación de volúmenes. Se puede aceptar el nombre predeterminado o se puede proporcionar un nombre más descriptivo que indique el tipo de datos almacenados en el volumen.
Capacidad notificada	Defina la capacidad del volumen nuevo y las unidades de capacidad que desea usar (MIB, GIB o TIB). Para los volúmenes gruesos, la capacidad mínima es 1 MIB y la capacidad máxima se determina mediante la cantidad y la capacidad de las unidades del pool o del grupo de volúmenes. Recuerde que la capacidad de almacenamiento también es necesaria para los servicios de copia (imágenes Snapshot, volúmenes Snapshot, copias de volúmenes y reflejos remotos), por lo tanto, no asigne toda la capacidad a los volúmenes estándar. La capacidad de un pool se asigna en incrementos de 4 GIB o 8 GIB, según el tipo de unidad. Se asigna cualquier capacidad que no sea múltiplo de 4 o 8 GIB, pero no se puede usar. Para asegurarse de que toda la capacidad se pueda usar, especifique la capacidad en incrementos de 4 GIB o 8 GIB. Si hubiese capacidad que no puede usar, la única manera de recuperarla es aumentar la capacidad del volumen.
Tipo de volumen	Tipo de volumen indica el tipo de volumen que se creó para una carga de trabajo específica de la aplicación.
Tamaño de bloque de volumen (solo EF300 y EF600)	Muestra los tamaños de bloque que se pueden crear para el volumen: • 512 — 512 bytes • 4K — 4,096 bytes

Campo	Descripción
Tamaño del segmento	Muestra la configuración del ajuste de tamaño de segmentos, que solo aparece para los volúmenes de un grupo de volúmenes. Se puede cambiar el tamaño del segmento para optimizar el rendimiento. **Transiciones de tamaño de segmento permitidas** — System Manager determina las transiciones de tamaño de segmento permitidas. Los tamaños de segmento que no son transiciones adecuadas para el tamaño de segmento actual no están disponibles en la lista desplegable. Las transiciones permitidas, por lo general, son el doble o la mitad del tamaño de segmento actual. Por ejemplo, si el tamaño de segmento del volumen actual es 32 KiB, se permite un tamaño de segmento de volumen nuevo de 16 KiB o 64 KiB. **Volúmenes con caché SSD** habilitada — se puede especificar un tamaño de segmento de 4 KiB para volúmenes con caché SSD habilitada. Asegúrese de seleccionar el tamaño de segmento 4 KiB solo para los volúmenes con la función SSD Cache habilitada que controlan operaciones de I/o en bloques pequeños (por ejemplo, tamaños de bloques de I/o de 16 KiB o menos). El rendimiento podría verse afectado si selecciona 4 KiB para el tamaño de segmento en los volúmenes con la función SSD Cache habilitada que controlan operaciones secuenciales de bloques grandes. **Cantidad de tiempo para cambiar el tamaño del segmento** — la cantidad de tiempo para cambiar el tamaño del segmento de un volumen depende de estas variables: • La carga de I/o desde el host • La prioridad de modificación del volumen • La cantidad de unidades del grupo de volúmenes • La cantidad de canales de unidades • La potencia de procesamiento de las controladoras de la cabina de almacenamiento cuando se cambia el tamaño de segmento de un volumen, el rendimiento de I/o se ve afectado, pero los datos siguen disponibles.

Campo	Descripción
Compatible con la función de seguridad	**Sí** aparece junto a "compatible con la función de seguridad" solo si las unidades del pool o grupo de volúmenes son compatibles con la función de seguridad. Drive Security evita el acceso no autorizado a los datos de una unidad que se quita físicamente de la cabina de almacenamiento. Esta opción solo está disponible si la función Drive Security está habilitada y hay una clave de seguridad configurada para la cabina de almacenamiento. Un pool o un grupo de volúmenes pueden contener tanto una unidad compatible con la función de seguridad como una que no lo sea, pero todas las unidades deben ser compatibles con la función de seguridad para usar la funcionalidad de cifrado.
DA	**Sí** aparece junto a "DA" solo si las unidades del pool o grupo de volúmenes admiten Data Assurance (DA). DA mejora la integridad de los datos en todo el sistema de almacenamiento. DA permite que la cabina de almacenamiento compruebe y corrija los errores que se pueden producir durante la transferencia de datos a través de las controladoras hasta las unidades. El uso DE DA en el volumen nuevo garantiza la detección de cualquier error.
Recurso aprovisionado (solo EF300 y EF600)	**Sí** aparece junto a "recurso aprovisionado" sólo si las unidades admiten esta opción. El aprovisionamiento de recursos es una función disponible en las cabinas de almacenamiento EF300 y EF600, lo que permite poner en uso los volúmenes de inmediato sin proceso de inicialización en segundo plano.

2. Para continuar la secuencia de creación de volúmenes para la aplicación seleccionada, haga clic en **Siguiente** y vaya a. Paso 4: Revisar la configuración de volumen.

Paso 4: Revisar la configuración de volumen

Revise un resumen de los volúmenes que pretende crear y realizar los cambios necesarios.

Pasos

1. Revise los volúmenes que desea crear. Haga clic en **Atrás** para realizar cualquier cambio.

2. Cuando esté satisfecho con la configuración del volumen, haga clic en **Finalizar**.

Resultados

System Manager crea los volúmenes nuevos en los pools y grupos de volúmenes seleccionados y, a continuación, muestra los volúmenes nuevos en la tabla todos los volúmenes.

Después de terminar

- Realice cualquier modificación necesaria del sistema operativo en el host de la aplicación para que las aplicaciones puedan usar el volumen.
- Ejecute cualquiera de los basados en host `hot_add` utilidad o utilidad específica del sistema operativo (disponible de otro proveedor) y, a continuación, ejecute la `SMdevices` utilidad para correlacionar los nombres de los volúmenes con los nombres de las cabinas de almacenamiento del host.

  La `hot_add` utilidad y la `SMdevices` la utilidad se incluye como parte de la `SMutils` paquete. La `SMutils` el paquete es una recogida de utilidades para verificar lo que el host puede ver en la cabina de almacenamiento. Se incluye como parte de la instalación del software SANtricity.

Añadir volúmenes a la carga de trabajo

Es posible añadir uno o más volúmenes a una carga de trabajo nueva o ya existente, en el caso de volúmenes que actualmente no estén asociados con una carga de trabajo.

Acerca de esta tarea

Los volúmenes no se asocian a una carga de trabajo si se los creó mediante la interfaz de línea de comandos (CLI) o si se migraron (importaron/exportaron) desde una cabina de almacenamiento diferente.

Pasos

1. Seleccione MENU:Storage[Volumes].
2. Seleccione la ficha **aplicaciones y cargas de trabajo**.

   Se muestra la vista aplicaciones y cargas de trabajo.

3. Seleccione **Agregar a carga de trabajo**.

   Se muestra el cuadro de diálogo Seleccionar carga de trabajo.

4. Realice una de las siguientes acciones:
   - **Añadir volúmenes a una carga de trabajo existente** — Seleccione esta opción para agregar volúmenes a una carga de trabajo existente.

     Use el menú desplegable para seleccionar una carga de trabajo. El tipo de aplicación asociada a la carga de trabajo se asigna a los volúmenes que se añaden a esta carga de trabajo.

   - **Añadir volúmenes a una nueva carga de trabajo** — Seleccione esta opción para definir una nueva carga de trabajo para un tipo de aplicación y agregar volúmenes a la nueva carga de trabajo.
5. Seleccione **Siguiente** para continuar con la secuencia de añadir a carga de trabajo.

   Se muestra el cuadro de diálogo Seleccionar volúmenes.

6. Seleccione los volúmenes que desea añadir a la carga de trabajo.

7. Revise los volúmenes que desea añadir a la carga de trabajo seleccionada.
8. Cuando esté satisfecho con la configuración de su carga de trabajo, haga clic en **Finalizar**.

Gestione los volúmenes

Aumente la capacidad de un volumen

Es posible aumentar la capacidad notificada (a los hosts) de un volumen con la capacidad libre que está disponible en el pool o el grupo de volúmenes.

Antes de empezar

- Existe capacidad libre suficiente disponible en el pool o el grupo de volúmenes asociado.
- El volumen es óptimo y no está en ningún estado de modificación.
- No se alcanzó la capacidad notificada máxima de 256 TIB para volúmenes finos.
- No existen unidades de repuesto en uso en el volumen. (Esto se aplica solo a volúmenes que pertenecen a grupos de volúmenes.)

Acerca de esta tarea

Tenga en cuenta todos los requisitos de capacidad futuros que puede tener para otros volúmenes en este pool o grupo de volúmenes. Asegúrese de tener suficiente capacidad libre para crear imágenes Snapshot, volúmenes Snapshot o reflejos remotos.

> Solo ciertos sistemas operativos permiten aumentar la capacidad de un volumen. Si aumenta la capacidad de un volumen en un sistema operativo que no lo permite, la capacidad ampliada será inutilizable y no se podrá restaurar la capacidad de volumen original.

Pasos

1. Seleccione MENU:Storage[Volumes].
2. Seleccione el volumen para el que desea aumentar la capacidad y, a continuación, seleccione **aumentar capacidad**.

   Se muestra el cuadro de diálogo Confirmar aumento de capacidad.

3. Seleccione **Sí** para continuar.

   Se muestra el cuadro de diálogo aumentar capacidad notificada.

   En este cuadro de diálogo, se muestran la capacidad notificada actual y la capacidad libre disponibles en el pool o el grupo de volúmenes asociado.

4. Utilice el cuadro **aumentar capacidad notificada agregando…** para añadir capacidad a la capacidad informada disponible actual. Es posible cambiar el valor de capacidad para que se muestre en mebibytes (MIB), gibibytes (GIB) o tebibytes (TIB).
5. Haga clic en **aumentar**.

Resultados

- System Manager aumenta la capacidad del volumen según lo seleccionado.
- Seleccione MENU:Inicio[Ver operaciones en curso] para ver el progreso de la operación de aumento de capacidad que está en ejecución actualmente para el volumen seleccionado. Es posible que esta

operación demore y que afecte el rendimiento del sistema.

Después de terminar

Después de expandir la capacidad del volumen, debe aumentar manualmente el tamaño del sistema de archivos para que coincidan. La forma de hacerlo depende del sistema de archivos utilizado. Para obtener detalles, compruebe la documentación del sistema operativo del host.

Inicializar volúmenes

Un volumen se inicializa automáticamente cuando se crea por primera vez. Sin embargo, es posible que Recovery Guru recomiende inicializar manualmente un volumen para la recuperación de ciertas condiciones de fallo. Use esta opción solo bajo la supervisión del soporte técnico. Es posible seleccionar uno o varios volúmenes para su inicialización.

Antes de empezar

- Todas las operaciones de I/o se detuvieron.
- Todos los dispositivos o sistemas de archivos en los volúmenes que se desean inicializar están desmontados.
- El volumen está en estado óptima y no hay operaciones de modificación en curso en el volumen.

> No se puede cancelar la operación una vez iniciada. Se borran todos los datos del volumen. No intente esta operación a menos que Recovery Guru le recomiende hacerlo. Antes de iniciar este procedimiento, póngase en contacto con el soporte técnico.

Acerca de esta tarea

Cuando se inicializa un volumen, este conserva su configuración de WWN, asignaciones de hosts, capacidad asignada y capacidad reservada. También conserva la misma configuración de Data Assurance (DA) y de seguridad.

Los siguientes tipos de volúmenes _no se pueden inicializar:

- Volumen base de un volumen Snapshot
- Volumen primario en una relación de reflejo
- Volumen secundario en una relación de reflejo
- Volumen de origen en una copia de volumen
- Volumen objetivo en una copia de volumen
- Volumen que ya posee una inicialización en curso

Este tema se aplica solo a volúmenes estándar creados a partir de pools o grupos de volúmenes.

Pasos

1. Seleccione MENU:Storage[Volumes].
2. Seleccione cualquier volumen y, a continuación, seleccione MENU:más[inicializar volúmenes].

   Se muestra el cuadro de diálogo inicializar volúmenes. Todos los volúmenes en la cabina de almacenamiento aparecen en este cuadro de diálogo.

3. Seleccione uno o varios volúmenes para inicializar y confirme que desea realizar la operación.

Resultados

System Manager realiza lo siguiente:

- Borra todos los datos de los volúmenes que se inicializaron.
- Borra los índices de bloque, lo que provoca que los bloques no escritos se lean como si estuvieran llenos de ceros (el volumen aparecerá como completamente vacío).

Seleccione MENU:Inicio[Ver operaciones en curso] para ver el progreso de la operación de inicialización que está en ejecución actualmente para el volumen seleccionado. Es posible que esta operación demore y que afecte el rendimiento del sistema.

Redistribuir volúmenes

Es posible redistribuir volúmenes para moverlos nuevamente a sus propietarios de controladoras preferidos. Por lo general, los controladores multivía mueven volúmenes de su propietario de controladora preferido cuando se produce un problema en la ruta de datos entre el host y la cabina de almacenamiento.

Antes de empezar

- Los volúmenes que desea redistribuir no están en uso o se producirán errores de I/O.
- Se ha instalado un controlador multivía en todos los hosts que utilizan los volúmenes. De lo contrario, se producirán errores de I/O.

  Si se desea redistribuir volúmenes sin un controlador multivía en los hosts, es necesario detener toda la actividad de I/o en los volúmenes *mientras se realiza la operación de redistribución en curso* para evitar errores en las aplicaciones.

Acerca de esta tarea

La mayoría de los controladores multivía intentan acceder a cada volumen en una ruta a su propietario de controladora preferido. Sin embargo, si esta ruta preferida no está disponible, el controlador multivía en el host conmuta al nodo de respaldo a una ruta alternativa. Esta conmutación al nodo de respaldo puede provocar que la propiedad del volumen cambie a la controladora alternativa. Después de resolver la condición que provocó la conmutación al nodo de respaldo, es posible que algunos hosts muevan automáticamente la propiedad del volumen nuevamente al propietario de la controladora preferido; sin embargo, en algunos casos es posible que deba redistribuir manualmente los volúmenes.

Pasos

1. Seleccione MENU:Storage[Volumes].
2. Seleccione MENU:More[redistribuir volúmenes].

   Se muestra el cuadro de diálogo redistribuir volúmenes. Todos los volúmenes de la cabina de almacenamiento con un propietario de controladora preferido que no coincida con el propietario actual se mostrarán en este cuadro de diálogo.

3. Seleccione el o los volúmenes que desea redistribuir y confirme que desea ejecutar la operación.

Resultados

System Manager moverá los volúmenes seleccionados a sus propietarios de controladora preferidos o se mostrará el cuadro de diálogo no es necesario redistribuir volúmenes.

Cambiar propiedad de la controladora de un volumen

Es posible cambiar la propiedad de la controladora preferida de un volumen, para que las operaciones de I/o de las aplicaciones host se redirijan por la ruta nueva.

Antes de empezar

Si no se utiliza un controlador multivía, se deben cerrar todas las aplicaciones host que actualmente utilizan el volumen. Esta acción previene errores de las aplicaciones cuando se realizan cambios de ruta de I/O.

Acerca de esta tarea

Es posible cambiar la propiedad de la controladora de uno o más volúmenes en un pool o grupo de volúmenes.

Pasos

1. Seleccione MENU:Storage[Volumes].
2. Seleccione cualquier volumen y, a continuación, seleccione MENU:more[Cambiar propiedad].

   Se muestra el cuadro de diálogo Cambiar propiedad del volumen. Todos los volúmenes en la cabina de almacenamiento aparecen en este cuadro de diálogo.

3. Utilice la lista desplegable **propietario preferido** para cambiar el controlador preferido para cada volumen que desee cambiar y confirme que desea realizar la operación.

Resultados

- System Manager cambia la propiedad de la controladora del volumen. Las operaciones de I/o del volumen ahora se redirigen por esta ruta de I/O.
- Es posible que el volumen no utilice la ruta de I/o nueva hasta que se vuelva a configurar el controlador multivía para que reconozca la ruta nueva. Por lo general, esta acción tarda menos de cinco minutos.

Elimine el volumen

Por lo general, debe eliminar volúmenes si se crearon con los parámetros o la capacidad equivocados, ya no satisfacen las necesidades de configuración del almacenamiento o son imágenes Snapshot que ya no se necesitan para backup o prueba de aplicaciones.

Al eliminar un volumen, aumenta la capacidad libre en el pool o el grupo de volúmenes. Puede seleccionar uno o varios volúmenes para eliminarlos.

Antes de empezar

Asegúrese de que se cumplan las siguientes condiciones en los volúmenes que desea eliminar:

- Existen backups de todos los datos.
- Todas las entradas y las salidas (I/o) están detenidas.
- Todos los dispositivos y los sistemas de archivos están desmontados.

Acerca de esta tarea

No es posible eliminar un volumen que tenga una de las siguientes condiciones:

- El volumen se está inicializando.
- El volumen se está reconstruyendo.

- El volumen forma parte de un grupo de volúmenes que contiene una unidad que está realizando una operación de copyback.
- El volumen está sometido a una operación de modificación, como un cambio de tamaño de segmento, a menos que el volumen esté ahora en estado con errores.
- El volumen mantiene cualquier tipo de reserva persistente.
- El volumen es un volumen de origen o un volumen objetivo en una operación Copiar volumen con estado Pending, In Progress o con errores.

Al eliminar un volumen, se produce la pérdida de todos los datos en estos volúmenes.

Cuando un volumen supera un tamaño determinado (actualmente 128 TB), la eliminación se lleva a cabo en segundo plano y es posible que el espacio liberado no esté disponible inmediatamente.

Pasos

1. Seleccione MENU:Storage[Volumes].
2. Haga clic en **Eliminar**.

   Se muestra el cuadro de diálogo Eliminar volúmenes.

3. Seleccione uno o varios volúmenes para eliminar y confirme que desea realizar la operación.
4. Haga clic en **Eliminar**.

Resultados

System Manager realiza lo siguiente:

- Elimina todas las imágenes Snapshot, las programaciones y las Snapshot asociadas.
- Elimina todas las relaciones de mirroring.
- Aumenta la capacidad libre en el pool o el grupo de volúmenes.

Cambiar el límite de capacidad asignada para un volumen fino

En el caso de los volúmenes finos con capacidad para asignar espacio bajo demanda, se puede cambiar el límite que restringe la capacidad asignada a la que un volumen fino se puede expandir automáticamente.

También se puede modificar el porcentaje en el que se envía una alerta (umbral de advertencia superado) al área Notificaciones de la página Inicio cuando un volumen fino está cerca del límite de capacidad asignado. Se puede habilitar o deshabilitar esta notificación de alerta.

Esta función no está disponible en los sistemas de almacenamiento EF600 o EF300.

El sistema expande automáticamente la capacidad asignada de acuerdo con el límite de capacidad establecido. El límite de capacidad establecido permite limitar el crecimiento automático del volumen fino por debajo de la capacidad notificada. Cuando la cantidad de datos escritos se acerca a la capacidad asignada, es posible cambiar el límite de capacidad establecido.

Cuando se modifican el límite de capacidad asignada y el umbral de advertencia de un volumen fino, se debe tener en cuenta el espacio que consumirán los datos de usuario del volumen y los datos de los servicios de

copia.

Pasos

1. Seleccione MENU:Storage[Volumes].
2. Seleccione la ficha **Supervisión de volumen fino**.

   Se muestra la vista Supervisión de volumen fino.

3. Seleccione el volumen fino que desea cambiar y, a continuación, seleccione **Cambiar límite**.

   Se muestra el cuadro de diálogo Cambiar límite. La configuración del límite de capacidad asignada y el umbral de advertencia del volumen fino seleccionado aparecen en este cuadro de diálogo.

4. Modifique el límite de capacidad asignada y el umbral de advertencia según sea necesario.

   Detalles del campo

Ajuste	Descripción
Cambiar límite de capacidad asignada a…	El umbral en el que no es posible completar la operación de escritura y no se permite que el volumen fino consuma recursos adicionales. Este umbral es un porcentaje de la capacidad notificada del volumen.
Enviarme una alerta cuando… (umbral de advertencia)	Marque la casilla de comprobación si desea que el sistema genere una alerta cuando haya un volumen fino cerca del límite de capacidad asignada. La alerta se envía al área Notificaciones de la página Inicio. Este umbral es un porcentaje de la capacidad notificada del volumen. Si desea deshabilitar la notificación de alerta de umbral de advertencia, desmarque la casilla de comprobación.

5. Haga clic en **Guardar**.

Gestionar configuración

Cambiar la configuración de un volumen

Es posible cambiar la configuración de un volumen, como el nombre, la asignación de host, el tamaño de segmento, la prioridad de modificación, el almacenamiento en caché y así sucesivamente.

Antes de empezar

El volumen que desea cambiar debe estar en estado óptimo.

> Es posible que algunas operaciones no estén disponibles mientras haya cambios en la configuración del volumen en curso

Pasos

1. Seleccione MENU:Storage[Volumes].

2. Seleccione el volumen que desea cambiar y, a continuación, seleccione **Ver/editar configuración**.

   Se muestra el cuadro de diálogo Configuración de volumen. La configuración del volumen seleccionado aparece en este cuadro de diálogo.

3. Seleccione la ficha **básico** para cambiar el nombre del volumen y la asignación de host.

Detalles del campo

Ajuste	Descripción
Nombre	Muestra el nombre del volumen. Cambie el nombre de un volumen cuando el actual ya no sea significativo o no corresponda.
Capacidades	Muestra la capacidad notificada y asignada del volumen seleccionado. La capacidad notificada y la capacidad asignada son iguales en los volúmenes gruesos, pero son diferentes en los volúmenes finos. En el caso de un volumen grueso, el espacio físicamente asignado es igual al espacio que se informa en el host. En un volumen fino, la capacidad notificada es la capacidad que se notifica a los hosts, mientras que la capacidad asignada es la cantidad de espacio de la unidad asignado para la escritura de datos.
Pool / grupo de volúmenes	Muestra el nombre y nivel de RAID del pool o grupo de volúmenes. Indica si el pool o grupo de volúmenes es compatible con la función de seguridad y si está habilitada.
Host	Muestra la asignación del volumen. Es posible asignar un volumen a un host o clúster de hosts para poder acceder a él como parte de operaciones de I/O. Esta asignación otorga acceso a un host o un clúster de hosts a un volumen determinado o a una cantidad de volúmenes en una cabina de almacenamiento. • **Asignado a** — identifica el host o clúster de hosts que tiene acceso al volumen seleccionado. • **LUN** — un número de unidad lógica (LUN) es el número asignado al espacio de dirección que un host utiliza para acceder a un volumen. El volumen se presenta al host como capacidad en forma de LUN. Cada host tiene su propio espacio de dirección de LUN. Por lo tanto, distintos hosts pueden utilizar el mismo LUN para acceder a diferentes volúmenes. En las interfaces NVMe, esta columna muestra Namespace ID. Un espacio de nombres es almacenamiento NVM que se formateó para el acceso en bloque. Es análogo a una unidad lógica en SCSI, que se relaciona con un volumen en la cabina de almacenamiento. El ID del espacio de nombres es el identificador único de la controladora NVMe para el espacio de nombres y se puede configurar con un valor entre 1 y 255. Es análogo a un número de unidad lógica (LUN) en SCSI.

Ajuste	Descripción
Identificadores	Muestra los identificadores del volumen seleccionado. • **Identificador mundial (WWID)** — un identificador hexadecimal único para el volumen. • **Identificador único extendido (EUI)** — un identificador EUI-64 del volumen. • **Identificador del subsistema (SSID)** — el identificador del subsistema de la matriz de almacenamiento de un volumen.

4. Seleccione la ficha **Avanzado** para cambiar los ajustes de configuración adicionales de un volumen de un pool o de un grupo de volúmenes.

Detalles del campo

Ajuste	Descripción
Información de carga de trabajo y aplicación	Durante la creación del volumen, es posible generar cargas de trabajo específicas de la aplicación u otras cargas de trabajo. Si corresponde, aparece el nombre de la carga de trabajo, el tipo de aplicación y el tipo de volumen del volumen seleccionado. Es posible cambiar el nombre de la carga de trabajo, si así lo desea.
Configuración de calidad de servicio	**Deshabilitar permanentemente la garantía de datos** — esta configuración aparece sólo si el volumen está habilitado para la garantía de datos (DA). DA comprueba y corrige los errores que se pueden producir durante la transferencia de datos a través de las controladoras hasta las unidades. Utilice esta opción para deshabilitar permanentemente LA función DA en el volumen seleccionado. Una vez deshabilitada, LA función DA no puede volver a habilitarse en este volumen. **Activar comprobación de redundancia de lectura previa** — esta configuración aparece sólo si el volumen es un volumen grueso. Las comprobaciones de redundancia de lectura previa determinan si los datos de un volumen son consistentes cada vez que se realiza una lectura. Un volumen con esta función habilitada devuelve errores de lectura si el firmware de la controladora determina que los datos no son consistentes.
Propiedad de la controladora	Define la controladora designada como la controladora propietaria, o primaria, del volumen. La propiedad de la controladora es sumamente importante y debe planificarse con cuidado. Las controladoras deben equilibrarse lo más posible en cuanto a las operaciones de I/o totales.

Ajuste	Descripción
Ajuste de tamaño del segmento	Muestra la configuración de ajuste de tamaño, que solo aparece para los volúmenes de un grupo de volúmenes. Se puede cambiar el tamaño del segmento para optimizar el rendimiento. **Transiciones de tamaño de segmento permitidas** — System Manager determina las transiciones de tamaño de segmento permitidas. Los tamaños de segmento que no son transiciones adecuadas para el tamaño de segmento actual no están disponibles en la lista desplegable. Las transiciones permitidas, por lo general, son el doble o la mitad del tamaño de segmento actual. Por ejemplo, si el tamaño de segmento del volumen actual es 32 KiB, se permite un tamaño de segmento de volumen nuevo de 16 KiB o 64 KiB. **Volúmenes con caché SSD** habilitada — se puede especificar un tamaño de segmento de 4 KiB para volúmenes con caché SSD habilitada. Asegúrese de seleccionar el tamaño de segmento 4 KiB solo para los volúmenes con la función SSD Cache habilitada que controlan operaciones de I/o en bloques pequeños (por ejemplo, tamaños de bloques de I/o de 16 KiB o menos). El rendimiento podría verse afectado si selecciona 4 KiB para el tamaño de segmento en los volúmenes con la función SSD Cache habilitada que controlan operaciones secuenciales de bloques grandes. **Cantidad de tiempo para cambiar el tamaño del segmento** — la cantidad de tiempo para cambiar el tamaño del segmento de un volumen depende de estas variables: • La carga de I/o desde el host • La prioridad de modificación del volumen • La cantidad de unidades del grupo de volúmenes • La cantidad de canales de unidades • La potencia de procesamiento de las controladoras de la cabina de almacenamiento cuando se cambia el tamaño de segmento de un volumen, el rendimiento de I/o se ve afectado, pero los datos siguen disponibles.

Ajuste	Descripción
Prioridad de modificación	Muestra la configuración de prioridad de modificación, que solo aparece para los volúmenes en un grupo de volúmenes. La prioridad de modificación define la cantidad de tiempo de procesamiento que se asigna a las operaciones de modificación del volumen en relación con el rendimiento del sistema. Es posible aumentar la prioridad de modificación del volumen, pero esto puede afectar al rendimiento del sistema. Mueva las barras del control deslizante para seleccionar un nivel de prioridad. **Tasas de prioridad de modificación** — la tasa de prioridad más baja beneficia el rendimiento del sistema, pero la operación de modificación lleva más tiempo. La tasa de prioridad más alta beneficia a la operación de modificación, pero el rendimiento del sistema puede verse afectado.
Almacenamiento en caché	Muestra la configuración de almacenamiento en caché, que se puede modificar para afectar el rendimiento de I/o general de un volumen.
Caché SSD	Muestra la configuración de caché SSD, que se puede habilitar en volúmenes compatibles a fin de mejorar el rendimiento de solo lectura. Los volúmenes son compatibles si comparten las mismas capacidades Drive Security y Garantía de datos. **La función SSD Cache utiliza uno o varios discos de estado sólido (SSD) para implementar una memoria caché de lectura**. Se mejora el rendimiento de la aplicación gracias a los tiempos de lectura más rápidos de SSD. Debido a que la caché de lectura se encuentra en la cabina de almacenamiento, todas las aplicaciones que utilizan la cabina de almacenamiento comparten el almacenamiento en caché. Simplemente, seleccione el volumen que desea almacenar en caché y se realizará de forma automática y dinámica.

5. Haga clic en **Guardar**.

   System Manager cambia la configuración del volumen según sus preferencias.

Después de terminar

Seleccione MENU:Inicio[Ver operaciones en curso] para ver el progreso de las operaciones de cambio que se están ejecutando actualmente para el volumen seleccionado.

Cambiar configuración de carga de trabajo

Es posible cambiar el nombre de una carga de trabajo y ver el tipo de aplicación asociada a esta. Cambie el nombre de una carga de trabajo cuando el nombre actual ya no tiene sentido o no corresponde.

Pasos

1. Seleccione MENU:Storage[Volumes].
2. Seleccione la ficha **aplicaciones y cargas de trabajo**.

   Se muestra la vista aplicaciones y cargas de trabajo.

3. Seleccione la carga de trabajo que desea cambiar y, a continuación, seleccione **Ver/editar configuración**.

   Se muestra el cuadro de diálogo Configuración de aplicaciones y cargas de trabajo.

4. **Opcional:** cambie el nombre de la carga de trabajo proporcionado por el usuario.
5. Haga clic en **Guardar**.

Cambiar la configuración de caché de un volumen

Es posible modificar la configuración de la caché de lectura y la caché de escritura para afectar el rendimiento de I/o general de un volumen.

Acerca de esta tarea

Tenga en cuenta estas directrices al cambiar la configuración de caché de un volumen:

- Al abrir el cuadro de diálogo Cambiar configuración de caché, es posible que se muestre un icono junto a las propiedades de caché seleccionadas. Este icono indica que la controladora ha suspendido temporalmente las operaciones de almacenamiento en caché.

  Esta acción puede ser tomada cuando se carga una nueva batería, se elimina una controladora o la controladora detecta que los tamaños de caché no coinciden. Una vez despejada la condición, las propiedades de caché seleccionadas en el cuadro de diálogo se mostrarán activas. Si las propiedades de caché seleccionadas no se activan, póngase en contacto con el soporte técnico.

- Es posible cambiar la configuración de caché para un solo volumen o para varios volúmenes de una cabina de almacenamiento. Es posible cambiar la configuración de caché para todos los volúmenes estándar o todos los volúmenes finos al mismo tiempo.

Pasos

1. Seleccione MENU:Storage[Volumes].
2. Seleccione cualquier volumen y luego seleccione MENU:más[Cambiar configuración de caché].

   Se muestra el cuadro de diálogo Cambiar configuración de caché. Todos los volúmenes en la cabina de almacenamiento aparecen en este cuadro de diálogo.

3. Seleccione la ficha **básico** para cambiar la configuración del almacenamiento en caché de lectura y de escritura.

Detalles del campo

Configuración de caché	Descripción
Almacenamiento en caché de lectura	La caché de lectura es un búfer que almacena datos que se leyeron de las unidades. Es posible que los datos de una operación de lectura ya deban estar en la caché debido a una operación anterior, por lo tanto, no es necesario acceder a las unidades. Los datos se conservan en la caché de lectura hasta que esta se vacía.
Almacenamiento en caché de escritura	La caché de escritura es un búfer que almacena datos del host que todavía no se escribieron en las unidades. Los datos permanecen en la caché de escritura hasta que se escriben en las unidades. El almacenamiento en caché de escritura puede aumentar el rendimiento de I/O. La caché se vacía automáticamente después de que se deshabilita **almacenamiento en caché de escritura** para un volumen.

4. Seleccione la ficha **Avanzado** para cambiar la configuración avanzada de los volúmenes gruesos. La configuración avanzada de caché solo está disponible para volúmenes gruesos.

Detalles del campo

Configuración de caché	Descripción
Captura previa de caché de lectura dinámica	La captura previa de lectura de la caché dinámica permite a la controladora copiar otros bloques de datos secuenciales en la caché mientras lee bloques de datos de una unidad en la caché. Ese almacenamiento en caché aumenta la posibilidad de que se puedan cumplir futuras solicitudes de datos de la caché. La captura previa de lectura de la caché dinámica es importante para las aplicaciones multimedia que utilizan I/o secuencial La cantidad y la velocidad de las capturas previas de los datos en la caché se ajustan automáticamente según la velocidad y el tamaño de solicitud de las lecturas del host. El acceso aleatorio no provoca la captura previa de los datos en la caché. Esta función no se aplica cuando el almacenamiento en caché de lectura está deshabilitado. En el caso de volumen fino, la captura previa de la lectura de caché dinámica siempre está deshabilitada y no se puede modificar.
Almacenamiento en caché de escritura sin baterías	La configuración de almacenamiento en caché de escritura sin baterías permite que el almacenamiento en caché de escritura continúe incluso si las baterías faltan, fallan, están completamente descargadas o no están totalmente cargadas. Por lo general, no se recomienda elegir el almacenamiento en caché de escritura sin baterías porque se pueden perder los datos en caso de interrupción del suministro eléctrico. Comúnmente, la controladora desactiva en forma temporal el almacenamiento en caché de escritura hasta que se cargan las baterías o se reemplaza una batería con errores. **Posible pérdida de datos** — Si selecciona esta opción y no dispone de una fuente de alimentación universal de protección, podría perder datos. Además, puede perder datos si no tiene baterías de controlador y activa la opción **almacenamiento en caché de escritura sin baterías**. Esta configuración solo está disponible si se habilita el almacenamiento en caché de escritura. Esta configuración no está disponible para volúmenes finos.

Configuración de caché	Descripción
Almacenamiento en caché de escritura con mirroring	El almacenamiento en caché de escritura con mirroring se produce cuando los datos escritos en la memoria caché de una controladora también se escriben en la memoria caché de otra controladora. Por lo tanto, si una controladora falla, la otra puede completar todas las operaciones de escritura pendientes. El mirroring de la caché de escritura está disponible solo si el almacenamiento en caché de escritura está habilitado y existen dos controladoras. El almacenamiento en caché de escritura con mirroring es la configuración predeterminada cuando se crea un volumen. Esta configuración solo está disponible si se habilita el almacenamiento en caché de escritura. Esta configuración no está disponible para volúmenes finos.

5. Haga clic en **Guardar** para cambiar la configuración de la caché.

Cambiar la configuración de análisis de medios para un volumen

Un análisis de medios es una operación que se ejecuta en segundo plano, que analiza todos los datos e información de redundancia del volumen. Use esta opción para habilitar o deshabilitar la configuración del análisis de medios para un volumen o varios, o bien para cambiar la duración del análisis.

Antes de empezar

Se debe comprender lo siguiente:

- Los análisis de medios se ejecutan continuamente a una tasa constante sobre la base de la capacidad que se analizará y la duración del análisis. Una tarea que se ejecuta en segundo plano de mayor prioridad puede suspender temporalmente los análisis que se ejecutan en segundo plano (por ejemplo, una reconstrucción), pero se reanudan a la misma velocidad constante.
- Un volumen solo se analiza cuando está habilitada la opción de análisis de medios para la cabina de almacenamiento y para ese volumen. Si también se habilita la verificación de redundancia para ese volumen, la información de redundancia del volumen se verifica para ver si coincide con los datos, siempre y cuando el volumen tenga redundancia. El análisis de medios con verificación de redundancia está habilitado de forma predeterminada para cada volumen cuando se crea.
- Si se encuentra un error de medio irrecuperable durante el análisis, los datos se repararán usando la información de redundancia, si está disponible.

  Por ejemplo, la información de redundancia está disponible en volúmenes RAID 5 óptimos o en volúmenes RAID 6 que son óptimos o que solo tienen una sola unidad con fallos. Si el error irrecuperable no puede repararse mediante el uso de la información de redundancia, el bloque de datos se añade al registro de sectores ilegibles. Tanto los errores de medios que pueden corregirse como los que no pueden corregirse se informan en el registro de eventos.

  Si se encuentra una incoherencia entre los datos y la información de redundancia en la verificación de redundancia, se informa en el registro de eventos.

Acerca de esta tarea

En los análisis de medios, se detectan y reparan errores de medios en bloques de discos que las aplicaciones leen con poca frecuencia. Esto puede evitar la pérdida de datos en el caso de un fallo de unidad, ya que los datos para unidades con fallo se reconstruyen mediante el uso de la información de redundancia y datos de otras unidades del grupo de volúmenes o pool.

Es posible realizar las siguientes acciones:

- Habilite o deshabilite los análisis de medios en segundo plano para toda la cabina de almacenamiento
- Cambie la duración del análisis para toda la cabina de almacenamiento
- Habilite o deshabilite el análisis de medios para un volumen o más
- Habilite o deshabilite la verificación de redundancia para un volumen o más

Pasos

1. Seleccione MENU:Storage[Volumes].
2. Seleccione cualquier volumen y luego seleccione MENU:más[Cambiar configuración de análisis de medios].

   Se muestra el cuadro de diálogo Cambiar configuración de escaneo de medios de unidad. Todos los volúmenes en la cabina de almacenamiento aparecen en este cuadro de diálogo.

3. Para activar el escaneo de medios, seleccione la casilla de verificación **Escanear medios durante…**.

   La desactivación de la casilla de comprobación del análisis de medios suspende toda la configuración del análisis de medios.

4. Especifique el número de días durante los cuales desea que se ejecute el análisis de medios.
5. Seleccione la casilla de comprobación **escaneo de medios** para cada volumen donde desea realizar un análisis de medios.

   System Manager habilita la opción Comprobación de redundancia para cada volumen donde se desea realizar un análisis de medios. Si hay volúmenes individuales para los que no desea realizar una comprobación de redundancia, anule la selección de la casilla de verificación **Comprobación de redundancia**.

6. Haga clic en **Guardar**.

   System Manager aplica los cambios de los análisis de medios en segundo plano sobre la base de la selección.

Usar servicios de copia

Información general acerca de Copy Volume

La función Copy Volume permite crear una copia de un momento específico de un volumen. Para ello, se crean dos volúmenes independientes, el volumen de origen y el volumen objetivo en la misma cabina de almacenamiento.

Por medio de esta función se realiza una copia byte por byte del volumen de origen al volumen objetivo, que permite que los datos del volumen objetivo queden idénticos a los datos del volumen de origen.

Copiado de datos para aumentar el acceso

A medida que cambian los requisitos de almacenamiento de volúmenes, se puede usar la función Copy Volume para copiar datos de pools o grupos de volúmenes que utilizan unidades de menor capacidad a pools o grupos de volúmenes que utilizan unidades de mayor capacidad. Por ejemplo, se puede usar la función Copy Volume para lo siguiente:

- Transferir datos a unidades más grandes
- Cambiar a unidades con mayor tasa de transferencia de datos
- Cambiar a unidades que utilizan nuevas tecnologías para un mayor rendimiento
- Cambiar de un volumen fino a un volumen grueso

Cambiar de un volumen fino a un volumen grueso

Si se desea cambiar un volumen fino a un volumen grueso, se debe usar la operación Copy Volume para crear una copia del volumen fino. El objetivo de una operación Copy Volume siempre es obtener un volumen grueso.

System Manager no proporciona ninguna opción para crear volúmenes finos. Si se desea crear volúmenes finos, se debe usar la interfaz de línea de comandos (CLI).

Datos de respaldo

La función Copy Volume permite crear un backup de un volumen, ya que copia datos de un volumen a otro en la misma cabina de almacenamiento. Se puede usar el volumen objetivo como backup para el volumen de origen, para la prueba del sistema o para realizar un backup a otro dispositivo, como una unidad de cinta.

Restaurar los datos de un volumen Snapshot al volumen base

Si se necesitan restaurar datos en el volumen base desde su volumen Snapshot asociado, se puede usar la función Copy Volume para copiar datos del volumen Snapshot al volumen base. Se puede crear una copia del volumen de los datos del volumen Snapshot y, luego, copiar los datos al volumen base.

Volúmenes de origen y objetivo

En la siguiente tabla, se especifican los tipos de volúmenes que se pueden usar como volúmenes de origen y objetivo con la función Copy Volume.

Tipo de volumen	Volumen de origen de copia de volumen sin conexión	Volumen de origen de copia de volumen en línea	Volumen objetivo en línea y sin conexión
Volumen grueso de un pool	Sí	Sí	Sí
Volumen grueso de un grupo de volúmenes	Sí	Sí	Sí
Volumen fino	Sí 1	Sí	No
Volumen Snapshot	Sí 2	No	No

Tipo de volumen	Volumen de origen de copia de volumen sin conexión	Volumen de origen de copia de volumen en línea	Volumen objetivo en línea y sin conexión
Volumen base Snapshot	Sí	No	No
Volumen primario de reflejos remoto	Sí[3]	No	Sí

[1] El volumen objetivo debe tener una capacidad igual o superior a la Capacidad notificada de un volumen fino.

[2] No se puede usar la copia del volumen Snapshot hasta que finalice la operación de copia en línea.

[3] Si el volumen de origen es un volumen primario, la capacidad del volumen objetivo debe ser igual o mayor que la capacidad utilizable del volumen de origen.

Tipos de operaciones de copia de volumen

Es posible ejecutar una operación de copia de volumen *sin conexión* o una operación *online* Copy Volume. Las operaciones sin conexión leen datos de un volumen de origen y los copian en un volumen objetivo. Las operaciones en línea usan un volumen Snapshot como origen y copian sus datos en un volumen objetivo.

Para garantizar la integridad de los datos, toda la actividad de I/o del volumen objetivo se suspende durante cualquier operación de copia de volumen. Esta suspensión ocurre porque el estado de los datos del volumen objetivo es incoherente hasta que el procedimiento se completa.

A continuación, se describen las operaciones de copia de volumen sin conexión y en línea.

Operación de copia de volumen sin conexión

La relación de copia de volumen sin conexión se da entre un volumen de origen y un volumen objetivo. Una copia sin conexión lee datos del volumen de origen y los copia en un volumen objetivo, mientras suspende todas las actualizaciones al volumen de origen con la copia en curso. Todas las actualizaciones al volumen de origen se suspenden para evitar que se generen incoherencias cronológicas en el volumen objetivo.

Conocimientos necesarios sobre las operaciones de copia sin conexión	
Solicitudes de lectura y escritura	• Los volúmenes de origen que participan en una copia sin conexión están disponibles para la actividad de I/o de solo lectura mientras el estado de una operación de copia de volumen es en curso o pendiente. • Las solicitudes de escritura se permiten una vez que se completa la copia sin conexión. • Para evitar que aparezcan mensajes de error de protección contra escritura, no se debe acceder al volumen de origen que participa en una operación de copia de volumen cuyo estado es en curso.

Conocimientos necesarios sobre las operaciones de copia sin conexión	
Sistema de archivos de registro en diario	• Si el volumen de origen se formateó con un sistema de archivos de registro en diario, es posible que las controladoras de la cabina de almacenamiento rechacen cualquier intento de emitir una solicitud de lectura al volumen de origen y se muestre un mensaje de error. • La unidad del sistema de archivos de registro en diario emite una solicitud de escritura antes de emitir la solicitud de lectura. La controladora rechaza la solicitud de escritura y es posible que esto impida la emisión de la solicitud de lectura. En esta situación, es posible que se muestre un mensaje de error que indica que el volumen de origen está protegido contra escritura. • Para evitar este problema, no se debe acceder al volumen de origen que está participando en una copia sin conexión mientras el estado de la operación de copia de volumen es en curso.

Operación de copia de volumen en línea

La relación de copia de volumen en línea se establece entre un volumen Snapshot y un volumen objetivo. Se puede iniciar una operación de copia de volumen mientras el volumen de origen está en línea y disponible para la escritura de datos. Para obtener esta función, se crea una copia de Snapshot del volumen y se usa la copia de Snapshot como volumen de origen real.

Cuando se inicia una operación de copia de volumen para un volumen de origen, System Manager crea una imagen Snapshot del volumen base y una relación de copia entre la imagen Snapshot del volumen base y un volumen objetivo. Si se utiliza la imagen Snapshot como volumen de origen, la cabina de almacenamiento podrá seguir escribiendo en el volumen de origen mientras la copia está en progreso.

Durante las operaciones de copia en línea hay un impacto en el rendimiento debido al procedimiento de copia en escritura. Una vez que se completa la copia en línea, se restablece el rendimiento del volumen base.

Conocimientos necesarios sobre las operaciones de copia en línea	
¿Qué clases de volúmenes se pueden utilizar?	• El volumen para el que se crea la imagen de un momento específico se conoce como volumen base y debe ser un volumen estándar o un volumen fino en la cabina de almacenamiento. • Un volumen objetivo puede ser un volumen estándar en un grupo de volúmenes o un volumen estándar en un pool. Un volumen objetivo no puede ser un volumen fino ni un volumen base en un grupo Snapshot. • Se puede usar la función Copy Volume en línea para copiar datos de un volumen fino a un volumen estándar en un pool que reside dentro de la misma cabina de almacenamiento. Pero no se puede usar la función Copy Volume para copiar datos de un volumen estándar a un volumen fino.
Rendimiento del volumen base	• Si el volumen Snapshot que se utiliza como la copia de origen está activo, el rendimiento del volumen base se degrada debido a las operaciones de copia en escritura. Cuando la copia se completa, se deshabilita la Snapshot y se restablece el rendimiento del volumen base. A pesar de que la Snapshot está deshabilitada, el volumen de capacidad reservada y la relación de copia permanecen intactos.

Conocimientos necesarios sobre las operaciones de copia en línea	
Tipos de volúmenes creados	• Durante la operación de copia en línea, se crea un volumen Snapshot y un volumen de capacidad reservada. • El volumen Snapshot no es un volumen real que contiene datos, más bien, es una referencia hacia los datos que estaban contenidos en un volumen en un momento determinado. • Para cada snapshot que se toma, se crea un volumen de capacidad reservada para conservar los datos de la Snapshot. El volumen de capacidad reservada se utiliza solo para gestionar la imagen Snapshot.
Volumen de capacidad reservada	• Antes de modificar un bloque de datos del volumen de origen, el contenido del bloque que se va a modificar se copia en el volumen de capacidad reservada para garantizar su seguridad. • Como el volumen de capacidad reservada almacena copias de los datos originales en esos bloques de datos, los demás cambios en esos bloques de datos se escriben solo en el volumen de origen. • La operación de copia en línea utiliza menos espacio en disco que una copia física completa porque los únicos bloques de datos que se almacenan en el volumen de capacidad reservada son los que se modificaron desde el momento en que se tomó la Snapshot.

Copiar volumen

Se pueden copiar datos de un volumen a otro de la misma cabina de almacenamiento y crear un duplicado físico de un momento específico (clon) de un volumen de origen.

Antes de empezar

- Se debe suspender toda la actividad de I/o del volumen de origen y objetivo.
- Se deben desmontar todos los sistemas de archivos del volumen de origen y del volumen objetivo.
- Si se usó el volumen objetivo en una operación Copy Volume anterior, ya no se necesitan esos datos o si ya se realizó un backup de esos datos.

Acerca de esta tarea

El volumen de origen es el volumen que acepta I/o del host y almacena los datos de la aplicación. Cuando comienza la operación Copy Volume, los datos del volumen de origen se copian íntegramente en el volumen objetivo.

El volumen objetivo es un volumen estándar que conserva una copia de los datos del volumen de origen. El volumen objetivo es idéntico al volumen de origen una vez que finaliza la operación Copy Volume. El volumen objetivo debe tener la misma capacidad o más que el volumen de origen, no obstante, puede tener un nivel de RAID diferente.

Más información acerca de las copias en línea y sin conexión

Copia en línea

Una copia en línea crea una copia de un momento específico de cualquier volumen dentro de la cabina de almacenamiento, mientras todavía es posible escribir en ese volumen durante la ejecución de la copia. Para obtener esta función, se crea una copia de Snapshot del volumen y se usa la copia de Snapshot como volumen de origen real. El volumen para el cual se crea una imagen de un momento específico se denomina volumen base y puede ser un volumen estándar o fino de la cabina de almacenamiento.

Copia sin conexión

Una copia sin conexión lee datos del volumen de origen y los copia en un volumen objetivo, mientras suspende todas las actualizaciones al volumen de origen con la copia en curso. Todas las actualizaciones al volumen de origen se suspenden para evitar que se generen incoherencias cronológicas en el volumen objetivo. La relación de copia de volumen sin conexión se da entre un volumen de origen y un volumen objetivo.

Una operación Copy Volume sobrescribe los datos en el volumen objetivo y omite todos los volúmenes Snapshot asociados con el volumen objetivo, si corresponde.

Pasos

1. Seleccione MENU:Storage[Volumes].
2. Seleccione el volumen que desea usar como origen para la operación Copy Volume y, luego, seleccione MENU:Servicios de copia[Copy volume].

   Se muestra el cuadro de diálogo Copiar volumen-Seleccionar objetivo.

3. Seleccione el volumen objetivo al que se desea copiar los datos.

   En la tabla que se muestra en este cuadro de diálogo, se indican todos los volúmenes objetivo aptos.

4. Use la barra de desplazamiento para configurar la prioridad de copiado para la operación Copy Volume.

   La prioridad de copiado determina cuántos recursos del sistema se usan para completar la operación Copy Volume en comparación con las solicitudes de I/o de servicio.

Más información acerca de las tasas de prioridad de copiado

Las tasas de prioridad de copiado son las siguientes cinco:

- El más bajo
- Bajo
- Mediano
- Alto
- Máxima

Si la prioridad de copiado se configuró con la tasa mínima, se prioriza la actividad de I/o y la operación Copy Volume lleva más tiempo. Si la prioridad de copiado se configuró con la tasa máxima, la operación Copy Volume tiene prioridad, pero podría afectar a la actividad de I/o de la cabina de almacenamiento.

5. Seleccione si desea crear una copia en línea o sin conexión. Para crear una copia en línea, active la casilla de verificación **mantener el volumen de origen en línea durante la operación de copia**.
6. Debe realizar una de las siguientes acciones:
   - Para realizar una operación de copia *online*, haga clic en **Siguiente** para continuar con el cuadro de diálogo **capacidad de reserva**.
   - Para realizar una operación de copia *offline*, haga clic en **Finalizar** para iniciar la copia sin conexión.
7. Si decide crear una copia en línea, establezca la capacidad reservada necesaria para almacenar datos y otra información para la copia en línea y, a continuación, haga clic en **Finalizar** para iniciar la copia en línea.

   En la tabla Volume Candidate, solo se muestran los candidatos que admiten la capacidad reservada especificada. La capacidad reservada es la capacidad física asignada que se usa para cualquier operación de servicio de copia y objeto de almacenamiento. El host no puede leerla directamente.

   Utilice las siguientes directrices para asignar la capacidad reservada:

   - La configuración predeterminada para la capacidad reservada es del 40 % del volumen base y, por lo general, esta capacidad es suficiente.
   - No obstante, la capacidad reservada varía, según la cantidad de cambios en los datos originales. Cuanto más tiempo está activo un objeto de almacenamiento, mayor es la capacidad reservada.

Resultados

System Manager copia todos los datos del volumen de origen al volumen objetivo. Una vez que finaliza la operación Copy Volume, el volumen objetivo pasa automáticamente a ser solo de lectura para los hosts.

Después de terminar

Seleccione MENU:Inicio[Ver operaciones en curso] para ver el progreso de la operación Copy Volume. Es posible que esta operación demore y que afecte el rendimiento del sistema.

Actuar sobre una operación de copia de volumen

Es posible ver una operación de copia de volumen en curso y detenerla, cambiar su prioridad, volver a copiarla o eliminarla.

Pasos

1. Seleccione MENU:Inicio[Ver operaciones en curso].

   Se muestra el cuadro de diálogo Operaciones en curso.

2. Busque la operación Copiar volumen sobre la que desea actuar y, a continuación, haga clic en el enlace de la columna **acciones** para realizar una de las siguientes acciones.

   Lea todo el texto de precaución que se proporciona en los cuadros de diálogo, especialmente cuando desee detener una operación.

Acción	Descripción
Pare	Puede detener una operación de copia de volumen mientras su estado sea en curso, pendiente o con errores. Cuando se detiene una copia de volumen, todos los hosts asignados obtienen acceso de escritura al volumen de origen. Si se escriben datos en el volumen de origen, los datos en el volumen objetivo ya no coincidirán con los datos en el volumen de origen.
Cambiar prioridad	Puede cambiar la prioridad de una operación de copia de volumen mientras su estado sea en curso para seleccionar la velocidad a la que se debe completar la operación de copia de volumen.
Volver a copiar	Puede volver a copiar un volumen si desea iniciar nuevamente una operación de copia de volumen detenida o cuando se producen errores o interrupciones en una operación de copia de volumen. La operación de copia de volumen se iniciará nuevamente de cero. Al volver a copiar, esta acción sobrescribirá los datos existentes en el volumen objetivo y anulará todos los volúmenes Snapshot asociados con ese volumen, si existe alguno.
Claro	Puede quitar la operación de copia de volumen mientras su estado sea en curso, pendiente o con errores. Asegúrese de que desea realizar esta operación antes de seleccionar **Borrar**. No se mostrará ningún cuadro de diálogo de confirmación.

Preguntas frecuentes

¿Qué es un volumen?

Un volumen es un contenedor en el cual las aplicaciones, las bases de datos y los sistemas de archivos almacenan datos. Es el componente lógico que se crea para que el host acceda al almacenamiento de la cabina de almacenamiento.

Un volumen se crea a partir de la capacidad disponible de un pool o un grupo de volúmenes. Un volumen tiene una capacidad definida. Aunque es posible que un volumen conste de más de una unidad, un volumen

aparece como un componente lógico para el host.

¿Por qué veo un error de sobreasignación de capacidad si tengo capacidad libre suficiente en un grupo de volúmenes para crear volúmenes?

Es posible que el grupo de volúmenes seleccionado tenga una o más áreas de capacidad libre. Un área de capacidad libre es la capacidad libre que puede surgir después de eliminar un volumen o por no utilizar toda la capacidad libre disponible durante la creación de un volumen.

Cuando se crea un volumen en un grupo de volúmenes que tiene una o más áreas de capacidad libre, la capacidad del volumen se limita al área de capacidad libre más grande de ese grupo de volúmenes. Por ejemplo, si un grupo de volúmenes tiene una capacidad libre total de 15 GIB y el área de capacidad libre más grande es 10 GIB, el volumen más grande que se puede crear es de 10 GIB.

Si un grupo de volúmenes tiene áreas de capacidad libre, el gráfico de grupo de volúmenes contiene un enlace que indica la cantidad de áreas de capacidad libre existentes. Seleccione el enlace para ver un cuadro emergente que indica la capacidad de cada área.

Al consolidar la capacidad libre, se pueden crear volúmenes adicionales de la cantidad máxima de capacidad libre de un grupo de volúmenes. Se puede consolidar la capacidad libre existente en un grupo de volúmenes seleccionado mediante uno de los siguientes métodos:

- Si se detecta al menos un área de capacidad libre para un grupo de volúmenes, se muestra la recomendación de que se debe consolidar la capacidad libre en la página Inicio del área notificación. Haga clic en el enlace **consolidar capacidad libre** para abrir el cuadro de diálogo.
- También se puede seleccionar **Pools y grupos de volúmenes › tareas no comunes › consolidar la capacidad libre del grupo de volúmenes** para abrir el cuadro de diálogo.

Si desea utilizar un área de capacidad libre específica en lugar del área de mayor capacidad, utilice la interfaz de línea de comandos (CLI) o Script Editor.

¿Cómo afecta la creación de volúmenes la carga de trabajo seleccionada?

Durante la creación de un volumen, se solicita información sobre el uso de la carga de trabajo. El sistema utiliza esta información para crear una configuración de volumen óptima para el usuario, que se puede editar en caso de ser necesario. De manera opcional, es posible omitir este paso en la secuencia de creación de volúmenes.

Una carga de trabajo es un objeto de almacenamiento que admite una aplicación. Se pueden definir una o más cargas de trabajo o instancias por aplicación. En algunas aplicaciones, el sistema configura la carga de trabajo para contener volúmenes con características subyacentes similares. Estas características de volumen se optimizan según el tipo de aplicación que es compatible con la carga de trabajo. Por ejemplo, si crea una carga de trabajo que es compatible con la aplicación Microsoft SQL Server y, a continuación, crea volúmenes para esa carga de trabajo, las características de volumen subyacentes se optimizan para ser compatibles con Microsoft SQL Server.

- **Específico de la aplicación** — cuando se crean volúmenes con una carga de trabajo específica de la aplicación, el sistema puede recomendar una configuración de volumen optimizada para minimizar la contención entre las E/S de la carga de trabajo de la aplicación y otro tráfico de la instancia de la aplicación. Las características del volumen, como tipo de I/o, tamaño de segmentos, propiedad de la controladora, y caché de lectura y escritura, se recomiendan y se optimizan automáticamente para las cargas de trabajo que se crean para los siguientes tipos de aplicaciones.

- Microsoft® SQL Server™
- Microsoft® Exchange Server™
- Aplicaciones de videovigilancia
- VMware ESXi™ (para volúmenes que se usarán con Virtual Machine File System)

  Se puede revisar la configuración de volumen recomendada y editar, añadir o eliminar volúmenes y características recomendados por el sistema mediante el cuadro de diálogo Añadir/editar volúmenes.

- **Otros** (o aplicaciones sin compatibilidad con la creación de volúmenes específicos) — Otras cargas de trabajo utilizan una configuración de volumen que debe especificar manualmente cuando desea crear una carga de trabajo no asociada con una aplicación específica, o si no hay optimización integrada para la aplicación que piensa utilizar en la cabina de almacenamiento. Debe especificar manualmente la configuración del volumen en el cuadro de diálogo Añadir/editar volúmenes.

¿Por qué estos volúmenes no están asociados con una carga de trabajo?

Los volúmenes no se asocian a una carga de trabajo si se los creó mediante la interfaz de línea de comandos (CLI) o si se migraron (importaron/exportaron) desde una cabina de almacenamiento diferente.

¿Por qué no puedo eliminar la carga de trabajo seleccionada?

Esta carga de trabajo consta de un grupo de volúmenes que se creó mediante la interfaz de línea de comandos (CLI) o se migró (se importó/exportó) de una cabina de almacenamiento diferente. Como resultado, los volúmenes de esta carga de trabajo no están asociados a una carga de trabajo específica de la aplicación, por lo que no es posible eliminar la carga de trabajo.

¿Cómo ayudan las cargas de trabajo específicas de la aplicación a gestionar la cabina de almacenamiento?

Las características de volumen de la carga de trabajo específica de la aplicación determinan la manera en que la carga de trabajo interactúa con los componentes de la cabina de almacenamiento, y ayudan a determinar el rendimiento de su entorno en una determinada configuración.

Una aplicación es un software, como SQL Server o Exchange. Se definen una o más cargas de trabajo que sean compatibles con cada aplicación. En algunas aplicaciones, el sistema recomienda automáticamente una configuración de volumen que optimice el almacenamiento. Las características como el tipo de I/o, el tamaño de segmento, la propiedad de controladora y la caché de lectura y escritura se incluyen en la configuración de volumen.

¿Cómo ayuda esta información a crear almacenamiento?

La información de carga de trabajo se utiliza para optimizar características del volumen como tipo de E/S, tamaño de segmento y caché de lectura/escritura para la carga de trabajo seleccionada. Estas características optimizadas dictan la forma en que la carga de trabajo interactúa con los componentes de la cabina de almacenamiento.

Según la información de carga de trabajo que se proporcione, System Manager crea los volúmenes apropiados y los coloca en los pools o los grupos de volúmenes disponibles actualmente en el sistema. El sistema crea los volúmenes y optimiza sus características según las prácticas recomendadas vigentes para la carga de trabajo seleccionada.

Antes de terminar de crear volúmenes para una carga de trabajo determinada, puede revisar la configuración de volumen recomendada y editar, añadir o eliminar los volúmenes y las características que recomienda el sistema mediante el cuadro de diálogo Añadir/editar volúmenes.

Para obtener información sobre las prácticas recomendadas, consulte la documentación específica de la aplicación.

¿Qué debo hacer para reconocer la capacidad expandida?

Si se aumenta la capacidad de un volumen, es posible que el host no reconozca de inmediato el aumento de la capacidad del volumen.

La mayoría de los sistemas operativos reconocen la capacidad expandida del volumen y se expanden automáticamente después de que se inicia la expansión de volumen. Sin embargo, es posible que algunos no lo hagan. Si el sistema operativo no reconoce automáticamente la capacidad de volumen expandida, es posible que se deba volver a analizar el disco o reiniciar.

Después de haber expandido la capacidad del volumen, se debe aumentar manualmente el tamaño del sistema de archivos para que coincida. La forma de hacerlo depende del sistema de archivos utilizado.

Consulte la documentación del sistema operativo host para obtener más detalles.

¿Por qué no se muestran todos los pools y/o los grupos de volúmenes?

No se muestra en la lista ningún pool o grupo de volúmenes al que no se pueda mover el volumen.

Los pools o grupos de volúmenes no serán aptos por cualquiera de los motivos siguientes:

- Las funcionalidades de Data Assurance (DA) de un pool o un pool de grupo de volúmenes no coinciden.
- Un pool o un grupo de volúmenes se encuentra en un estado distinto a Optimal.
- La capacidad de un pool o grupo de volúmenes es muy reducida.

¿Qué es el tamaño de segmento?

Un segmento es la cantidad de datos en kilobytes (KiB) que se almacenan en una unidad antes de que la cabina de almacenamiento pase a la unidad siguiente en la franja (grupo RAID). El tamaño de segmento aplica solo a grupos de volúmenes, no a pools.

El tamaño de los segmentos está definido por la cantidad de bloques de datos que contiene. Para determinar el tamaño de segmento, se debe conocer el tipo de datos que se almacenará en un volumen. Si una aplicación utiliza habitualmente escrituras y lecturas aleatorias pequeñas (IOPS), por lo general, funcionará mejor un tamaño de segmento más pequeño. Por el contrario, si la aplicación realiza escrituras y lecturas secuenciales grandes (rendimiento), por lo general, funcionará mejor un tamaño de segmento grande.

Independientemente de si una aplicación utiliza escrituras y lecturas aleatorias pequeñas o escrituras y lecturas secuenciales grandes, la cabina de almacenamiento rendirá mejor si el tamaño del segmento es mayor al tamaño típico del fragmento de bloque de datos. Habitualmente, esto facilita y agiliza el acceso de

las unidades a los datos, lo cual resulta importante para un mejor rendimiento de la cabina de almacenamiento.

Entornos en los que el rendimiento de IOPS es importante

En un entorno de operaciones de I/o por segundo (IOPS), la cabina de almacenamiento tiene un mejor rendimiento si se utiliza un tamaño de segmento mayor al tamaño típico del bloque de datos ("fragmento"") que se lee/escribe en una unidad. Esto garantiza que cada fragmento se escriba en una unidad única.

Entornos en los que el rendimiento es importante

En un entorno de rendimiento, el tamaño del segmento debe ser una fracción entera de las unidades totales para los datos y del tamaño de fragmento de datos típico (tamaño de I/o). Esto permite la distribución de los datos como una franja única en las unidades del grupo de volúmenes, lo que lleva a lecturas y escrituras más rápidas.

¿Qué es la propiedad de controladora preferida?

La propiedad de controladora preferida define la controladora designada como la controladora propietaria, o primaria, del volumen.

La propiedad de la controladora es sumamente importante y debe planificarse con cuidado. Las controladoras deben equilibrarse lo más posible en cuanto a las operaciones de I/o totales.

Por ejemplo, si una controladora lee principalmente bloques de datos secuenciales grandes y la otra posee bloques de datos pequeños con lecturas y escrituras frecuentes, las cargas son muy diferentes. Conocer cuáles volúmenes contienen qué tipo de datos permite equilibrar las transferencias de I/o de forma equitativa en ambas controladoras.

¿Cuándo quieres usar la selección asignar el host más adelante?

Si desea acelerar el proceso para crear volúmenes, puede omitir el paso de asignación de host para que los volúmenes recién creados se inicialicen sin conexión.

Los volúmenes recién creados deben inicializarse. El sistema puede inicializarlos utilizando uno de los dos modos: Un proceso de inicialización en segundo plano de formato disponible inmediato (IAF) o un proceso fuera de línea.

Cuando se asigna un volumen a un host, se fuerza la inicialización de todos los volúmenes en ese grupo a realizar la transición a la inicialización en segundo plano. Este proceso de inicialización en segundo plano permite realizar operaciones de I/o del host simultáneas, que a veces pueden requerir mucho tiempo.

Cuando ninguno de los volúmenes de un grupo de volúmenes se asigna, se realiza una inicialización sin conexión. El proceso fuera de línea es mucho más rápido que el proceso en segundo plano.

¿Qué debo saber acerca de los requisitos de tamaño de bloque del host?

Para los sistemas EF300 y EF600, es posible configurar un volumen para que admita un tamaño de bloque de 512 bytes o 4 KiB (también llamado "tamaño de sector"). Debe configurar el valor correcto durante la creación del volumen. Si es posible, el sistema sugiere el valor predeterminado adecuado.

Antes de configurar el tamaño de bloque de volumen, lea las siguientes limitaciones y directrices.

- Algunos sistemas operativos y máquinas virtuales (principalmente VMware, por el momento) requieren un tamaño de bloque de 512 bytes y no admiten 4 KiB, por lo tanto, asegúrese de conocer los requisitos del host antes de crear un volumen. Normalmente, puede lograr el mejor rendimiento configurando un volumen para que presente un tamaño de bloque de 4 KiB; sin embargo, asegúrese de que su host permita bloques de 4 KiB (o "'4Kn'").
- El tipo de unidades que se selecciona para el pool o el grupo de volúmenes también determina qué tamaños de bloque de volumen se admiten, como se indica a continuación:
  - Si se crea un grupo de volúmenes con unidades que escriben en bloques de 512 bytes, solo se pueden crear volúmenes con bloques de 512 bytes.
  - Si crea un grupo de volúmenes con unidades que escriben en bloques de 4 KiB, puede crear volúmenes con bloques de 512 bytes o 4 KiB.
- Si la cabina tiene una tarjeta de interfaz del host iSCSI, todos los volúmenes se limitan a bloques de 512 bytes (independientemente del tamaño de bloque del grupo de volúmenes). Esto se debe a una implementación específica del hardware.
- No se puede cambiar el tamaño de un bloque una vez configurado. Si necesita cambiar el tamaño de bloque, debe eliminar el volumen y volver a crearlo.

Hosts y clústeres de hosts

Información general sobre los hosts y los clústeres de hosts

Es posible configurar hosts y clústeres de hosts, que definen las conexiones entre la cabina de almacenamiento y los servidores de datos.

¿Qué son los hosts y los clústeres de hosts?

Un *host* es un servidor que envía I/o a un volumen de una cabina de almacenamiento. Un *host cluster* es un grupo de hosts, que se puede crear para asignar los mismos volúmenes a varios hosts.

Obtenga más información:

- "Terminología de host"
- "Volúmenes de acceso"
- "Número máximo de LUN"

¿Cómo se configuran los hosts y los clústeres de hosts?

Para definir las conexiones de hosts, es posible permitir que un agente de contexto de host (HCA) detecte automáticamente los hosts, o bien puede ir a **Storage › hosts** para configurar manualmente el host. Si desea que dos o más hosts compartan el acceso al mismo conjunto de volúmenes, puede definir un clúster y asignar los volúmenes a ese clúster.

Obtenga más información:

- "Creación de hosts automática versus manual"
- "Cómo se asignan volúmenes a hosts y clústeres de hosts"
- "Flujo de trabajo para la creación de hosts y la asignación de volúmenes"
- "Crear un host automáticamente"

- "Crear hosts manualmente"
- "Cree un clúster de hosts"
- "Asignar volúmenes a hosts"

Información relacionada

Obtenga más información acerca de las tareas relacionadas con hosts:

- "Establecer equilibrio de carga automático"
- "Establezca la generación de informes de conectividad de host"
- "Cambiar el tipo de host predeterminado"

Conceptos

Terminología de host

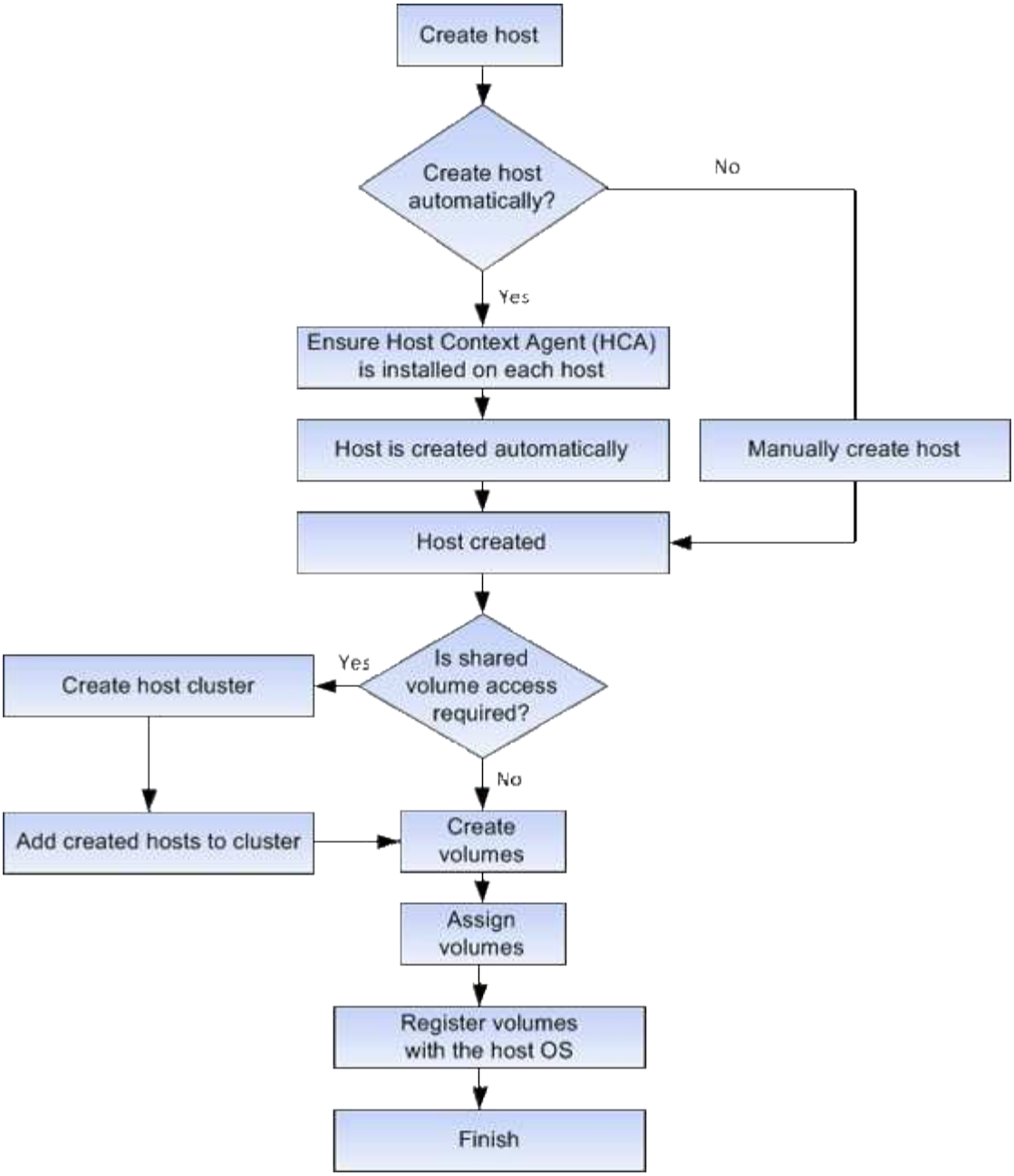
Conozca la forma en que los términos de host se aplican a su cabina de almacenamiento.

Componente	Definición
Host	Un host es un servidor que envía I/o a un volumen de una cabina de almacenamiento.
Nombre de host	El nombre de host debe ser igual al nombre de sistema del host.
Clúster de hosts	Un clúster de hosts es un grupo de hosts. Se crea un clúster de hosts para facilitar la asignación de los mismos volúmenes en varios hosts.
Protocolo de interfaz del host	Un protocolo de interfaz del host es la conexión (como Fibre Channel, iSCSI, etc.) entre las controladoras y los hosts.
HBA o tarjeta de interfaz de red (NIC)	Un adaptador de bus de host (HBA) es una placa que se encuentra en un host y tiene uno o más puertos de host.
Puerto de host	Un puerto de host es un puerto en un adaptador de bus de host (HBA) que facilita la conexión física a una controladora y se usa en operaciones de I/O.

Componente	Definición
Identificador de puerto de host	Un identificador de puerto de host es un nombre a nivel mundial único relacionado con cada puerto de host de un adaptador de bus de host (HBA). • Los identificadores de puertos de host de la interfaz estándar de equipos pequeños de Internet (iSCSI) deben contener de 1 a 233 caracteres. Los identificadores de puertos de host de iSCSI se muestran en un formato IQN estándar (p. ej., `iqn.xxx.com.xxx:8b3ad`). • Los identificadores de puertos de host que no pertenecen a iSCSI, como Fibre Channel y SAS, se muestran delimitados por dos puntos después de cada dos caracteres (p. ej., `xx:yy:zz`). Los identificadores de puertos de host de Fibre Channel deben tener 16 caracteres.
Tipo de sistema operativo de host	El tipo de sistema operativo del host es una opción de configuración que define cómo las controladoras de una cabina de almacenamiento reaccionan frente a las operaciones de I/o según el sistema operativo (o variante) del host. Esto también se denomina en ocasiones *host type* para abreviar.
Puerto de host de la controladora	Un puerto de host de controladora es un puerto en la controladora que facilita la conexión física a un host y se usa en operaciones de I/O.
LUN	Un número de unidad lógica (LUN) es el número asignado al espacio de dirección que utiliza un host para acceder a un volumen. El volumen se presenta al host como capacidad en forma de LUN. Cada host tiene su propio espacio de dirección de LUN. Por lo tanto, distintos hosts pueden utilizar el mismo LUN para acceder a diferentes volúmenes.

Flujo de trabajo para la creación de hosts y la asignación de volúmenes

La figura que se presenta a continuación señala cómo configurar el acceso al host.



Creación de hosts automática versus manual

La creación de un host es uno de los pasos necesarios para indicar a la cabina de almacenamiento qué hosts están conectados a ella y para permitir el acceso de I/o a los volúmenes. Es posible crear un host de manera automática o manual.

Creación automática

La creación automática de hosts para hosts basados en SCSI (no NVMe-of) se inicia desde el agente de contexto de host (HCA). HCA es una utilidad que puede instalar en cada host conectado a la cabina de almacenamiento. Cada host que posee HCA instalado inserta su información de configuración en la cabina de almacenamiento a través de la ruta de I/O. Según la información del host, las controladoras crean automáticamente el host y los puertos de host asociados para establecer el tipo de host. Si es necesario, puede realizar cualquier cambio adicional en la configuración del host con System Manager.

Después de que HCA realiza la detección automática, el host aparece automáticamente en la página hosts con los siguientes atributos:

- El nombre de host derivado del nombre de sistema del host.
- Los puertos identificadores del host que están asociados con el host.
- El tipo de sistema operativo del host.

Los hosts se crean como hosts independientes; HCA no los crea ni los añade automáticamente a clústeres de hosts.

Creación manual

Quizás sea conveniente crear manualmente un host por uno de los siguientes motivos:

1. Decide no instalar la utilidad HCA en los hosts.
2. Quiere asegurarse de que los identificadores de puerto de host que detectaron las controladoras de la cabina de almacenamiento están asociados correctamente con los hosts.

Durante la creación manual de hosts, debe seleccionar manualmente los identificadores de puerto de host o introducirlos manualmente para asociarlos. Después de crear un host, puede asignar volúmenes a él o añadirlo a un clúster de hosts si el objetivo es compartir el acceso a los volúmenes.

Cómo se asignan volúmenes a hosts y clústeres de hosts

Para que un host o un clúster de hosts envíe I/o a un volumen, se debe asignar el volumen al host o al clúster de hosts.

Es posible seleccionar un host o un clúster de hosts cuando se crea un volumen, o asignar un volumen a un host o clúster de hosts más adelante. Un clúster de hosts es un grupo de hosts. Se crea un clúster de hosts para facilitar la asignación de los mismos volúmenes en varios hosts.

La asignación de volúmenes a hosts es flexible y permite satisfacer necesidades de almacenamiento específicas.

- **Host autónomo, no parte de un cluster host** — puede asignar un volumen a un host individual. Un solo host puede acceder al volumen.
- **Clúster de host** — puede asignar un volumen a un clúster de hosts. Todos los hosts del clúster de hosts pueden acceder al volumen.
- **Host dentro de un cluster host** — puede asignar un volumen a un host individual que forma parte de un cluster de host. Aunque el host forma parte de un clúster de hosts, solo el host individual puede acceder al volumen y no ningún otro host del clúster de hosts.

Cuando se crean volúmenes, se asignan automáticamente números de unidad lógica (LUN). Los LUN actúan como "dirección" entre el host y la controladora durante las operaciones de I/O. Es posible cambiar el LUN después de crear un volumen.

Volúmenes de acceso

Un volumen de acceso es un volumen configurado en fábrica de la cabina de almacenamiento que se utiliza para la comunicación con la cabina de almacenamiento y el host mediante la conexión de I/o del host. El volumen de acceso requiere un número

de unidad lógica (LUN).

El volumen de acceso se utiliza en dos instancias:

- **Creación automática de host** — el volumen de acceso es utilizado por la utilidad Agente de contexto de host (HCA) para insertar la información del host (nombre, puertos, tipo de host) en System Manager para la creación automática de host.
- **Administración en banda** — el volumen de acceso se utiliza para una conexión en banda para administrar la matriz de almacenamiento. Esto solo puede llevarse a cabo si la cabina de almacenamiento se gestiona con la interfaz de línea de comandos (CLI).

> La gestión en banda no está disponible para los sistemas de almacenamiento EF600 o EF300.

Un volumen de acceso se crea automáticamente la primera vez que se asigna un volumen a un host. Por ejemplo, si asigna Volume_1 y Volume_2 a un host, cuando observe los resultados de esa asignación, notará la existencia de tres volúmenes (Volume_1, Volume_2 y Access).

Si no desea crear hosts automáticamente ni gestionar una cabina de almacenamiento en banda con la CLI, no necesita el volumen de acceso; por lo tanto, puede eliminarlo para liberar el LUN. Esta acción quita la asignación de volumen a LUN y todas las conexiones de gestión en banda al host.

Número máximo de LUN

La cabina de almacenamiento tiene un número máximo de números de unidad lógica (LUN) que pueden usarse para cada host.

El número máximo depende del sistema operativo del host. La cabina de almacenamiento realiza un seguimiento del número de LUN utilizados. Si se intenta asignar un volumen a un host que supera la cantidad máxima de LUN, el host no podrá acceder al volumen.

Tipo de sistema operativo del host predeterminado

La cabina de almacenamiento utiliza el tipo de host predeterminado cuando se conectan inicialmente los hosts. Define la manera en que funcionan las controladoras en la cabina de almacenamiento con el sistema operativo del host cuando se accede a los volúmenes.

Es posible cambiar el tipo de host si hay una necesidad de cambiar la manera en que opera la cabina de almacenamiento en relación con los hosts que están conectados con ella. En general, se debe cambiar el tipo de host predeterminado antes de conectar hosts a la cabina de almacenamiento o al añadir hosts adicionales.

Tenga en cuenta estas directrices:

- Si todos los hosts que piensa conectar a la cabina de almacenamiento tienen el mismo sistema operativo (entorno de host homogéneo), cambie el tipo de host para que coincida con el sistema operativo.
- Si hay hosts con diferentes sistemas operativos que piensa conectar a la cabina de almacenamiento (entorno de host heterogéneo), cambie el tipo de host para que coincida con la mayoría de los sistemas operativos de los hosts.

  Por ejemplo, si va a conectar ocho hosts diferentes a la cabina de almacenamiento y seis de ellos tienen un sistema operativo Windows, debe seleccionar Windows como tipo de sistema operativo de host

predeterminado.

- Si la mayoría de los hosts conectados poseen una combinación de sistemas operativos diferentes, cambie el tipo de host a opción predeterminada de fábrica.

  Por ejemplo, si va a conectar ocho hosts diferentes a la cabina de almacenamiento y dos de ellos tienen un sistema operativo Windows, tres ejecutan un sistema operativo VMware, Y otros tres ejecutan un sistema operativo Linux, debe seleccionar opción predeterminada de fábrica como el tipo de sistema operativo del host predeterminado.

Configurar el acceso de hosts

Crear un host automáticamente

Puede dejar que el agente de contexto de host (HCA) detecte automáticamente los hosts y, luego, verificar que la información sea correcta. La creación de un host es uno de los pasos necesarios para indicar a la cabina de almacenamiento qué hosts están conectados a ella y para permitir el acceso de I/o a los volúmenes.

Antes de empezar

Asegúrese de que el agente de contexto de host (HCA) esté instalado y se ejecute en cada host conectado a la cabina de almacenamiento. Los hosts que tienen HCA instalado y están conectados a la cabina de almacenamiento se crean automáticamente. Para instalar HCA, instale SANtricity Storage Manager en el host y seleccione la opción Host. HCA no está disponible en todos los sistemas operativos compatibles. Si no está disponible, debe crear el host manualmente.

Pasos

1. Seleccione MENU:Storage[hosts].

   En la tabla, se indican los hosts que se crearon automáticamente.

2. Verifique que la información provista por HCA sea correcta (nombre, tipo de host, identificadores de puertos de host).

   Si necesita cambiar alguna información, seleccione el host y, a continuación, haga clic en **Ver/editar configuración**.

3. **Opcional:** Si desea que el host creado automáticamente esté en un clúster, cree un clúster de hosts y agregue el host o los hosts.

Resultados

Una vez que el host se creó automáticamente, el sistema muestra los siguientes elementos en la tabla del icono hosts.

- El nombre de host derivado del nombre de sistema del host.
- Los puertos identificadores del host que están asociados con el host.
- El tipo de sistema operativo del host.

Crear hosts manualmente

Aquellos hosts que no se pueden detectar automáticamente, se pueden crear de forma manual. La creación de un host es uno de los pasos necesarios para indicar a la cabina de almacenamiento qué hosts están conectados a ella y para permitir el acceso de I/o a los volúmenes.

Acerca de esta tarea

Tenga en cuenta estas directrices al crear un host:

- Se deben definir los puertos identificadores de host que están asociados con el host.
- Asegúrese de proporcionar el mismo nombre que el nombre de sistema del host asignado.
- Esta operación no funciona si el nombre que eligió ya está en uso.
- La longitud del nombre no puede ser mayor de 30 caracteres.

Pasos

1. Seleccione MENU:Storage[hosts].
2. Haga clic en MENU:Create[Host].

   Se muestra el cuadro de diálogo Crear host.

3. Seleccione la configuración del host que corresponda.

Detalles del campo

Ajuste	Descripción
Nombre	Escriba un nombre para el host nuevo.
Tipo de sistema operativo de host	Seleccione el sistema operativo que funciona en el host nuevo de la lista desplegable.
Tipo de interfaz del host	(Opcional) Si la cabina de almacenamiento es compatible con más de un tipo de interfaz del host, seleccione el tipo de interfaz del host que desea usar.
Puertos host	Debe realizar una de las siguientes acciones: • **Seleccione la interfaz de E/S** Por lo general, los puertos de host deben haber iniciado sesión y estar disponibles en la lista desplegable. Puede seleccionar los identificadores de puerto de host de la lista. • **Adición manual** Si un identificador de puerto de host no aparece en la lista, significa que el puerto de host no inició sesión. Se puede usar una utilidad de HBA o una utilidad de iniciador de iSCSI para encontrar los identificadores de puerto de host y asociarlos con el host. Puede introducir manualmente los identificadores de puerto de host o copiarlos/pegarlos desde la utilidad (de uno en uno) en el campo **puertos de host**. Se debe seleccionar un identificador de puerto de host para asociarlo con el host, pero es posible seguir seleccionando identificadores que estén asociados con el host. Cada identificador se muestra en el campo **puertos de host**. Si es necesario, también puede eliminar un identificador seleccionando **X** junto a él.

Ajuste	Descripción
Iniciador CHAP	(Opcional) Si seleccionó o introdujo manualmente un puerto de host mediante un IQN iSCSI y desea solicitar la autenticación de un host que intenta acceder a la matriz de almacenamiento mediante un protocolo de autenticación por desafío mutuo (CHAP), seleccione la casilla de verificación **Iniciador CHAP**. Para cada puerto de host iSCSI que seleccione o introduzca manualmente, haga lo siguiente: • Introduzca el mismo secreto CHAP que se estableció en cada iniciador de host iSCSI para la autenticación de CHAP. Si va a utilizar la autenticación CHAP mutuo (autenticación bidireccional que permite la validación de un host en la cabina de almacenamiento y de una cabina de almacenamiento en el host), también debe configurar el secreto CHAP para la cabina de almacenamiento en la configuración inicial o cambiar la configuración. • Deje el campo en blanco si no requiere la autenticación del host. Actualmente, el único método de autenticación de iSCSI que utiliza System Manager es CHAP.

4. Haga clic en **Crear**.

Resultados

Una vez que el host se creó correctamente, el sistema crea un nombre predeterminado para cada puerto de host configurado para el host (etiqueta de usuario).

El alias predeterminado es `<Hostname_Port Number>`. Por ejemplo, el alias predeterminado para el primer puerto creado para `host IPT is IPT_1`.

Cree un clúster de hosts

Se crea un clúster de hosts cuando dos o más hosts requieren acceso de I/o a los mismos volúmenes.

Acerca de esta tarea

Tenga en cuenta estas directrices al crear un clúster de hosts:

- Esta operación no comienza a menos que haya dos o más hosts disponibles para crear el clúster.
- Los hosts de los clústeres de hosts pueden tener sistemas operativos diferentes (heterogéneos).
- Los hosts NVMe en clústeres de hosts no pueden combinarse con hosts que no son NVMe.
- Para crear un volumen que tenga habilitada la función Garantía de datos (DA), la conexión de host que se planea usar debe admitir DA.

  Si alguna de las conexiones de host de las controladoras de la cabina de almacenamiento no admite DA, los hosts asociados no podrán acceder a los datos de los volúmenes con la función DA habilitada.

- Esta operación no funciona si el nombre que eligió ya está en uso.
- La longitud del nombre no puede ser mayor de 30 caracteres.

Pasos

1. Seleccione MENU:Storage[hosts].
2. Seleccione MENU:Create[Host Cluster].

   Se muestra el cuadro de diálogo Crear clúster de hosts.

3. Seleccione la configuración del clúster de hosts que corresponda.

   Detalles del campo

Ajuste	Descripción
Nombre	Escriba un nombre para el clúster de hosts nuevo.
Seleccione los hosts para compartir acceso al volumen	Seleccione dos o más hosts de la lista desplegable. Solo se muestran en la lista los hosts que todavía no forman parte del clúster de hosts.

4. Haga clic en **Crear**.

   Si los hosts seleccionados están conectados a los tipos de interfaz que tienen distintas funcionalidades de Data Assurance (DA), se muestra un cuadro de diálogo con el mensaje de que DA no estará disponible en el clúster de hosts. Esta falta de disponibilidad evita que los volúmenes con la función DA habilitada se añadan al clúster de hosts. Seleccione **Sí** para continuar o **no** para cancelar.

   DA mejora la integridad de los datos en todo el sistema de almacenamiento. DA permite a la cabina de almacenamiento comprobar si se producen errores cuando se transfieren datos entre hosts y unidades. El uso DE DA en el volumen nuevo garantiza la detección de cualquier error.

Resultados

El nuevo clúster de hosts se muestra en la tabla con los hosts asignados en las filas de abajo.

Asignar volúmenes a hosts

Se debe asignar un volumen a un host o un clúster de hosts para poder usarlo con operaciones de I/O. Esta asignación otorga a un host o un clúster de hosts acceso a uno o varios volúmenes en una cabina de almacenamiento.

Acerca de esta tarea

Tenga en cuenta estas directrices al asignar volúmenes a hosts:

- Es posible asignar un volumen a un solo host o clúster de hosts al mismo tiempo.
- Los volúmenes asignados se comparten entre controladoras de la cabina de almacenamiento.
- El host o un clúster de hosts no pueden usar el mismo número de unidad lógica (LUN) dos veces para acceder a un volumen. Se debe usar un LUN único.
- En el caso de los grupos de volúmenes nuevos, si espera hasta que se crean e inicializan todos los volúmenes antes de asignarles un host, se reduce el tiempo de inicialización del volumen. Tenga en cuenta que, una vez asignado un volumen asociado con el grupo de volúmenes, *All* Volumes revertirá la inicialización más lenta. Puede comprobar el progreso de inicialización desde el menú:Inicio[Operaciones

en curso].

La asignación de un volumen falla en las siguientes condiciones:

- Todos los volúmenes están asignados.
- El volumen ya está asignado a otro host o clúster de hosts.

La capacidad para asignar un volumen no está disponible debido a las siguientes condiciones:

- No existen hosts ni clústeres de hosts válidos.
- No se definieron identificadores de puertos para el host.
- Se definieron todas las asignaciones de volúmenes.

Todos los volúmenes sin asignar se muestran durante esta tarea, pero las funciones para hosts con o sin Data Assurance (DA) se aplican de la siguiente manera:

- Para un host compatible con DA, es posible seleccionar volúmenes con o sin LA función DA habilitada.
- Para un host no compatible con DA, si selecciona un volumen con la función DA habilitada, una advertencia indica que el sistema debe desactivar automáticamente DA antes de asignar el volumen al host.

Pasos

1. Seleccione MENU:Storage[hosts].
2. Seleccione el host o clúster de hosts al que desea asignar volúmenes y, a continuación, haga clic en **asignar volúmenes**.

   Se muestra un cuadro de diálogo que enumera todos los volúmenes que pueden asignarse. Puede ordenar cualquiera de las columnas o escribir algo en el cuadro **filtro** para facilitar la búsqueda de volúmenes concretos.

3. Seleccione la casilla de comprobación ubicada junto a cada volumen que desea asignar, o bien seleccione la casilla de comprobación en el encabezado de la tabla para seleccionar todos los volúmenes.
4. Haga clic en **asignar** para completar la operación.

Resultados

Después de asignar correctamente uno o varios volúmenes a un host o un clúster de hosts, el sistema realiza las siguientes acciones:

- El volumen asignado recibe el próximo número de unidad lógica disponible. El host utiliza el número de unidad lógica para acceder al volumen.
- El nombre del volumen proporcionado por el usuario aparece en los listados de volúmenes asociados al host. Si corresponde, el volumen de acceso configurado de fábrica también aparece en los listados de volúmenes asociados al host.

Gestione hosts y clústeres

Cambiar el tipo de host predeterminado

Use la opción de configuración Cambiar el sistema operativo del host predeterminado para cambiar el tipo de host predeterminado en el nivel de la cabina de almacenamiento. En general, se debe cambiar el tipo de host predeterminado antes de conectar hosts a la

cabina de almacenamiento o al añadir hosts adicionales.

Acerca de esta tarea

Tenga en cuenta estas directrices:

- Si todos los hosts que piensa conectar a la cabina de almacenamiento tienen el mismo sistema operativo (entorno de host homogéneo), cambie el tipo de host para que coincida con el sistema operativo.
- Si hay hosts con diferentes sistemas operativos que piensa conectar a la cabina de almacenamiento (entorno de host heterogéneo), cambie el tipo de host para que coincida con la mayoría de los sistemas operativos de los hosts.

  Por ejemplo, si va a conectar ocho hosts diferentes a la cabina de almacenamiento y seis de ellos tienen un sistema operativo Windows, debe seleccionar Windows como tipo de sistema operativo de host predeterminado.

- Si la mayoría de los hosts conectados poseen una combinación de sistemas operativos diferentes, cambie el tipo de host a opción predeterminada de fábrica.

  Por ejemplo, si va a conectar ocho hosts diferentes a la cabina de almacenamiento y dos de ellos tienen un sistema operativo Windows, tres ejecutan un sistema operativo VMware, Y otros tres ejecutan un sistema operativo Linux, debe seleccionar opción predeterminada de fábrica como el tipo de sistema operativo del host predeterminado.

Pasos

1. Seleccione MENU:Settings[System].
2. Desplácese hasta **Configuración adicional** y, a continuación, haga clic en **Cambiar el tipo de sistema operativo del host** predeterminado.
3. Seleccione el tipo de sistema operativo de host que desea usar como predeterminado.
4. Haga clic en **Cambiar**.

Anule la asignación de volúmenes

Anule la asignación de volúmenes de los hosts o clústeres de hosts si ya no necesita acceso a I/o en ese volumen del host o clúster de hosts.

Acerca de esta tarea

Recuerde estas directrices cuando anule la asignación de un volumen:

- Si va a eliminar el último volumen asignado de un clúster de hosts, y el clúster de hosts también tiene hosts con volúmenes específicos asignados, asegúrese de eliminar o mover tales asignaciones antes de eliminar la última asignación para el clúster de hosts.
- Si se asignan un clúster de hosts, un host o un puerto de host a un volumen que está registrado en el sistema operativo, se debe borrar este registro para poder eliminar estos nodos.

Pasos

1. Seleccione MENU:Storage[hosts].
2. Seleccione el host o clúster de hosts que desea editar y, a continuación, haga clic en **Anular asignación de volúmenes**.

   Se muestra un cuadro de diálogo que muestra todos los volúmenes asignados actualmente.

3. Seleccione la casilla de comprobación junto a cada volumen cuya asignación desee anular o seleccione la casilla de comprobación en el encabezado de la tabla para seleccionar todos los volúmenes.
4. Haga clic en **Anular asignación**.

Resultados

- Los volúmenes para los cuales se anuló la asignación están disponibles para una nueva asignación.
- El sistema operativo del host sigue reconociendo el volumen hasta que se configuran los cambios en el host.

Elimine host o clúster de hosts

Es posible eliminar un host o un clúster de hosts.

Acerca de esta tarea

Tenga en cuenta lo siguiente al eliminar un host o un clúster de hosts:

- Se eliminan todas las asignaciones de volúmenes específicas, y los volúmenes asociados están disponibles para una nueva asignación.
- Si el host forma parte de un clúster de hosts que posee sus propias asignaciones específicas, el clúster de hosts no se ve afectado. Sin embargo, si el host forma parte de un clúster de hosts que no tiene ninguna otra asignación, el clúster de hosts y todos los demás hosts o identificadores de puertos de hosts asociados heredan las asignaciones predeterminadas.
- Todos los identificadores de puertos de hosts que se asociaron con el host quedan sin definir.

Pasos

1. Seleccione MENU:Storage[hosts].
2. Seleccione el host o clúster de hosts que desea eliminar y, a continuación, haga clic en **Eliminar**.

   Se muestra un cuadro de diálogo de confirmación.

3. Confirme que desea realizar la operación y, a continuación, haga clic en **Eliminar**.

Resultados

Si eliminó un host, el sistema realiza las siguientes acciones:

- Elimina el host y, si corresponde, lo elimina del clúster de hosts.
- Elimina el acceso a todos los volúmenes asignados.
- Vuelve a colocar los volúmenes asociados en el estado Unassigned.
- Vuelve a colocar todos los identificadores de puerto de host asociados con el host en el estado Unassociated.

Si eliminó un clúster de hosts, el sistema realiza las siguientes acciones:

- Elimina el clúster de hosts y sus hosts asociados (si los hubiera).
- Elimina el acceso a todos los volúmenes asignados.
- Vuelve a colocar los volúmenes asociados en el estado Unassigned.
- Vuelve a colocar todos los identificadores de puerto de host asociados con los hosts en un estado sin asociación.

Establezca la generación de informes de conectividad de host

Es posible habilitar la generación de informes de conectividad de host para que la cabina de almacenamiento supervise constantemente la conexión entre las controladoras y los hosts configurados, y emita alertas si se interrumpe la conexión. Esta función está habilitada de forma predeterminada.

Acerca de esta tarea

Si se deshabilita la generación de informes de conectividad de host, el sistema ya no supervisa la conectividad ni los problemas de los controladores multivía con un host conectado a la cabina de almacenamiento.

> Al deshabilitar la generación de informes de conectividad de host, también se deshabilita el equilibrio de carga automático que supervisa y equilibra la utilización de recursos de la controladora.

Pasos

1. Seleccione MENU:Settings[System].
2. Desplácese hasta **Configuración adicional** y, a continuación, haga clic en **Activar/Desactivar generación de informes de conectividad de host**.

   El texto debajo de esta opción indica si se encuentra habilitada o deshabilitada.

   Se abre un cuadro de diálogo de confirmación.

3. Haga clic en **Sí** para continuar.

   Al seleccionar esta opción, es posible alternar entre habilitar o deshabilitar la función.

Gestionar configuración

Cambiar la configuración de un host

Es posible modificar el nombre, el tipo de sistema operativo del host y los clústeres de hosts asociados de un host.

Pasos

1. Seleccione MENU:Storage[hosts].
2. Seleccione el host que desea editar y, a continuación, haga clic en **Ver/editar configuración**.

   Se muestra un cuadro de diálogo en el que se proporciona la configuración actual de los hosts.

3. Si aún no está seleccionada, haga clic en la ficha **Propiedades**.
4. Cambie la configuración según corresponda.

Detalles del campo

Ajuste	Descripción
Nombre	Es posible modificar el nombre del host provisto por el usuario. Es necesario especificar un nombre para el host.
Clúster de hosts asociado	Es posible elegir una de las siguientes opciones: • **Ninguno** — el host sigue siendo un host independiente. Si el host se asoció a un clúster, el sistema elimina el host de ese clúster. • **<Host Cluster>** — el sistema asocia el host al clúster seleccionado.
Tipo de sistema operativo de host	Es posible modificar la clase de sistema operativo que se ejecuta en el host definido.

5. Haga clic en **Guardar**.

Cambiar la configuración de un clúster de hosts

Es posible cambiar el nombre del clúster de hosts, o bien añadir o eliminar hosts de un clúster.

Pasos

1. Seleccione MENU:Storage[hosts].
2. Seleccione el clúster de hosts que desea editar y, a continuación, haga clic en **Ver/editar configuración**.

   Se muestra un cuadro de diálogo que indica la configuración actual del clúster de hosts.

3. Cambie la configuración del clúster de hosts según sea necesario.

   Detalles del campo

Ajuste	Descripción
Nombre	Es posible especificar el nombre provisto por el usuario del clúster de hosts. Es necesario especificar el nombre de un clúster.
Hosts asociados	Para agregar un host, haga clic en el cuadro **hosts asociados** y, a continuación, seleccione un nombre de host en la lista desplegable. El nombre de host no se puede introducir manualmente. Para eliminar un host, haga clic en **X** junto al nombre de host.

4. Haga clic en **Guardar**.

Cambiar los identificadores de puerto de host para un host

Los identificadores de puerto de host se cambian cuando se desea cambiar la etiqueta de usuario en un identificador de puerto de host, agregar un nuevo identificador de puerto de host al host o eliminar un identificador de puerto de host del host.

Acerca de esta tarea

Cuando se cambian identificadores de puerto de host, se deben tener en cuenta las siguientes directrices:

- **Add** — cuando se agrega un puerto de host, se asocia el identificador de puerto de host al host creado para conectarse a la matriz de almacenamiento. Es posible introducir información manualmente mediante una utilidad de adaptador de bus de host (HBA).
- **Editar** — puede editar los puertos de host para mover (asociar) un puerto de host a otro host. Es posible que se haya movido el adaptador de bus de host o iniciador de iSCSI a otro host, de modo que se debe mover (asociar) el puerto de host al nuevo host.
- **Eliminar** — puede eliminar puertos de host para eliminar (desasociar) puertos de host de un host.

Pasos

1. Seleccione MENU:Storage[hosts].
2. Seleccione el host al que se asociarán los puertos y, a continuación, haga clic en **Ver/editar configuración**.

   Si desea añadir puertos a un host en un clúster de hosts, expanda el clúster de hosts y seleccione el host deseado. No se pueden añadir puertos en el nivel del clúster de hosts.

   Se muestra un cuadro de diálogo en el que se proporciona la configuración actual de los hosts.

3. Haga clic en la ficha **puertos de host**.

   En el cuadro de diálogo, se muestran los identificadores de puerto de host actuales.

4. Cambie la configuración del identificador de puerto de host, según corresponda.

Ajuste	Descripción
Puerto de host	Es posible elegir una de las siguientes opciones: • **Agregar** — Utilice Agregar para asociar un nuevo identificador de puerto de host al host. La longitud del nombre del identificador de puerto de host se determina mediante la tecnología de interfaz del host. Los nombres de identificador de puerto de host de Fibre Channel e Infiniband deben tener 16 caracteres. Los nombres de identificador de puerto de host iSCSI tienen un máximo de 223 caracteres. El puerto debe ser único. No se permite un número de puerto que ya se haya configurado. • **Eliminar** — Utilice Eliminar para eliminar (desasociar) un identificador de puerto de host. La opción Eliminar no quita físicamente el puerto de host. Esta opción elimina la asociación entre el puerto de host y el host. Salvo que se eliminen el adaptador de bus de host o el iniciador de iSCSI, la controladora seguirá reconociendo el puerto de host. Si se elimina el identificador de puerto de host, el identificador ya no sigue asociado a este host. Además, el host pierde acceso a cualquiera de los volúmenes asignados a través de este identificador de puerto de host.
Etiqueta	Para cambiar el nombre de la etiqueta del puerto, haga clic en el icono **Editar** (lápiz). El nombre de etiqueta del puerto debe ser único. No se permite un nombre de etiqueta que ya se haya configurado.
Secreto CHAP	Solo se muestra para los hosts iSCSI. Es posible configurar o cambiar el secreto CHAP para los iniciadores (hosts iSCSI). System Manager usa el método de protocolo de autenticación por desafío mutuo (CHAP), que valida la identidad de los destinos e iniciadores durante el enlace inicial. La autenticación se basa en una clave de seguridad compartida denominada secreto CHAP.

5. Haga clic en **Guardar**.

Preguntas frecuentes

¿Qué son los hosts y los clústeres de hosts?

Un host es un servidor que envía I/o a un volumen de una cabina de almacenamiento. Un clúster de hosts es un grupo de hosts. Se crea un clúster de hosts para facilitar la asignación de los mismos volúmenes en varios hosts.

Un host se define por separado. Puede ser una entidad independiente o añadirse a un clúster de hosts. Es posible asignar volúmenes a un host individual, o bien un host puede formar parte de un clúster de hosts que comparta acceso a un volumen o más con otros hosts del clúster de hosts.

El clúster de hosts es una entidad lógica que se crea en SANtricity System Manager. Se deben añadir hosts al clúster de hosts para poder asignar volúmenes.

¿Por qué debería crear un clúster de hosts?

Debe crear un clúster de hosts si desea que dos o más hosts compartan el acceso al mismo conjunto de volúmenes. Por lo general, los hosts individuales tienen instalado software de clustering a fin de coordinar el acceso a los volúmenes.

¿Cómo saber cuál es el tipo de sistema operativo de host correcto?

El campo Tipo de sistema operativo de host contiene el sistema operativo del host. Es posible seleccionar el tipo de host recomendado en la lista desplegable, o bien permitir que el agente de contexto de host (HCA) configure el host y el tipo de sistema operativo de host adecuado.

Los tipos de hosts que aparecen en la lista desplegable dependen del modelo de cabina de almacenamiento y la versión del firmware. Las versiones más recientes muestran primero las opciones más comunes, que son las más probables ser apropiadas. La aparición en esta lista no implica que la opción esté totalmente admitida.

> Para obtener más información sobre la compatibilidad con hosts, consulte "Herramienta de matriz de interoperabilidad de NetApp".

En la lista pueden aparecer algunos de los siguientes tipos de hosts:

Tipo de sistema operativo de host	Sistema operativo (SO) y controlador multivía
Linux DM-MP (Kernel 3.10 o posterior)	Es compatible con sistemas operativos Linux que utilizan una solución de conmutación por error multivía de Device Mapper con un kernel 3.10 o posterior.
VMware ESXi	Es compatible con los sistemas operativos VMware ESXi que ejecutan la arquitectura nativa del complemento multivía (NMP) mediante el módulo VMware incorporado Storage Array Type Policy SATP_ALUA.
Windows (en clúster o sin clúster)	Admite configuraciones en clúster o no en clúster de Windows que no ejecuten el controlador multivía de ATTO.
Clúster ATTO (todos los sistemas operativos)	Admite todas las configuraciones de clúster con el controlador ATTO Technology, Inc. Y multipathing.
Linux (Veritas DMP)	Admite sistemas operativos Linux mediante una solución multivía Veritas DMP.
Linux (ATTO)	Admite sistemas operativos Linux que usan un controlador ATTO Technology, Inc. Y multiruta.
Mac OS (ATTO)	Admite versiones de Mac OS que usan un controlador ATTO Technology, Inc. Y multipathing.
Windows (ATTO)	Admite sistemas operativos Windows que usan un controlador ATTO Technology, Inc. Y multiruta.

Tipo de sistema operativo de host	Sistema operativo (SO) y controlador multivía
FlexArray (ALUA)	Admite un sistema FlexArray de NetApp mediante ALUA para accesos múltiples.
SVC DE IBM	Es compatible con la configuración de la controladora de volúmenes SAN de IBM.
Predeterminado de fábrica	Reservada para el inicio inicial de la cabina de almacenamiento. Si el tipo de sistema operativo del host está configurado como valor predeterminado de fábrica, cambie este valor para que coincida con el sistema operativo del host y el controlador multivía que se ejecuta en el host conectado.
Linux DM-MP (Kernel 3.9 o anterior)	Es compatible con sistemas operativos Linux que utilizan una solución de conmutación por error multivía de Device Mapper con un kernel 3.9 o anterior.
Ventana en clúster (obsoleto)	Si el tipo de sistema operativo del host está establecido en este valor, utilice la opción Windows (almacenado en clúster o no en clúster).

Después de instalar el HCA y de conectar el almacenamiento al host, el HCA envía la topología del host a la controladoras de almacenamiento a través de la ruta de I/O. Según la topología del host, las controladoras de almacenamiento definen automáticamente el host y los puertos de host asociados para luego establecer el tipo de host.

Si el HCA no selecciona el tipo de host recomendado, debe configurar manualmente el tipo de host.

¿Qué son los HBA y los puertos de adaptador?

Un adaptador de bus de host (HBA) es una placa que se encuentra en un host y tiene uno o más puertos de host. Un puerto de host es un puerto en un adaptador de bus de host (HBA) que facilita la conexión física a una controladora y se usa en operaciones de I/O.

Los puertos de adaptador en el HBA se denominan puertos de host. La mayoría de los HBA tiene uno o dos puertos de host. El HBA tiene un identificador a nivel mundial (WWID) y cada puerto de host de HBA tiene un WWID único. Los identificadores de puertos de host se usan para asociar el HBA adecuado al host físico cuando se crea manualmente el host mediante SANtricity System Manager o se crea automáticamente el host mediante el agente de contexto de host.

¿Cómo se emparejan los puertos de host con un host?

Si se crea manualmente un host, en primer lugar debe usarse la utilidad de adaptador de bus de host (HBA) adecuada disponible en el host para determinar los identificadores de puerto de host asociados con cada HBA instalada en el host.

Cuando cuente con esta información, seleccione los identificadores de puerto de host con los cuales se inició sesión en la cabina de almacenamiento de la lista proporcionada en el cuadro de diálogo Crear host.

> Asegúrese de seleccionar los identificadores de puerto de host adecuados para el host que va a crear. Si asocia los identificadores de puerto de host incorrectos, es posible que se provoque un acceso no intencional de otro host a estos datos.

Si va a crear hosts automáticamente con el agente de contexto de host (HCA) instalado en cada host, el HCA debe asociar automáticamente los identificadores de puerto de host con cada host y configurarlos adecuadamente.

¿Cómo se crean los secretos CHAP?

Si se configuró la autenticación mediante protocolo de autenticación por desafío mutuo (CHAP) en cualquier host iSCSI conectado a la cabina de almacenamiento, debe volver a introducir el secreto CHAP de ese iniciador para cada host iSCSI.

Para hacerlo, es posible usar System Manager como parte de la operación Create Host o a través de la opción Ver/editar configuración.

Si se utiliza la autenticación mutua de CHAP, también debe definirse un secreto CHAP para la cabina de almacenamiento en la página Configuración y volver a introducirse ese secreto CHAP de destino en cada host iSCSI.

¿Qué es el clúster predeterminado?

El clúster predeterminado es una entidad definida por el sistema que permite que cualquier identificador de puerto de host no asociado que haya iniciado sesión en la cabina de almacenamiento acceda a los volúmenes asignados al clúster predeterminado. Un identificador de puerto de host no asociado es un puerto de host que no está asociado de forma lógica con un host en particular, pero se instala físicamente en un host y se inicia sesión en la cabina de almacenamiento.

> Si desea que los hosts tengan acceso específico a ciertos volúmenes en la cabina de almacenamiento, se debe *no* utilizar el clúster predeterminado. En cambio, se deben asociar los identificadores del puerto de host con sus hosts correspondientes. Esta tarea puede realizarse de forma manual durante la operación Create Host, o bien de forma automática mediante el agente de contexto de host (HCA) instalado en cada host. A continuación, se deben asignar los volúmenes a un host individual o a un clúster de hosts.

Se debe *solo* usar el clúster predeterminado en situaciones especiales en las que el entorno de almacenamiento externo sea propicio para permitir que todos los hosts y todos los identificadores de puerto de host con sesión iniciada conectados a la cabina de almacenamiento tengan acceso a todos los volúmenes (modo de acceso total) sin dar a conocer específicamente los hosts a la cabina de almacenamiento o a la interfaz de usuario.

Inicialmente, se pueden asignar los volúmenes solo al clúster predeterminado a través de la interfaz de línea de comandos (CLI). Sin embargo, luego de asignar al menos un volumen al clúster predeterminado, esta entidad (denominada clúster predeterminado) se muestra en la interfaz de usuario donde podrá gestionar esta entidad.

¿Qué es la generación de informes de conectividad de host?

Cuando la opción de generación de informes de conectividad de host está habilitada, la

cabina de almacenamiento supervisa continuamente la conexión entre las controladoras y los hosts configurados, y luego notifica si se interrumpió la conexión.

Pueden producirse interrupciones en la conexión si hay algún cable suelto, dañado o faltante, o si hay otro problema con el host. En estas situaciones, es posible que el sistema abra un mensaje de Recovery Guru:

- **Pérdida de redundancia del host** — se abre si alguno de los controladores no puede comunicarse con el host.
- **Tipo de host incorrecto** — se abre si el tipo de host se ha especificado incorrectamente en la matriz de almacenamiento, lo que podría dar lugar a problemas de conmutación por error.

Puede ser conveniente deshabilitar la generación de informes de conectividad de host cuando la operación de reinicio de una controladora puede demorar más que el tiempo de espera de conexión. Cuando se deshabilita esta función, se suprimen los mensajes de Recovery Guru.

> Además, al deshabilitar la generación de informes de conectividad de host también se deshabilita el equilibrio de carga automático, que supervisa y equilibra el uso de recursos de la controladora. Sin embargo, si se vuelve a habilitar la generación de informes de conectividad de host, la función de equilibrio de carga automático no se vuelve a habilitar automáticamente.

Snapshot

Información general de Snapshot

La función Snapshot permite crear imágenes de un momento específico de los volúmenes de una cabina de almacenamiento y utilizarlas para realizar backups o pruebas.

¿Qué son las imágenes Snapshot?

Un *snapshot image* es una copia lógica de datos de volúmenes capturados en un momento específico. Al igual que un punto de restauración, las imágenes Snapshot permiten revertir a un conjunto de datos bien conocidos. Si bien el host puede acceder a la imagen Snapshot, no puede leer ni escribir allí directamente.

Obtenga más información:

- "Cómo funciona el almacenamiento Snapshot"
- "Terminología Snapshot"
- "Volúmenes base, capacidad reservada y grupos Snapshot"
- "Programaciones Snapshot y grupos de coherencia"
- "Volúmenes Snapshot"

¿Cómo se crean las snapshots?

Es posible crear manualmente una imagen Snapshot desde un volumen base o un grupo de coherencia Snapshot. Este procedimiento está disponible en el menú:almacenamiento[instantáneas].

Obtenga más información:

- "Requisitos y directrices para Snapshot"

- "Flujo de trabajo para crear imágenes y volúmenes Snapshot"
- "Crear una imagen Snapshot"
- "Programar imágenes Snapshot"
- "Crear un grupo de coherencia Snapshot"
- "Crear un volumen Snapshot"

¿Cómo revertir los datos de una copia Snapshot?

Un *rollback* es el proceso de devolver los datos de un volumen base a un momento específico anterior. Es posible revertir los datos de las instantáneas desde MENU:Storage[Snapshots].

Obtenga más información:

- "Reversión Snapshot"
- "Iniciar una reversión de imagen Snapshot para un volumen base"
- "Iniciar una reversión de imagen Snapshot para un miembro del grupo de coherencia"

Información relacionada

Obtenga más información acerca de las tareas relacionadas con las instantáneas:

- "Cambiar la capacidad reservada para un volumen Snapshot"
- "Cambiar la capacidad reservada de un grupo Snapshot"

Conceptos

Cómo funciona el almacenamiento Snapshot

La función Snapshot utiliza la tecnología copy-on-write para almacenar imágenes Snapshot y utilizar la capacidad reservada asignada.

Cómo se utilizan las imágenes Snapshot

Una imagen Snapshot es una copia lógica de solo lectura del contenido de un volumen capturado en un momento particular en el tiempo. Es posible usar Snapshot para protegerse contra la pérdida de datos.

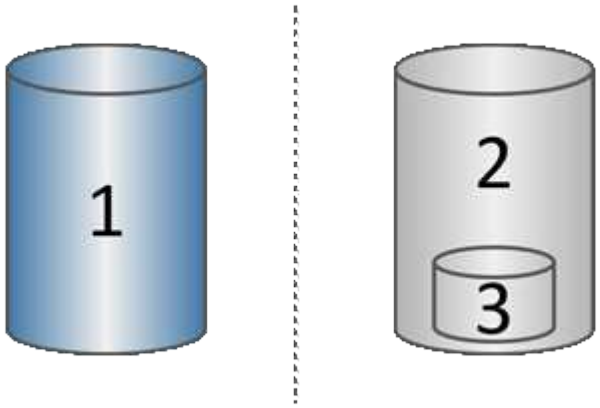
Las imágenes Snapshot también son útiles para los entornos de prueba. Mediante la creación de una copia virtual de los datos, es posible probar los datos mediante la Snapshot sin alterar el volumen. Además, los hosts no tienen acceso de escritura a imágenes Snapshot, por lo que las Snapshot siempre son un recurso de backup seguro.

Creación de Snapshot

A medida que se crean Snapshot, la función Snapshot almacena datos de imágenes de la siguiente manera:

- Cuando se crea una imagen Snapshot, la imagen coincide exactamente con el volumen base. La función Snapshot utiliza la tecnología copy-on-write. Después de realizar la Snapshot, la primera escritura en cualquier bloque o conjunto de bloques en el volumen base provoca la copia de los datos originales en la capacidad reservada antes de la escritura de los datos nuevos en el volumen base.
- Las Snapshot posteriores incluyen solo bloque de datos modificados. Antes de sobrescribir los datos en el

volumen base, la función Snapshot utiliza su tecnología copy-on-write para guardar las imágenes requeridas de los sectores afectados en la capacidad reservada de la Snapshot.



Volumen base de esta aplicación 1 (capacidad física del disco); 2 Snapshots (capacidad lógica del disco); capacidad reservada de esta aplicación 3 (capacidad física del disco)

- La capacidad reservada almacena bloques de datos originales para las porciones del volumen base que se modificaron después de realizar la Snapshot, e incluye un índice para realizar un seguimiento de los cambios. Por lo general, el tamaño de la capacidad reservada es el 40 % del volumen base de manera predeterminada. (Si se necesita más capacidad reservada, es posible aumentarla.)
- Las imágenes Snapshot se almacenan en un orden específico según su Marca de hora. Solo la imagen Snapshot más antigua de un volumen base está disponible para su eliminación manual.

Restauración de Snapshot

Para restaurar datos en un volumen base, es posible usar un volumen Snapshot o una imagen Snapshot:

- **Volumen Snapshot** — Si necesita recuperar archivos eliminados, cree un volumen de instantáneas a partir de una imagen Snapshot en buen estado y, a continuación, asígnela al host.
- **Imagen Snapshot** — Si necesita restaurar un volumen base a un momento específico, utilice una imagen Snapshot anterior para revertir los datos al volumen base.

Terminología Snapshot

Conozca la forma en que los términos Snapshot se aplican a su cabina de almacenamiento.

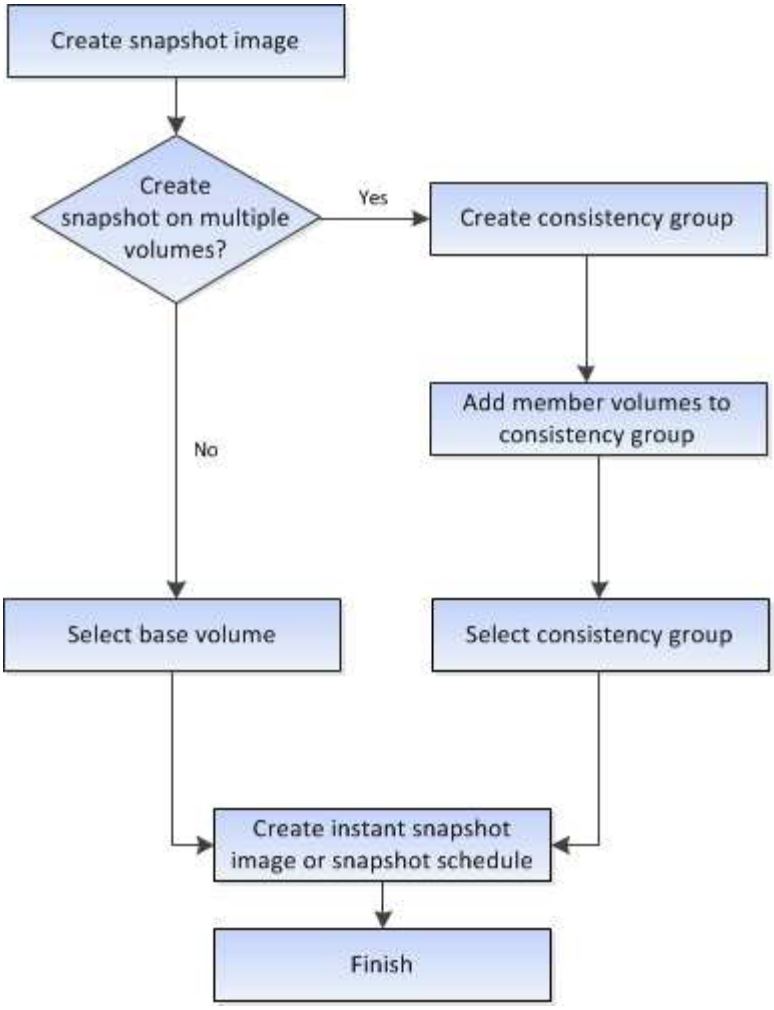
Duración	Descripción
Función Snapshot	La función Snapshot se usa para crear y gestionar imágenes de volúmenes.
Imagen Snapshot	Una imagen Snapshot es una copia lógica de datos de volúmenes capturados en un momento específico. Al igual que un punto de restauración, las imágenes Snapshot permiten revertir a un conjunto de datos bien conocidos. Si bien el host puede acceder a la imagen Snapshot, no puede leer ni escribir allí directamente.

Duración	Descripción
Volumen base	Un volumen base es el origen desde el cual se crea una imagen Snapshot. Puede ser un volumen grueso o fino y, por lo general, se asigna a un host. El volumen base puede residir en un grupo de volúmenes o un pool de discos.
Volumen Snapshot	Un volumen Snapshot permite que el host acceda a los datos de la imagen Snapshot. El volumen Snapshot tiene su propia capacidad reservada que almacena cualquier modificación del volumen base sin afectar a la imagen Snapshot original.
Grupo Snapshot	Un grupo Snapshot es una recogida de imágenes Snapshot de un volumen base único.
Volumen de capacidad reservada	Un volumen de capacidad reservada rastrea qué bloques de datos del volumen base se sobrescribieron y el contenido conservado de esos bloques.
Programación Snapshot	Una programación Snapshot es un cronograma para crear imágenes Snapshot automatizadas. A través de la programación, se puede controlar la frecuencia de la creación de imágenes.
Grupo de coherencia Snapshot	Un grupo de coherencia Snapshot es una recogida de volúmenes que se tratan como una entidad única cuando se crea una imagen Snapshot. Cada uno de estos volúmenes tiene su propia imagen Snapshot, pero todas las imágenes se crean en el mismo momento específico.
Volumen miembro del grupo de coherencia Snapshot	Cada volumen que pertenece a un grupo de coherencia Snapshot se denomina volumen miembro. Si se añade un volumen a un grupo de coherencia Snapshot, System Manager automáticamente crea un grupo Snapshot nuevo que corresponde a este volumen miembro.
Revertir	Una reversión es el proceso de regresar los datos del volumen base a un momento específico anterior.
Capacidad reservada	La capacidad reservada es la capacidad física asignada que se usa para cualquier operación de servicio de copia y objeto de almacenamiento. El host no puede leerla directamente.

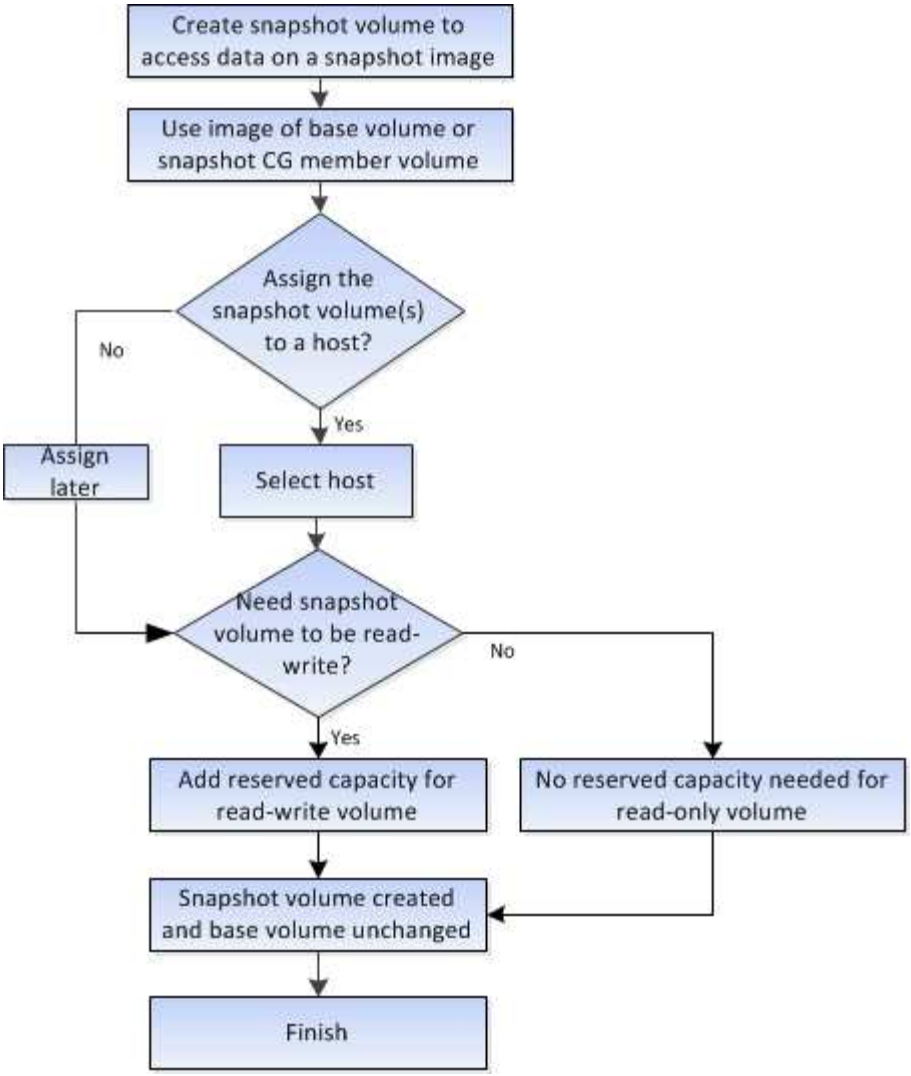
Flujo de trabajo para crear imágenes Snapshot y volúmenes de snapshots

En System Manager, se pueden crear imágenes y volúmenes Snapshot mediante los pasos siguientes.

Flujo de trabajo para crear imágenes de snapshots



Flujo de trabajo para crear volúmenes de snapshots



Requisitos y directrices para Snapshot

Al crear y utilizar Snapshot, revise los siguientes requisitos y directrices.

Imágenes Snapshot y grupos Snapshot

- Cada imagen Snapshot se asocia con exactamente un grupo Snapshot.
- Se crea un grupo Snapshot la primera vez que se crea una imagen Snapshot instantánea o programada para un objeto asociado. Esto genera capacidad reservada.

  Es posible ver los grupos Snapshot en la página Pools y grupos de volúmenes.

- No se producen imágenes Snapshot programadas cuando la cabina de almacenamiento se encuentra apagada o sin conexión.
- Si se elimina un grupo Snapshot que contiene una programación Snapshot, también se elimina esa programación.
- Si existe un volumen Snapshot que ya no se necesita, es posible reutilizarlo, junto con la capacidad reservada asociada, en lugar de eliminarlo. Esto crea un volumen Snapshot diferente del mismo volumen base. Es posible volver a asociar el volumen Snapshot o el volumen Snapshot de grupo de coherencia Snapshot a la misma imagen Snapshot o una diferente, siempre y cuando la imagen Snapshot se encuentre en el mismo volumen base.

Grupo de coherencia Snapshot

- Un grupo de coherencia Snapshot contiene un grupo Snapshot para cada volumen miembro del grupo de coherencia Snapshot.
- Es posible asociar un grupo de coherencia Snapshot con una sola programación.
- Si se elimina un grupo de coherencia Snapshot que contiene una programación Snapshot, también se elimina esa programación.
- No se puede gestionar de forma individual un grupo Snapshot asociado a un grupo de coherencia Snapshot. En lugar de eso, se deben ejecutar las operaciones de gestión (crear una imagen Snapshot, eliminar una imagen Snapshot o un grupo Snapshot y revertir la imagen Snapshot) en el nivel del grupo de coherencia Snapshot.

Volumen base

- Un volumen Snapshot debe tener la misma configuración de Data Assurance (DA) y seguridad que el volumen base asociado.
- No se puede crear un volumen Snapshot a partir de un volumen base con errores.
- Si el volumen base reside en un grupo de volúmenes, los volúmenes miembro de cualquier grupo de coherencia Snapshot asociado pueden residir en un pool o un grupo de volúmenes.
- Si un volumen reside en un pool, todos los volúmenes miembro de cualquier grupo de coherencia Snapshot asociado deben residir en el mismo pool que el volumen base.

Capacidad reservada

- La capacidad reservada se asocia a un solo volumen base.
- El uso de una programación puede generar grandes cantidades de imágenes Snapshot. Asegúrese de contar con suficiente capacidad reservada para las Snapshot programadas.
- El volumen de capacidad reservada para un grupo de coherencia Snapshot debe tener la misma configuración de Data Assurance (DA) y seguridad que el volumen base asociado para el volumen miembro del grupo de coherencia Snapshot.

Imágenes Snapshot pendientes

La creación de una imagen Snapshot puede permanecer en estado pendiente en las siguientes condiciones:

- El volumen base que contiene la imagen Snapshot es miembro de un grupo de reflejos asíncronos.
- El volumen base está realizando una operación de sincronización. La creación de imágenes Snapshot finaliza apenas se completa la operación de sincronización.

Cantidad máxima de imágenes Snapshot

- Si un volumen es miembro de un grupo de coherencia Snapshot, System Manager crea un grupo Snapshot para ese volumen miembro. Este grupo Snapshot cuenta para la cantidad máxima permitida de grupos Snapshot por volumen base.
- Si intenta crear una imagen Snapshot en un grupo Snapshot o un grupo de coherencia Snapshot, pero el grupo asociado alcanzó la cantidad máxima de imágenes Snapshot, tiene dos opciones:
  - Habilite la eliminación automática para el grupo Snapshot o el grupo de coherencia Snapshot.
  - Elimine manualmente una o más imágenes Snapshot del grupo Snapshot o del grupo de coherencia Snapshot y vuelva a intentar la operación.

Eliminación automática

Si se habilitó la eliminación automática en el grupo Snapshot o el grupo de coherencia Snapshot, cuando el sistema crea una imagen Snapshot nueva para el grupo, System Manager elimina la imagen más antigua.

Operación de reversión

- No se pueden realizar las siguientes acciones con una operación de reversión en curso:
  - Eliminar la imagen Snapshot que se está utilizando para la reversión
  - Crear una imagen Snapshot nueva para un volumen base que está participando en una operación de reversión
  - Modificar la política de repositorio lleno del grupo Snapshot asociado
- No se puede iniciar una operación de reversión si hay alguna de estas operaciones en curso:
  - Ampliación de capacidad (añadir capacidad a un pool o un grupo de volúmenes)
  - Expansión de volumen (aumentar la capacidad de un volumen)
  - Cambio de nivel de RAID de un grupo de volúmenes
  - Cambio de tamaño de los segmentos de un volumen
- No se puede iniciar una operación de reversión si el volumen base está participando en una copia de volumen.
- No se puede iniciar una operación de reversión si el volumen base es un volumen secundario en un reflejo remoto.
- Se produce un error en la operación de reversión si la capacidad utilizada en el volumen del repositorio Snapshot asociado contiene sectores ilegibles.

Volúmenes base, capacidad reservada y grupos Snapshot

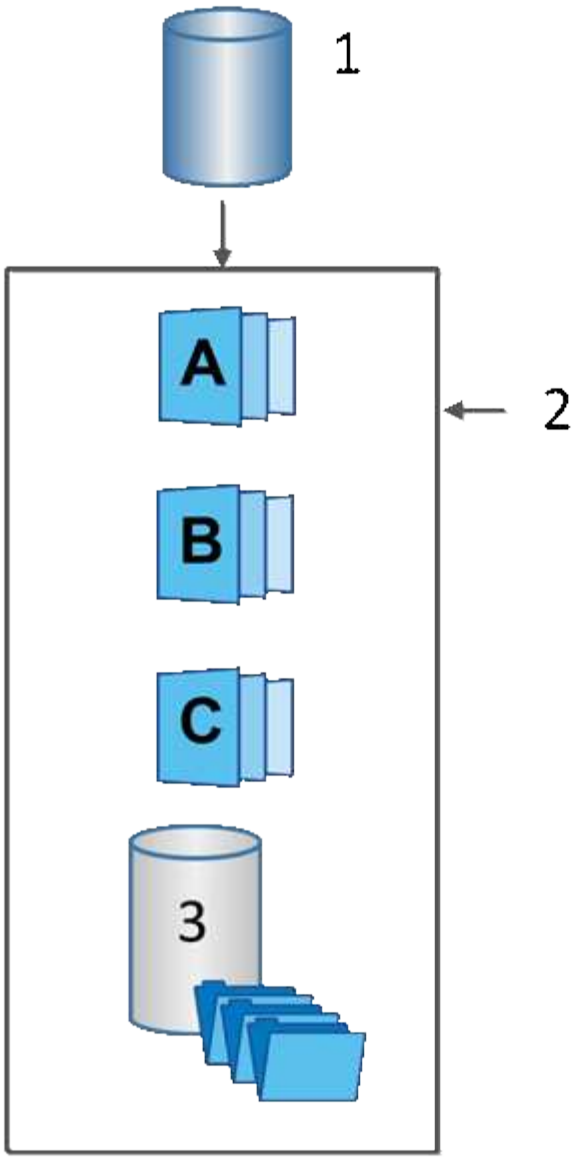
La función Snapshot utiliza volúmenes base, capacidad reservada y grupos Snapshot.

Volúmenes base

Un *volumen base* es el volumen utilizado como origen de una imagen Snapshot. Un volumen base puede ser un volumen grueso o un volumen fino, y puede residir en un pool o un grupo de volúmenes.

Para realizar Snapshot del volumen base, es posible crear una imagen instantánea en cualquier momento, o bien se puede automatizar el proceso definiendo una programación regular para las Snapshot.

En la siguiente figura, se muestra la relación entre los objetos Snapshot y el volumen base.



Volumen base de esta aplicación 1; estos 2 objetos Snapshot en el grupo (imágenes y capacidad reservada); Microsoft 3 capacidad reservada para el grupo Snapshot.

Capacidad reservada y grupos Snapshot

System Manager organiza las imágenes Snapshot en *grupos Snapshot*. Cuando System Manager establece el grupo Snapshot, crea automáticamente una capacidad *reservada* asociada para contener las imágenes Snapshot del grupo y realizar un seguimiento de los futuros cambios en las Snapshot adicionales.

Si el volumen base reside en un grupo de volúmenes, la capacidad reservada puede ubicarse en un pool o un grupo de volúmenes. Si el volumen base reside en un pool, la capacidad reservada debe ubicarse en el mismo pool que el volumen base.

Los grupos Snapshot no requieren ninguna acción del usuario, pero se puede ajustar la capacidad de un grupo Snapshot en cualquier momento. Además, es posible que se muestre un mensaje para crear capacidad reservada cuando se cumplan las siguientes condiciones:

- Siempre que se realiza una Snapshot de un volumen base que no tiene grupo Snapshot, System Manager

crea automáticamente un grupo Snapshot. Esta acción también crea capacidad reservada para el volumen base que se utiliza para almacenar las futuras imágenes Snapshot.

- Siempre que se crea una programación Snapshot para un volumen base, System Manager crea automáticamente un grupo Snapshot.

Eliminación automática

Al trabajar con Snapshot, utilice la opción predeterminada para activar la eliminación automática. La eliminación automática elimina automáticamente la imagen Snapshot más antigua cuando el grupo Snapshot llega al límite de 32 imágenes. Si se desactiva la eliminación automática, los límites del grupo Snapshot se superarán en algún momento, y deberá realizar acciones manuales para configurar las opciones del grupo Snapshot y gestionar la capacidad reservada.

Programaciones Snapshot y grupos de coherencia Snapshot

Utilice programaciones para recoger imágenes Snapshot y utilice grupos de coherencia Snapshot para gestionar varios volúmenes base.

Para gestionar de forma fácil las operaciones Snapshot en volúmenes base, es posible utilizar las siguientes funciones:

- **Horario de instantánea** — automatizar las instantáneas para un solo volumen base.
- **Grupo de consistencia de instantánea** — Administrar varios volúmenes base como una sola entidad.

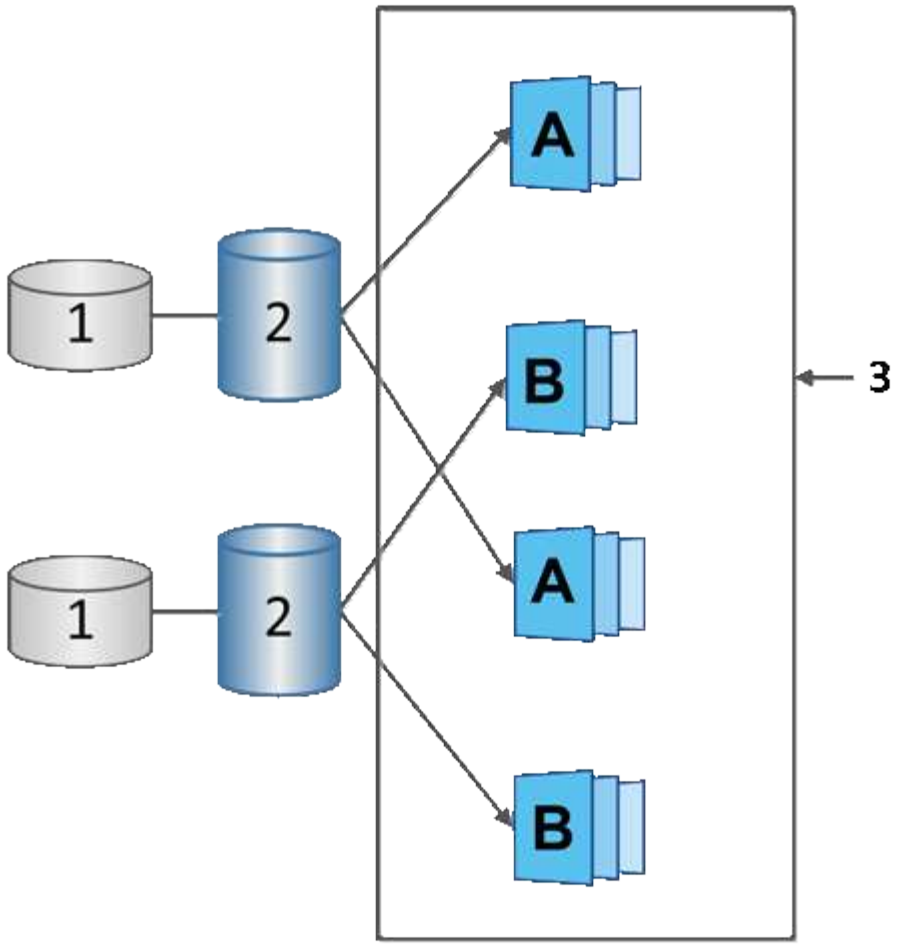
Programación Snapshot

Si desea capturar Snapshot automáticamente para un volumen base, puede crear una programación. Por ejemplo, puede definir una programación para capturar imágenes Snapshot todos los sábados a la medianoche, el primer día de cada mes o en las fechas y los horarios que decida. Al alcanzar el máximo de 32 Snapshot para una sola programación, puede suspender las Snapshot programadas, aumentar la capacidad reservada o eliminar Snapshot. Es posible eliminar Snapshot manualmente o mediante la automatización del proceso de eliminación. Cuando se elimina una imagen Snapshot, se puede reutilizar la capacidad reservada adicional disponible.

Grupo de coherencia Snapshot

Si desea que se capturen imágenes Snapshot de varios volúmenes al mismo tiempo, puede crear un grupo de coherencia Snapshot. Las acciones de imágenes Snapshot se realizan en el grupo de coherencia Snapshot en conjunto. Por ejemplo, puede programar Snapshot sincronizadas de todos los volúmenes con la misma Marca de hora. Los grupos de coherencia Snapshot son ideales para las aplicaciones que abarcan varios volúmenes, como las aplicaciones de base de datos que almacenan los registros en un volumen y los archivos de base de datos en otro volumen.

Los volúmenes incluidos en un grupo de coherencia Snapshot se denominan volúmenes miembro. Cuando se añade un volumen a un grupo de coherencia System Manager genera automáticamente capacidad reservada nueva equivalente a ese volumen miembro. Puede definir una programación para crear de forma automática una imagen Snapshot para cada volumen miembro.



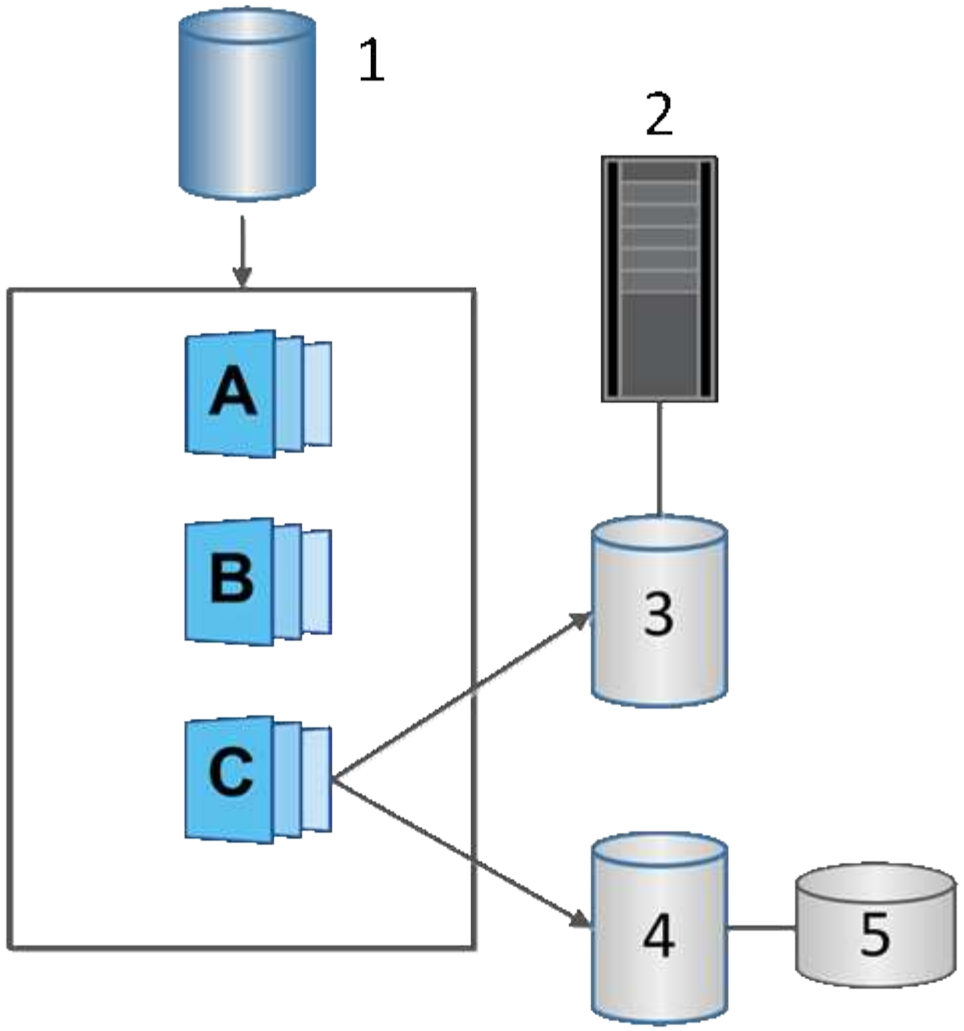
Esta 1 capacidad reservada; este 2 volumen miembro; e imágenes Snapshot de grupo de coherencia de aplicaciones 3

Volúmenes Snapshot

Es posible crear un volumen Snapshot y asignarlo a un host para leer o escribir datos Snapshot. El volumen Snapshot comparte las mismas características que el volumen base (nivel de RAID, características de I/o, etc.).

Al crear un volumen Snapshot, es posible designarlo como *Read-only* o *Read-write Accessible*.

Cuando se crean volúmenes Snapshot de solo lectura, no es necesario añadir capacidad reservada. Cuando se crean volúmenes Snapshot de lectura/escritura, es necesario añadir capacidad reservada para proporcionar acceso de escritura.



Volumen base de esta aplicación; servidor de aplicaciones 2; volumen Snapshot de sólo lectura de 3; volumen Snapshot de lectura y escritura de 4; capacidad reservada de esta versión 5

Reversión Snapshot

Una operación de reversión vuelve a colocar un volumen base en el estado anterior, determinada por la snapshot seleccionada.

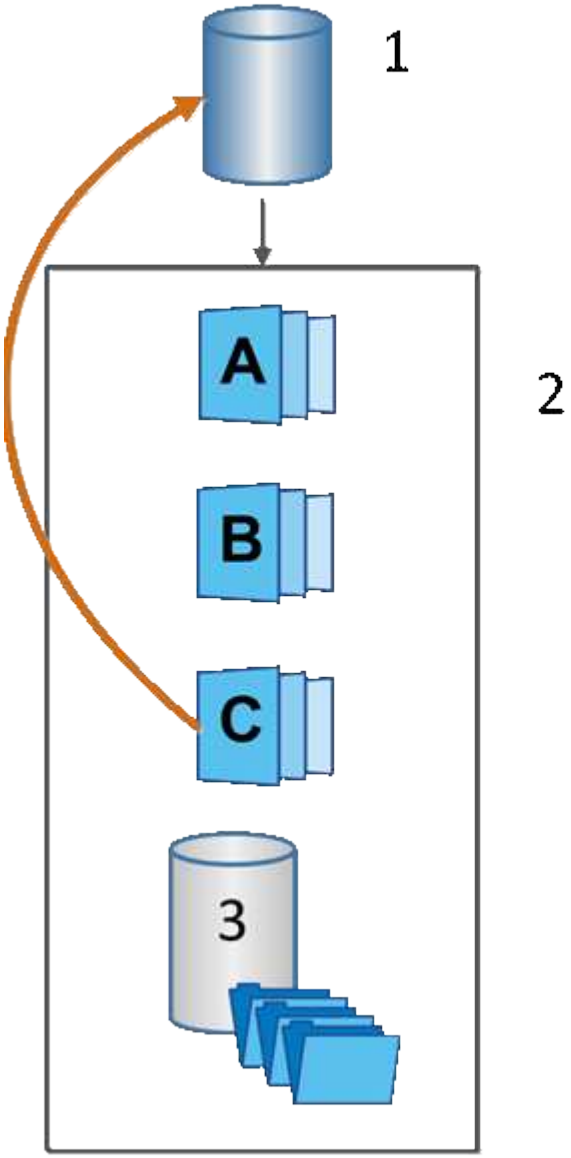
Para una reversión, es posible seleccionar una imagen Snapshot de uno de los siguientes orígenes:

- **Reversión de imagen Snapshot**, para una restauración completa de un volumen base.
- **Reversión de grupo de coherencia Snapshot**, que se puede utilizar para revertir uno o más volúmenes.

Durante una reversión, la función Snapshot conserva todas las imágenes Snapshot del grupo. Con esta función, el host puede acceder al volumen base durante el proceso, si es necesario para operaciones de I/O.

Cuando se inicia una reversión, un proceso en segundo plano revisa las direcciones de bloque lógico (LBA) para el volumen base y busca datos de copia en escritura en la imagen Snapshot de reversión que se desea restaurar. Como el host tiene acceso de lectura y escritura al volumen base, y todos los datos escritos previamente se encuentran disponibles de inmediato, el volumen de capacidad reservada debe ser suficientemente grande como para alojar todos los cambios durante el procesamiento de la reversión. La

transferencia de datos continúa como una operación en segundo plano hasta que se completa la reversión.



Volumen base de esta aplicación; estos 2 objetos Snapshot en un grupo; capacidad reservada de este grupo de copias Snapshot de 3

Crear Snapshot y objetos Snapshot

Crear una imagen Snapshot

Es posible crear manualmente una imagen Snapshot desde un volumen base o un grupo de coherencia Snapshot. Esto también se denomina *instantánea* o *instantánea*.

Antes de empezar

- El estado del volumen base debe ser óptima.
- El estado de la unidad debe ser Optimal.
- El grupo de instantáneas no podrá designarse como «citado».

- El volumen de capacidad reservada debe tener la misma configuración de Data Assurance (DA) que el volumen base asociado para el grupo Snapshot.

Pasos

1. Debe realizar una de las siguientes acciones para crear una imagen Snapshot:
    - Seleccione MENU:Storage[Volumes]. Seleccione el objeto (volumen base o grupo de coherencia Snapshot) y, luego, seleccione menú:Servicios de copia[Crear snapshot instantánea].
    - Seleccione MENU:Storage[Snapshots]. Seleccione la ficha **Imágenes Snapshot** y, a continuación, elija menú:Crear[instantánea].

      Se muestra el cuadro de diálogo Crear imagen Snapshot. Seleccione el objeto (volumen base o grupo de coherencia Snapshot) y haga clic en **Siguiente**. Si se creó una imagen Snapshot anterior para el volumen o grupo de coherencia Snapshot, el sistema crea una Snapshot instantánea de inmediato. De lo contrario, si es la primera vez que se crea una imagen Snapshot para el volumen o el grupo de coherencia Snapshot, se muestra el cuadro de diálogo Confirmar creación de imagen Snapshot.

2. Haga clic en **Crear** para aceptar la notificación de que se necesita capacidad reservada y continuar con el paso Reservar capacidad.

   Se muestra el cuadro de diálogo Reservar capacidad.

3. Utilice el cuadro de desplazamiento para ajustar el porcentaje de capacidad y, a continuación, haga clic en **Siguiente** para aceptar el volumen del candidato destacado en la tabla.

   Se muestra el cuadro de diálogo Editar configuración.

4. Seleccione la configuración para la imagen Snapshot que corresponda y confirme que desea realizar la operación.

Detalles del campo

Ajuste	Descripción
Ajustes de imagen Snapshot	Límite de la imagen Snapshot
Deje seleccionada la casilla de comprobación si desea que las imágenes Snapshot se eliminen automáticamente después del límite especificado; use el cuadro de desplazamiento para cambiar el límite. Si desmarca esta casilla de comprobación, la creación de imágenes Snapshot se detiene después de 32 imágenes.	**Ajustes de capacidad reservada**
Enviarme una alerta cuando…	Use el cuadro de desplazamiento para ajustar el valor del porcentaje en el cual el sistema envía una notificación de alerta cuando la capacidad reservada para un grupo Snapshot está casi completa. Cuando la capacidad reservada para el grupo Snapshot supera el umbral específico, use los avisos por adelantado para aumentar la capacidad reservada o eliminar los objetos innecesarios antes de quedarse sin espacio.
Política para capacidad reservada completa	Seleccione una de las siguientes políticas: • **Purga la imagen Snapshot más antigua** — el sistema purga automáticamente la imagen Snapshot más antigua del grupo Snapshot, lo que libera la capacidad reservada de la imagen Snapshot para su reutilización dentro del grupo. • **Rechazar escrituras en volumen base**: Cuando la capacidad reservada alcanza el porcentaje máximo definido, el sistema rechaza cualquier solicitud de escritura de I/o en el volumen base que activó el acceso a la capacidad reservada.

Resultados

- System Manager muestra la imagen Snapshot nueva en la tabla Imágenes Snapshot. En la tabla, se muestra la imagen nueva según la Marca de hora y el volumen base o el grupo de coherencia Snapshot asociado.

- Si la creación Snapshot queda en estado Pending, se debe a las siguientes condiciones:
  - El volumen base que contiene la imagen Snapshot es miembro de un grupo de reflejos asíncronos.
  - El volumen base está realizando una operación de sincronización. La creación de imágenes Snapshot finaliza apenas se completa la operación de sincronización.

Programar imágenes Snapshot

Es posible crear una programación Snapshot para habilitar la recuperación por un problema con el volumen base y para ejecutar backups programados. Se pueden crear Snapshot de volúmenes base o grupos de coherencia Snapshot a diario, semanal o mensualmente, a cualquier hora del día.

Antes de empezar

El estado del volumen base debe ser óptima.

Acerca de esta tarea

En esta tarea, se describe la forma de crear una programación Snapshot para un volumen base o un grupo de coherencia Snapshot existente.

> También se puede crear una programación Snapshot en el mismo momento que se crea una imagen Snapshot de un volumen base o un grupo de coherencia Snapshot.

Pasos

1. Realice una de las siguientes acciones para crear una programación Snapshot:
   - Seleccione MENU:Storage[Volumes].

     Seleccione el objeto (volumen o grupo de coherencia Snapshot) para esta programación Snapshot y haga clic en **Servicios de copia › Crear programación Snapshot**.

   - Seleccione MENU:Storage[Snapshots].

     Seleccione la ficha **programas** y haga clic en **Crear**.

2. Seleccione el objeto (volumen o grupo de coherencia Snapshot) para esta programación Snapshot y haga clic en **Siguiente**.

   Se muestra el cuadro de diálogo Crear programación Snapshot.

3. Realice una de las siguientes acciones:

   - **Utilice una programación definida anteriormente de otro objeto de instantánea**.

     Asegúrese de que se muestren las opciones avanzadas. Haga clic en **Mostrar más opciones**. Haga clic en **Importar programación**, seleccione el objeto con la programación que desea importar y, a continuación, haga clic en **Importar**.

   - **Modificar las opciones básicas o avanzadas**.

     En la esquina superior derecha del cuadro de diálogo, haga clic en **Mostrar más opciones** para ver todas las opciones y, a continuación, consulte la siguiente tabla.

Detalles del campo

Campo	Descripción
Ajustes básicos	Seleccione días
Seleccione días individuales de la semana para las imágenes Snapshot.	Hora de inicio
En la lista desplegable, seleccione una nueva hora de inicio para las Snapshot diarias (se proporcionan opciones en incrementos de media hora). La hora de inicio predeterminada es media hora antes de la hora actual.	Zona horaria
En la lista desplegable, seleccione la zona horaria de su cabina.	**Ajustes avanzados**
Día / mes	Seleccione una de las siguientes opciones: • **Diario / Semanal** — Seleccione días individuales para la sincronización de instantáneas. También puede seleccionar la casilla de verificación **Seleccionar todos los días** en la parte superior derecha si desea una programación diaria. • **Mensual / Anual** — Seleccione meses individuales para las instantáneas de sincronización. En el campo **el día**, introduzca los días del mes para ejecutar las sincronizaciones. Las entradas válidas son de **1** a **31** y **último**. Puede separar varios días con coma o punto y coma. Utilice un guion para indicar fechas inclusivas. Por ejemplo: 1,3,4,10-15,último. También puede seleccionar la casilla de verificación **Seleccionar todos los meses** en la parte superior derecha si desea una programación mensual.
Hora de inicio	En la lista desplegable, seleccione una nueva hora de inicio para las Snapshot diarias (se proporcionan opciones en incrementos de media hora). La hora de inicio predeterminada es media hora antes de la hora actual.
Zona horaria	En la lista desplegable, seleccione la zona horaria de su cabina.

Campo	Descripción
Snapshot por día/tiempo entre snapshots	Seleccione la cantidad de imágenes Snapshot que desea crear por día. Si selecciona más de una, seleccione también la hora entre una imagen Snapshot y otra. Si desea crear varias imágenes Snapshot, asegúrese de disponer de capacidad reservada suficiente.
Crear imagen Snapshot ahora mismo?	Seleccione esta casilla de comprobación para crear una imagen instantánea además de las imágenes automáticas programadas.
Start/End date o no end date	Introduzca la fecha de inicio para que comiencen las sincronizaciones. Introduzca también una fecha de finalización o seleccione **sin fecha de finalización**.

4. Realice una de las siguientes acciones:
   - Si el objeto es un grupo de coherencia de instantánea, haga clic en **Crear** para aceptar la configuración y crear la programación.
   - Si el objeto es un volumen, haga clic en **Siguiente** para asignar capacidad reservada a las imágenes Snapshot.

     En la tabla Volume Candidate, solo se muestran los candidatos que admiten la capacidad reservada especificada. La capacidad reservada es la capacidad física asignada que se usa para cualquier operación de servicio de copia y objeto de almacenamiento. El host no puede leerla directamente.
5. Utilice el cuadro de desplazamiento para asignar capacidad reservada a las imágenes Snapshot. Realice una de las siguientes acciones:
   - **Acepte la configuración predeterminada.**

     Utilice esta opción recomendada para asignar capacidad reservada a las imágenes Snapshot con la configuración predeterminada.
   - **Asigne su propia configuración de capacidad reservada para satisfacer sus necesidades de almacenamiento de datos.**

     Si cambia los ajustes predeterminados de capacidad reservada, haga clic en **Actualizar candidatos** para actualizar la lista de candidatos de la capacidad reservada que especificó.

     Utilice las siguientes directrices para asignar la capacidad reservada:
     - La configuración predeterminada para la capacidad reservada es del 40 % del volumen base. Por lo general, esta capacidad es suficiente.
     - La capacidad necesaria varía, según la frecuencia y el tamaño de escrituras de I/o en los volúmenes y la cantidad y la duración de la recogida de imágenes Snapshot.
6. Haga clic en **Siguiente**.

   Se muestra el cuadro de diálogo Editar configuración.
7. Edite la configuración de la programación de instantáneas según sea necesario y, a continuación, haga clic en **Finalizar**.

Detalles del campo

Ajuste	Descripción
Límite de imagen Snapshot	Habilitar la eliminación automática de imágenes Snapshot cuando…
Deje seleccionada la casilla de comprobación si desea que las imágenes Snapshot se eliminen automáticamente después del límite especificado; use el cuadro de desplazamiento para cambiar el límite. Si desmarca esta casilla de comprobación, la creación de imágenes Snapshot se detiene después de 32 imágenes.	**Ajustes de capacidad reservada**
Enviarme una alerta cuando…	Utilice el cuadro de desplazamiento para ajustar el punto porcentual en el que el sistema debe enviar una notificación de alerta si la capacidad reservada para una programación está casi completa. Cuando la capacidad reservada para la programación supere el umbral especificado, utilice los avisos por adelantado para aumentar la capacidad reservada o eliminar los objetos innecesarios antes de agotar el espacio restante.
Política para capacidad reservada completa	Seleccione una de las siguientes políticas: • **Purga la imagen Snapshot más antigua** — el sistema purga automáticamente la imagen Snapshot más antigua, lo que libera la capacidad reservada de la imagen Snapshot para que se pueda reutilizar dentro del grupo Snapshot. • **Rechazar escrituras en volumen base**: Cuando la capacidad reservada alcanza el porcentaje máximo definido, el sistema rechaza cualquier solicitud de escritura de I/o en el volumen base que activó el acceso a la capacidad reservada.

Crear un grupo de coherencia Snapshot

Para garantizar que las copias sean coherentes, puede crear un conjunto de varios volúmenes denominado *grupo de coherencia Snapshot*.

El grupo permite realizar imágenes Snapshot de todos los volúmenes al mismo tiempo para fines de coherencia. Cada volumen que pertenece a un grupo de coherencia Snapshot se denomina *volumen miembro*. Si se añade un volumen a un grupo de coherencia Snapshot, el sistema crea automáticamente un grupo Snapshot nuevo que corresponde a este volumen miembro.

Acerca de esta tarea

La secuencia de creación de un grupo de coherencia Snapshot permite seleccionar volúmenes miembro para el grupo y asignar capacidad a los volúmenes miembro.

El proceso para crear un grupo de coherencia Snapshot es un procedimiento de varios pasos.

Paso 1: Añadir miembros a un grupo de coherencia Snapshot

Seleccione miembros para especificar una recogida de los volúmenes que componen el grupo de coherencia Snapshot. Cualquier acción que se realice en el grupo de coherencia Snapshot se extiende de manera uniforme a los volúmenes miembro seleccionados.

Antes de empezar

El estado de los volúmenes miembro debe ser óptima.

Pasos

1. Seleccione MENU:Storage[Snapshots].
2. Haga clic en la ficha **grupos de coherencia de instantánea**.
3. Seleccione **Crear › Grupo de coherencia Snapshot**.

   Se muestra el cuadro de diálogo Crear grupo de coherencia Snapshot.

4. Seleccione los volúmenes que se añadirán como volúmenes miembro al grupo de coherencia Snapshot.
5. Haga clic en **Siguiente** y vaya a. Paso 2: Reservar capacidad para un grupo de coherencia Snapshot.

Paso 2: Reservar capacidad para un grupo de coherencia Snapshot

Asocie la capacidad reservada al grupo de coherencia Snapshot. System Manager sugiere los volúmenes y la capacidad según las propiedades del grupo de coherencia Snapshot. Se puede aceptar la configuración recomendada para la capacidad reservada o personalizar el almacenamiento asignado.

Acerca de esta tarea

En el cuadro de diálogo Reservar capacidad, la tabla de candidatos de volúmenes muestra solo los candidatos que admiten la capacidad reservada específica. La capacidad reservada es la capacidad física asignada que se usa para cualquier operación de servicio de copia y objeto de almacenamiento. El host no puede leerla directamente.

Pasos

1. Use el cuadro de desplazamiento para asignar la capacidad reservada para el grupo de coherencia Snapshot. Realice una de las siguientes acciones:
   - **Acepte la configuración predeterminada**.

     Use la opción recomendada Accept the default settings para asignar la capacidad reservada a cada volumen miembro con la configuración predeterminada.

   - **Asigne su propia configuración de capacidad reservada para satisfacer sus necesidades de almacenamiento de datos.**

Utilice las siguientes directrices para asignar la capacidad reservada:

- La configuración predeterminada para la capacidad reservada es del 40 % del volumen base. Por lo general, esta capacidad es suficiente.
- La capacidad necesaria varía, según la frecuencia y el tamaño de escrituras de I/o en los volúmenes y la cantidad y la duración de la recogida de imágenes Snapshot.

2. **Opcional:** Si cambia la configuración predeterminada de capacidad reservada, haga clic en **Actualizar candidatos** para actualizar la lista de candidatos de la capacidad reservada que especificó.
3. Haga clic en **Siguiente** y vaya a. Paso 3: Editar la configuración para un grupo de coherencia Snapshot.

Paso 3: Editar la configuración para un grupo de coherencia Snapshot

Acepte o seleccione la configuración de eliminación automática y los umbrales de alerta de capacidad reservada para el grupo de coherencia Snapshot.

Acerca de esta tarea

La secuencia de creación de un grupo de coherencia Snapshot permite seleccionar volúmenes miembro para el grupo y asignar capacidad a los volúmenes miembro.

Pasos

1. Acepte o cambie los ajustes predeterminados del grupo de coherencia Snapshot según corresponda.

Detalles del campo

Ajuste	Descripción
Ajustes del grupo de coherencia de instantáneas	Nombre
Especifique el nombre del grupo de coherencia Snapshot.	Habilitar la eliminación automática de imágenes Snapshot cuando…
Deje seleccionada la casilla de comprobación si desea que las imágenes Snapshot se eliminen automáticamente después del límite especificado; use el cuadro de desplazamiento para cambiar el límite. Si desmarca esta casilla de comprobación, la creación de imágenes Snapshot se detiene después de 32 imágenes.	**Ajustes de capacidad reservada**
Enviarme una alerta cuando…	Use el cuadro de desplazamiento para ajustar el valor del porcentaje en el cual el sistema envía una notificación de alerta cuando la capacidad reservada para un grupo de coherencia Snapshot está casi completa. Cuando la capacidad reservada para el grupo de coherencia Snapshot supera el umbral específico, use los avisos por adelantado para aumentar la capacidad reservada o eliminar los objetos innecesarios antes de quedarse sin espacio.
Política para capacidad reservada completa	Seleccione una de las siguientes políticas: • **Purgar imagen Snapshot más antigua** — el sistema automáticamente purga la imagen Snapshot más antigua del grupo de coherencia Snapshot, lo cual libera la capacidad reservada de la imagen Snapshot para reutilizarla dentro del grupo. • **Rechazar escrituras en volumen base**: Cuando la capacidad reservada alcanza el porcentaje máximo definido, el sistema rechaza cualquier solicitud de escritura de I/o en el volumen base que activó el acceso a la capacidad reservada.

2. Una vez que esté satisfecho con la configuración del grupo de coherencia Snapshot, haga clic en **Finalizar**.

Crear un volumen Snapshot

Se crea un volumen Snapshot para ofrecer acceso de host a la imagen Snapshot de un volumen o un grupo de coherencia Snapshot. Es posible designar el volumen Snapshot como de solo lectura o de lectura y escritura.

Acerca de esta tarea

La secuencia de creación del volumen Snapshot permite crear un volumen Snapshot desde una imagen Snapshot, y ofrece opciones para asignar capacidad reservada si el volumen es de lectura/escritura. Es posible designar un volumen Snapshot como:

- Un volumen Snapshot de solo lectura ofrece una aplicación host con acceso de lectura a una copia de los datos incluidos en la imagen Snapshot, pero sin la capacidad para modificarla. Un volumen Snapshot de solo lectura no tiene capacidad reservada asociada.
- Un volumen Snapshot de lectura y escritura le ofrece a la aplicación host acceso de escritura a una copia de los datos incluidos en la imagen Snapshot. Tiene su propia capacidad reservada, que se usa para guardar todas las modificaciones posteriores realizadas por la aplicación host al volumen base sin afectar a la imagen Snapshot de referencia.

El proceso para crear un volumen Snapshot tiene varios pasos.

Paso 1: Revise los miembros de un volumen Snapshot

Seleccione una imagen Snapshot de un volumen base o un grupo de coherencia Snapshot. Si selecciona una imagen de grupo de coherencia Snapshot, aparecen los volúmenes miembro del grupo de coherencia Snapshot para su revisión.

Pasos

1. Seleccione MENU:Storage[Snapshots].
2. Seleccione la ficha **volúmenes Snapshot**.
3. Seleccione **Crear**.

   Se muestra el cuadro de diálogo Crear volumen Snapshot.

4. Seleccione la imagen Snapshot (volumen o grupo de coherencia Snapshot) que desea convertir en volumen Snapshot y, a continuación, haga clic en **Siguiente**. Utilice una entrada de texto en el campo **filtro** para restringir la lista.

   Si se seleccionó una imagen Snapshot de grupo de coherencia Snapshot, se muestra el cuadro de diálogo revisar miembros.

   En el cuadro de diálogo revisar miembros, revise la lista de volúmenes seleccionados para su conversión a volúmenes Snapshot y haga clic en **Siguiente**.

5. Vaya a. Paso 2: Asignar volumen Snapshot a un host.

Paso 2: Asignar volumen Snapshot a un host

Seleccione un host o un clúster de hosts específico para asignarlo al volumen Snapshot. La asignación otorga acceso al volumen Snapshot para un host o un clúster de hosts. Puede elegir asignar un host más adelante, si

fuera necesario.

Antes de empezar

- Los hosts o clústeres de hosts válidos existen en la página hosts.
- Deben haberse definido los identificadores de puerto de host correspondientes.
- Antes de crear un volumen con la función DA habilitada, verifique que la conexión de host prevista sea compatible con la función Data Assurance (DA). Si alguna de las conexiones de host de las controladoras de la cabina de almacenamiento no admite DA, los hosts asociados no podrán acceder a los datos de los volúmenes con la función DA habilitada.

Acerca de esta tarea

Al asignar volúmenes, tenga en cuenta estas directrices:

- El sistema operativo de un host puede tener límites específicos acerca de la cantidad de volúmenes a los que puede acceder el host.
- Es posible definir una asignación de hosts para cada volumen Snapshot en la cabina de almacenamiento.
- Los volúmenes asignados se comparten entre controladoras de la cabina de almacenamiento.
- Un host o un clúster de hosts no puede usar dos veces el mismo número de unidad lógica (LUN) para acceder a un volumen Snapshot. Se debe usar un LUN único.

> La asignación de un volumen a un host no se realiza correctamente si se intenta asignar un volumen a un clúster de hosts que tiene conflictos con una asignación establecida para un host del clúster de hosts.

Pasos

1. En el cuadro de diálogo **asignar al host**, seleccione el host o clúster de hosts que desea asignar al nuevo volumen. Si desea crear el volumen sin asignar un host, seleccione **asignar más tarde** en la lista desplegable.
2. Seleccione el modo de acceso. Elija una de las siguientes opciones:
   - **Read/write** — esta opción proporciona al host acceso de lectura/escritura al volumen Snapshot y requiere capacidad reservada.
   - **Sólo lectura** — esta opción proporciona al host acceso de sólo lectura al volumen Snapshot y no requiere capacidad reservada.
3. Haga clic en **Siguiente** y siga uno de estos procedimientos:
   - Si el volumen Snapshot es de lectura/escritura, se muestra el cuadro de diálogo revisar capacidad. Vaya a. Paso 3: Reservar capacidad para un volumen Snapshot.
   - Si el volumen Snapshot es de solo lectura, se muestra el cuadro de diálogo Editar prioridad. Vaya a. Paso 4: Editar la configuración de un volumen Snapshot.

Paso 3: Reservar capacidad para un volumen Snapshot

Asocie la capacidad reservada a un volumen Snapshot de lectura/escritura. System Manager sugiere los volúmenes y la capacidad según las propiedades del volumen base o del grupo de coherencia Snapshot. Se puede aceptar la configuración recomendada para la capacidad reservada o personalizar el almacenamiento asignado.

Acerca de esta tarea

Es posible aumentar o reducir la capacidad reservada del volumen Snapshot según se requiera. Si la

capacidad reservada de la Snapshot es más grande de lo necesario, es posible reducir su tamaño para liberar espacio que necesitan otros volúmenes lógicos.

Pasos

1. Utilice el cuadro de desplazamiento para asignar la capacidad reservada al volumen Snapshot.

   En la tabla candidato de volumen, solo se muestran los candidatos que admiten la capacidad reservada especificada.

   Realice una de las siguientes acciones:

   - **Acepte la configuración predeterminada**.

     Utilice esta opción recomendada para asignar la capacidad de reserva al volumen Snapshot con la configuración predeterminada.

   - **Asigne su propia configuración de capacidad reservada para satisfacer sus necesidades de almacenamiento de datos**.

     Si cambia los ajustes predeterminados de capacidad reservada, haga clic en **Actualizar candidatos** para actualizar la lista de candidatos de la capacidad reservada que especificó.

     Utilice las siguientes directrices para asignar la capacidad reservada:

     - La configuración predeterminada para la capacidad reservada es del 40 % del volumen base y, por lo general, esta capacidad es suficiente.
     - La capacidad necesaria varía, según la frecuencia y el tamaño de escrituras de I/o en los volúmenes y la cantidad y la duración de la recogida de imágenes Snapshot.

2. **Opcional:** Si crea un volumen Snapshot para un grupo de coherencia Snapshot, la opción "Cambiar candidato" aparece en la tabla candidatos de capacidad reservada. Haga clic en **Cambiar candidato** para seleccionar un candidato de capacidad reservada alternativo.
3. Haga clic en **Siguiente** y vaya a. Paso 4: Editar la configuración de un volumen Snapshot.

Paso 4: Editar la configuración de un volumen Snapshot

Cambie la configuración de un volumen Snapshot, por ejemplo, nombre, almacenamiento en caché, umbrales de alerta de capacidad reservada, etc.

Acerca de esta tarea

El volumen se puede añadir a una caché de unidad de estado sólido (SSD) como una manera de mejorar el rendimiento de solo lectura. La caché SSD consiste en una serie de unidades SSD que se agrupan lógicamente en una cabina de almacenamiento.

Pasos

1. Acepte o cambie los ajustes del volumen Snapshot según corresponda.

Detalles del campo

Ajuste	Descripción
Ajustes de volumen Snapshot	Nombre
Especifique el nombre del volumen Snapshot.	Habilite la caché SSD
Seleccione esta opción para habilitar el almacenamiento en caché de solo lectura en SSD.	**Ajustes de capacidad reservada**
Enviarme una alerta cuando…	**Sólo aparece para un volumen de instantánea de lectura/escritura**. Use el cuadro de desplazamiento para ajustar el valor del porcentaje en el cual el sistema envía una notificación de alerta cuando la capacidad reservada para un grupo Snapshot está casi completa. Cuando la capacidad reservada para el grupo Snapshot supera el umbral específico, use los avisos por adelantado para aumentar la capacidad reservada o eliminar los objetos innecesarios antes de quedarse sin espacio.

2. Revise la configuración del volumen Snapshot. Haga clic en **Atrás** para realizar cualquier cambio.
3. Cuando esté satisfecho con la configuración del volumen Snapshot, haga clic en **Finalizar**.

Gestionar programaciones Snapshot

Cambiar la configuración de una programación Snapshot

En el caso de una programación Snapshot, se pueden cambiar los horarios o la frecuencia de las recogidas automáticas.

Acerca de esta tarea

Es posible importar la configuración de una programación Snapshot existente, o bien se puede modificar la configuración según sea necesario.

Dado que la programación Snapshot está asociada a un grupo Snapshot o de coherencia Snapshot, la capacidad reservada puede verse afectada por los cambios realizados en la configuración de la programación.

Pasos

1. Seleccione MENU:Storage[Snapshots].
2. Haga clic en la ficha **programaciones**.
3. Seleccione la programación de instantáneas que desea cambiar y, a continuación, haga clic en **Editar**.

Se muestra el cuadro de diálogo Editar programación Snapshot.

4. Debe realizar una de las siguientes acciones:
   - **Utilice una programación definida anteriormente de otro objeto de instantánea** — haga clic en **Importar programación**, seleccione el objeto con la programación que desea importar y, a continuación, haga clic en **Importar**.
   - **Edite la configuración del programa** — consulte Detalles del campo a continuación.

     Detalles del campo

Ajuste	Descripción
Día / mes	Seleccione una de las siguientes opciones: • **Diario / Semanal** — Seleccione días individuales para la sincronización de instantáneas. También puede seleccionar la casilla de verificación **Seleccionar todos los días** en la parte superior derecha si desea una programación diaria. • **Mensual / Anual** — Seleccione meses individuales para las instantáneas de sincronización. En el campo **el día**, introduzca los días del mes para ejecutar las sincronizaciones. Las entradas válidas son de **1** a **31** y **último**. Puede separar varios días con coma o punto y coma. Utilice un guion para indicar fechas inclusivas. Por ejemplo: 1,3,4,10-15,último. También puede seleccionar la casilla de verificación **Seleccionar todos los meses** en la parte superior derecha si desea una programación mensual.
Hora de inicio	En la lista desplegable, seleccione una hora de inicio para los snapshots diarios. Las selecciones se ofrecen en incrementos de media hora. La hora de inicio predeterminada es media hora antes de la hora actual.
Zona horaria	En la lista desplegable, seleccione la zona horaria de la cabina de almacenamiento.
Snapshot por día Tiempo entre Snapshot	Seleccione la cantidad de imágenes Snapshot que desea crear por día. Si selecciona más de una opción, seleccione además el tiempo transcurrido entre los puntos de restauración. En caso de existir varios puntos de restauración, asegúrese de contar con capacidad reservada suficiente.
Fecha de inicio Fecha de finalización Sin fecha de finalización	Introduzca la fecha de inicio para que comiencen las sincronizaciones. Introduzca también una fecha de finalización o seleccione **sin fecha de finalización**.

5. Haga clic en **Guardar**.

Activar y suspender la programación Snapshot

Se puede suspender temporalmente la recogida programada de imágenes Snapshot si se necesita conservar espacio de almacenamiento. Este método es más eficiente que eliminar y después volver a crear la programación Snapshot.

Acerca de esta tarea

El estado de la programación de instantáneas permanece suspendido hasta que se utiliza la opción **Activar** para reanudar la actividad de instantánea programada.

Pasos

1. Seleccione MENU:Storage[Snapshots].
2. Si aún no aparece, haga clic en la ficha **programaciones**.

   Se muestra una lista de las programaciones en la página.

3. Seleccione una programación de instantánea activa que desee suspender y, a continuación, haga clic en **Activar/Suspender**.

   El estado de la columna Estado cambia a **suspendido** y la programación de instantáneas detiene la recopilación de todas las imágenes de instantánea.

4. Para reanudar la recopilación de imágenes Snapshot, seleccione la programación de instantáneas suspendida que desea reanudar y haga clic en **Activar/Suspender**.

   El estado de la columna Estado cambia a **activo**.

Eliminar programación Snapshot

Si ya no desea recoger imágenes Snapshot, es posible eliminar una programación Snapshot existente.

Acerca de esta tarea

Cuando se elimina una programación Snapshot, no se eliminan las imágenes Snapshot junto con ella. Si considera que la recogida de imágenes Snapshot puede reanudarse en algún momento, debe suspender la programación Snapshot en lugar de eliminarla.

Pasos

1. Seleccione MENU:Storage[Snapshots].
2. Haga clic en la ficha **programaciones**.
3. Seleccione la programación Snapshot que desea eliminar y confirme la operación.

Resultados

El sistema elimina todos los atributos de la programación del volumen base o del grupo de coherencia Snapshot.

Gestionar imágenes Snapshot

Ver la configuración de imágenes Snapshot

Es posible ver las propiedades, el estado, la capacidad reservada y los objetos asignados asociados a cada imagen Snapshot.

Acerca de esta tarea

Los objetos asociados a una imagen Snapshot incluyen el volumen base o grupo de coherencia Snapshot para el cual esta imagen Snapshot es un punto de restauración, el grupo Snapshot asociado y cualquier volumen Snapshot creado a partir de la imagen Snapshot. Use la configuración Snapshot para determinar si desea copiar o convertir la imagen Snapshot.

Pasos

1. Seleccione MENU:Storage[Snapshots].
2. Haga clic en la ficha **Imágenes Snapshot**.
3. Seleccione la imagen de instantánea que desea ver y haga clic en **Ver configuración**.

   Se muestra el cuadro de diálogo Configuración de la imagen Snapshot.

4. Vea la configuración de la imagen Snapshot.

Iniciar reversión de imagen Snapshot para un volumen base

Es posible ejecutar una operación de reversión para cambiar el contenido de un volumen base de modo que este coincida con el contenido guardado en una imagen Snapshot.

La operación de reversión no cambia el contenido de las imágenes Snapshot asociadas con el volumen base.

Antes de empezar

- La capacidad reservada disponible es suficiente para iniciar una operación de reversión.
- El estado de la imagen Snapshot seleccionada y el volumen seleccionado es óptimo.
- No existe una operación de reversión en curso en el volumen seleccionado.

Acerca de esta tarea

Con la secuencia de inicio de la reversión, es posible iniciar la reversión sobre una imagen Snapshot de un volumen base y seleccionar opciones para añadir capacidad de almacenamiento. Solo se puede iniciar una operación de reversión para un volumen base a la vez.

> El host no puede obtener acceso de lectura/escritura al volumen base existente después de que se inicia la reversión, pero puede acceder de inmediato al nuevo volumen base revertido. Es posible crear una Snapshot del volumen base justo antes de iniciar la reversión a fin de conservar el volumen base previo a la reversión para la recuperación.

Pasos

1. Seleccione MENU:Storage[Snapshots].
2. Seleccione la ficha **Imágenes Snapshot**.
3. Seleccione la imagen Snapshot y, a continuación, seleccione MENU:Rollback[Start].

   Se muestra el cuadro de diálogo Confirmar inicio de reversión.

4. **Opcional:** Seleccione la opción **aumentar capacidad** si es necesario.

   Se muestra el cuadro de diálogo aumentar la capacidad reservada.

   a. Utilice el cuadro de desplazamiento para ajustar el porcentaje de capacidad.

      Si el pool o el grupo de volúmenes en el que se encuentra el objeto de almacenamiento seleccionado no tiene capacidad libre y la cabina de almacenamiento tiene capacidad sin asignar, puede añadir capacidad. Puede crear un nuevo pool o grupo de volúmenes y volver a intentar esta operación con la nueva capacidad libre de ese pool o grupo de volúmenes.

   b. Haga clic en **aumentar**.

5. Confirme que desea realizar esta operación y haga clic en **revertir**.

Resultados

System Manager realiza lo siguiente:

- Restaurará el volumen con el contenido guardado en la imagen Snapshot seleccionada.
- Habilitará inmediatamente el acceso del host a los volúmenes revertidos. No es necesario esperar hasta que se complete la operación de reversión.

Después de terminar

Seleccione MENU:Inicio[Ver operaciones en curso] para ver el progreso de la operación de reversión.

Si la operación de reversión no se realiza correctamente, se coloca en pausa. Puede reanudar la operación en pausa y, si no se realiza correctamente, puede seguir el procedimiento de Recovery Guru para corregir el problema o ponerse en contacto con el soporte técnico.

Iniciar reversión de imagen Snapshot para volúmenes miembro de un grupo de coherencia Snapshot

Es posible ejecutar una operación de reversión para cambiar el contenido de los volúmenes miembro de un grupo de coherencia Snapshot de modo que este coincida con el contenido guardado en una imagen Snapshot.

La operación de reversión no cambia el contenido de las imágenes Snapshot asociadas con el grupo de coherencia Snapshot.

Antes de empezar

- La capacidad reservada disponible es suficiente para iniciar una operación de reversión.
- El estado de la imagen Snapshot seleccionada y el volumen seleccionado es óptimo.
- No existe una operación de reversión en curso en el volumen seleccionado.

Acerca de esta tarea

Con la secuencia de inicio de la reversión, es posible iniciar la reversión sobre una imagen Snapshot de un grupo de coherencia Snapshot y seleccionar opciones para añadir capacidad de almacenamiento. Solo se puede iniciar una operación de reversión para un grupo de coherencia Snapshot a la vez.

> El host no puede obtener acceso de lectura/escritura a los volúmenes miembro existentes después de que se inicia la reversión, pero puede obtener acceso inmediato a los nuevos volúmenes revertidos. Es posible crear una imagen Snapshot de los volúmenes miembro justo antes de iniciar la reversión a fin de conservar los volúmenes base previos a la reversión para fines de recuperación.

El proceso para iniciar la reversión de una imagen Snapshot de un grupo de coherencia Snapshot es un procedimiento de varios pasos.

Paso 1: Seleccionar miembros

Debe seleccionar los volúmenes miembro que desea revertir.

Pasos

1. Seleccione MENU:Storage[Snapshots].
2. Seleccione la ficha **Imágenes Snapshot**.
3. Seleccione la imagen Snapshot del grupo de coherencia Snapshot y haga clic en **Rollback › Start**.

   Se muestra el cuadro de diálogo Iniciar reversión.

4. Seleccione el o los volúmenes miembro.
5. Haga clic en **Siguiente** y siga uno de estos procedimientos:
   - Si alguno de los volúmenes miembro seleccionados se encuentra asociado con más de un objeto de capacidad reservada en el que se almacenan imágenes Snapshot, se muestra el cuadro de diálogo revisar capacidad. Vaya a. Paso 2: Revisar la capacidad.
   - Si ninguno de los volúmenes miembro seleccionados se encuentra asociado con más de un objeto de capacidad reservada en el que se almacenan imágenes Snapshot, se muestra el cuadro de diálogo Editar prioridad. Vaya a. Paso 3: Editar prioridad.

Paso 2: Revisar la capacidad

Si seleccionó volúmenes miembro asociados con más de un objeto de capacidad reservada, como un grupo Snapshot y un volumen de capacidad reservada, puede revisar y aumentar la capacidad reservada para el o los volúmenes revertidos.

Pasos

1. Junto a cualquier volumen miembro con una capacidad reservada muy baja (o nula), haga clic en el enlace **aumentar capacidad** de la columna **Editar**.

   Se muestra el cuadro de diálogo aumentar la capacidad reservada.

2. Utilice el cuadro de desplazamiento para ajustar el porcentaje de capacidad y, a continuación, haga clic en **aumentar**.

   Si el pool o el grupo de volúmenes en el que se encuentra el objeto de almacenamiento seleccionado no tiene capacidad libre y la cabina de almacenamiento tiene capacidad sin asignar, puede añadir capacidad. Puede crear un nuevo pool o grupo de volúmenes y volver a intentar esta operación con la nueva capacidad libre de ese pool o grupo de volúmenes.

3. Haga clic en **Siguiente** y vaya a. Paso 3: Editar prioridad.

   Se muestra el cuadro de diálogo Editar prioridad.

Paso 3: Editar prioridad

Es posible editar la prioridad de la operación de reversión si es necesario.

Acerca de esta tarea

La prioridad de la reversión determina la cantidad de recursos del sistema que se deben dedicar a la operación de reversión a expensas del rendimiento del sistema.

Pasos

1. Utilice el control deslizante para ajustar la prioridad de la reversión según sea necesario.
2. Confirme que desea realizar esta operación y haga clic en **Finalizar**.

Resultados

System Manager realiza lo siguiente:

- Restaurará los volúmenes miembro del grupo de coherencia Snapshot con el contenido guardado en la imagen Snapshot seleccionada.
- Habilitará inmediatamente el acceso del host a los volúmenes revertidos. No es necesario esperar hasta que se complete la operación de reversión.

Después de terminar

Seleccione MENU:Inicio[Ver operaciones en curso] para ver el progreso de la operación de reversión.

Si la operación de reversión no se realiza correctamente, se coloca en pausa. Puede reanudar la operación en pausa y, si no se realiza correctamente, puede seguir el procedimiento de Recovery Guru para corregir el problema o ponerse en contacto con el soporte técnico.

Reanudar una reversión de imagen Snapshot

Si se produce un error durante una reversión de imagen Snapshot, la operación se coloca automáticamente en pausa. Es posible reanudar una operación de reversión que se encuentra en estado de pausa.

Pasos

1. Seleccione MENU:Storage[Snapshots].
2. Haga clic en la ficha **Imágenes Snapshot**.
3. Resalte la reversión en pausa y, a continuación, seleccione MENU:Rollback[Reanudar].

   Se reanudará la operación.

Resultados

System Manager realiza lo siguiente:

- Si la operación de reversión se reanuda correctamente, puede ver el progreso de la operación en la ventana Operaciones en curso.
- Si la operación de reversión no se realiza correctamente, se vuelve a colocar en pausa. Puede seguir el procedimiento de Recovery Guru para corregir el problema o ponerse en contacto con el soporte técnico.

Cancelar una reversión de imagen Snapshot

Es posible cancelar una reversión activa en curso (con copia activa de datos), una reversión pendiente (en una cola pendiente a la espera de que se inicien los recursos) o una reversión en pausa debido a un error.

Acerca de esta tarea

Cuando se cancela una operación de reversión en curso, el volumen base se revierte a un estado inservible y se muestra con errores. Por lo tanto, piense en cancelar una operación de reversión únicamente cuando disponga de opciones de recuperación para restaurar el contenido del volumen base.

> Si el grupo Snapshot en el que se encuentra la imagen Snapshot contiene una o varias imágenes Snapshot depuradas automáticamente, es posible que la imagen Snapshot utilizada en la operación de reversión no esté disponible en reversiones futuras.

Pasos

1. Seleccione MENU:Storage[Snapshots].
2. Haga clic en la ficha **Imágenes Snapshot**.
3. Seleccione la reversión activa o en pausa y, a continuación, seleccione MENU:Rollback[Cancel].

   Se muestra el cuadro de diálogo Confirmar cancelación de reversión.

4. Haga clic en **Sí** para confirmar.

Resultados

System Manager detendrá la operación de reversión. El volumen base es utilizable, pero puede contener datos incoherentes o no intactos.

Después de terminar

Después de cancelar una operación de reversión, debe realizar una de las siguientes acciones:

- Reinicie el contenido del volumen base.
- Ejecute una nueva operación de reversión para restaurar el volumen base mediante la misma imagen Snapshot utilizada en la operación para cancelar la reversión o una imagen Snapshot diferente para ejecutar la nueva operación de reversión.

Eliminar imagen Snapshot

Se eliminan las imágenes Snapshot para borrar la imagen Snapshot más antigua de un grupo Snapshot o un grupo de coherencia Snapshot.

Acerca de esta tarea

Se puede eliminar una sola imagen Snapshot, o bien es posible eliminar grupos de coherencia Snapshot que tienen la misma Marca de hora de creación. También es posible eliminar imágenes Snapshot de un grupo Snapshot.

No es posible eliminar una imagen Snapshot si no es la imagen Snapshot del volumen base o del grupo de coherencia Snapshot asociado.

Pasos

1. Seleccione MENU:Storage[Snapshots].
2. Haga clic en la ficha **Imágenes Snapshot**.
3. Seleccione la imagen Snapshot que desea eliminar y confirme que desea realizar la operación.

   Si selecciona la imagen Snapshot de un grupo de coherencia Snapshot, seleccione cada volumen miembro que desea eliminar y confirme que desea realizar la operación.

4. Haga clic en **Eliminar**.

Resultados

System Manager realiza lo siguiente:

- Elimina la imagen Snapshot de la cabina de almacenamiento.
- Libera la capacidad reservada para reutilizarla dentro del grupo Snapshot o grupo de coherencia Snapshot.
- Deshabilita todos los volúmenes Snapshot asociados que existen para la imagen Snapshot eliminada.
- A partir de la eliminación de un grupo de coherencia Snapshot, mueve todos los volúmenes miembro asociados con la imagen Snapshot al estado detenido.

Gestione grupos de coherencia Snapshot

Añadir un volumen miembro a un grupo de coherencia Snapshot

Es posible añadir un volumen miembro nuevo a un grupo de coherencia Snapshot existente. Cuando se añade un volumen miembro nuevo, también se debe reservar capacidad para el volumen miembro.

Antes de empezar

- El volumen miembro debe ser óptimo.
- El grupo de coherencia Snapshot debe tener una cantidad menor a la cantidad máxima de volúmenes permitidos (tal como se define en la configuración).
- Cada volumen con capacidad reservada debe tener la misma configuración de Data Assurance (DA) y de seguridad que el volumen miembro asociado.

Acerca de esta tarea

Es posible añadir volúmenes estándar o finos al grupo de coherencia Snapshot. El volumen base puede estar en un pool o un grupo de volúmenes.

Pasos

1. Seleccione MENU:Storage[Snapshots].
2. Seleccione la ficha **grupos de coherencia de instantánea**.

   Se muestra la tabla y se indican todos los grupos de coherencia Snapshot asociados con la cabina de almacenamiento.

3. Seleccione el grupo de coherencia Snapshot que desea modificar y haga clic en **Añadir miembros**.

   Se muestra el cuadro de diálogo Añadir miembros.

4. Seleccione los volúmenes miembro que desea agregar y haga clic en **Siguiente**.

   Se muestra el paso de capacidad reservada. En la tabla candidato de volumen, solo se muestran los candidatos que admiten la capacidad reservada especificada.

5. Use el cuadro de desplazamiento para asignar la capacidad reservada del volumen miembro. Realice una de las siguientes acciones:
   - **Acepte la configuración predeterminada.**

     Use esta opción recomendada para asignar la capacidad reservada del volumen miembro con la configuración predeterminada.

   - **Asigne su propia configuración de capacidad reservada para satisfacer sus necesidades de almacenamiento de datos.**

     Si cambia los ajustes predeterminados de capacidad reservada, haga clic en **Actualizar candidatos** para actualizar la lista de candidatos de la capacidad reservada que especificó.

     Utilice las siguientes directrices para asignar la capacidad reservada:

     - La configuración predeterminada para la capacidad reservada es del 40 % del volumen base y, por lo general, esta capacidad es suficiente.
     - La capacidad necesaria varía, según la frecuencia y el tamaño de escrituras de I/o en los volúmenes y la cantidad y la duración de la recogida de imágenes Snapshot.
6. Haga clic en **Finalizar** para agregar los volúmenes miembro.

Quite un volumen miembro de un grupo de coherencia Snapshot

Es posible quitar un volumen miembro de un grupo de coherencia Snapshot existente.

Acerca de esta tarea

Cuando se quita un volumen miembro de un grupo de coherencia Snapshot, System Manager elimina automáticamente los objetos Snapshot asociados con el volumen miembro.

Pasos

1. Seleccione MENU:Storage[Snapshots].
2. Haga clic en la ficha **grupos de coherencia de instantánea**.
3. Expanda el grupo de coherencia Snapshot que desea modificar mediante el signo más (+) junto al grupo.
4. Seleccione el volumen miembro que desea eliminar y, a continuación, haga clic en **Quitar**.
5. Confirme que desea realizar la operación y haga clic en **Quitar**.

Resultados

System Manager realiza lo siguiente:

- Elimina todas las imágenes Snapshot y los volúmenes Snapshot asociados con el volumen miembro.
- Elimina el grupo Snapshot asociado con el volumen miembro.
- El volumen miembro no se modificará ni eliminará de otra manera.

Cambiar la configuración de un grupo de coherencia Snapshot

Es posible cambiar la configuración de un grupo de coherencia Snapshot cuando se desea cambiar el nombre de dicho grupo, la configuración de eliminación automática o la cantidad máxima de imágenes Snapshot permitidas.

Pasos

1. Seleccione MENU:Storage[Snapshots].
2. Haga clic en la ficha **grupos de coherencia de instantánea**.
3. Seleccione el grupo de coherencia Snapshot que desea editar y haga clic en **Ver/editar configuración**.

   Se muestra el cuadro de diálogo Configuración del grupo de coherencia Snapshot.

4. Cambie la configuración del grupo de coherencia Snapshot según corresponda.

Detalles del campo

Ajuste	Descripción
Ajustes del grupo de coherencia de instantáneas	Nombre
Es posible cambiar el nombre del grupo de coherencia Snapshot.	Eliminación automática
Deje seleccionada la casilla de comprobación si desea que las imágenes Snapshot se eliminen automáticamente después del límite especificado; use el cuadro de desplazamiento para cambiar el límite. Si desmarca esta casilla de comprobación, la creación de imágenes Snapshot se detiene después de 32 imágenes.	Límite de la imagen Snapshot
Es posible modificar la cantidad máxima de imágenes Snapshot que se permiten en un grupo.	Programación Snapshot
Este campo indica si una programación está asociada con el grupo de coherencia Snapshot.	**Objetos asociados**
Volúmenes miembro	Se puede ver la cantidad de volúmenes miembro que están asociados al grupo de coherencia Snapshot.

5. Haga clic en **Guardar**.

Eliminar el grupo de coherencia Snapshot

Es posible eliminar grupos de coherencia Snapshot cuando ya no son necesarios.

Antes de empezar

Confirme que las imágenes de todos los volúmenes miembro ya no son necesarias para fines de backup o prueba.

Acerca de esta tarea

Esta operación elimina todas las imágenes Snapshot asociadas con el grupo de coherencia Snapshot.

Pasos

1. Seleccione MENU:Storage[Snapshots].
2. Seleccione la ficha **grupos de coherencia de instantánea**.
3. Seleccione el grupo de coherencia Snapshot que desea eliminar y, a continuación, seleccione menú:tareas no comunes[Eliminar].

   Se muestra el cuadro de diálogo Confirmar eliminación de grupo de coherencia Snapshot.

4. Confirme que desea realizar esta operación y haga clic en **Eliminar**.

Resultados

System Manager realiza lo siguiente:

- Elimina todas las imágenes Snapshot y los volúmenes Snapshot del grupo de coherencia Snapshot.
- Elimina todas las imágenes Snapshot asociadas que existen para cada volumen miembro del grupo de coherencia Snapshot.
- Elimina todos los volúmenes Snapshot asociados que existen para cada volumen miembro del grupo de coherencia Snapshot.
- Elimina toda la capacidad reservada para cada volumen miembro del grupo de coherencia Snapshot (si está seleccionado).

Permite gestionar volúmenes Snapshot

Convierta un volumen Snapshot al modo de lectura/escritura

Se puede convertir un volumen Snapshot o un volumen Snapshot del grupo de coherencia Snapshot de solo lectura al modo de lectura/escritura si fuera necesario.

Un volumen Snapshot que se convierte para permitir la lectura/escritura tiene su propia capacidad reservada. Esta capacidad se usa para guardar cualquier modificación subsiguiente que realice la aplicación host al volumen base sin afectar a la imagen Snapshot de referencia.

Pasos

1. Seleccione MENU:Storage[Snapshots].
2. Seleccione la ficha **volúmenes Snapshot**.

   Se muestra la tabla volúmenes Snapshot con todos los volúmenes Snapshot asociados con la cabina de almacenamiento.

3. Seleccione el volumen Snapshot de sólo lectura que desea convertir y, a continuación, haga clic en **convertir a lectura/escritura**.

   Aparece el cuadro de diálogo convertir a lectura/escritura con el paso **capacidad de reserva** activado. En

la tabla candidato de volumen, solo se muestran los candidatos que admiten la capacidad reservada especificada.

4. Si desea asignar la capacidad reservada para el volumen Snapshot de lectura/escritura, debe realizar una de las siguientes acciones.
   - **Acepte la configuración predeterminada** — utilice esta opción recomendada para asignar la capacidad reservada para el volumen Snapshot con la configuración predeterminada.
   - **Asigne su propia configuración de capacidad reservada para satisfacer sus necesidades de almacenamiento de datos** — asigne la capacidad reservada usando las siguientes directrices.
     - La configuración predeterminada para la capacidad reservada es del 40 % del volumen base y, por lo general, esta capacidad es suficiente.
     - La capacidad necesaria varía, según la frecuencia y el tamaño de escrituras de I/o en el volumen.
5. Seleccione **Siguiente** para revisar o editar la configuración.

   Se muestra el cuadro de diálogo Editar configuración.

6. Acepte o especifique la configuración para el volumen de instantánea según corresponda y, a continuación, seleccione **Finalizar** para convertir el volumen de instantánea.

   Detalles del campo

Ajuste	Descripción
Ajustes de capacidad reservada	Enviarme una alerta cuando…

Cambiar la configuración de volumen para un volumen Snapshot

Es posible cambiar la configuración de un volumen Snapshot o un volumen Snapshot de grupo de coherencia Snapshot para cambiar el nombre, habilitar o deshabilitar el almacenamiento en caché SSD, o cambiar la asignación de hosts, clúster de hosts o número de unidad lógica (LUN).

Pasos

1. Seleccione MENU:Storage[Snapshots].
2. Haga clic en la ficha **volúmenes Snapshot**.
3. Seleccione el volumen de instantánea que desea cambiar y, a continuación, haga clic en **Ver/editar configuración**.

   Se muestra el cuadro de diálogo Configuración del volumen Snapshot.

4. Es posible ver o editar la configuración de un volumen Snapshot según sea necesario.

Detalles del campo

Ajuste	Descripción
Volumen Snapshot	Nombre
Permite cambiar el nombre del volumen Snapshot.	Asignado a.
Permite cambiar la asignación de hosts o clúster de hosts del volumen Snapshot.	LUN
Permite cambiar la asignación de LUN del volumen Snapshot.	Caché SSD
Permite habilitar y deshabilitar el almacenamiento en caché de solo lectura en unidades de estado sólido (SSD).	**Objetos asociados**
Imagen Snapshot	Permite ver las imágenes Snapshot asociadas con el volumen Snapshot. Una imagen Snapshot es una copia lógica de datos de volúmenes capturados en un momento específico. Al igual que un punto de restauración, las imágenes Snapshot permiten revertir a un conjunto de datos bien conocidos. Si bien el host puede acceder a la imagen Snapshot, no puede leer ni escribir allí directamente.
Volumen base	Permite ver el volumen de base asociado con el volumen Snapshot. Un volumen base es el origen desde el cual se crea una imagen Snapshot. Puede ser un volumen grueso o fino y, por lo general, se asigna a un host. El volumen base puede residir en un grupo de volúmenes o un pool de discos.
Grupo Snapshot	Permite ver el grupo Snapshot asociado con el volumen Snapshot. Un grupo Snapshot es una recogida de imágenes Snapshot de un volumen base único.

Copiar un volumen Snapshot

Se puede realizar un proceso Copy Volume en un volumen Snapshot o un volumen Snapshot de un grupo de coherencia Snapshot.

Acerca de esta tarea

Se puede copiar un volumen Snapshot en el volumen objetivo como se realiza en una operación Copy Volume normal. No obstante, los volúmenes Snapshot no pueden permanecer en línea durante el proceso de copia de volumen.

Pasos

1. Seleccione MENU:Storage[Snapshots].
2. Seleccione la ficha **volúmenes Snapshot**.

   Se muestra la tabla volúmenes Snapshot con todos los volúmenes Snapshot asociados con la cabina de almacenamiento.

3. Seleccione el volumen de instantánea que desea copiar y, a continuación, seleccione **Copiar volumen**.

   Se muestra el cuadro de diálogo Copiar volumen que solicita seleccionar un objetivo.

4. Seleccione el volumen de destino que se va a utilizar como destino de copia y, a continuación, haga clic en **Finalizar**.

Vuelva a crear el volumen Snapshot

Es posible volver a crear un volumen Snapshot o un volumen Snapshot de grupo de coherencia Snapshot que se haya deshabilitado anteriormente. Cuando se vuelve a crear un volumen Snapshot, se requiere menos tiempo que crear uno nuevo.

Antes de empezar

- El volumen Snapshot debe estar en un estado óptimo o deshabilitado.
- Todos los volúmenes Snapshot miembro deben estar en estado deshabilitado para poder volver a crear el volumen Snapshot del grupo de coherencia Snapshot.

Acerca de esta tarea

No se puede volver a crear un volumen Snapshot miembro individual; solo se puede volver a crear el volumen Snapshot de grupo de coherencia Snapshot completo.

> Si el volumen Snapshot o el volumen Snapshot de grupo de coherencia Snapshot forma parte de una relación de copia en línea, no se puede ejecutar la opción de recreación en el volumen.

Pasos

1. Seleccione MENU:Storage[Snapshots].
2. Seleccione la ficha **volúmenes Snapshot**.

   Se muestra la tabla volúmenes Snapshot con todos los volúmenes Snapshot asociados con la cabina de almacenamiento.

3. Seleccione el volumen Snapshot que desea volver a crear y haga clic en menú:tareas no comunes[Volver a crear].

   Se muestra el cuadro de diálogo Volver a crear el volumen Snapshot.

4. Seleccione una de las siguientes opciones:
   - **Una imagen Snapshot existente creada a partir de <name> para volúmenes**

Seleccione esta opción para indicar la imagen Snapshot existente a partir de la cual desea volver a crear el volumen Snapshot.

- **Una nueva imagen instantánea (instantánea) del volumen <name>**

  Seleccione esta opción para crear una imagen Snapshot nueva a partir de la cual desea volver a crear el volumen Snapshot.

5. Haga clic en **Volver a crear**.

Resultados

System Manager realiza lo siguiente:

- Elimina todo `write` datos en cualquier volumen de repositorios snapshot asociado.
- Mantiene los mismos parámetros de los volúmenes deshabilitados anteriormente para el volumen Snapshot o el volumen Snapshot de grupo de coherencia Snapshot.
- Conserva el nombre original del volumen Snapshot o del volumen Snapshot de grupo de coherencia Snapshot.

Deshabilitar volumen Snapshot

Es posible deshabilitar un volumen Snapshot o un volumen Snapshot en un grupo de coherencia cuando ya no se lo necesita o se desea dejar de usarlo de manera temporal.

Acerca de esta tarea

Utilice la opción Deshabilitar si se aplica alguna de estas condiciones:

- Terminó sus tareas con el volumen Snapshot o el volumen Snapshot de un grupo de coherencia Snapshot por el momento.
- Desea volver a crear el volumen Snapshot o el volumen Snapshot de un grupo de coherencia Snapshot (que está designado como de lectura y escritura) en el futuro y quiere conservar la capacidad reservada asociada para no tener que volver a crearla.
- Desea aumentar el rendimiento de la cabina de almacenamiento deteniendo la actividad de escritura en un volumen Snapshot de lectura y escritura.

Si el volumen Snapshot o el volumen Snapshot de un grupo de coherencia Snapshot se designa como de lectura y escritura, esta opción también le permite detener toda la actividad de escritura futura con su volumen de capacidad reservada asociado. Si decide volver a crear el volumen Snapshot o el volumen Snapshot de un grupo de coherencia Snapshot, debe seleccionar una imagen Snapshot en el mismo volumen base.

> Si el volumen Snapshot o el volumen Snapshot de un grupo de coherencia Snapshot forma parte de una relación de copia en línea, no podrá utilizar la opción Deshabilitar en el volumen.

Pasos

1. Seleccione MENU:Storage[Snapshots].
2. Seleccione la ficha **volúmenes Snapshot**.

   System Manager muestra todos los volúmenes Snapshot asociados con la cabina de almacenamiento.

3. Seleccione el volumen Snapshot que desea deshabilitar y, a continuación, seleccione menú:tareas no comunes[Deshabilitar].

4. Confirme que desea realizar la operación y haga clic en **Desactivar**.

Resultados

- El volumen Snapshot sigue asociado con su volumen base.
- El volumen Snapshot conserva su nombre WWN.
- Si es de lectura y escritura, el volumen Snapshot conserva su capacidad reservada asociada.
- El volumen Snapshot conserva todas las asignaciones de hosts y puede acceder a ellos. Sin embargo, se producen fallos en las solicitudes de lectura y escritura.
- El volumen Snapshot pierde la asociación con su imagen Snapshot.

Eliminar volumen Snapshot

Es posible eliminar un volumen Snapshot o un grupo de coherencia Snapshot que ya no se necesitan para fines de backup o prueba de aplicaciones de software.

También es posible especificar si se desea eliminar el volumen de capacidad reservada Snapshot asociado a `read-write` volumen snapshot o conservar el volumen de capacidad reservada snapshot como volumen sin asignar.

Acerca de esta tarea

Si se elimina un volumen base, automáticamente se eliminan todos los volúmenes Snapshot o grupos de coherencia Snapshot asociados. No se puede eliminar un volumen Snapshot que está en una copia de volumen con el estado **en curso**.

Pasos

1. Seleccione MENU:Storage[Snapshots].
2. Seleccione la ficha **volúmenes Snapshot**.

   System Manager muestra todos los volúmenes Snapshot asociados con la cabina de almacenamiento.

3. Seleccione el volumen Snapshot que desea eliminar y, a continuación, seleccione menú:tareas no comunes[Eliminar].
4. Confirme que desea realizar la operación y, a continuación, haga clic en **Eliminar**.

Resultados

System Manager realiza lo siguiente:

- Elimina todos los volúmenes Snapshot miembro (para un volumen Snapshot en un grupo de coherencia Snapshot).
- Elimina todas las asignaciones de hosts asociadas.

Preguntas frecuentes

¿Por qué no se muestran todos los volúmenes, los hosts o los clústeres de hosts?

Los volúmenes Snapshot que incluyen un volumen base con la función DA habilitada no son aptos para asignarse a un host que no es compatible con la función Data Assurance (DA). Debe deshabilitar DA en el volumen base para poder asignar un volumen Snapshot a un host que no es compatible con DA.

Tenga en cuenta las siguientes directrices para el host al cual planea asignar el volumen Snapshot:

- Un host no es compatible con DA si está conectado a la cabina de almacenamiento a través de una interfaz de I/o que no es compatible con DA.
- Un clúster de hosts no es compatible con DA si tiene al menos un miembro de host que no es compatible con DA.

> No se puede deshabilitar LA DA en un volumen asociado con Snapshot (grupos de coherencia, grupos Snapshot, imágenes Snapshot y volúmenes Snapshot), copias de volumen, y espejos. Toda la capacidad reservada y los objetos Snapshot asociados deben eliminarse para poder deshabilitar DA en el volumen base.

¿Qué es una imagen Snapshot?

Una imagen Snapshot es una copia lógica de contenido del volumen, capturado en un momento específico. Las imágenes Snapshot utilizan un espacio de almacenamiento mínimo.

Los datos de imagen Snapshot se almacenan de la siguiente manera:

- Cuando se crea una imagen Snapshot, la imagen coincide exactamente con el volumen base. Una vez realizada la Snapshot, cuando se produce la primera solicitud de escritura de cualquier bloque o conjunto de bloques de un volumen base, los datos originales se copian en la capacidad reservada Snapshot.
- Las Snapshot posteriores incluyen solo los bloques de datos que se modificaron desde la creación de la primera imagen Snapshot. Cada operación de copia en escritura posterior guarda los datos originales que están por sobrescribirse en el volumen base de la capacidad reservada Snapshot antes de que se escriban los datos nuevos en el volumen base.

¿Por qué se deben utilizar imágenes Snapshot?

Se pueden utilizar snapshots como medida de protección contra el daño o la pérdida de datos, accidental o intencional, y para permitir la recuperación.

Seleccione un volumen base o un grupo de volúmenes base, denominado grupo de coherencia Snapshot, y luego capture las imágenes Snapshot en una o varias de las siguientes maneras:

- Puede crear una imagen Snapshot de un volumen base único o un grupo de coherencia Snapshot compuesto por varios volúmenes base.
- Puede tomar las Snapshot de forma manual o crear una programación para que un volumen base o grupo de coherencia Snapshot capture automáticamente imágenes Snapshot de forma periódica.
- Puede crear un volumen Snapshot de una imagen Snapshot que sea accesible desde el host.
- Puede realizar una operación de reversión para restaurar una imagen Snapshot.

El sistema retiene varias imágenes Snapshot como puntos de restauración que se pueden utilizar para la reversión a conjuntos de datos en buen estado en momentos específicos. La capacidad de reversión brinda protección contra la eliminación accidental de datos y los daños en los datos.

¿Qué tipos de volúmenes pueden utilizarse para las Snapshot?

Los volúmenes estándares y finos son los únicos tipos de volúmenes que se pueden

utilizar para almacenar las imágenes Snapshot. No se pueden utilizar volúmenes no estándares. El volumen base puede residir en un pool o en un grupo de volúmenes.

¿Por qué debería crear un grupo de coherencia Snapshot?

Si desea que se capturen imágenes Snapshot de varios volúmenes al mismo tiempo, puede crear un grupo de coherencia Snapshot.

Por ejemplo, una base de datos compuesta por varios volúmenes que necesitan mantener la consistencia a los fines de la recuperación requeriría un grupo de coherencia Snapshot para recoger snapshots coordinadas de todos los volúmenes y utilizarlas para restaurar la base de datos completa.

Los volúmenes incluidos en un grupo de coherencia Snapshot se denominan *volúmenes miembro*.

Se pueden realizar las siguientes operaciones Snapshot en un grupo de coherencia Snapshot:

- Crear una imagen Snapshot de un grupo de coherencia Snapshot para obtener imágenes en simultáneo de los volúmenes miembro.
- Crear una programación para que el grupo de coherencia Snapshot capture automáticamente imágenes en simultáneo de forma periódica de los volúmenes miembro.
- Crear un volumen Snapshot de una imagen de grupo de coherencia Snapshot que sea accesible desde el host.
- Realizar una operación de reversión para un grupo de coherencia Snapshot.

¿Qué es un volumen Snapshot y cuándo necesita capacidad reservada?

Un volumen Snapshot permite que el host acceda a los datos de la imagen Snapshot. El volumen Snapshot tiene su propia capacidad reservada que almacena cualquier modificación del volumen base sin afectar a la imagen Snapshot original. Los hosts no tienen permisos de lectura ni escritura en las imágenes Snapshot. Si desea leer o escribir datos Snapshot, cree un volumen Snapshot y asigne este volumen a un host.

Es posible crear dos tipos de volúmenes Snapshot. El tipo de volumen Snapshot determina si utiliza capacidad reservada.

- **Sólo lectura** — Un volumen de instantáneas creado como de sólo lectura proporciona una aplicación host con acceso de lectura a una copia de los datos contenidos en la imagen instantánea. Un volumen Snapshot de solo lectura no utiliza capacidad reservada.
- **Read-write** — un volumen de instantáneas que se crea como de lectura y escritura le permite realizar cambios en el volumen de instantáneas sin afectar a la imagen de instantánea de referencia. Un volumen Snapshot de lectura y escritura utiliza capacidad reservada para almacenar los cambios. Es posible convertir un volumen Snapshot de solo lectura a lectura y escritura en cualquier momento.

¿Qué es un grupo Snapshot?

Un grupo Snapshot es una recogida de imágenes Snapshot de momentos específicos de un único volumen base asociado.

System Manager organiza las imágenes Snapshot en *grupos Snapshot*. Los grupos Snapshot no requieren ninguna acción del usuario, pero se puede ajustar la capacidad de un grupo Snapshot en cualquier momento. Además, es posible que se muestre un mensaje para crear capacidad reservada cuando se cumplan las

siguientes condiciones:

- Siempre que se realiza una Snapshot de un volumen base que no tiene grupo Snapshot, System Manager crea automáticamente un grupo Snapshot. Esto genera capacidad reservada para el volumen base que se utiliza para almacenar imágenes Snapshot posteriores.
- Siempre que se crea una programación Snapshot para un volumen base, System Manager crea automáticamente un grupo Snapshot.

¿Por qué debería deshabilitar un volumen Snapshot?

El volumen Snapshot se deshabilita cuando se desea asignar un volumen Snapshot diferente a la imagen Snapshot. Se puede reservar el volumen Snapshot deshabilitado para usarlo más adelante.

Si ya no necesita el volumen Snapshot o el volumen Snapshot del grupo de coherencia y no tiene intenciones de volver a crear ese volumen más adelante, debe eliminar el volumen en lugar de deshabilitarlo.

¿Qué es el estado deshabilitado?

Un volumen Snapshot en estado deshabilitado no se encuentra asignado actualmente a una imagen Snapshot. Para habilitar el volumen Snapshot, se debe utilizar la operación recrear para asignar una imagen Snapshot nueva al volumen Snapshot deshabilitado.

Las características del volumen Snapshot quedan definidas por la imagen Snapshot asignada. La actividad de lectura y escritura en un volumen Snapshot en estado deshabilitado se encuentra suspendida.

¿Por qué debería suspender una programación Snapshot?

Cuando se suspende una programación, no se ejecutan las creaciones de imágenes Snapshot programadas. Es posible poner en pausa una programación Snapshot para conservar el espacio de almacenamiento, y reanudar las Snapshot programadas más adelante.

Si no necesita la programación Snapshot, debe eliminarla en lugar de suspenderla.

Mirroring

Descripción general

Información general de mirroring asíncrono

La función Asynchronous Mirroring ofrece un mecanismo basado en firmware en el nivel de la controladora para la replicación de datos entre una cabina de almacenamiento local y una cabina de almacenamiento remota.

¿Qué es el mirroring asíncrono?

Asynchronous Mirroring captura el estado de un volumen primario en un momento específico y copia solo los datos que han cambiado desde la última captura de imagen. El sitio primario se puede actualizar de inmediato y el sitio secundario se puede actualizar según lo permita el ancho de banda. La información se guarda en la

caché y se envía más tarde, a medida que los recursos de red se vuelven disponibles.

El mirroring asíncrono se crea por volumen, pero se gestiona en el nivel de grupo, lo que permite asociar un volumen reflejado remoto distinto a cualquier volumen primario en una cabina de almacenamiento determinada. Este tipo de mirroring es ideal para satisfacer la demanda de operaciones ininterrumpidas y, en general, es mucho más eficiente para la red en procesos periódicos.

Obtenga más información:

- "Cómo funciona el mirroring asíncrono"
- "Terminología de mirroring asíncrono"
- "Estado de reflejo asíncrono"
- "Propiedad del volumen"
- "Cambio de roles de un grupo de coherencia de reflejos"

¿Cómo se configura el mirroring asíncrono?

Es necesario usar la interfaz de Unified Manager para realizar la configuración de mirroring inicial entre las cabinas. Una vez que se configura, puede gestionar las parejas reflejadas y los grupos de consistencia en System Manager.

Obtenga más información:

- "Requisitos para mirroring asíncrono"
- "Flujo de trabajo para reflejar un volumen de manera asíncrona"
- "Crear una pareja reflejada asíncrona (en Unified Manager)"

Información relacionada

Obtenga más información acerca de conceptos relacionados con el mirroring asíncrono:

- "Qué debe saber antes de crear un grupo de coherencia de reflejos"
- "Lo que debe saber antes de crear una pareja reflejada"
- "La diferencia que el mirroring asíncrono es el mirroring síncrono"

Información general de mirroring síncrono

La función Synchronous Mirroring proporciona la replicación de datos en línea en tiempo real entre las cabinas de almacenamiento a una distancia remota.

> Esta función no está disponible en los sistemas de almacenamiento EF600 o EF300.

¿Qué es el mirroring síncrono?

Synchronous Mirroring replica los volúmenes de datos en tiempo real para garantizar la disponibilidad continua. Las controladoras de la cabina de almacenamiento gestionan la operación de mirroring, que es transparente para el equipo host y las aplicaciones de software.

Este tipo de mirroring es ideal para fines de continuidad del negocio como la recuperación ante desastres.

Obtenga más información:

- "Cómo funciona el mirroring síncrono"
- "Terminología de mirroring síncrono"
- "Estado de mirroring síncrono"
- "Propiedad del volumen"
- "Cambio de roles entre volúmenes de una pareja reflejada"

¿Cómo se configura el mirroring síncrono?

Es necesario usar la interfaz de Unified Manager para realizar la configuración de mirroring inicial entre las cabinas. Una vez que se configura, puede gestionar las parejas reflejadas en System Manager.

Obtenga más información:

- "Requisitos para mirroring síncrono"
- "Flujo de trabajo para reflejar un volumen de forma síncrona"
- "Crear una pareja reflejada síncrona (en Unified Manager)"

Información relacionada

Más información acerca de conceptos relacionados con el mirroring síncrono:

- "Lo que debe saber antes de crear una pareja reflejada"
- "La diferencia que el mirroring asíncrono es el mirroring síncrono"

Conceptos de la asincrónica

Cómo funciona el mirroring asíncrono

El mirroring asíncrono copia los volúmenes de datos bajo demanda o por programación, lo que minimiza o evita el tiempo de inactividad que se puede producir por pérdidas o daños en los datos.

El mirroring asíncrono captura el estado de un volumen primario en un momento específico y copia solo los datos que han cambiado desde la última captura de imagen. El sitio primario se puede actualizar de inmediato y el sitio secundario se puede actualizar según lo permita el ancho de banda. La información se guarda en la caché y se envía más tarde, a medida que los recursos de red se vuelven disponibles.

Este tipo de mirroring es ideal para satisfacer la demanda de operaciones ininterrumpidas y, en general, es mucho más eficiente para la red en procesos periódicos como backup y archivado. Algunos motivos para utilizar el mirroring asíncrono son los siguientes:

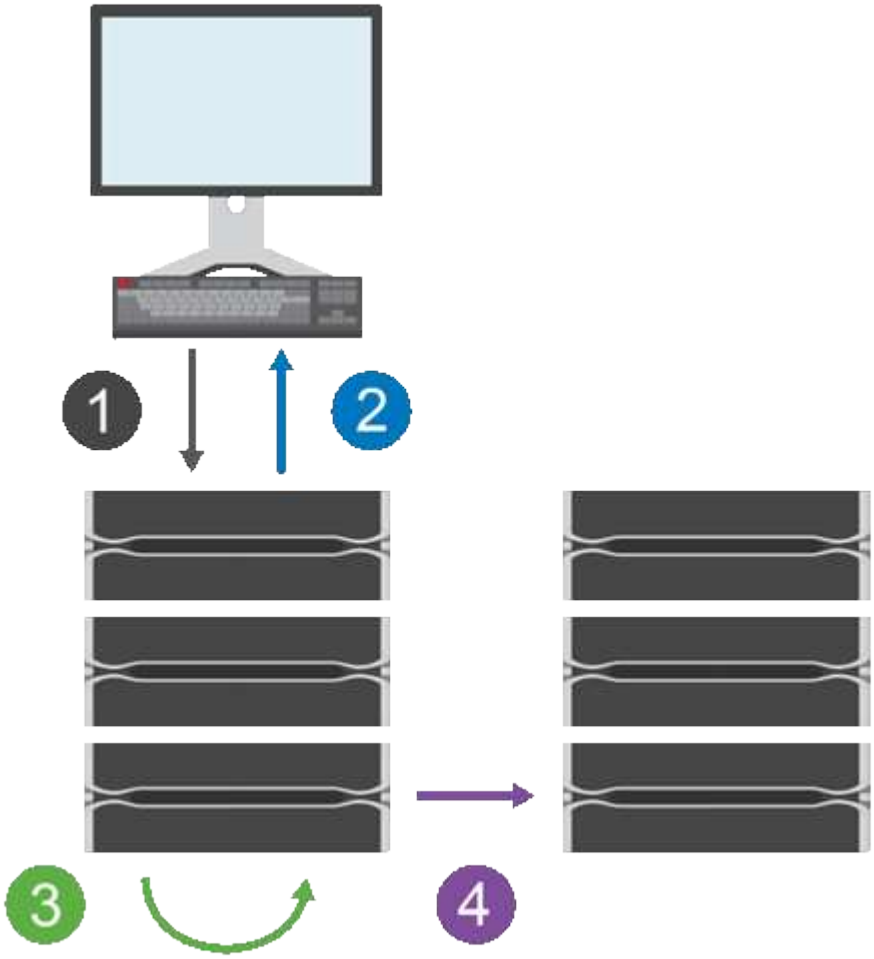
- Consolidación de backup remoto.
- Protección contra desastres locales o de área amplia.
- Desarrollo y prueba de aplicaciones en una imagen de un momento específico de datos en directo.

Sesión de mirroring asíncrono

El mirroring asíncrono captura el estado de un volumen primario en un momento específico y copia solo los datos que han cambiado desde la última captura de imagen. El mirroring asíncrono permite actualizar el sitio primario inmediatamente y el sitio secundario a medida que el ancho de banda lo permita. La información se

guarda en la caché y se envía más tarde, a medida que los recursos de red se vuelven disponibles.

Una sesión activa de mirroring asíncrono se compone de cuatro pasos primarios.



1. Una operación de escritura se produce primero en la cabina de almacenamiento del volumen primario.
2. El estado de la operación se devuelve al host.
3. Todos los cambios en el volumen primario se registran y se realiza un seguimiento sobre ellos.
4. Todos los cambios se envían a la cabina de almacenamiento del volumen secundario como proceso en segundo plano.

Estos pasos se repiten según los intervalos de sincronización definidos, o bien los pasos pueden repetirse manualmente si no existen intervalos definidos.

El mirroring asíncrono transfiere datos al sitio remoto únicamente según los intervalos establecidos, de modo que las operaciones locales de I/o no se vean tan afectadas por las conexiones de red lentas. Debido a que esta transferencia no está vinculada con las operaciones locales de I/o, no afecta al rendimiento de la aplicación. Por lo tanto, el mirroring asíncrono puede utilizar conexiones más lentas, como iSCSI, y ejecutarse en distancias más largas entre los sistemas de almacenamiento local y remoto.

Las cabinas de almacenamiento deben tener la versión de firmware 7.84 como mínimo. (Cada una puede ejecutar versiones de sistema operativo diferentes).

Grupos de coherencia de reflejos y parejas reflejadas

Es posible crear un grupo de coherencia de reflejos para establecer la relación de mirroring entre la cabina de almacenamiento remota y local. La relación de mirroring asíncrono consiste en una pareja reflejada: Un volumen primario en una cabina de almacenamiento y un volumen secundario en otra.

La cabina de almacenamiento que contiene el volumen primario está ubicada generalmente en el sitio primario y presta servicios para los hosts activos. La cabina de almacenamiento que contiene el volumen secundario está ubicada generalmente en un sitio secundario y contiene una réplica de los datos. Por lo general, el volumen secundario contiene una copia de backup de los datos y se usa para la recuperación ante desastres.

Configuración de sincronización

Cuando se crea una pareja reflejada, también se define la prioridad de sincronización y la política de resincronización que utiliza la pareja reflejada para completar la operación de resincronización después de una interrupción de comunicación.

Al crear un grupo de coherencia de reflejos, también se define la prioridad de sincronización y la política de resincronización para todas las parejas reflejadas dentro del grupo. Las parejas reflejadas utilizan la prioridad de sincronización y la política de resincronización para completar la operación de resincronización después de una interrupción de comunicación.

Los volúmenes primario y secundario en una pareja reflejada pueden dejar de estar sincronizados cuando la cabina de almacenamiento del volumen primario no puede escribir datos en el volumen secundario. Esta condición puede deberse a los siguientes problemas:

- Problemas de red entre las cabinas de almacenamiento remota y local.
- Un volumen secundario con errores.
- Una sincronización que se suspende manualmente en la pareja reflejada.
- Conflicto de roles del grupo de reflejos.

Puede sincronizar datos en la cabina de almacenamiento remota de forma manual o automática.

Capacidad reservada y mirroring asíncrono

La capacidad reservada se utiliza para realizar un seguimiento de las diferencias entre el volumen primario y secundario cuando no se produce una sincronización. También realiza un seguimiento de las estadísticas de sincronización para cada pareja reflejada.

Cada volumen de una pareja reflejada requiere su propia capacidad reservada.

Configuración y gestión

Para habilitar y configurar el mirroring entre dos cabinas, debe usar la interfaz de Unified Manager. Una vez habilitado el mirroring, puede gestionar las parejas reflejadas y las configuraciones de sincronización en System Manager.

Terminología de mirroring asíncrono

Conozca la forma en que los términos de mirroring asíncrono se aplican a su cabina de almacenamiento.

Duración	Descripción
Cabina de almacenamiento local	La cabina de almacenamiento local es aquella sobre la que se actúa en el momento. Cuando se observa **primario** en la columna rol local, la cabina de almacenamiento contiene el volumen que tiene el rol primario en la relación de reflejo. Cuando se observa **secundario** en la columna rol local, la cabina de almacenamiento contiene el volumen que tiene el rol secundario en la relación de reflejo.
Grupo de coherencia de reflejos	Un grupo de coherencia de reflejos es un contenedor para una o más parejas reflejadas. Para las operaciones de mirroring asíncrono, se debe crear un grupo de coherencia de reflejos.
Pareja reflejada	Una pareja reflejada comprende dos volúmenes: Un volumen primario y uno secundario. En el mirroring asíncrono, una pareja reflejada siempre pertenece a un grupo de coherencia de reflejos. Primero, se realizan las operaciones de escritura en el volumen primario y, luego, se replican en el secundario. Cada pareja reflejada de un grupo de coherencia de reflejos comparte la misma configuración de sincronización.
Volumen primario	El volumen primario de una pareja reflejada es el volumen de origen que se reflejará.
Cabina de almacenamiento remota	La cabina de almacenamiento remota se designa normalmente como el sitio secundario, que normalmente contiene una réplica de los datos en una configuración de mirroring.
Capacidad reservada	La capacidad reservada es la capacidad física asignada que se usa para cualquier operación de servicio de copia y objeto de almacenamiento. El host no puede leerla directamente.
Cambio de roles	El cambio de rol es asignar el rol primario al volumen secundario y viceversa.
Volumen secundario	El volumen secundario de una pareja reflejada está normalmente ubicado en un sitio secundario y contiene una réplica de los datos.
Sincronización	La sincronización se produce en la sincronización inicial entre la cabina de almacenamiento local y la cabina de almacenamiento remota. La sincronización también se produce cuando los volúmenes primario y secundario dejan de estar sincronizados después de una interrupción de comunicación. Cuando el enlace de comunicación se restablece, todos los datos sin replicar se sincronizan con la cabina de almacenamiento del volumen secundario.

Flujo de trabajo para reflejar un volumen de manera asíncrona

El mirroring asíncrono se debe configurar mediante el siguiente flujo de trabajo.

1. Realice la configuración inicial en Unified Manager:
   a. Seleccione la cabina de almacenamiento local como el origen de la transferencia de datos.
   b. Cree un grupo de coherencia de reflejos o seleccione uno existente que funcione como contenedor para el volumen primario de la cabina local y el volumen secundario de la cabina remota. Los volúmenes primario y secundario se conocen como la "pareja reflejada". Si es la primera vez que crea el grupo de coherencia de reflejos, debe especificar si desea ejecutar sincronizaciones manuales o programadas.
   c. Seleccione un volumen primario de la cabina de almacenamiento local y determine su capacidad reservada. La capacidad reservada es la capacidad física asignada que se utilizará para la operación de copia.
   d. Seleccione una cabina de almacenamiento remota como el destino de la transferencia y un volumen secundario y, a continuación, determine su capacidad reservada.
   e. Inicie la transferencia de datos inicial desde el volumen primario hacia el volumen secundario. Según el tamaño de los volúmenes, esta transferencia inicial puede tardar varias horas.
2. Compruebe el progreso de la sincronización inicial:
   a. En Unified Manager, inicie la instancia de System Manager para la cabina local.
   b. En System Manager, consulte el estado de la operación de mirroring. Cuando se complete el mirroring, el estado de la pareja reflejada será "óptimo".
3. **Opcional:** puede reprogramar o realizar manualmente transferencias de datos posteriores en System Manager. Solo se transferirán los bloques nuevos y cambiados del volumen primario al volumen secundario.

> Como la replicación asíncrona es periódica, el sistema puede consolidar los bloques cambiados y ahorrar ancho de banda de red. El impacto sobre el rendimiento de escritura y la latencia de escritura es mínimo.

Requisitos para mirroring asíncrono

Si planea utilizar la función de mirroring asíncrono, tenga en cuenta los siguientes requisitos.

Unified Manager

Para habilitar y configurar el mirroring entre dos cabinas, debe usar la interfaz de Unified Manager. Unified Manager debe estar instalado en un sistema host junto con el proxy de servicios web.

- El proxy de servicios web se encuentra en ejecución.
- Unified Manager se ejecuta en el host local a través de una conexión HTTPS.
- SANtricity Unified Manager debe mostrar los certificados SSL válidos para la cabina de almacenamiento. Es posible aceptar un certificado autofirmado o instalar una certificación de seguridad propia con Unified Manager. Para hacerlo, debe navegar hasta MENU:Certificate[Gestión de certificados].

Cabinas de almacenamiento

- Debe tener dos cabinas de almacenamiento.
- Cada cabina de almacenamiento debe tener dos controladoras.
- Las dos cabinas de almacenamiento se encuentran detectadas en Unified Manager.

- Cada controladora en la cabina primaria y la cabina secundaria debe tener un puerto Ethernet de gestión configurado y debe estar conectada a la red.
- Las cabinas de almacenamiento deben tener la versión de firmware 7.84 como mínimo. (Cada una puede ejecutar versiones de sistema operativo diferentes).
- Debe conocer la contraseña de las cabinas de almacenamiento remota y local.
- Debe tener suficiente capacidad libre en la cabina de almacenamiento remota para crear un volumen secundario mayor o igual que el volumen primario que desea reflejar.
- Las cabinas de almacenamiento local y remota se encuentran conectadas a través de una estructura Fibre Channel o una interfaz iSCSI.

Conexiones admitidas

En el mirroring asíncrono, se pueden usar las conexiones FC o iSCSI, o ambas, para la comunicación entre los sistemas de almacenamiento local y remoto. Cuando se crea un grupo de coherencia de reflejos, el administrador puede seleccionar FC o iSCSI para ese grupo si se establecen ambas conexiones en la cabina de almacenamiento remota. No existe conmutación al nodo de respaldo de un tipo de canal al otro.

En el mirroring asíncrono, se utilizan los puertos de I/o del host de la cabina de almacenamiento para transferir los datos reflejados del área primaria a la secundaria.

- **Duplicación a través de una interfaz Fibre Channel (FC)**

  Cada controladora de la cabina de almacenamiento dedica su puerto de host FC numerado más alto a las operaciones de mirroring.

  Si la controladora tiene tanto puertos base FC como puertos FC de tarjeta de interfaz del host (HIC), en la HIC se encuentra el puerto numerado más alto. Se cerrará la sesión de cualquier host que haya iniciado sesión en el puerto dedicado y no se aceptará ninguna solicitud de inicio de sesión de host. Solo se aceptan las solicitudes I/o en este puerto de las controladoras que participan en las operaciones de mirroring.

  Los puertos de mirroring dedicados deben pertenecer al entorno estructural de FC que sea compatible con el servicio de directorio y las interfaces del servicio de nombres. En particular, FC-AL y punto a punto no son opciones de conectividad compatibles entre las controladoras que participan en las relaciones de mirroring.

- **Duplicación a través de una interfaz iSCSI**

  A diferencia de FC, iSCSI no requiere un puerto dedicado. Cuando se utiliza el mirroring asíncrono en entornos iSCSI, no es necesario dedicar ninguno de los puertos iSCSI front-end de la cabina de almacenamiento para usarlos con mirroring asíncrono; esos puertos se comparten tanto para las conexiones de tráfico de reflejos asíncronos como de I/o de host a cabina.

  La controladora conserva una lista de los sistemas de almacenamiento remoto con los cuales el iniciador de iSCSI intenta establecer una sesión. El primer puerto que logra establecer una conexión iSCSI se utiliza para todas las comunicaciones subsiguientes con esa cabina de almacenamiento remota. Si no se produce la comunicación, se intenta una nueva sesión con todos los puertos disponibles.

  Los puertos iSCSI se configuran en el nivel de la cabina, puerto por puerto. La comunicación entre controladoras para la mensajería de configuración y la transferencia de datos utiliza la configuración global, lo que incluye:

  - VLAN: Tanto los sistemas locales como los remotos deben tener el mismo valor de VLAN para

comunicarse

- Puertos de escucha iSCSI
- Tramas gigantes
- Prioridad para Ethernet

> La comunicación entre las controladoras iSCSI debe utilizar un puerto con conexión a un host y no el puerto Ethernet de gestión.

En el mirroring asíncrono, se utilizan los puertos de I/o del host de la cabina de almacenamiento para transferir los datos reflejados del área primaria a la secundaria. Debido a que el mirroring asíncrono está previsto para redes de mayor latencia y menor coste, las conexiones iSCSI (y, por lo tanto, basadas en TCP/IP) son buenas opciones. Cuando se utiliza el mirroring asíncrono en entornos iSCSI, no es necesario dedicar ninguno de los puertos iSCSI front-end de la cabina para usarlos con mirroring asíncrono; esos puertos se comparten tanto para las conexiones de tráfico de reflejos asíncronos como de I/o de host a cabina

Candidatos de volumen reflejado

- El nivel de RAID, los parámetros de almacenamiento en caché y el tamaño de los segmentos pueden ser diferentes en los volúmenes primario y secundario de una pareja reflejada asíncrona.

> Para las controladoras EF600 y EF300, los volúmenes primario y secundario de una pareja reflejada asíncrona deben coincidir con el mismo protocolo, nivel de soporte, tamaño de segmento, tipo de seguridad y nivel de RAID. Las parejas reflejadas asíncronas no elegibles no aparecerán en la lista de volúmenes disponibles.

- El volumen secundario deber tener al menos el tamaño del volumen primario.
- Un volumen puede participar solo en una relación de reflejo.
- Los candidatos de volúmenes deben compartir las mismas funcionalidades de seguridad de datos.
  - Si el volumen primario es compatible con FIPS, el volumen secundario debe ser compatible con FIPS.
  - Si el volumen primario es compatible con FDE, el volumen secundario debe ser compatible con FDE.
  - Si el volumen primario no utiliza Drive Security, el volumen secundario no debe usar Drive Security.

Capacidad reservada

- Se requiere un volumen de capacidad reservada en el volumen primario y en el volumen secundario de una pareja reflejada para registrar la información de escritura que se utiliza en la recuperación de los restablecimientos de la controladora y otras interrupciones temporales.
- Debido a que tanto el volumen primario como el volumen secundario de una pareja reflejada requieren capacidad reservada adicional, debe asegurarse de contar con capacidad libre disponible en ambas cabinas de almacenamiento de la relación de reflejo.

Función Drive Security

- Si utiliza unidades compatibles con la función de seguridad, tanto el volumen primario como el secundario deben tener una configuración de seguridad compatible. Esta restricción no se aplica; por lo tanto, debe verificarlo por su cuenta.
- Si utiliza unidades compatibles con la función de seguridad, tanto el volumen primario como el secundario deberían usar el mismo tipo de unidad. Esta restricción no se aplica; por lo tanto, debe verificarlo por su

cuenta.

- Si utiliza Data Assurance (DA), el volumen primario y el secundario deben tener la misma configuración DE DA.

Estado de reflejo asíncrono

El estado de reflejo define el estado de los grupos de coherencia de reflejos y las parejas de volúmenes reflejadas.

Estado para grupos de coherencia de reflejos

Estado	Descripción
Sincronizando (sincronización inicial)	El progreso de la sincronización de datos inicial que se completó entre las parejas de volúmenes reflejadas. Durante una sincronización inicial, los volúmenes pueden presentar una transición hacia los siguientes estados: Degradado/con errores/óptima/Desconocido.
Sincronización (sincronización de intervalos)	El progreso de la sincronización de datos periódica que se completó entre las parejas de volúmenes reflejadas.
Sistema suspendido	El sistema de almacenamiento suspendió la sincronización de datos en todas las parejas reflejadas en el nivel del grupo de coherencia de reflejos. Al menos una pareja reflejada en el grupo de coherencia de reflejos tiene el estado detenido o con errores.
Usuario suspendido	El usuario suspendió la sincronización de datos en todas las parejas reflejadas en el nivel del grupo de coherencia de reflejos. Este estado ayuda a reducir cualquier impacto sobre el rendimiento de la aplicación host que puede producirse mientras se copian datos modificados de la cabina de almacenamiento local a la cabina de almacenamiento remota.
En pausa	El proceso de sincronización de datos se puso en pausa temporalmente debido a un error de acceso a la cabina de almacenamiento remota.
Huérfano	Se crea un volumen de parejas reflejadas huérfanas cuando se elimina un volumen miembro de un grupo de coherencia de reflejos de un lado del grupo (el primario o el secundario), pero no del otro. Los volúmenes de parejas reflejadas huérfanas se detectan cuando se restaura la comunicación entre las cabinas y los dos lados de la configuración reflejada concilian los parámetros de reflejo. Puede eliminar una pareja reflejada para corregir un estado de pareja reflejada huérfana.

Estado	Descripción
Cambio de roles pendiente/en curso	Un cambio de rol entre los grupos de coherencia de reflejos está pendiente o en curso. El cambio de inversión de roles (a un rol primario o secundario) afecta a todas las parejas reflejadas asíncronas dentro del grupo de coherencia de reflejos seleccionado. Es posible cancelar un cambio de rol pendiente, pero no un cambio de rol en curso.
Conflicto de roles	Se produjo un conflicto de roles entre grupos de coherencia de reflejos debido a un problema de comunicación entre la cabina de almacenamiento local y la cabina de almacenamiento remota durante una operación de cambio de rol. Cuando se resuelve el problema de comunicación, se produce un conflicto de roles. Utilice Recovery Guru para recuperar el sistema de este error. No se permite una promoción forzada al resolver un conflicto de roles.

Estado para parejas reflejadas

El estado de una pareja reflejada indica si los datos en el volumen primario y en el volumen secundario están sincronizados.

Estado	Descripción
Sincronizando	El progreso de la sincronización de datos inicial o periódica que se completó entre las parejas reflejadas. Hay dos tipos de sincronización: Sincronización inicial y sincronización periódica. El progreso de la sincronización inicial también se muestra en el cuadro de diálogo Operaciones de larga ejecución.
Óptimo	Los volúmenes de la pareja reflejada están sincronizados, lo que indica que la conexión entre la cabina de almacenamiento funciona y cada volumen está en la condición operativa deseada.
Incompleto	La pareja reflejada asíncrona está incompleta en la cabina de almacenamiento remota porque la secuencia de creación de parejas reflejadas se inició en una cabina de almacenamiento no compatible con System Manager, y la pareja reflejada no se completó en el volumen secundario. El proceso de creación de parejas reflejadas se completa cuando se agrega un volumen al grupo de coherencia de reflejos en la cabina de almacenamiento remota. Este volumen se convierte en el volumen secundario en la pareja reflejada asíncrona. La pareja reflejada se completa automáticamente si la cabina de almacenamiento remota está gestionada por System Manager.

Estado	Descripción
Error	La operación de mirroring asíncrono no puede funcionar normalmente debido a una falla en el volumen primario, el volumen secundario o la capacidad reservada de reflejo.
Huérfano	Se crea un volumen de parejas reflejadas huérfanas cuando se elimina un volumen miembro de un grupo de coherencia de reflejos de un lado del grupo (el primario o el secundario), pero no del otro. Los volúmenes de parejas reflejadas huérfanas se detectan cuando se restaura la comunicación entre las dos cabinas de almacenamiento y los dos lados de la configuración reflejada concilian los parámetros de reflejo. Puede eliminar una pareja reflejada para corregir un estado de pareja reflejada huérfana.
Detenido	La pareja reflejada está en un estado detenido debido a que el grupo de coherencia de reflejos está en un estado suspendido por el sistema.

Propiedad del volumen

Es posible cambiar el propietario preferido de la controladora de una pareja reflejada.

Si el volumen primario de la pareja reflejada pertenece a la controladora A, el volumen secundario también pertenecerá a la controladora A en la cabina De almacenamiento remota. Al cambiar el propietario del volumen primario, se modificará automáticamente el propietario del volumen secundario para garantizar que los dos volúmenes pertenezcan a la misma controladora. Los cambios de propiedad actuales en el lado primario se propagan automáticamente a los cambios de propiedad correspondientes en el lado secundario.

Por ejemplo, un volumen primario que pertenece a la controladora A y que luego se cambia a la controladora B. En este caso, la próxima escritura remota cambia la propiedad de la controladora del volumen secundario de la controladora A a la B. Debido a que los cambios en la propiedad de la controladora en el lado secundario son controlados por el lado primario, no requieren ninguna intervención especial del administrador de almacenamiento.

Se restablece la controladora

El restablecimiento de una controladora produce un cambio de propiedad de los volúmenes en el lado primario del propietario preferido de la controladora a la controladora alternativa de la cabina de almacenamiento.

A veces, el restablecimiento de una controladora o un ciclo de alimentación de la cabina de almacenamiento interrumpen una escritura remota antes de que se pueda escribir en el volumen secundario. En este caso, la controladora no necesita realizar una sincronización completa de la pareja reflejada.

Cuando se interrumpe una escritura remota durante el restablecimiento de una controladora, el nuevo propietario de la controladora en el lado primario lee la información almacenada en un archivo de registro en el volumen de capacidad reservada del propietario preferido de la controladora. El nuevo propietario de la controladora luego copia los bloques de datos afectados del volumen primario al secundario, lo que elimina la necesidad de una sincronización completa de los volúmenes reflejados.

Cambio de roles de un grupo de coherencia de reflejos

Es posible cambiar el rol entre las parejas reflejadas de un grupo de coherencia de reflejos. Para ello, se puede degradar el grupo de coherencia de reflejos primario al rol secundario o promocionar el grupo de coherencia de reflejos secundario al rol primario.

Revise la siguiente información sobre la operación de cambio de roles:

- El cambio de rol afecta a todas las parejas reflejadas dentro del grupo de coherencia de reflejos seleccionado.
- Cuando se degrada un grupo de coherencia de reflejos al rol secundario, también se degradan todas las parejas reflejadas dentro de ese grupo de coherencia de reflejos al rol secundario y viceversa.
- Cuando se degrada el grupo de coherencia de reflejos primario al rol secundario, los hosts asignados a los volúmenes miembro de ese grupo ya no tienen acceso de escritura a ellos.
- Cuando se promociona un grupo de coherencia de reflejos al rol primario, todos los hosts con acceso a los volúmenes miembro dentro de ese grupo pueden escribir en ellos.
- Si la cabina de almacenamiento local no puede comunicarse con la cabina de almacenamiento remota, es posible forzar un cambio de rol en la cabina de almacenamiento local.

Forzar cambio de rol

Es posible forzar un cambio de rol entre los grupos de coherencia de reflejos cuando un problema de comunicación entre la cabina de almacenamiento local y la cabina de almacenamiento remota impide la promoción de los volúmenes miembro dentro del grupo de coherencia de reflejos secundario o la degradación de los volúmenes miembro dentro de la coherencia de reflejos primario grupo.

Se puede forzar la transición del grupo de coherencia de reflejos en el lado secundario al rol primario. El host de recuperación podrá acceder a los volúmenes miembro recientemente promocionados dentro de ese grupo de coherencia de reflejos y las operaciones empresariales podrán seguir su curso.

¿Cuándo se permite y no se permite una promoción forzada?

La promoción forzada de un grupo de coherencia de reflejos solo se permite si todos los volúmenes miembro del grupo de coherencia de reflejos están sincronizados y tienen puntos de recuperación consistentes.

La promoción forzada de un grupo de coherencia de reflejos no se permite en las siguientes condiciones:

- Alguno de los volúmenes miembro de un grupo de coherencia de reflejos está en el proceso de sincronización inicial.
- Alguno de los volúmenes miembro de un grupo de coherencia de reflejos no tiene una imagen de un momento específico del punto de recuperación (por ejemplo, debido a un error de capacidad reservada completa).
- El grupo de coherencia de reflejos no contiene volúmenes miembro.
- El grupo de coherencia de reflejos presenta los estados Failed, Role-Change-Pending o Role-Change-In-Progress, o alguno de los volúmenes miembro o los volúmenes de capacidad reservada asociados presenta errores.

Conflicto de roles del grupo de reflejos

Cuando se resuelve un problema de comunicación entre las cabinas de almacenamiento local y remota, se produce una condición de conflicto de roles en grupo de reflejos. Utilice Recovery Guru para recuperar el

sistema de este error. No se permite la promoción forzada para resolver un conflicto de doble rol.

Para evitar la condición de conflicto de roles en grupo de reflejos y los pasos de recuperación subsiguientes, espere hasta que se restablezca la conexión entre las cabinas de almacenamiento para forzar el cambio de rol.

Estado de cambio de rol en curso

Si se desconectan dos cabinas de almacenamiento en una configuración de mirroring, y se fuerza la degradación del lado primario de un grupo de coherencia de reflejos al rol secundario y la promoción del lado secundario de un grupo de coherencia de reflejos al rol primario, A continuación, cuando se restaura la comunicación, los grupos de coherencia de reflejos en ambas cabinas de almacenamiento se colocan en el estado de cambio de rol en curso.

Para completar el proceso de cambio de roles, el sistema transfiere los registros de cambios, vuelve a sincronizar, establece el grupo de coherencia de reflejos de vuelta a su estado operativo normal y prosigue con las sincronizaciones periódicas.

Conceptos de sincronización

Cómo funciona el mirroring síncrono

El mirroring síncrono replica los volúmenes de datos en tiempo real para garantizar la disponibilidad continua.

> El mirroring síncrono no está disponible en las cabinas de almacenamiento EF600 o EF300.

El mirroring síncrono logra un objetivo de punto de recuperación (RPO) de cero datos perdidos mediante la conservación de una copia de los datos importantes disponible en caso de que se produzca un desastre en una de las dos cabinas de almacenamiento. La copia es idéntica a los datos de producción en cada momento, ya que cada vez que se realiza una escritura en el volumen primario, se realiza una escritura en el volumen secundario. El host no recibe la confirmación de que la escritura se realizó correctamente hasta que el volumen secundario se actualiza correctamente con los cambios realizados en el volumen primario.

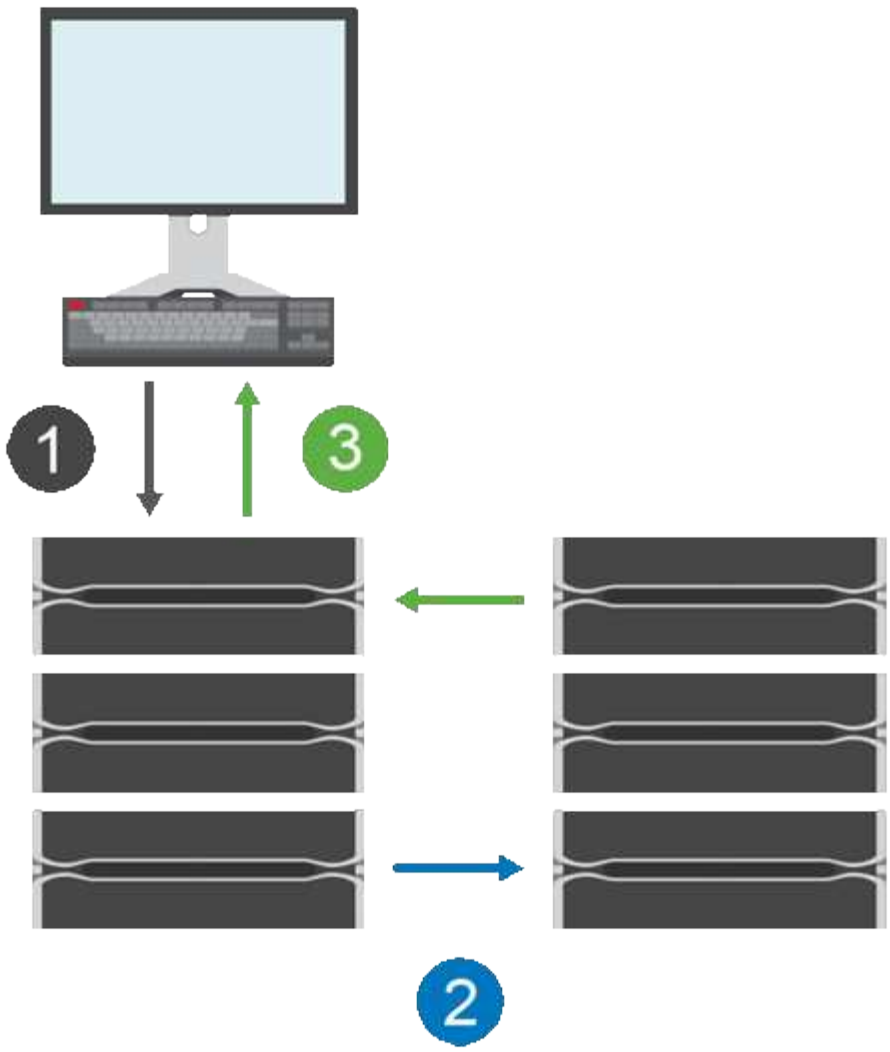
Este tipo de mirroring es ideal para fines de continuidad del negocio como la recuperación ante desastres.

Relación de mirroring síncrono

Una relación de mirroring síncrono consiste en un volumen primario y un volumen secundario en cabinas de almacenamiento individuales. La cabina de almacenamiento que contiene el volumen primario está ubicada generalmente en el sitio primario y presta servicios para los hosts activos. La cabina de almacenamiento que contiene el volumen secundario está ubicada generalmente en un sitio secundario y contiene una réplica de los datos. El volumen secundario se usa si la cabina de almacenamiento del volumen primario no está disponible debido a, por ejemplo, una interrupción del servicio total, un incendio o un error de hardware en el sitio primario.

Sesión de mirroring síncrono

El proceso de configuración de mirroring síncrono implica configurar volúmenes en parejas. Después de crear una pareja reflejada, que consiste en un volumen primario en una cabina de almacenamiento y un volumen secundario en otra, puede comenzar con el mirroring síncrono. Los pasos del mirroring síncrono se describen a continuación.



1. Llega una escritura del host.
2. La escritura se confirma en el volumen primario, se propaga al sistema remoto y luego se confirma en el volumen secundario.
3. La cabina de almacenamiento del volumen primario envía un mensaje de finalización de I/o al sistema host *after* que las dos operaciones de escritura finalizaron correctamente.

La capacidad reservada se utiliza para registrar información sobre la solicitud de escritura entrante desde un host.

Cuando la controladora actual que es propietaria del volumen primario recibe una solicitud de escritura de un host, la controladora primero registra información sobre la escritura en la capacidad reservada del volumen primario. Luego escribe los datos en el volumen primario. A continuación, la controladora inicia una operación de escritura remota para copiar los bloques de datos afectados en el volumen secundario de la cabina de almacenamiento remota.

Debido a que la aplicación host debe esperar que se produzca la escritura en la cabina de almacenamiento local y en toda la red de la cabina de almacenamiento remota, Se requiere una conexión muy rápida entre la cabina de almacenamiento local y la cabina de almacenamiento remota para mantener la relación de reflejo sin reducir demasiado el rendimiento de I/o local.

Recuperación tras siniestros

El mirroring síncrono mantiene una copia de los datos que están físicamente distantes del sitio donde residen. Si se produce un desastre en el sitio primario, como un apagón de energía o una inundación, puede accederse rápidamente a los datos desde el sitio secundario.

El volumen secundario no está disponible para aplicaciones host donde hay operaciones de mirroring síncrono en curso; por lo tanto, ante un desastre en la cabina de almacenamiento local, se puede conmutar al nodo de respaldo de la cabina de almacenamiento remota. Para conmutar al nodo de respaldo, promocione el volumen secundario al rol primario. A continuación, el host de recuperación puede acceder al volumen recientemente promovido y las operaciones empresariales pueden continuar.

Configuración de sincronización

Cuando se crea una pareja reflejada, también se define la prioridad de sincronización y la política de resincronización que utiliza la pareja reflejada para completar la operación de resincronización después de una interrupción de comunicación.

Si el enlace de comunicación entre las dos cabinas de almacenamiento deja de funcionar, los hosts siguen recibiendo reconocimientos de la cabina de almacenamiento local para evitar una pérdida de acceso. Cuando el enlace de comunicación vuelve a funcionar, todos los datos no replicados pueden volver a sincronizarse manual o automáticamente en la cabina de almacenamiento remota.

Si los datos se resincronizan automáticamente o no depende de la política de resincronización de la pareja reflejada. Una política de resincronización automática permite que la pareja reflejada se resincronice automáticamente cuando el enlace vuelve a funcionar. Una política de resincronización manual lo obliga a reanudar manualmente la resincronización después de un problema de comunicación. Se recomienda la política de resincronización manual.

Es posible editar la configuración de sincronización para una pareja reflejada solo en la cabina de almacenamiento que contiene el volumen primario.

Datos no sincronizados

Los volúmenes primario y secundario dejan de estar sincronizados cuando la cabina de almacenamiento del volumen primario no puede escribir datos en el volumen secundario. Esto puede deberse a los siguientes problemas:

- Problemas de red entre las cabinas de almacenamiento remota y local
- Un volumen secundario con errores
- Una sincronización que se suspende manualmente en la pareja reflejada

Una pareja reflejada huérfana

Se crea un volumen de pareja reflejada huérfano cuando se elimina un volumen miembro de un lado (ya sea el lado primario o el lado secundario), pero no del otro lado.

Los volúmenes de parejas reflejadas huérfanas se detectan cuando se restaura la comunicación entre las cabinas y los dos lados de la configuración reflejada concilian los parámetros de reflejo.

Puede eliminar una pareja reflejada para corregir un estado de pareja reflejada huérfana.

Configuración y gestión

Para habilitar y configurar el mirroring entre dos cabinas, debe usar la interfaz de Unified Manager. Una vez habilitado el mirroring, puede gestionar las parejas reflejadas y las configuraciones de sincronización en System Manager.

Terminología de mirroring síncrono

Conozca la forma en que los términos de mirroring síncrono se aplican a su cabina de almacenamiento.

Duración	Descripción
Cabina de almacenamiento local	La cabina de almacenamiento local es aquella sobre la que se actúa en el momento. Cuando se observa **primario** en la columna rol local, la cabina de almacenamiento contiene el volumen que tiene el rol primario en la relación de reflejo. Cuando se observa **secundario** en la columna rol local, la cabina de almacenamiento contiene el volumen que tiene el rol secundario en la relación de reflejo.
Pareja reflejada	Una pareja reflejada comprende dos volúmenes: Un volumen primario y uno secundario.
Volumen primario	El volumen primario de una pareja reflejada es el volumen de origen que se reflejará.
Objetivo de punto de recuperación (RPO)	El objetivo de punto de recuperación (RPO) representa un objetivo que indica la diferencia que se considera aceptable entre el volumen primario y el secundario en una pareja reflejada. Un RPO de cero indica que no se puede tolerar la diferencia entre el volumen primario y el secundario. Un RPO mayor de cero indica que el volumen secundario es menos actual o está retrasado con respecto al volumen primario.
Cabina de almacenamiento remota	La cabina de almacenamiento remota se designa normalmente como el sitio secundario, que normalmente contiene una réplica de los datos en una configuración de mirroring.
Capacidad reservada	La capacidad reservada es la capacidad física asignada que se usa para cualquier operación de servicio de copia y objeto de almacenamiento. El host no puede leerla directamente.
Cambio de roles	El cambio de rol es asignar el rol primario al volumen secundario y viceversa.
Volumen secundario	El volumen secundario de una pareja reflejada está normalmente ubicado en un sitio secundario y contiene una réplica de los datos.

Duración	Descripción
Sincronización	La sincronización se produce en la sincronización inicial entre la cabina de almacenamiento local y la cabina de almacenamiento remota. La sincronización también se produce cuando los volúmenes primario y secundario dejan de estar sincronizados después de una interrupción de comunicación. Cuando el enlace de comunicación se restablece, todos los datos sin replicar se sincronizan con la cabina de almacenamiento del volumen secundario.

Flujo de trabajo para reflejar un volumen de forma síncrona

El mirroring síncrono se debe configurar mediante el siguiente flujo de trabajo.

> Esta función no está disponible en los sistemas de almacenamiento EF600 o EF300.

1. Realice la configuración inicial en Unified Manager:
   a. Seleccione una cabina de almacenamiento local como el origen de la transferencia de datos.
   b. Seleccione un volumen primario de la cabina de almacenamiento local.
   c. Seleccione una cabina de almacenamiento remota como el destino de la transferencia de datos y, a continuación, seleccione un volumen secundario.
   d. Seleccione las prioridades de sincronización y resincronización.
   e. Inicie la transferencia de datos inicial desde el volumen primario hacia el volumen secundario. Según el tamaño de los volúmenes, esta transferencia inicial puede tardar varias horas.
2. Compruebe el progreso de la sincronización inicial:
   a. En Unified Manager, inicie la instancia de System Manager para la cabina local.
   b. En System Manager, consulte el estado de la operación de mirroring. Cuando se complete el mirroring, el estado de la pareja reflejada será "óptimo". Las dos cabinas intentarán mantener la sincronización a través de las operaciones normales. Solo se transferirán los bloques nuevos y cambiados del volumen primario al volumen secundario.
3. **Opcional:** puede cambiar la configuración de sincronización en System Manager.

> Como la replicación síncrona es continua, el enlace de replicación entre los dos sitios debe proporcionar funcionalidades de ancho de banda suficientes.

Requisitos para mirroring síncrono

Si planea utilizar la función de mirroring síncrono, tenga en cuenta los siguientes requisitos.

Unified Manager

Para habilitar y configurar el mirroring entre dos cabinas, debe usar la interfaz de Unified Manager. Unified Manager debe estar instalado en un sistema host junto con el proxy de servicios web.

- El proxy de servicios web se encuentra en ejecución.
- Unified Manager se ejecuta en el host local a través de una conexión HTTPS.

- SANtricity Unified Manager debe mostrar los certificados SSL válidos para la cabina de almacenamiento. Es posible aceptar un certificado autofirmado o instalar una certificación de seguridad propia con Unified Manager. Para hacerlo, debe navegar hasta MENU:Certificate[Gestión de certificados].

Cabinas de almacenamiento

> El mirroring síncrono no está disponible en las cabinas de almacenamiento EF300 o EF600.

- Debe tener dos cabinas de almacenamiento.
- Cada cabina de almacenamiento debe tener dos controladoras.
- Las dos cabinas de almacenamiento se encuentran detectadas en Unified Manager.
- Cada controladora en la cabina primaria y la cabina secundaria debe tener un puerto Ethernet de gestión configurado y debe estar conectada a la red.
- Las cabinas de almacenamiento deben tener la versión de firmware 7.84 como mínimo. (Cada una puede ejecutar versiones de sistema operativo diferentes).
- Debe conocer la contraseña de las cabinas de almacenamiento remota y local.
- Debe tener suficiente capacidad libre en la cabina de almacenamiento remota para crear un volumen secundario mayor o igual que el volumen primario que desea reflejar.
- Las cabinas de almacenamiento local y remota se encuentran conectadas a través de una estructura Fibre Channel.

Conexiones admitidas

La comunicación para la función Synchronous Mirroring solo se admite en las controladoras con puertos de host Fibre Channel (FC).

La función utiliza el puerto de host con el número más alto de cada controladora en la cabina de almacenamiento local y la cabina de almacenamiento remota. Por lo general, el puerto de host 4 del adaptador de bus de host (HBA) de la controladora se reserva para la transmisión de datos reflejados.

Candidatos de volumen reflejado

- El nivel de RAID, los parámetros de almacenamiento en caché y el tamaño de los segmentos pueden ser diferentes en los volúmenes primario y secundario de una pareja reflejada síncrona.
- Los volúmenes primario y secundario de una pareja reflejada síncrona deben ser volúmenes estándar. No pueden ser volúmenes finos o Snapshot.
- El volumen secundario deber tener al menos el tamaño del volumen primario.
- Solo el volumen primario puede contener Snapshot asociadas y/o ser el volumen objetivo o de origen en una operación de copia de volumen.
- Un volumen puede participar solo en una relación de reflejo.
- Existen límites para la cantidad de volúmenes que se admiten en una cabina de almacenamiento determinada. Asegúrese de que la cantidad de volúmenes configurados en la cabina de almacenamiento sea menor que el límite admitido. Cuando se activa el mirroring síncrono, los dos volúmenes de capacidad reservada creados se cuentan para el límite de volúmenes.

Capacidad reservada

- Se requiere capacidad reservada en el volumen primario y en el volumen secundario para registrar la información de escritura que se utiliza en la recuperación de los restablecimientos de la controladora y

otras interrupciones temporales.

- Los volúmenes de capacidad reservada se crean automáticamente cuando se activa el mirroring síncrono. Debido a que tanto el volumen primario como el volumen secundario de una pareja reflejada requieren capacidad reservada, debe asegurarse de contar con capacidad libre suficiente en ambas cabinas de almacenamiento que participan en la relación de reflejo síncrono.

Función Drive Security

- Si utiliza unidades compatibles con la función de seguridad, tanto el volumen primario como el secundario deben tener una configuración de seguridad compatible. Esta restricción no se aplica; por lo tanto, debe verificarlo por su cuenta.
- Si utiliza unidades compatibles con la función de seguridad, tanto el volumen primario como el secundario deberían usar el mismo tipo de unidad. Esta restricción no se aplica; por lo tanto, debe verificarlo por su cuenta.
  - Si el volumen primario utiliza unidades de cifrado de disco completo (FDE), el volumen secundario debe usar unidades FDE.
  - Si el volumen primario utiliza unidades validadas con el estándar de procesamiento de información federal 140-2 (FIPS), el volumen secundario también debe utilizarlas 140-2.
- Si utiliza Data Assurance (DA), el volumen primario y el secundario deben tener la misma configuración DE DA.

Estado de mirroring síncrono

El estado de una pareja reflejada síncrona indica si los datos en el volumen primario y el volumen secundario están sincronizados. El estado de reflejo es independiente del estado de componente de los volúmenes en la pareja reflejada.

> Esta función no está disponible en los sistemas de almacenamiento EF600 o EF300.

Las parejas reflejadas síncronas pueden tener uno de los siguientes Estados:

- **Óptimo**

  Indica que los volúmenes de la pareja reflejada están sincronizados, lo que significa que la conexión estructural entre la cabina de almacenamiento funciona y cada volumen está en la condición operativa deseada.

- **Sincronización**

  Muestra el progreso de la sincronización de datos entre las parejas reflejadas. Este estado también se muestra durante la sincronización inicial.

  Después de la interrupción de un enlace de comunicación, solo se copian al volumen secundario los bloques de datos que cambiaron en el volumen primario durante la interrupción del enlace.

- **No sincronizado**

  Indica que la cabina de almacenamiento del volumen primario no puede escribir los datos entrantes en la cabina remota. El host local puede seguir escribiendo en el volumen primario, pero no se producen escrituras remotas. Existen distintas condiciones que pueden evitar que la cabina de almacenamiento del volumen primario escriba los datos entrantes en el volumen secundario, por ejemplo:

- No se puede acceder al volumen secundario.
- No se puede acceder a la cabina de almacenamiento remota.
- No se puede acceder a la conexión estructural entre las cabinas de almacenamiento.
- No se puede actualizar el volumen secundario con un identificador a nivel mundial (WWID).

- **Suspendido**

  Indica que el usuario suspendió la operación de mirroring síncrono. Cuando se suspende una pareja reflejada, no se realiza ningún intento para comunicarse con el volumen secundario. Las escrituras en el volumen primario se registran de forma persistente en los volúmenes de capacidad reservada de reflejos.

- **Error**

  Indica que la operación de mirroring síncrono no funciona normalmente debido a un fallo en el volumen primario, el volumen secundario o la capacidad reservada de reflejos.

Propiedad del volumen

Es posible cambiar el propietario preferido de la controladora de una pareja reflejada.

> Esta función no está disponible para el mirroring síncrono en el sistema de almacenamiento EF600 o EF300.

Si el volumen primario de la pareja reflejada pertenece a la controladora A, el volumen secundario también pertenecerá a la controladora A en la cabina De almacenamiento remota. Al cambiar el propietario del volumen primario, se modificará automáticamente el propietario del volumen secundario para garantizar que los dos volúmenes pertenezcan a la misma controladora. Los cambios de propiedad actuales en el lado primario se propagan automáticamente a los cambios de propiedad correspondientes en el lado secundario.

Por ejemplo, un volumen primario que pertenece a la controladora A y que luego se cambia a la controladora B. En este caso, la próxima escritura remota cambia la propiedad de la controladora del volumen secundario de la controladora A a la B. Debido a que los cambios en la propiedad de la controladora en el lado secundario son controlados por el lado primario, no requieren ninguna intervención especial del administrador de almacenamiento.

Se restablece la controladora

El restablecimiento de una controladora produce un cambio de propiedad de los volúmenes en el lado primario del propietario preferido de la controladora a la controladora alternativa de la cabina de almacenamiento.

A veces, el restablecimiento de una controladora o un ciclo de alimentación de la cabina de almacenamiento interrumpen una escritura remota antes de que se pueda escribir en el volumen secundario. En este caso, la controladora no necesita realizar una sincronización completa de la pareja reflejada.

Cuando se interrumpe una escritura remota durante el restablecimiento de una controladora, el nuevo propietario de la controladora en el lado primario lee la información almacenada en un archivo de registro en el volumen de capacidad reservada del propietario preferido de la controladora. El nuevo propietario de la controladora luego copia los bloques de datos afectados del volumen primario al secundario, lo que elimina la necesidad de una sincronización completa de los volúmenes reflejados.

Cambio de roles entre volúmenes de una pareja reflejada

Es posible cambiar el rol entre los volúmenes de una pareja reflejada. Para ello, se puede degradar el volumen primario al rol secundario o promocionar el volumen secundario al rol primario.

> El mirroring síncrono no está disponible en los sistemas de almacenamiento EF600 o EF300.

Revise la siguiente información sobre la operación de cambio de roles:

- Cuando se degrada un volumen primario al rol secundario, se promociona el volumen secundario de esa pareja reflejada al rol primario y viceversa.
- Cuando se degrada el volumen primario al rol secundario, los hosts asignados a ese volumen ya no tienen acceso de escritura a él.
- Cuando se promociona el volumen secundario al rol primario, todos los hosts con acceso a ese volumen pueden escribir en él.
- Si la cabina de almacenamiento local no puede comunicarse con la cabina de almacenamiento remota, es posible forzar un cambio de rol en la cabina de almacenamiento local.

Forzar cambio de rol

Es posible forzar un cambio de rol entre los volúmenes de una pareja reflejada cuando un problema de comunicación entre la cabina de almacenamiento local y la cabina de almacenamiento remota impide la promoción del volumen secundario o la degradación del volumen primario.

Se puede forzar la transición del volumen en el lado secundario al rol primario. El host de recuperación podrá acceder al volumen recientemente promocionado y las operaciones empresariales podrán seguir su curso.

> Cuando se recupera la cabina de almacenamiento remota y se resuelven todos los problemas de comunicación, se produce una condición de conflicto de mirroring síncrono y volumen primario. Los pasos de recuperación incluyen volver a sincronizar los volúmenes. Utilice Recovery Guru para recuperar el sistema de este error.

¿Cuándo se permite y no se permite una promoción forzada?

La promoción forzada de un volumen de una pareja reflejada no se permite en las siguientes condiciones:

- Alguno de los volúmenes de una pareja reflejada está en el proceso de sincronización inicial.
- La pareja reflejada presenta los estados Failed, Role-Change-Pending o Role-Change-In-Progress, o alguno de los volúmenes de capacidad reservada asociados presenta errores.

Estado de cambio de rol en curso

Si se desconectan dos cabinas de almacenamiento en una configuración de mirroring, y se fuerza la degradación del volumen primario de una pareja reflejada al rol secundario y la promoción del volumen secundario de una pareja reflejada al rol primario, A continuación, cuando se restaura la comunicación, los volúmenes en ambas cabinas de almacenamiento se colocan en el estado de cambio de rol en curso.

Para completar el proceso de cambio de roles, el sistema transfiere los registros de cambios, vuelve a sincronizar, establece la pareja reflejada de vuelta a su estado operativo normal y prosigue con las sincronizaciones.

Gestione grupos de coherencia de reflejos asíncronos

Prueba de comunicación para grupo de coherencia de reflejos

Se puede probar el enlace de comunicación para diagnosticar posibles problemas de comunicación entre la cabina de almacenamiento local y la cabina de almacenamiento remota asociada con un grupo de coherencia de reflejos.

Antes de empezar

El grupo de coherencia de reflejos que desea probar debe existir en las cabinas de almacenamiento local y remota.

Acerca de esta tarea

Se pueden ejecutar cuatro pruebas distintas:

- **Conectividad** — verifica que los dos controladores tengan una ruta de comunicación. La prueba de conectividad envía un mensaje entre cabinas entre las cabinas de almacenamiento y, a continuación, valida la existencia del grupo de coherencia de reflejos correspondiente en la cabina de almacenamiento remota. También valida que los volúmenes miembro del grupo de coherencia de reflejos en la cabina de almacenamiento remota coincidan con los volúmenes miembro del grupo de coherencia de reflejos en la cabina de almacenamiento local.
- **Latencia** — envía un comando de unidad de prueba SCSI a cada volumen reflejado en la matriz de almacenamiento remota asociada con el grupo de consistencia de mirroring para probar la latencia mínima, media y máxima.
- **Bandwidth** — envía dos mensajes entre matrices a la matriz de almacenamiento remota para probar el ancho de banda mínimo, medio y máximo, así como la velocidad de enlace negociada del puerto en la matriz que realiza la prueba.
- **Conexiones de puerto**: Muestra el puerto que se utiliza para la duplicación en la matriz de almacenamiento local y el puerto que recibe los datos reflejados en la matriz de almacenamiento remota.

Pasos

1. Seleccione **Storage › Asynchronous Mirroring**.
2. Seleccione la ficha **grupos de consistencia en mirroring** y, a continuación, seleccione el grupo de consistencia en mirroring que desea probar.
3. Seleccione **probar comunicación**.

   Se muestra el cuadro de diálogo probar comunicación.

4. Seleccione una o más pruebas de comunicación para realizar entre las matrices de almacenamiento local y remota asociadas con el grupo de consistencia de mirroring seleccionado y, a continuación, haga clic en **probar**.
5. Revise la información que se muestra en la ventana resultados.

Estado de la prueba de comunicación	Descripción
Normal sin errores	El grupo de coherencia de reflejos se comunica correctamente.

Estado de la prueba de comunicación	Descripción
Estado superado (pero no normal)	Se debe comprobar que no haya problemas de red ni de conexión, y se debe volver a realizar la prueba.
Estado con errores	Se indica el motivo del fallo. Consulte Recovery Guru para corregir el problema.
Error de conexión de puerto	El motivo puede ser que la cabina de almacenamiento local no está conectada o que no se puede contactar a la cabina de almacenamiento remota. Consulte Recovery Guru para corregir el problema.

Resultados

Cuando se completa la prueba de comunicación, el cuadro de diálogo muestra los Estados normal, superada o con errores.

Si el resultado de la prueba de comunicación es con errores, la prueba se sigue ejecutando después de cerrar este cuadro de diálogo hasta que se restablezca la comunicación entre los grupos de coherencia de reflejos.

Suspender o reanudar la sincronización de un grupo de coherencia de reflejos

Se puede suspender o reanudar la sincronización de datos en todas las parejas reflejadas dentro de un grupo de coherencia de reflejos, que es más eficiente que hacerlo en parejas reflejadas individuales.

Acerca de esta tarea

La suspensión y la reanudación de la sincronización en los grupos ayuda a reducir el impacto en el rendimiento de la aplicación host, lo cual puede ocurrir mientras se copian los datos modificados de la cabina de almacenamiento local en la cabina de almacenamiento remota.

El estado del grupo de coherencia de reflejos y sus parejas reflejadas sigue suspendido hasta que se utiliza la opción Reanudar para reanudar la actividad de sincronización.

Pasos

1. Seleccione **Storage › Asynchronous Mirroring**.
2. Seleccione la ficha **grupos de consistencia de mirroring**.

   Aparece la tabla de grupo de coherencia de reflejos y se muestran todos los grupos de coherencia de reflejos asociados con la cabina de almacenamiento.

3. Seleccione el grupo de coherencia de reflejos que desea suspender o reanudar y, a continuación, seleccione menú:más[Suspender] o menú:más[Reanudar].

   El sistema muestra una confirmación.

4. Seleccione **Sí** para confirmar.

Resultados

System Manager realiza lo siguiente:

- Suspende o reanuda la transferencia de datos entre todas las parejas reflejadas de un grupo de coherencia de reflejos sin quitar la relación de reflejo.
- Registra los datos que se escribieron en el lado primario del grupo de consistencia en mirroring mientras el grupo de consistencia en mirroring está suspendido y escribe los datos automáticamente en el lado secundario del grupo de consistencia en mirroring cuando se reanuda el grupo de consistencia en mirroring. No es necesario realizar una sincronización completa.
- En el caso de los grupos de consistencia en mirroring *suspended*, muestra **suspendido por el usuario** en la tabla grupos de consistencia en mirroring.
- En el caso de un grupo de coherencia de reflejos *reanudado*, los datos que se escribieron en los volúmenes primarios mientras el grupo de coherencia reflejos estaba suspendido se escriben en los volúmenes secundarios inmediatamente. La sincronización periódica se reanuda si se estableció un intervalo de sincronización automática.

Cambiar la configuración de sincronización de un grupo de coherencia de reflejos

Es posible cambiar la configuración de sincronización y los umbrales de advertencia que utiliza el grupo de coherencia de reflejos en la cabina de almacenamiento local cuando los datos se sincronizan inicialmente o cuando se vuelven a sincronizar durante las operaciones de mirroring asíncrono.

Acerca de esta tarea

Un cambio en la configuración de sincronización afecta las operaciones de sincronización de todas las parejas reflejadas dentro del grupo de coherencia de reflejos.

Pasos

1. Seleccione **Storage › Asynchronous Mirroring**.
2. Seleccione la ficha **grupos de consistencia de mirroring**.

   Aparece la tabla de grupo de coherencia de reflejos y se muestran todos los grupos de coherencia de reflejos asociados con la cabina de almacenamiento.

3. Seleccione el grupo de coherencia de reflejos que desea editar y, a continuación, seleccione MENU:más[Editar configuración].

   Se muestra en el sistema el cuadro de diálogo Editar configuración.

4. Edite la configuración de sincronización y alertas según corresponda y, a continuación, haga clic en **Guardar**.

Detalles del campo

Campo	Descripción
Sincronizar las parejas reflejadas…	Especifique si desea sincronizar las parejas reflejadas en la cabina de almacenamiento remota de forma manual o automática. • **Manualmente**: Seleccione esta opción para sincronizar manualmente las parejas reflejadas en la cabina de almacenamiento remota. • **Automáticamente, cada**: Seleccione esta opción para sincronizar automáticamente las parejas reflejadas en la cabina de almacenamiento remota especificando el intervalo desde el comienzo de la actualización anterior hasta el comienzo de la siguiente. El intervalo predeterminado es de 10 minutos.
Enviarme una alerta…	Si configura el método de sincronización para que se produzca automáticamente, configure las siguientes alertas: • **Sincronización**: Configure el período de tiempo después del cual System Manager envía una alerta de que la sincronización no se ha completado. • **Punto de recuperación remoto**: Establezca un límite de tiempo después del cual System Manager envía una alerta para indicar que los datos del punto de recuperación en la cabina de almacenamiento remota son más antiguos que el límite de tiempo definido. Defina el límite de tiempo desde la finalización de la actualización anterior. • **Umbral de capacidad reservada**: Defina una cantidad de capacidad reservada en la que System Manager envía una alerta para indicar que está acercándose al umbral de capacidad reservada. El umbral se define según un porcentaje de la capacidad restante.

Resultados

System Manager modifica la configuración de sincronización de todas las parejas reflejadas en el grupo de coherencia de reflejos.

Volver a sincronizar manualmente un grupo de coherencia de reflejos

Es posible iniciar manualmente la resincronización de todas las parejas reflejadas dentro de un grupo de coherencia de reflejos.

Pasos

1. Seleccione **Storage › Asynchronous Mirroring**.
2. Seleccione la ficha **grupos de consistencia de mirroring**.

   Se muestra la tabla Grupo de coherencia de reflejos donde se detallan los grupos de coherencia de reflejos asociados con la cabina de almacenamiento.

3. Seleccione el grupo de coherencia de reflejos que desea volver a sincronizar y, a continuación, seleccione **más › Resincronizar manualmente**.

El sistema muestra una confirmación.

4. Seleccione **Sí** para confirmar.

Resultados

El sistema ejecuta las siguientes acciones:

- Inicia la resincronización de los datos de todas las parejas reflejadas dentro del grupo de coherencia de reflejos que se seleccionó.
- Actualiza los datos modificados de la cabina de almacenamiento local a la cabina de almacenamiento remota.

Ver cantidad de datos no sincronizados entre grupos de coherencia de reflejos

Es posible ver la cantidad de datos no sincronizados entre grupos de coherencia de reflejos en la cabina de almacenamiento local y en la cabina de almacenamiento remota. Mientras el grupo de coherencia de reflejos se encuentra en el estado no sincronizado, no se produce ninguna actividad de mirroring.

Acerca de esta tarea

Es posible realizar esta tarea cuando el grupo de coherencia de reflejos seleccionado contiene parejas reflejadas y cuando la sincronización no se encuentra en curso.

Pasos

1. Seleccione **Storage › Asynchronous Mirroring**.
2. Seleccione la ficha **grupos de consistencia de mirroring**.

   Se muestra la tabla Grupo de coherencia de reflejos donde se detallan los grupos de coherencia de reflejos asociados con la cabina de almacenamiento.

3. Haga clic en MENU:More [Ver cantidad de datos no sincronizados].

   Si existen datos no sincronizados, los valores de la tabla lo reflejan. En la columna de cantidad de datos, se enumera la cantidad de datos no sincronizados en MIB.

Actualice la dirección IP remota

Es posible actualizar la dirección IP de iSCSI para que se vuelva a establecer la conexión entre la cabina de almacenamiento remota y la cabina de almacenamiento local.

Antes de empezar

Tanto la cabina de almacenamiento local como la remota deben configurarse para operaciones de mirroring asíncrono mediante una conexión iSCSI.

Pasos

1. Seleccione **Storage › Asynchronous Mirroring**.
2. Seleccione la ficha **grupos de consistencia de mirroring**.

   La tabla de grupo de coherencia de reflejos muestra todos los grupos de coherencia de reflejos asociados

con la cabina de almacenamiento.

3. Seleccione el grupo de coherencia de reflejos que desea actualizar y, a continuación, seleccione MENU:más[Actualizar dirección IP remota].

   El sistema muestra el cuadro de diálogo Actualizar dirección IP remota.

4. Seleccione **Actualizar** para actualizar la dirección IP de iSCSI de la matriz de almacenamiento remota.

Resultados

El sistema restablece la dirección IP de la cabina de almacenamiento remota para restablecer la conexión con la cabina de almacenamiento local.

Cambie el rol de un grupo de coherencia de reflejos a primario o secundario

Es posible cambiar el rol entre grupos de coherencia de reflejos para fines administrativos o en el caso de un desastre en la cabina de almacenamiento local.

Acerca de esta tarea

Los grupos de coherencia de reflejos creados en la cabina de almacenamiento local conservan el rol primario. Los grupos de coherencia de reflejos creados en la cabina de almacenamiento remota conservan el rol secundario. Es posible degradar el grupo de coherencia de reflejos local a un rol secundario o promocionar el grupo de coherencia de reflejos remoto a un rol primario.

Pasos

1. Seleccione **Storage › Asynchronous Mirroring**.
2. Seleccione la ficha **grupos de consistencia de mirroring**.

   Se muestra la tabla Grupo de coherencia de reflejos donde se detallan los grupos de coherencia de reflejos asociados con la cabina de almacenamiento.

3. Seleccione el grupo de coherencia de reflejos con el rol que desea cambiar y, a continuación, seleccione **más › Cambiar rol a <Primary | Secondary>**.

   El sistema muestra una confirmación.

4. Confirme que desea cambiar el rol del grupo de consistencia en mirroring y haga clic en **Cambiar rol**.

   Se muestra el cuadro de diálogo no se puede establecer contacto con la cabina de almacenamiento en el sistema cuando se solicita un cambio de rol, pero la cabina de almacenamiento remota no puede contactarse. Haga clic en **Sí** para forzar el cambio de rol.

Resultados

System Manager realiza lo siguiente:

- En la tabla del grupo de coherencia de reflejos, se muestran los Estados "pending" o "in-progress", para indicar una operación pendiente o en curso, junto al grupo de coherencia de reflejos donde se está produciendo el cambio de rol. Puede cancelar una operación de cambio de rol pendiente haciendo clic en el enlace **Cancelar** que se encuentra dentro de la celda de la tabla.
- Si es posible comunicarse con el grupo de coherencia de reflejos asociado, cambian los roles entre los grupos de coherencia de reflejos. En System Manager, se promueve el grupo de coherencia de reflejos secundario a un rol primario o se degrada el grupo de coherencia de reflejos primario a un rol secundario

(según la selección). El cambio de rol afecta a todas las parejas reflejadas dentro del grupo de coherencia de reflejos seleccionado.

Elimine grupo de coherencia de reflejos

Es posible eliminar grupos de coherencia de reflejos que ya no son necesarios en la cabina de almacenamiento local y en la cabina de almacenamiento remota.

Antes de empezar

Deben eliminarse todas las parejas reflejadas del grupo de coherencia de reflejos.

Pasos

1. Seleccione **Storage › Asynchronous Mirroring**.
2. Seleccione la ficha **grupos de consistencia de mirroring**.

   Se muestra la tabla Grupo de coherencia de reflejos donde se detallan los grupos de coherencia de reflejos asociados con la cabina de almacenamiento.

3. Seleccione el grupo de coherencia de reflejos que desea eliminar y, a continuación, seleccione menú:tareas no comunes[Eliminar].

   El sistema muestra una confirmación.

4. Seleccione **Sí** para eliminar el grupo de consistencia en mirroring.

Resultados

System Manager realiza lo siguiente:

- Elimina el grupo de coherencia de reflejos en la cabina de almacenamiento local en primer lugar, y luego elimina el grupo de coherencia de reflejos en la cabina de almacenamiento remota.
- Elimina el grupo de coherencia de reflejos de la tabla Grupo de coherencia de reflejos.

Después de terminar

Ocasionalmente, es posible que existan instancias donde el grupo de coherencia de reflejos se elimina correctamente de la cabina de almacenamiento local, pero un error de comunicación impide eliminar el grupo de coherencia de reflejos de la cabina de almacenamiento remota. En este caso, debe acceder a la cabina de almacenamiento remota para eliminar el correspondiente grupo de coherencia de reflejos.

Gestione parejas reflejadas asíncronas

Quite la relación de reflejo asíncrono

Quite una pareja reflejada para eliminar la relación de reflejo del volumen primario en la cabina de almacenamiento local y el volumen secundario en la cabina de almacenamiento remota.

Acerca de esta tarea

Revise la siguiente información sobre parejas reflejadas huérfanas:

- Se crea una pareja reflejada huérfana cuando se quita un volumen miembro de un grupo de coherencia de reflejos de un lado (ya sea el lado de la cabina de almacenamiento local o el lado de la cabina de

almacenamiento remota), pero no del otro lado.

- Las parejas reflejadas huérfanas se detectan cuando se restaura la comunicación dentro de la cabina y los dos lados de la configuración reflejada concilian los parámetros de reflejo.
- Puede eliminar una pareja reflejada para corregir un estado de pareja reflejada huérfana.

Pasos

1. Seleccione **Storage › Asynchronous Mirroring**.
2. Seleccione la ficha **par reflejado**.

   Se muestra la tabla Mirrored Pairs con todas las parejas reflejadas asociadas con la cabina de almacenamiento.

3. Seleccione la pareja reflejada que desea quitar y haga clic en **Quitar**.
4. Confirme que desea eliminar la pareja reflejada y, a continuación, haga clic en **Quitar**.

Resultados

System Manager realiza lo siguiente:

- Quita la relación de reflejo del grupo de coherencia de reflejos en la cabina de almacenamiento local y en la cabina de almacenamiento remota, y elimina la capacidad reservada.
- Devuelve el volumen primario y el volumen secundario a los volúmenes no reflejados a los que se puede acceder desde hosts.
- Actualiza el icono Mirroring asíncrono con la eliminación de la pareja reflejada asíncrona.

Aumente la capacidad reservada

Es posible aumentar la capacidad reservada, que es la capacidad asignada físicamente para cualquier operación de servicio de copia en un objeto de almacenamiento.

Para las operaciones Snapshot, generalmente representa el 40 % del volumen base; para las operaciones de mirroring asíncrono, generalmente se trata del 20 % del volumen base. En términos generales, se aumenta la capacidad reservada cuando se recibe una advertencia de que la capacidad reservada del objeto de almacenamiento se está llenando.

Antes de empezar

- El volumen en el pool o el grupo de volúmenes debe tener el estado óptima y no debe estar en ningún estado de modificación.
- Debe existir capacidad libre en el pool o grupo de volúmenes que desea usar para aumentar la capacidad.

  Si no hay capacidad libre en ningún pool o grupo de volúmenes, es posible añadir capacidad sin asignar en forma de unidades no utilizadas a un pool o un grupo de volúmenes.

Acerca de esta tarea

Es posible aumentar la capacidad reservada solo en incrementos de 8 GIB para los siguientes objetos de almacenamiento:

- Grupo Snapshot
- Volumen Snapshot
- Volumen miembro del grupo de coherencia

- Volumen de pareja reflejada

Use un porcentaje alto si considera que el volumen primario se someterá a muchos cambios o si la vida útil de una operación de servicio de copia será muy prolongada.

> No es posible aumentar la capacidad reservada para un volumen Snapshot de solo lectura. Solo los volúmenes Snapshot que son de lectura y escritura requieren capacidad reservada.

Pasos

1. Seleccione MENU:almacenamiento[Pools y grupos de volúmenes].
2. Seleccione la pestaña **capacidad reservada**.
3. Seleccione el objeto de almacenamiento para el que desea aumentar la capacidad reservada y haga clic en **aumentar capacidad**.

   Se muestra el cuadro de diálogo aumentar la capacidad reservada.

4. Utilice el cuadro de desplazamiento para ajustar el porcentaje de capacidad.

   Si no hay capacidad libre en el pool o el grupo de volúmenes que contiene el objeto de almacenamiento seleccionado y la cabina de almacenamiento posee capacidad sin asignar, es posible crear un nuevo pool o grupo de volúmenes. Puede volver a intentar esta operación con la nueva capacidad libre en ese pool o grupo de volúmenes.

5. Haga clic en **aumentar**.

Resultados

System Manager realiza lo siguiente:

- Aumenta la capacidad reservada del objeto de almacenamiento.
- Muestra la capacidad reservada recientemente añadida.

Cambie la configuración de capacidad reservada para un volumen de parejas reflejadas

Puede cambiar la configuración del volumen de una pareja reflejada a fin de ajustar el punto de porcentaje en el que System Manager envía una notificación de alerta cuando la capacidad reservada para una pareja reflejada está casi completa.

Pasos

1. Seleccione MENU:almacenamiento[Pools y grupos de volúmenes].
2. Seleccione la pestaña **capacidad reservada**.
3. Seleccione el volumen de la pareja reflejada que desea editar y, a continuación, haga clic en **Ver/editar configuración**.

   Se muestra el cuadro de diálogo Configuración de capacidad reservada de volumen de pareja reflejada.

4. Cambie la configuración de la capacidad reservada para el volumen de la pareja reflejada, según sea necesario.

Detalles del campo

Ajuste	Descripción
Enviarme una alerta cuando…	Use el cuadro de desplazamiento para ajustar el punto de porcentaje en el que System Manager envía una notificación de alerta cuando la capacidad reservada de una pareja reflejada está casi completa. Cuando la capacidad reservada de la pareja reflejada supera el umbral especificado, System Manager envía una alerta que otorga tiempo para aumentar la capacidad reservada. Si se cambia la configuración de alertas de una pareja reflejada, se modifica la configuración de alertas de todas las parejas reflejadas que pertenecen al mismo grupo de coherencia reflejado.

5. Haga clic en **Guardar** para aplicar los cambios.

Completar pareja reflejada para volúmenes primarios creados en un sistema heredado

Si creó un volumen primario en una cabina de almacenamiento heredada que System Manager no puede gestionar, es posible crear el volumen secundario en esta cabina con System Manager.

Acerca de esta tarea

Es posible realizar un mirroring asíncrono entre las cabinas heredadas que usan una interfaz diferente y las cabinas más recientes que pueden gestionarse mediante System Manager.

- Si está por crear reflejos entre dos cabinas de almacenamiento que usan System Manager, puede omitir esta tarea porque ya finalizó la pareja reflejada en la secuencia de creación de parejas reflejadas.
- Lleve a cabo esta tarea en la cabina de almacenamiento remota.

Pasos

1. Seleccione **Storage › Asynchronous Mirroring**.
2. Seleccione la ficha **par reflejado**.

   Se muestra la tabla Mirrored Pairs con todas las parejas reflejadas asociadas con la cabina de almacenamiento.

3. Busque el volumen de la pareja reflejada con el estado incompleto y haga clic en el enlace **completar pareja reflejada** que aparece en la columna de la pareja reflejada.
4. Elija si desea completar la secuencia de creación de la pareja reflejada de manera automática o manual. Para ello, seleccione uno de los siguientes botones de opción:
   - **Automático** — crea un nuevo volumen secundario.

     Acepte la configuración predeterminada del lado remoto de la pareja reflejada. Para hacerlo, seleccione un pool o grupo de volúmenes donde desee crear el volumen secundario. Use esta opción recomendada para asignar la capacidad reservada para el volumen secundario con la configuración

predeterminada.

- **Manual** — Seleccione un volumen existente.

  Defina sus propios parámetros para el volumen secundario.

  i. Haga clic en **Siguiente** para seleccionar el volumen secundario.
  ii. Seleccione un volumen existente que desea utilizar como volumen secundario y después haga clic en **Siguiente** para asignar la capacidad reservada.
  iii. Asigne la capacidad reservada. Debe realizar una de las siguientes acciones:
    - Acepte la configuración predeterminada.

      La configuración predeterminada para la capacidad reservada es del 20 % del volumen base y, por lo general, esta capacidad es suficiente.

    - Asigne su propia configuración de capacidad reservada para satisfacer sus necesidades de almacenamiento de datos relacionadas con el mirroring asíncrono.

      La capacidad necesaria varía, según la frecuencia y el tamaño de las escrituras de I/o en el volumen primario y el tiempo que se requiere conservar la capacidad. En general, elija una capacidad mayor para la capacidad reservada si se presentan una o ambas de estas condiciones:

      - Se pretende conservar la pareja reflejada por un periodo prolongado.
      - Un gran porcentaje de bloques de datos cambiará en el volumen primario debido a una gran actividad de I/O. Utilice datos históricos de rendimiento u otra utilidad del sistema operativo para determinar la actividad de I/o típica del volumen primario.

5. Seleccione **completado**.

Resultados

System Manager realiza lo siguiente:

- Crea el volumen secundario en la cabina de almacenamiento remota y asigna la capacidad reservada del lado remoto de la pareja reflejada.
- Comienza la sincronización inicial entre la cabina de almacenamiento local y la remota.
- Si el volumen que se refleja es un volumen fino, solamente los bloques asignados se transfieren al volumen secundario durante la sincronización inicial. Esta transferencia reduce la cantidad de datos que se deben transferir para completar la sincronización inicial.
- Crea la capacidad reservada para la pareja reflejada en la cabina de almacenamiento local y la remota.

Gestionar parejas reflejadas síncronas

Prueba de comunicación para mirroring síncrono

Se puede probar la comunicación entre una cabina de almacenamiento local y una cabina de almacenamiento remota para diagnosticar posibles problemas de comunicación para una pareja reflejada que está participando en un mirroring síncrono.

Acerca de esta tarea

Se ejecutan dos pruebas diferentes:

- **Comunicación** — verifica que las dos matrices de almacenamiento tengan una ruta de comunicación. La prueba de comunicación valida la comunicación entre la cabina de almacenamiento y la cabina de almacenamiento remota, así como la existencia del volumen secundario asociado con la pareja reflejada en la cabina de almacenamiento remota.
- **Latencia** — envía un comando de unidad de prueba SCSI al volumen secundario en la matriz de almacenamiento remota asociada con la pareja reflejada para probar la latencia mínima, media y máxima.

Pasos

1. Seleccione MENU:Storage[Synchronous Mirroring].
2. Seleccione la pareja reflejada que desea probar y, a continuación, seleccione **probar comunicación**.
3. Revise la información que se muestra en la ventana resultados y, si fuera necesario, siga la acción correctiva indicada.

> Si la prueba de comunicación presenta un error, se sigue ejecutando después de cerrar este cuadro de diálogo hasta que se restablezca la comunicación entre la pareja reflejada.

Suspenda y reanude la sincronización de una pareja reflejada

Las opciones Suspender y Reanudar se pueden usar para controlar cuándo se deben sincronizar los datos en el volumen primario y en el volumen secundario en una pareja reflejada.

Acerca de esta tarea

Si una pareja reflejada se suspende de manera manual, la pareja reflejada no se sincroniza hasta que se la reanuda manualmente.

Pasos

1. Seleccione MENU:Storage[Synchronous Mirroring].
2. Debe seleccionar la pareja reflejada que desea suspender o reanudar y, a continuación, seleccionar MENU:más[Suspender] o MENU:más[Reanudar].

   El sistema muestra una confirmación.

3. Seleccione **Sí** para confirmar.

Resultados

System Manager realiza lo siguiente:

- Suspende o reanuda la transferencia de datos entre la pareja reflejada sin quitar la relación de reflejo.
- Para una pareja reflejada *suspended*:
  - Muestra **suspendido** en la tabla de parejas reflejadas.
  - Registra los datos que se escribieron en el volumen primario de la pareja reflejada mientras la sincronización se encuentra suspendida.
- En el caso de una pareja reflejada *reanuded*, escribe los datos automáticamente en el volumen secundario de la pareja reflejada cuando se reanuda la sincronización. No es necesario realizar una sincronización completa.

Cambiar roles entre volúmenes de una pareja reflejada

Es posible realizar una reversión de roles entre los dos volúmenes de una pareja reflejada que participan en un mirroring síncrono. Esta tarea puede ser necesaria para fines administrativos o en el caso de un desastre en la cabina de almacenamiento local.

Acerca de esta tarea

Es posible degradar el volumen principal al rol secundario o promocionar el volumen secundario al rol primario. Cualquier host que acceda al volumen primario tiene acceso de lectura/escritura al volumen. Cuando el volumen primario se convierte en un volumen secundario, solo se escriben en el volumen las escrituras remotas iniciadas por la controladora primaria.

Pasos

1. Seleccione MENU:Storage[Synchronous Mirroring].
2. Seleccione la pareja reflejada que contiene los volúmenes con los roles que desea cambiar y luego seleccione **más › Cambiar rol**.

   El sistema muestra una confirmación.

3. Confirme que desea cambiar el rol de los volúmenes y seleccione **Cambiar rol**.

> Si la cabina de almacenamiento local no puede comunicarse con la cabina de almacenamiento remota, se muestra el cuadro de diálogo no se puede establecer contacto con la cabina de almacenamiento en el sistema cuando se solicita un cambio de rol, pero la cabina de almacenamiento remota no puede contactarse. Haga clic en **Sí** para forzar el cambio de rol.

Resultados

System Manager realiza la siguiente acción:

- Si el volumen asociado de la pareja reflejada puede contactarse, cambian los roles entre los volúmenes. En System Manager, se promociona el volumen secundario de la pareja reflejada al rol primario o se degrada el volumen primario de la pareja reflejada al rol secundario (según la selección).

Cambiar la configuración de sincronización para una pareja reflejada

Puede cambiar la prioridad de sincronización y la política de resincronización que la pareja reflejada usa para completar la operación de resincronización después de que se interrumpe una comunicación.

Acerca de esta tarea

Es posible editar la configuración de sincronización para una pareja reflejada solo en la cabina de almacenamiento que contiene el volumen primario.

Pasos

1. Seleccione MENU:Storage[Synchronous Mirroring].
2. Seleccione la pareja reflejada que desee editar y, a continuación, seleccione MENU:más[Editar configuración].

   El sistema muestra el cuadro de diálogo Ver/editar configuración.

3. Use la barra deslizante para editar la prioridad de sincronización.

   La prioridad de sincronización determina cuántos recursos del sistema se usan para completar la operación de resincronización después de que se interrumpe una comunicación, en comparación con las solicitudes de I/o de servicio.

   Más información acerca de las tasas de sincronización

   Las tasas de prioridad de sincronización son las siguientes cinco:

   - El más bajo
   - Bajo
   - Mediano
   - Alto
   - Máxima

   Si la prioridad de sincronización se configuró con la tasa mínima, se prioriza la actividad de I/o y la operación de resincronización lleva más tiempo. Si la prioridad de sincronización se configuró con la tasa máxima, la operación de resincronización tiene prioridad, pero podría afectar a la actividad de I/o de la cabina de almacenamiento.

4. Edite la política de resincronización según corresponda.

   Es posible resincronizar las parejas reflejadas en la cabina de almacenamiento remota, ya sea de forma manual o automática.

   - **Manual** (la opción recomendada) — Seleccione esta opción para requerir que la sincronización se reanude manualmente después de restaurar la comunicación a una pareja reflejada. Esta opción proporciona la mejor oportunidad para recuperar datos.
   - **Automático** — Seleccione esta opción para iniciar la resincronización automáticamente después de restaurar la comunicación a un par reflejado.

5. Seleccione **Guardar**.

Quitar una relación de reflejo síncrono

Quite una pareja reflejada para eliminar la relación de reflejo del volumen primario en la cabina de almacenamiento local y el volumen secundario en la cabina de almacenamiento remota.

Acerca de esta tarea

También se puede quitar una pareja reflejada para corregir un estado de pareja reflejada huérfana. Revise la siguiente información sobre parejas reflejadas huérfanas:

- Se crea una pareja reflejada huérfana cuando se quita un volumen miembro de un lado (local/remoto), pero no del otro lado.
- Las parejas reflejadas huérfanas se detectan cuando se restaura la comunicación dentro de la cabina.

Pasos

1. Seleccione MENU:Storage[Synchronous Mirroring].

2. Seleccione la pareja reflejada que desea quitar y haga clic en el menú:tareas no comunes[Quitar].

   Se muestra el cuadro de diálogo Eliminar relación de reflejo.

3. Confirme que desea eliminar la pareja reflejada y, a continuación, haga clic en **Quitar**.

Resultados

System Manager realiza lo siguiente:

- Elimina la relación de reflejo de la pareja reflejada en la cabina de almacenamiento local y en la cabina de almacenamiento remota.
- Devuelve el volumen primario y el volumen secundario a los volúmenes no reflejados a los que se puede acceder desde hosts.
- Actualiza el icono Mirroring síncrono con la eliminación de la pareja reflejada síncrona.

Desactivar las operaciones de mirroring

Desactivar las operaciones de mirroring asíncrono

Es posible desactivar el mirroring asíncrono en las cabinas de almacenamiento local y remota para restablecer el uso normal de los puertos dedicados en las cabinas de almacenamiento.

Antes de empezar

- Se deben haber borrado previamente todas las relaciones de reflejo. Verifique que todos los grupos de coherencia de reflejos y las parejas reflejadas se hayan eliminado de las cabinas de almacenamiento local y remota.
- La cabina de almacenamiento local y la cabina de almacenamiento remota deben conectarse a través de una interfaz de estructura Fibre Channel o iSCSI.

Acerca de esta tarea

Cuando se desactiva el mirroring asíncrono, no se puede realizar ningún tipo de actividad de reflejo en las cabinas de almacenamiento local y remota.

Pasos

1. Seleccione **Storage › Asynchronous Mirroring**.
2. Seleccione menú:tareas no comunes[Desactivar].

   El sistema muestra una confirmación.

3. Seleccione **Sí** para confirmar.

Resultados

- Los canales de host HBA de la controladora que estaban dedicados a la comunicación de las operaciones de mirroring asíncrono ahora pueden aceptar solicitudes de lectura y escritura del host.
- Ninguno de los volúmenes de esta cabina de almacenamiento puede participar en relaciones de reflejo como volumen primario o secundario.

Desactivar la función de mirroring síncrono

Puede desactivar la función Synchronous Mirroring en una cabina de almacenamiento para restablecer el uso normal del puerto de host 4 del adaptador de bus de host (HBA), que estaba reservado para la transmisión de datos reflejados.

Antes de empezar

Previamente deben haberse borrado todas las relaciones del reflejo síncrono. Verifique que todas las parejas reflejadas se hayan eliminado de la cabina de almacenamiento.

Pasos

1. Seleccione MENU:Storage[Synchronous Mirroring].
2. Seleccione menú:tareas no comunes[Desactivar].

   El sistema muestra una confirmación.

3. Seleccione **Sí** para confirmar.

Resultados

- El puerto de host 4 de HBA de la controladora, que estaba dedicado a la comunicación de las operaciones de mirroring síncronas, ahora puede aceptar solicitudes de lectura y escritura del host.
- Se eliminan los volúmenes de capacidad reservada en la cabina de almacenamiento.

Preguntas frecuentes sobre Async

¿En qué se diferencia el mirroring asíncrono del mirroring síncrono?

La función Asynchronous Mirroring es diferente de la función Synchronous Mirroring en un aspecto esencial: Captura el estado de un volumen de origen en un momento específico en particular, y copia solo los datos que cambiaron desde la última captura de imagen.

El mirroring síncrono no captura el estado del volumen primario en un momento en el tiempo, sino que refleja en el volumen secundario todos los cambios realizados en el volumen primario. El volumen secundario es idéntico al primario en todo momento, ya que, con este tipo de reflejo, cada vez que se produce una escritura en el volumen primario, se realiza otra en el secundario. El host no recibe la confirmación de que la escritura se realizó correctamente hasta que el volumen secundario se actualiza correctamente con los cambios realizados en el volumen primario.

Con el mirroring asíncrono, la cabina de almacenamiento remota no está completamente sincronizada con la cabina de almacenamiento local, por lo que si la aplicación necesita hacer una transición hacia la cabina de almacenamiento remota debido a una pérdida de la local, pueden perderse algunas transacciones.

Comparación entre funciones de mirroring:

Mirroring asíncrono	Mirroring síncrono
Método de replicación	• **Punto en tiempo** El mirroring se realiza bajo demanda o automáticamente según la programación definida por el usuario. Las programaciones pueden definirse con una granularidad de minutos. El tiempo mínimo entre sincronizaciones es de 10 minutos.
• **Continuo** El mirroring se ejecuta automáticamente de forma continua, copiando datos en cada escritura del host.	**Capacidad reservada**
• **Múltiples** Se requiere un volumen de capacidad reservada para cada pareja reflejada.	• **Individual** Se requiere un volumen de capacidad reservada individual para todos los volúmenes reflejados.
Comunicación	• **ISCSI y Fibre Channel** Admite interfaces iSCSI y Fibre Channel entre cabinas de almacenamiento.
• **Fibre Channel** Admite solo interfaces Fibre Channel entre cabinas de almacenamiento.	**Distancia**
• **Ilimitada** Admite distancias prácticamente ilimitadas entre la cabina de almacenamiento local y la cabina de almacenamiento remota, con la distancia generalmente limitada solo por las capacidades de la red y la tecnología de extensión de canal.	• **Restringido** Generalmente debe estar dentro de una distancia de 10 km (6.2 millas) aproximadamente de la cabina de almacenamiento local para satisfacer los requisitos de latencia y rendimiento de la aplicación.

¿Por qué no puedo acceder a la función de mirroring seleccionada?

La función de mirroring se configura en la interfaz de Unified Manager.

El mirroring síncrono no está disponible en las cabinas de almacenamiento EF600 o EF300.

Para habilitar y configurar el mirroring entre dos cabinas, compruebe lo siguiente:

- El proxy de servicios web se encuentra en ejecución. (Unified Manager se encuentra instalado en un sistema host junto con el proxy de servicios web.)
- Unified Manager se ejecuta en el host local a través de una conexión HTTPS.
- Las dos cabinas de almacenamiento que se desean usar para el mirroring se detectaron en Unified Manager.
- Unified Manager tiene certificados SSL válidos para las cabinas de almacenamiento. Puede aceptar un certificado autofirmado o instalar certificados firmados por CA desde Unified Manager.

Para obtener instrucciones de configuración, consulte lo siguiente:

- "Crear una pareja reflejada asíncrona (en Unified Manager)"
- "Crear una pareja reflejada síncrona (en Unified Manager)"

¿Qué debo saber antes de crear un grupo de coherencia de reflejos?

Siga estas directrices para poder crear un grupo de coherencia de reflejos.

> El mirroring síncrono no está disponible en los sistemas de almacenamiento EF600 o EF300.

El grupo de coherencia se crea en Unified Manager en el asistente Crear pareja reflejada.

Cumpla con los siguientes requisitos para Unified Manager:

- El proxy de servicios web se encuentra en ejecución.
- Unified Manager se ejecuta en el host local a través de una conexión HTTPS.
- SANtricity Unified Manager debe mostrar los certificados SSL válidos para la cabina de almacenamiento. Es posible aceptar un certificado autofirmado o instalar una certificación de seguridad propia con Unified Manager. Para hacerlo, debe navegar hasta MENU:Certificate[Gestión de certificados].

También debe cumplir con los siguientes requisitos para las cabinas de almacenamiento:

- Las dos cabinas de almacenamiento se encuentran detectadas en Unified Manager.
- Cada cabina de almacenamiento debe tener dos controladoras.
- Cada controladora en la cabina primaria y la cabina secundaria debe tener un puerto Ethernet de gestión configurado y debe estar conectada a la red.
- Las cabinas de almacenamiento deben tener la versión de firmware 7.84 como mínimo. (Cada una puede ejecutar versiones de sistema operativo diferentes).
- Debe conocer la contraseña de las cabinas de almacenamiento remota y local.
- Las cabinas de almacenamiento local y remota se encuentran conectadas a través de una estructura Fibre Channel o una interfaz iSCSI.

Mirroring asíncrono: ¿Qué debo saber antes de crear una pareja reflejada?

Las parejas reflejadas se configuran en la interfaz de Unified Manager y, posteriormente, se gestionan en System Manager.

Antes de crear una pareja reflejada, siga estas directrices.

- Debe tener dos cabinas de almacenamiento.
- Cada cabina de almacenamiento debe tener dos controladoras.
- Cada controladora en la cabina primaria y la cabina secundaria debe tener un puerto Ethernet de gestión configurado y debe estar conectada a la red.
- Las cabinas de almacenamiento local y remota se encuentran conectadas a través de una estructura Fibre Channel o una interfaz iSCSI.
- Las cabinas de almacenamiento deben tener la versión de firmware 7.84 como mínimo. (Cada una puede ejecutar versiones de sistema operativo diferentes).
- Debe conocer la contraseña de las cabinas de almacenamiento remota y local.
- Debe tener suficiente capacidad libre en la cabina de almacenamiento remota para crear un volumen secundario mayor o igual que el volumen primario que desea reflejar.
- Instaló el proxy de servicios web y Unified Manager. Las parejas reflejadas se configuran en la interfaz de Unified Manager.
- Las dos cabinas de almacenamiento se encuentran detectadas en Unified Manager.
- La cabina de almacenamiento debe contener al menos un grupo de coherencia de reflejos. El grupo de coherencia se crea en Unified Manager en el asistente Crear pareja reflejada.

¿Qué debo saber antes de aumentar la capacidad reservada en un volumen de parejas reflejadas?

Por lo general, se debe aumentar la capacidad reservada cuando se recibe una advertencia que indica que la capacidad reservada para una pareja reflejada está por completarse. Es posible aumentar la capacidad reservada únicamente en incrementos de 8 GIB.

Para operaciones de mirroring asíncrono, la capacidad reservada, por lo general, representa el 20 % del volumen base. Elija una capacidad mayor para capacidad reservada si existe una de las siguientes condiciones o ambas:

- Se pretende conservar la pareja reflejada por un periodo prolongado.
- Un gran porcentaje de bloques de datos cambiará en el volumen primario debido a una gran actividad de I/O. Utilice datos históricos de rendimiento u otra utilidad del sistema operativo para determinar la actividad de I/o típica del volumen primario.

Es posible aumentar la capacidad reservada para una pareja reflejada llevando a cabo una de las siguientes acciones:

- Ajuste el porcentaje de capacidad para un volumen de parejas reflejadas seleccionando MENU:almacenamiento[Pools y grupos de volúmenes] y luego haga clic en la pestaña **capacidad reservada**.
- Cree un volumen nuevo usando la capacidad libre que esté disponible en un pool o grupo de volúmenes.

  Si no hay capacidad libre en ningún pool o grupo de volúmenes, es posible añadir capacidad sin configurar en forma de unidades sin usar a un pool o grupo de volúmenes.

¿Por qué no puedo aumentar la capacidad reservada con la cantidad que he solicitado?

Es posible aumentar la capacidad reservada únicamente en incrementos de 4 GIB.

Revise las siguientes directrices:

- Debe tener suficiente capacidad libre en el pool o el grupo de volúmenes para poder realizar una expansión si es necesario.

  Si no hay capacidad libre en ningún pool o grupo de volúmenes, es posible añadir capacidad sin asignar en forma de unidades no utilizadas a un pool o un grupo de volúmenes.

- El volumen en el pool o el grupo de volúmenes debe tener el estado óptima y no debe estar en ningún estado de modificación.
- Debe existir capacidad libre en el pool o grupo de volúmenes que desea usar para aumentar la capacidad.

Para las operaciones de mirroring asíncrono, generalmente es el 20 % del volumen base. Use un porcentaje más alto si cree que el volumen base se someterá a muchos cambios, o si la expectativa de duración estimada de una operación de servicio de copia de un objeto de almacenamiento será muy larga.

¿Por qué debería cambiar este porcentaje?

En general, la capacidad reservada constituye el 40 % del volumen base para operaciones Snapshot y el 20 % del volumen base para operaciones de mirroring asíncrono.

Por lo general, esta capacidad es suficiente. La capacidad necesaria varía, según la frecuencia y el tamaño de las escrituras de I/o en el volumen base y el periodo durante el cual se pretenda utilizar la operación de servicios de copia del objeto de almacenamiento.

Por lo general, se debe seleccionar un porcentaje alto de capacidad reservada si existe una de estas condiciones, o ambas:

- Si la vida útil de la operación de servicios de copia de un objeto de almacenamiento en particular será muy prolongada.
- Si un gran porcentaje de bloques de datos cambiará en el volumen base debido a una gran actividad de I/O. Utilice los datos históricos de rendimiento u otras utilidades del sistema operativo como ayuda para determinar la actividad de I/o típica en el volumen base.

¿Por qué se muestra más de un candidato de capacidad reservada?

Si existe más de un volumen en un pool o grupo de volúmenes que cumple con el porcentaje de capacidad seleccionado para el objeto de almacenamiento, se mostrarán varios candidatos.

Para actualizar la lista de candidatos recomendados, es posible modificar el porcentaje de espacio de la unidad física que desea reservar en el volumen base para las operaciones de servicios de copia. Se mostrarán los mejores candidatos en función de su selección.

¿Por qué se muestran valores no disponibles en la tabla?

En la tabla se enumeran los valores no disponible cuando la visualización de los datos ubicados en la cabina de almacenamiento remota no se encuentra disponible.

Para visualizar los datos de la cabina de almacenamiento remota, ejecute System Manager desde Unified Manager.

¿Por qué no se muestran todos los pools y grupos de volúmenes?

Cuando se crea un volumen secundario para la pareja reflejada asíncrona, el sistema muestra una lista de todos los pools y los grupos de volúmenes elegibles para esa pareja reflejada asíncrona. En esa lista, no se muestra ningún pool o grupo de volúmenes que no sea elegible para su uso.

Los pools o grupos de volúmenes pueden no ser elegibles por cualquiera de los motivos siguientes.

- Las funcionalidades de seguridad de un pool o un grupo de volúmenes no coinciden.
- Un pool o un grupo de volúmenes se encuentra en un estado distinto a Optimal.
- La capacidad de un pool o grupo de volúmenes es muy reducida.

Mirroring asincrónico: ¿Por qué no se muestran todos los volúmenes?

Cuando se selecciona un volumen primario para una pareja reflejada, se muestra una lista con todos los volúmenes elegibles.

Si algún volumen no es apto para el uso, no se muestra en esa lista. Es posible que haya volúmenes no elegibles por alguno de los siguientes motivos:

- El volumen no está en estado óptimo.
- El volumen ya participa en una relación de mirroring.
- Para los volúmenes finos, se debe habilitar la expansión automática.

> Para las controladoras EF600 y EF300, los volúmenes primario y secundario de una pareja reflejada asíncrona deben coincidir con el mismo protocolo, nivel de soporte, tamaño de segmento, tipo de seguridad y nivel de RAID. Las parejas reflejadas asíncronas no elegibles no aparecerán en la lista de volúmenes disponibles.

Mirroring asíncrono: ¿Por qué no se muestran todos los volúmenes en la cabina de almacenamiento remota?

Cuando se selecciona un volumen secundario en la cabina de almacenamiento remota, se muestra una lista de todos los volúmenes elegibles para esa pareja reflejada.

Todos los volúmenes que no son elegibles no aparecen en esa lista. Es posible que los volúmenes no sean admisibles por uno de los siguientes motivos:

- El volumen no está en estado óptimo.
- El volumen ya participa en una relación de mirroring.
- Los atributos de volumen fino entre el volumen primario y el volumen secundario no coinciden.
- Si utiliza Data Assurance (DA), el volumen primario y el secundario deben tener la misma configuración DE DA.
  - Si el volumen primario tiene la función DA habilitada, el volumen secundario también debe tenerla.
  - Si el volumen primario no tiene la función DA habilitada, el volumen secundario tampoco debe tenerla.

¿Por qué debería actualizar la dirección IP de la cabina de almacenamiento remota?

La dirección IP de la cabina de almacenamiento remota se actualiza cuando cambia la dirección IP de un puerto iSCSI y la cabina de almacenamiento local no puede comunicarse con la cabina de almacenamiento remota.

Cuando se establece una relación de mirroring asíncrono con una conexión iSCSI, tanto la cabina de almacenamiento remota como la local guardan un registro de la dirección IP de la cabina de almacenamiento remota en la configuración de mirroring asíncrono. Si cambia la dirección IP de un puerto iSCSI, la cabina de almacenamiento remota que intenta utilizar ese puerto se encuentra con un error de comunicación.

La cabina de almacenamiento con la dirección IP modificada envía un mensaje a cada cabina de almacenamiento remota asociada con los grupos de coherencia de reflejos configurados para reflejar a través de una conexión iSCSI. Las cabinas de almacenamiento que reciben este mensaje actualizan automáticamente su dirección IP objetivo remota.

Si la cabina de almacenamiento con la dirección IP modificada no puede enviar el mensaje entre cabinas a una cabina de almacenamiento remota, el sistema envía una alerta del problema de conectividad. Utilice la opción Actualizar dirección IP remota para volver a establecer la conexión con la cabina de almacenamiento local.

Preguntas frecuentes de sincronización

¿En qué se diferencia el mirroring asíncrono del mirroring síncrono?

La función Asynchronous Mirroring es diferente de la función Synchronous Mirroring en un aspecto esencial: Captura el estado de un volumen de origen en un momento específico en particular, y copia solo los datos que cambiaron desde la última captura de imagen.

El mirroring síncrono no captura el estado del volumen primario en un momento en el tiempo, sino que refleja en el volumen secundario todos los cambios realizados en el volumen primario. El volumen secundario es idéntico al primario en todo momento, ya que, con este tipo de reflejo, cada vez que se produce una escritura en el volumen primario, se realiza otra en el secundario. El host no recibe la confirmación de que la escritura se realizó correctamente hasta que el volumen secundario se actualiza correctamente con los cambios realizados en el volumen primario.

Con el mirroring asíncrono, la cabina de almacenamiento remota no está completamente sincronizada con la cabina de almacenamiento local, por lo que si la aplicación necesita hacer una transición hacia la cabina de almacenamiento remota debido a una pérdida de la local, pueden perderse algunas transacciones.

Comparación entre funciones de mirroring:

Mirroring asíncrono	Mirroring síncrono
Método de replicación	• **Punto en tiempo** El mirroring se realiza bajo demanda o automáticamente según la programación definida por el usuario. Las programaciones pueden definirse con una granularidad de minutos. El tiempo mínimo entre sincronizaciones es de 10 minutos.
• **Continuo** El mirroring se ejecuta automáticamente de forma continua, copiando datos en cada escritura del host.	**Capacidad reservada**
• **Múltiples** Se requiere un volumen de capacidad reservada para cada pareja reflejada.	• **Individual** Se requiere un volumen de capacidad reservada individual para todos los volúmenes reflejados.
Comunicación	• **ISCSI y Fibre Channel** Admite interfaces iSCSI y Fibre Channel entre cabinas de almacenamiento.
• **Fibre Channel** Admite solo interfaces Fibre Channel entre cabinas de almacenamiento.	**Distancia**
• **Ilimitada** Admite distancias prácticamente ilimitadas entre la cabina de almacenamiento local y la cabina de almacenamiento remota, con la distancia generalmente limitada solo por las capacidades de la red y la tecnología de extensión de canal.	• **Restringido** Generalmente debe estar dentro de una distancia de 10 km (6.2 millas) aproximadamente de la cabina de almacenamiento local para satisfacer los requisitos de latencia y rendimiento de la aplicación.

Mirroring síncrono: ¿Por qué no se muestran todos los volúmenes?

Cuando se selecciona un volumen primario para una pareja reflejada, se muestra una lista con todos los volúmenes elegibles.

Si algún volumen no es apto para el uso, no se muestra en esa lista. Es posible que los volúmenes no sean admisibles por uno de los siguientes motivos:

- El volumen no es estándar, por ejemplo, un volumen Snapshot o un volumen fino.
- El volumen no está en estado óptimo.
- El volumen ya participa en una relación de mirroring.

Mirroring síncrono: ¿Por qué no se muestran todos los volúmenes en la cabina de almacenamiento remota?

Cuando se selecciona un volumen secundario en la cabina de almacenamiento remota, se muestra una lista de todos los volúmenes elegibles para esa pareja reflejada.

Todos los volúmenes que no son elegibles no aparecen en esa lista. Es posible que los volúmenes no sean admisibles por uno de los siguientes motivos:

- El volumen no es estándar, por ejemplo, un volumen Snapshot o un volumen fino.
- El volumen no está en estado óptimo.
- El volumen ya participa en una relación de mirroring.
- Si utiliza Data Assurance (DA), el volumen primario y el secundario deben tener la misma configuración DE DA.
  - Si el volumen primario tiene la función DA habilitada, el volumen secundario también debe tenerla.
  - Si el volumen primario no tiene la función DA habilitada, el volumen secundario tampoco debe tenerla.

Mirroring síncrono: ¿Qué debo saber antes de crear una pareja reflejada?

Las parejas reflejadas se configuran en la interfaz de Unified Manager y, posteriormente, se gestionan en System Manager.

Antes de crear una pareja reflejada, siga estas directrices:

- Debe tener dos cabinas de almacenamiento.
- Cada cabina de almacenamiento debe tener dos controladoras.
- Cada controladora en la cabina primaria y la cabina secundaria debe tener un puerto Ethernet de gestión configurado y debe estar conectada a la red.
- Las cabinas de almacenamiento local y remota se encuentran conectadas a través de una estructura Fibre Channel.
- Las cabinas de almacenamiento deben tener la versión de firmware 7.84 como mínimo. (Cada una puede ejecutar versiones de sistema operativo diferentes).
- Debe conocer la contraseña de las cabinas de almacenamiento remota y local.
- Debe tener suficiente capacidad libre en la cabina de almacenamiento remota para crear un volumen secundario mayor o igual que el volumen primario que desea reflejar.
- Instaló el proxy de servicios web y Unified Manager. Las parejas reflejadas se configuran en la interfaz de Unified Manager.
- Las dos cabinas de almacenamiento se encuentran detectadas en Unified Manager.

¿Qué impacto tiene la prioridad de sincronización en las tasas de sincronización?

La prioridad de sincronización define la cantidad de tiempo de procesamiento que se

asigna a las actividades de sincronización en relación con el rendimiento del sistema.

El propietario de la controladora del volumen primario realiza esta operación en segundo plano. Al mismo tiempo, el propietario de la controladora procesa las escrituras de I/o en el volumen primario y las escrituras remotas asociadas en el volumen secundario. Dado que la resincronización desvía los recursos de procesamiento de la controladora de la actividad de I/o, es posible que tenga un impacto en el rendimiento de la aplicación host.

Tenga en cuentas estas directrices para determinar cuánto puede demorar una prioridad de sincronización y cómo las prioridades de sincronización pueden afectar al rendimiento del sistema.

Acerca de las tasas de prioridad de sincronización

Las siguientes tasas de prioridad se encuentran disponibles:

- El más bajo
- Bajo
- Mediano
- Alto
- Máxima

La tasa de prioridad más baja es compatible con el rendimiento del sistema, pero la resincronización demora más tiempo. La tasa de prioridad más alta es compatible con la resincronización, pero el rendimiento del sistema puede verse afectado.

Estas directrices aproximan aproximadamente las diferencias entre las prioridades.

Tasa de prioridad para la sincronización completa	Tiempo transcurrido en comparación con la tasa de sincronización más alta
El más bajo	Tiempo aproximadamente 8 veces superior a la tasa de prioridad más alta
Bajo	Tiempo aproximadamente 6 veces superior a la tasa de prioridad más alta
Mediano	Tiempo aproximadamente 3,5 veces superior a la tasa de prioridad más alta
Alto	Tiempo aproximadamente 2 veces superior a la tasa de prioridad más alta

El tamaño del volumen y las cargas de la tasa de I/o del host afectan a las comparaciones de tiempo de sincronización.

¿Por qué se recomienda usar la política de sincronización manual?

Se recomienda la resincronización manual debido a que esta permite gestionar el proceso de resincronización de un modo que garantiza la mejor oportunidad para

recuperar los datos.

Si utiliza una política de resincronización automática y surgen problemas de comunicación ocasionales durante la resincronización, podrían dañarse temporalmente los datos del volumen secundario. Una vez finalizada la resincronización, los datos se corrigen.

Almacenamiento remoto

Información general sobre las funciones de almacenamiento remoto

Si tiene la función almacenamiento remoto, puede importar datos desde un sistema de almacenamiento remoto a la cabina de almacenamiento.

¿Qué es la función de almacenamiento remoto?

La función *Remote Storage* permite importar datos desde un sistema de almacenamiento remoto a un sistema de almacenamiento E-Series local. El sistema remoto puede ser otro sistema E-Series o un sistema de otro proveedor. Esta función es útil cuando se desea optimizar la migración de datos con un tiempo de inactividad mínimo, como durante las actualizaciones de equipos.

> Para utilizar almacenamiento remoto, esta función debe estar habilitada en el identificador de submodelo (SMID).

Obtenga más información:

- "Cómo funciona el almacenamiento remoto"
- "Terminología de almacenamiento remoto"
- "Requisitos para el almacenamiento remoto"
- "Requisitos del volumen de almacenamiento remoto"

¿Cómo se importan datos con esta función?

Con el asistente de almacenamiento remoto, debe asignar un dispositivo de almacenamiento remoto (el origen de la importación de datos) a un volumen de destino en el sistema E-Series. Este asistente está disponible en MENU:Storage[Remote Storage].

Obtenga más información:

- "Importe el almacenamiento remoto"
- "Gestione el progreso de la importación de datos"

Conceptos

Cómo funciona el almacenamiento remoto

La función almacenamiento remoto permite importar datos desde un sistema de almacenamiento remoto a un sistema de almacenamiento E-Series local. Esta función es útil cuando se desea optimizar la migración de datos con un tiempo de inactividad mínimo, como durante las actualizaciones de equipos.

Para configurar la función de almacenamiento remoto, debe configurar el hardware y luego usar System Manager para crear un objeto de almacenamiento remoto. Una vez completada la configuración, comienza el proceso de importación.

Configuración de hardware

Use el siguiente flujo de trabajo para preparar las conexiones de hardware.

Estos pasos se describen con mayor detalle en la guía del usuario de la función de almacenamiento remoto, disponible en el centro de documentación de E-Series y SANtricity en "Información general sobre volúmenes de almacenamiento remoto", y en "Informe técnico sobre almacenamiento remoto".

En el sistema de almacenamiento E-Series local:

1. Asegúrese de que cada controladora tenga una conexión iSCSI con el sistema de almacenamiento remoto. Con esta conexión, el sistema E-Series local actúa como un iniciador de iSCSI que puede configurarse como host en el sistema remoto.
2. Cree un volumen de destino para la operación de importación. Asegúrese de que el volumen tenga una capacidad igual o mayor que el volumen de origen en el sistema de almacenamiento remoto, tenga un tamaño de bloque coincidente y no esté asignado. Consulte "Cree volúmenes".
3. Recopile el nombre completo de iSCSI (IQN) para el sistema E-Series local desde su interfaz de System Manager. El IQN se utilizará más adelante para configurar el sistema E-Series local como un host en el sistema de almacenamiento remoto. En System Manager, vaya a: Menú:Configuración[sistema > Configuración de iSCSI > IQN de destino].

En el sistema de almacenamiento remoto:

1. Configure el sistema E-Series local como un host en el sistema remoto, mediante su IQN. Asegúrese de configurar el tipo de host adecuado, de la siguiente manera:
   - Si el sistema remoto es un modelo E-Series, consulte "Información general sobre los hosts y los clústeres de hosts". Use un tipo de host de "opción predeterminada de fábrica".
   - Si el sistema remoto es de otro proveedor, seleccione un tipo de host adecuado según las opciones disponibles.
2. Detenga todas las operaciones de I/o, desmonte todos los sistemas de archivos y quite todas las asignaciones de hosts o aplicaciones del volumen de origen.
3. Asigne el volumen al host del sistema de almacenamiento E-Series local recién creado.
4. Para el volumen de origen seleccionado, recopile la siguiente información del sistema de almacenamiento remoto para que se pueda crear la importación:
   - Nombre completo de iSCSI (IQN)
   - Dirección IP de iSCSI
   - El número de LUN del volumen de origen

Configuración de System Manager

Utilice el siguiente flujo de trabajo para crear un objeto de almacenamiento remoto para la importación:

1. Utilice el asistente Remote Storage de la interfaz de System Manager para asignar un dispositivo de almacenamiento remoto (el origen de la importación de datos) a un volumen de destino en el sistema E-Series. Al seleccionar **Finalizar**, comienza el proceso de importación.
2. Supervise la importación desde el cuadro de diálogo Ver operaciones o el panel Operaciones en curso. Si

es necesario, también puede pausar y reanudar el proceso.

3. Opcionalmente, rompa la conexión entre los volúmenes de origen y objetivo cuando finalice la importación o mantenga la conexión para importaciones futuras.

Terminología de almacenamiento remoto

Conozca la forma en que los términos de almacenamiento remoto se aplican a su cabina de almacenamiento.

Duración	Descripción
IQN	Identificador de nombre completo de iSCSI (IQN), que es un nombre único para un iniciador o un destino iSCSI.
LUN	Número de unidad lógica, que se utiliza para identificar una unidad lógica que se puede presentar a un host para acceder.
Sistema de almacenamiento remoto	El sistema de almacenamiento donde se encuentran inicialmente los datos. El sistema de almacenamiento remoto puede ser un modelo E-Series o un sistema de otro proveedor.
Dispositivo de almacenamiento remoto	El dispositivo físico o lógico en el que los datos se almacenan inicialmente en el sistema remoto. En un sistema de almacenamiento E-Series, este se denomina "volumen".
Objeto de almacenamiento remoto	Un objeto que contiene información que permite al sistema E-Series identificar y conectarse al sistema de almacenamiento remoto. Esta información incluye las direcciones IQN e IP del sistema de almacenamiento remoto. El objeto de almacenamiento remoto representa la comunicación entre el sistema de almacenamiento remoto y el sistema E-Series.
Volumen de almacenamiento remoto	Volumen estándar en el sistema E-Series que permite el acceso a los datos a un dispositivo de almacenamiento remoto.
Volumen	Contenedor en el que se almacenan los datos. Es el componente lógico que se crea para que el host acceda a los datos.

Requisitos de funciones de almacenamiento remoto

Antes de utilizar la función almacenamiento remoto, revise los siguientes requisitos y restricciones.

Protocolos compatibles

Se admiten los siguientes protocolos:

- ISCSI
- IPv4

Para obtener información actualizada sobre soporte y configuración de E-Series, consulte "Herramienta de

matriz de interoperabilidad de NetApp".

Requisitos de hardware

El sistema de almacenamiento E-Series debe incluir:

- Dos controladoras (modo doble)
- Conexiones iSCSI para las dos controladoras E-Series para comunicarse con el sistema de almacenamiento remoto a través de una o varias conexiones iSCSI
- SANtricity OS 11.71 o superior
- Función de almacenamiento remoto habilitada en el ID de submodelo (SMID)

El sistema remoto puede ser un sistema de almacenamiento E-Series o un sistema de otro proveedor. Debe incluir:

- Interfaces compatibles con iSCSI

Restricciones

La función de almacenamiento remoto tiene las siguientes restricciones:

- Debe deshabilitarse la función de mirroring.
- El volumen de destino del sistema E-Series no debe tener snapshots.
- El volumen de destino del sistema E-Series no debe asignarse a ningún host antes de que se inicie la importación.
- El volumen de destino del sistema E-Series debe tener deshabilitado el aprovisionamiento de recursos.
- No se admiten asignaciones directas del volumen de almacenamiento remoto a un host o varios hosts.
- No se admite el proxy de servicios web.
- No se admiten los secretos CHAP de iSCSI.
- SMcli no es compatible.
- No se admite el almacén de datos de VMware.
- Solo se puede actualizar un sistema de almacenamiento de la pareja de relación/importación a la vez cuando existe una pareja de importación.

Requisitos del volumen de almacenamiento remoto

Los volúmenes utilizados para las importaciones deben cumplir los requisitos de tamaño, estado y otros criterios.

Volumen de almacenamiento remoto

El volumen de origen de una importación se denomina "volumen de almacenamiento remoto". Este volumen debe cumplir con los siguientes criterios:

- No puede ser parte de otra importación
- Debe tener el estado en línea

Después de comenzar la importación, el firmware de la controladora crea un volumen de almacenamiento remoto en segundo plano. Debido a ese proceso en segundo plano, el volumen de almacenamiento remoto no

puede gestionarse en System Manager y solo se puede utilizar para la operación de importación.

Después de crearse, el volumen de almacenamiento remoto se trata como cualquier otro volumen estándar en el sistema E-Series, con las siguientes excepciones:

- Se pueden utilizar como proxies para el dispositivo de almacenamiento remoto.
- No se pueden usar como candidatos para otras copias de volumen o copias de Snapshot.
- No se puede cambiar la configuración de Garantía de datos mientras la importación está en curso.
- No puede asignarse a ningún host, ya que están reservados estrictamente para la operación de importación.

Cada volumen de almacenamiento remoto se asocia con un solo objeto de almacenamiento remoto; sin embargo, un objeto de almacenamiento remoto se puede asociar con varios volúmenes de almacenamiento remotos. El volumen de almacenamiento remoto se identifica de forma única mediante una combinación de lo siguiente:

- Identificador de objeto de almacenamiento remoto
- Número LUN del dispositivo de almacenamiento remoto

Candidatos de volumen objetivo

El volumen de destino es el volumen de destino en el sistema E-Series local. El volumen de destino debe cumplir con los siguientes criterios:

- Debe ser un volumen RAID/DDP.
- Debe tener una capacidad igual o mayor que el volumen de almacenamiento remoto.
- Debe tener un tamaño de bloque que sea igual al volumen de almacenamiento remoto.
- Debe tener un estado válido (óptimo).
- No puede tener ninguna de las siguientes relaciones: Copia de volumen, copias Snapshot, mirroring asíncrono o síncrono.
- No se pueden realizar operaciones de reconfiguración: Expansión de volumen dinámica, expansión de capacidad dinámica, tamaño de segmentos dinámico, migración RAID dinámica, reducción de capacidad dinámica, O desfragmentación.
- No se puede asignar a un host antes de que se inicie la importación (sin embargo, puede asignarse una vez que finaliza la importación).
- No se puede activar la función de lectura en caché (FRC) de Flash.

System Manager comprueba automáticamente estos requisitos como parte del asistente Import Remote Storage. Para la selección del volumen de destino, solo se muestran los volúmenes que cumplen todos los requisitos.

Gestione el almacenamiento remoto

Importe el almacenamiento remoto

Para iniciar la importación de almacenamiento desde un sistema remoto a un sistema de almacenamiento E-Series local, utilice el asistente Importar almacenamiento remoto.

Antes de empezar

- El sistema de almacenamiento E-Series debe estar configurado para comunicarse con el sistema de almacenamiento remoto.

> La configuración del hardware se describe en la guía de usuario de la función de almacenamiento remoto, disponible en el centro de documentación de E-Series y SANtricity en "Configure el hardware", y en "Informe técnico sobre almacenamiento remoto".

- Para el sistema de almacenamiento remoto, recopile la siguiente información:
  - IQN de iSCSI
  - Direcciones IP de iSCSI
  - Número de LUN del dispositivo de almacenamiento remoto (volumen de origen)
- Para el sistema de almacenamiento E-Series local, cree o seleccione un volumen que usará para la importación de datos. Consulte "Cree volúmenes". El volumen objetivo debe cumplir con los siguientes requisitos:
  - Coincide con el tamaño de bloque del dispositivo de almacenamiento remoto (el volumen de origen).
  - Tiene una capacidad igual o mayor que el dispositivo de almacenamiento remoto.
  - Tiene un estado óptimo y está disponible.

Para obtener una lista completa de los requisitos, consulte "Requisitos del volumen de almacenamiento remoto".

- **Recomendado:** haga una copia de seguridad de los volúmenes en el sistema de almacenamiento remoto antes de iniciar el proceso de importación.

Acerca de esta tarea

En esta tarea, se crea un mapa entre el dispositivo de almacenamiento remoto y un volumen en el sistema de almacenamiento E-Series local. Cuando finalice la configuración, se iniciará la importación.

> Dado que muchas variables pueden afectar a la operación de importación y a su tiempo de finalización, recomendamos que realice primero importaciones más pequeñas de «prueba». Utilice estas pruebas para asegurarse de que todas las conexiones funcionan según lo esperado y de que la operación de importación finaliza en un tiempo adecuado.

Pasos

1. Seleccione MENU:Storage[Remote Storage].
2. Haga clic en **Importar almacenamiento remoto**.

   Se muestra el asistente para importar el almacenamiento remoto.

3. En **Paso 1a** del panel Configurar origen, introduzca la información de conexión. Si desea agregar otra conexión iSCSI, haga clic en **Añadir otra dirección IP** para incluir una dirección IP adicional para el almacenamiento remoto. Cuando haya terminado, haga clic en **Siguiente**.

Detalles del campo

Ajuste	Descripción
Nombre	Introduzca un nombre para el dispositivo de almacenamiento remoto e identificarlo en la interfaz de System Manager. Un nombre puede incluir hasta 30 caracteres, y puede contener sólo letras, números y los siguientes caracteres especiales: Subrayado (_), guión (-), y el signo de hash (#). Un nombre no puede contener espacios.
Propiedades de la conexión iSCSI	Introduzca las propiedades de conexión del dispositivo de almacenamiento remoto: • **Nombre completo iSCSI (IQN)**: Introduzca el IQN iSCSI. • **Dirección IP**: Introduzca la dirección IPv4. • **Puerto**: Introduzca el número de puerto que se va a utilizar para las comunicaciones entre los dispositivos de origen y destino. De manera predeterminada, el número de puerto es 3260.

Después de hacer clic en **Siguiente**, se muestra el **Paso 1b** del panel Configurar origen.

4. En el campo **LUN**, seleccione el número de LUN del dispositivo de almacenamiento remoto que se va a utilizar como fuente y, a continuación, haga clic en **Siguiente**.

   Se abre el panel Configurar destino y se muestran candidatos de volumen que sirven como objetivo para la importación. Algunos volúmenes no se muestran en la lista de candidatos debido a la disponibilidad de los volúmenes, la capacidad o el tamaño de los bloques.

5. En la tabla, seleccione un volumen objetivo en el sistema de almacenamiento E-Series. Si es necesario, use el control deslizante para cambiar la prioridad de importación. Haga clic en **Siguiente**. Escriba para confirmar la operación en el siguiente cuadro de diálogo `continue`Y, a continuación, haga clic en **continuar**.

   Si el volumen objetivo tiene una capacidad mayor que el volumen de origen, no se informa de la capacidad adicional al host conectado al sistema E-Series. Para usar la nueva capacidad, debe ejecutar una operación de ampliación de sistema de archivos en el host una vez completada la operación de importación y desconectada.

   Después de confirmar la configuración en el cuadro de diálogo, se muestra el panel revisar.

6. En el panel Revisión, compruebe que los ajustes son precisos y, a continuación, haga clic en **Finalizar** para iniciar la importación.

   Se abre otro cuadro de diálogo preguntándole si desea iniciar otra importación.

7. Si es necesario, haga clic en **Sí** para crear otra importación de almacenamiento remoto. Al hacer clic en **Sí**, se vuelve a **Paso 1a** del panel Configurar origen, donde puede seleccionar la configuración existente o agregar una nueva. Si no desea crear otra importación, haga clic en **no** para salir del cuadro de diálogo.

   Una vez iniciado el proceso de importación, se sobrescribe todo el volumen objetivo con los datos copiados. Si el host escribe todos los datos nuevos en el volumen objetivo durante el proceso, esos datos

nuevos se propagan nuevamente al dispositivo remoto (volumen de origen).

8. Vea el progreso de la operación en el cuadro de diálogo Ver operaciones en el panel almacenamiento remoto.

Resultados

El tiempo requerido para completar la operación de importación depende del tamaño del sistema de almacenamiento remoto, de la configuración de prioridad para la importación y de la cantidad de carga de I/o tanto en los sistemas de almacenamiento como en los volúmenes asociados.

Una vez finalizada la importación, el volumen local es un duplicado del dispositivo de almacenamiento remoto.

Después de terminar

Cuando esté listo para romper la relación entre los dos volúmenes, seleccione **desconectar** en el objeto de importación de la vista Operaciones en curso. Una vez que se desconecta la relación, el rendimiento del volumen local vuelve a la normalidad y ya no se ve afectado por la conexión remota.

Gestione el progreso de las importaciones de almacenamiento remoto

Una vez que comienza el proceso de importación, puede ver y actuar sobre su progreso.

Acerca de esta tarea

Para cada operación de importación, el cuadro de diálogo Operaciones en curso muestra un porcentaje de finalización y el tiempo restante estimado. Las acciones incluyen cambiar la prioridad de importación, detener y reanudar operaciones, y desconectarse de la operación.

También es posible ver operaciones en curso en la página Inicio (MENU:Inicio[Mostrar operaciones en curso]).

Pasos

1. En la página almacenamiento remoto, seleccione **Ver operaciones**.

   Se muestra el cuadro de diálogo Operaciones en curso.

2. Si lo desea, utilice los vínculos de la columna **acciones** para detener y reanudar, cambiar la prioridad o desconectarse de una operación.
   - **Cambiar prioridad** — Seleccione **Cambiar prioridad** para cambiar la prioridad de procesamiento de una operación en curso o pendiente. Aplique una prioridad a la operación y, a continuación, haga clic en **Aceptar**.
   - **Stop** — Seleccione **Stop** para pausar la copia de datos del dispositivo de almacenamiento remoto. La relación entre el par de importación sigue intacta y puede seleccionar **Reanudar** cuando esté listo para continuar con la operación de importación.
   - **Reanudar** — Seleccione **Reanudar** para comenzar un proceso detenido o fallido desde el punto en que lo dejó. A continuación, aplique una prioridad a la operación Reanudar y, a continuación, haga clic en **Aceptar**. Esta operación *not* reinicia la importación desde el principio. Si desea reiniciar el proceso desde el principio, debe seleccionar **desconectar** y volver a crear la importación a través del asistente Importar almacenamiento remoto.
   - **Desconectar** — Seleccione **desconectar** para romper la relación entre los volúmenes de origen y destino para una operación de importación que se haya detenido, completado o fallido.

Modifique la configuración de conexión para el almacenamiento remoto

Es posible editar, añadir o eliminar la configuración de conexión para cualquier

configuración de almacenamiento remoto mediante la opción Ver/editar configuración.

Acerca de esta tarea

Realizar cambios en las propiedades de conexión afectará a las importaciones en curso. Para evitar interrupciones, sólo realice cambios en las propiedades de conexión cuando no se estén ejecutando las importaciones.

Pasos

1. Seleccione MENU:Storage[Remote Storage].
2. Seleccione el objeto de almacenamiento remoto de la lista que desea modificar.
3. Haga clic en **Ver/editar configuración**.

   Se muestra el cuadro de diálogo Configuración de almacenamiento remoto.

4. Haga clic en la ficha **Propiedades de conexión**.

   Se mostrarán la dirección IP configurada y la configuración de puerto para la importación de almacenamiento remoto.

5. Ejecute una de las siguientes acciones:
   - **Editar** — haga clic en **Editar** junto al elemento de línea correspondiente para el objeto de almacenamiento remoto. Introduzca la dirección IP revisada y/o la información del puerto en los campos.
   - **Agregar** — haga clic en **Agregar** y, a continuación, introduzca la nueva dirección IP e información del puerto en los campos proporcionados. Haga clic en **Agregar** para confirmar y, a continuación, la nueva conexión aparece en la lista de objetos de almacenamiento remoto.
   - **Eliminar** — Seleccione la conexión deseada de la lista y, a continuación, haga clic en **Eliminar**. Confirme la operación escribiendo `delete` En el campo proporcionado y, a continuación, haga clic en **Eliminar**. La conexión se elimina de la lista de objetos de almacenamiento remoto.
6. Haga clic en **Guardar**.

   La configuración de conexión modificada se aplica al objeto de almacenamiento remoto.

Quitar el objeto de almacenamiento remoto

Después de que finalice la importación, puede quitar un objeto de almacenamiento remoto si ya no desea copiar los datos entre los dispositivos local y remoto.

Antes de empezar

Asegúrese de que no haya importaciones asociadas con el objeto de almacenamiento remoto que desee quitar.

Acerca de esta tarea

Al quitar un objeto de almacenamiento remoto, se eliminan las conexiones entre los dispositivos local y remoto.

Pasos

1. Seleccione MENU:Storage[Remote Storage].
2. Seleccione el objeto de almacenamiento remoto que desea quitar de la lista.

3. Haga clic en **Quitar**.

   Se mostrará el cuadro de diálogo Confirmar eliminación de conexión de almacenamiento remoto.

4. Confirme la operación escribiendo `remove` Y, a continuación, haga clic en **Quitar**.

   Se elimina el objeto de almacenamiento remoto seleccionado.

Preguntas frecuentes

¿Qué debo saber antes de crear una conexión de almacenamiento remota?

Para configurar la función almacenamiento remoto, debe conectar directamente el dispositivo remoto y los sistemas de almacenamiento de destino a través de iSCSI.

Para configurar la conexión del sistema iSCSI, consulte:

- "Configure los puertos iSCSI"
- "Informe técnico sobre almacenamiento remoto"

¿Por qué se me pide que quite mis volúmenes remotos?

Cuando alcanza el número máximo de volúmenes remotos, el sistema de almacenamiento detecta automáticamente los volúmenes remotos sin usar y solicita su eliminación.

Hay algunos casos en los que los volúmenes remotos no utilizados no se borran durante el proceso de creación. Antes de iniciar cualquier operación de importación adicional, compruebe que sus sistemas son óptimos y que las conexiones de red son estables.

¿Por qué no se muestran todos los volúmenes en la cabina de destino?

Cuando se configura una importación para la función almacenamiento remoto, es posible que algunos volúmenes no aparezcan en la lista de candidatos de objetivo debido al tamaño de bloque, la capacidad o la disponibilidad de volumen.

Para que aparezca en la lista, los candidatos de volumen deben tener:

- Capacidad igual o mayor que el volumen remoto.
- El tamaño de bloque que es igual que el volumen remoto.
- Estado actual de óptima.

Volúmenes los candidatos se excluyen de la lista si tienen:

- Cualquiera de las siguientes relaciones: Copia de volumen, Snapshot o mirroring.
- Operación de reconfiguración en curso.
- Asignación a otro dispositivo (host o clúster de hosts).
- Flash Cache de lectura habilitada.

¿Qué debo saber acerca del volumen remoto de una importación?

Si utiliza la función de almacenamiento remoto, tenga en cuenta que el volumen remoto es el origen desde el que se originan los datos.

Cuando la importación está en curso, los datos se transfieren del volumen remoto al volumen de destino en el sistema de almacenamiento de destino. Estos dos volúmenes deben tener un tamaño de bloque coincidente.

¿Qué debo saber antes de iniciar una importación de almacenamiento remoto?

La función de almacenamiento remoto permite copiar datos desde un sistema de almacenamiento remoto a un volumen en un sistema de almacenamiento E-Series local. Antes de utilizar esta función, revise las siguientes directrices.

Configuración

Antes de crear la importación de almacenamiento remoto, debe completar las siguientes acciones y comprobar las siguientes condiciones:

- Asegúrese de que cada controladora del sistema de almacenamiento E-Series local tenga una conexión iSCSI con el sistema de almacenamiento remoto.
- En el sistema de almacenamiento E-Series local, cree un volumen objetivo para la operación de importación. Asegúrese de que el volumen tenga una capacidad igual o mayor que el volumen de origen, tenga un tamaño de bloque que coincida con el volumen de origen y no se asigne. Consulte "Cree volúmenes".
- Configure el sistema de almacenamiento E-Series local como un host en el sistema remoto mediante su nombre completo iSCSI (IQN). Es posible ver el IQN desde MENU:Settings[System > iSCSI settings > Target IQN]. Además, asegúrese de configurar el tipo de host adecuado según el sistema que se utilice.
- Detenga todas las operaciones de I/o, desmonte todos los sistemas de archivos y quite todas las asignaciones de hosts o aplicaciones del volumen seleccionado en el sistema de almacenamiento remoto.
- Asigne el volumen al sistema de almacenamiento remoto al host del sistema de almacenamiento E-Series local recién creado.
- Recopile la siguiente información del sistema de almacenamiento remoto para poder crear la importación:
  - Nombre completo de iSCSI (IQN)
  - Dirección IP de iSCSI
  - El número LUN del dispositivo de almacenamiento remoto, donde se originan los datos de origen
- Una vez iniciado el proceso de importación, se sobrescribe todo el volumen de destino local con los datos copiados. Todos los datos nuevos escritos en el volumen de destino local se propagan al volumen en el dispositivo de almacenamiento remoto una vez creada la importación. Por lo tanto, se recomienda realizar backups de los volúmenes en el sistema de almacenamiento remoto antes de iniciar el proceso de importación.

Proceso de importación

Los siguientes pasos describen el proceso de importación.

1. Acceda a la interfaz de System Manager y vaya a la página **almacenamiento remoto**. Seleccione **Importar** para iniciar una nueva creación de importación. Para obtener instrucciones detalladas, consulte "Importe el almacenamiento remoto".

Si desea realizar una importación sin conexión, no asigne el volumen de destino hasta que finalice la importación.

2. Supervise el progreso de la importación.

   Una vez iniciada la importación, se puede asignar el volumen de destino. El tiempo requerido para completar la operación de importación depende del tamaño del dispositivo de almacenamiento remoto (volumen de origen), la configuración de prioridad para la importación y la cantidad de carga de I/o tanto en los sistemas de almacenamiento como en los volúmenes asociados.

   Después de la importación completada, el volumen objetivo es un duplicado del origen.

3. Cuando esté listo para romper la relación de asignación, realice un **desconectar** en el objeto de importación desde el panel **Operaciones en curso**.

Una vez desconectada la importación, el rendimiento del destino local vuelve a la normalidad y ya no se ve afectado por la conexión remota.

Restricciones

La función de almacenamiento remoto tiene las siguientes restricciones:

- Debe deshabilitarse la función de mirroring.
- El volumen de destino del sistema E-Series no debe tener snapshots.
- El volumen de destino del sistema E-Series no debe asignarse a ningún host antes de que se inicie la importación.
- El volumen de destino del sistema E-Series debe tener deshabilitado el aprovisionamiento de recursos.
- No se admiten asignaciones directas del volumen de almacenamiento remoto a un host o varios hosts.
- No se admite el proxy de servicios web.
- No se admiten los secretos CHAP de iSCSI.
- SMcli no es compatible.
- No se admite el almacén de datos de VMware.
- Solo se puede actualizar un sistema de almacenamiento de la pareja de relación/importación a la vez cuando existe una pareja de importación.

Información adicional

Encontrará más información sobre la función almacenamiento remoto en la "Informe técnico sobre almacenamiento remoto".

Componentes de hardware

Información general de los componentes de hardware

Es posible comprobar el estado de los componentes en la página hardware y realizar algunas funciones relacionadas con ellos.

¿Qué componentes puedo gestionar?

Es posible comprobar el estado de los componentes y realizar algunas funciones relacionadas con estos componentes:

- **Bandejas** — a *shelf* es un componente que contiene el hardware de la cabina de almacenamiento (controladoras, contenedores de alimentación/ventilador y unidades). Las bandejas están disponibles en tres tamaños con capacidad para 12, 24 o 60 unidades.
- **Controllers** — A *Controller* es la combinación de hardware y firmware que implementa funciones de cabina de almacenamiento y administración. Incluye la memoria caché, el soporte para unidades y los puertos para las conexiones de host.
- **Drives** — a *drive* puede ser una unidad de disco duro (HDD) o una unidad de estado sólido (SSD). Según el tamaño de la bandeja, puede instalarse un máximo de 12, 24 o 60 unidades en la bandeja.

Obtenga más información:

- "Página hardware"
- "Terminología de hardware"

¿Cómo puedo ver los componentes de hardware?

Vaya a la página hardware, que ofrece una descripción gráfica de los componentes físicos de la cabina de almacenamiento. Puede alternar entre las vistas frontal y trasera de las estanterías de arrays seleccionando **Mostrar parte posterior de la estantería** o **Mostrar frente de la estantería** en la parte superior derecha de la vista de la estantería.

Obtenga más información:

- "Ver el estado y la configuración de componentes de bandejas"
- "Ver la configuración de la controladora"
- "Ver el estado y la configuración de las unidades"

Información relacionada

Más información acerca de conceptos relacionados con el hardware:

- "estados de la controladora"
- "estados de unidad"
- "Protección contra pérdida de bandeja y protección contra pérdida de cajón"

Conceptos

Componentes y página hardware

La página hardware ofrece una descripción gráfica de los componentes físicos de la cabina de almacenamiento. Desde aquí, es posible comprobar el estado de los componentes y realizar algunas funciones relacionadas con ellos.

Bandejas

Una bandeja es un componente que contiene el hardware de la cabina de almacenamiento (controladoras, contenedor de alimentación/ventilador y unidades). Existen dos clases de bandejas:

- **Bandeja de controladoras** — contiene las unidades, contenedores de alimentación/ventilador y controladores.
- **Bandeja de unidades** (o **Bandeja de expansión**): Contiene unidades, contenedores de alimentación/ventilador y dos módulos de entrada/salida (IOM). Los IOM, también denominados módulos de servicio de entorno (ESM), incluyen puertos SAS que conectan la bandeja de unidades con la bandeja de controladoras.

Las bandejas están disponibles en tres tamaños con capacidad para 12, 24 o 60 unidades. Cada bandeja incluye un número de ID, que asigna el firmware de la controladora. El ID se muestra en la esquina superior izquierda de la vista de bandeja.

La vista de bandeja en la página hardware muestra los componentes delanteros o traseros. Puede alternar entre las dos vistas seleccionando **Mostrar parte posterior de la estantería** o **Mostrar frente de la estantería** en la parte superior derecha de la vista de estantería. También puede seleccionar **Mostrar todo frente** o **Mostrar todo detrás** en la parte inferior de la página. Las vistas delantera y trasera muestran lo siguiente:

- **Componentes delanteros** — Drives y bahías de unidades vacías.
- **Componentes traseros** — controladoras y contenedores de alimentación/ventilador (para bandejas de controladoras) o los IOM y los contenedores de alimentación/ventilador (para bandejas de unidades).

Es posible ejecutar las siguientes funciones relacionadas con las bandejas:

- Encender la luz de localización de la bandeja para poder encontrar la ubicación física de la bandeja en el armario o rack.
- Cambiar el número de ID que se muestra en la esquina superior izquierda de la vista de bandeja.
- Ver la configuración de la bandeja, como los tipos de unidades instaladas y el número de serie.
- Mover las vistas de bandejas hacia arriba o hacia abajo para que coincidan con la disposición física en la cabina de almacenamiento.

Controladoras

Una controladora es la combinación de hardware y firmware que implementa funciones de cabina de almacenamiento y gestión. Incluye la memoria caché, el soporte para unidades y el soporte de interfaz host.

Es posible ejecutar las siguientes funciones relacionadas con las controladoras:

- Configurar la velocidad y las direcciones IP de los puertos de gestión.
- Configurar las conexiones de hosts iSCSI (en caso de que el usuario posea hosts iSCSI).
- Configurar un servidor de protocolo de tiempo de redes (NTP) y un servidor de sistema de nombres de dominio (DNS).
- Ver el estado y la configuración de las controladoras.
- Permitir que usuarios fuera de la red de área local inicien una sesión SSH y cambien la configuración en la controladora.
- Colocar la controladora en los modos en línea, sin conexión y de servicio.

Unidades

La cabina de almacenamiento puede incluir unidades de disco duro (HDD) o unidades de estado sólido (SSD). Según el tamaño de la bandeja, puede instalarse un máximo de 12, 24 o 60 unidades en la bandeja.

Se pueden ejecutar las siguientes funciones relacionadas con las unidades:

- Encender la luz de localización de la unidad para poder encontrar la ubicación física de la unidad en la bandeja.
- Ver el estado y la configuración de las unidades.
- Volver a asignar la unidad (reemplazar lógicamente la unidad con error por una unidad sin asignar) y reconstruir manualmente la unidad si es necesario.
- Relevar manualmente las funciones de una unidad para poder reemplazarla. (Si se produce un fallo en una unidad, es posible copiar el contenido de la unidad antes de sustituirla).
- Asignar o anular la asignación de piezas de repuesto.
- Borrar unidades.

Terminología de hardware

Los siguientes términos de hardware se aplican a las cabinas de almacenamiento.

Términos generales de hardware:

Componente	Descripción
Bahía	Una bahía es una ranura de la bandeja donde se instalan una unidad u otro componente.
Controladora	Una controladora consta de una placa, un firmware y un software. Controla las unidades e implementa las funciones de System Manager.
Bandeja de controladoras	Una bandeja de controladoras consta de un conjunto de unidades y uno o más contenedores de controladoras. Un contenedor de controladora contiene las controladoras, las tarjetas de interfaz del host (HIC) y las baterías.
Unidad	Una unidad es un dispositivo mecánico electromagnético o un dispositivo de memoria de estado sólido que proporciona medios de almacenamiento físico para datos.
Bandeja de unidades	Una bandeja de unidades, también denominada bandeja de expansión, consta de un conjunto de unidades y dos módulos de I/o (IOM). Los IOM tienen puertos SAS que permiten conectar una bandeja de unidades a una bandeja de controladoras o a otras bandejas de unidades.
IOM (ESM)	Un IOM es un módulo de entrada/salida que incluye puertos SAS para conectar la bandeja de unidades a la bandeja de controladoras. En los modelos anteriores de la controladora, el IOM se denominaba módulo de servicios de entorno (ESM).
Contenedor de alimentación/ventilador	Un contenedor de alimentación/ventilador es un ensamblaje que se desliza en una bandeja. Incluye un suministro de alimentación y un ventilador incorporado.
SFP	Un SFP es un transceptor de factor de forma pequeño conectable.
Bandeja	Una bandeja es un compartimento que se instala en un armario o rack. Incluye componentes de hardware para la cabina de almacenamiento. Existen dos tipos de bandejas: Una bandeja de controladoras y una de unidades. La bandeja de controladoras incluye controladoras y unidades. Una bandeja de unidades incluye módulos de I/o (IOM) y unidades.
Cabina de almacenamiento	Una cabina de almacenamiento comprende las bandejas, las controladoras, las unidades, el software y el firmware.

Términos de la controladora:

Componente	Descripción
Controladora	Una controladora consta de una placa, un firmware y un software. Controla las unidades e implementa las funciones de System Manager.
Bandeja de controladoras	Una bandeja de controladoras consta de un conjunto de unidades y uno o más contenedores de controladoras. Un contenedor de controladora contiene las controladoras, las tarjetas de interfaz del host (HIC) y las baterías.
DHCP	El protocolo de configuración dinámica de hosts (DHCP) es un protocolo que se usa en las redes de protocolo de Internet (IP) para los parámetros de configuración de red de distribución dinámica, como las direcciones IP.
DNS	El sistema de nombres de dominio (DNS) es un sistema de nomenclatura para los dispositivos conectados a Internet o a una red privada. El servidor DNS conserva un directorio de nombres de dominio y los convierte en direcciones de protocolos de Internet (IP).
Configuraciones dobles	Se denomina "doble" a la configuración de un módulo de dos controladoras dentro de la cabina de almacenamiento. Los sistemas dobles son completamente redundantes con respecto a las controladoras, las rutas de volumen lógico y las rutas de discos. Si se produce un error en una controladora, la otra se encarga de las operaciones de I/o para mantener la disponibilidad. Los sistemas dobles también tienen ventiladores y suministros de alimentación redundantes.
Conexiones doble total/doble parcial	Las denominaciones doble total y doble parcial se relacionan con los modos de conexión. En el modo doble total, dos dispositivos se pueden comunicar de forma simultánea en ambas direcciones. En el modo doble parcial, los dispositivos se pueden comunicar en una dirección a la vez (un dispositivo envía un mensaje, mientras el otro lo recibe).
HIC	En forma opcional, se puede instalar una tarjeta de interfaz del host (HIC) en un contenedor de controladora. Los puertos de host que están incorporados en la controladora se denominan puertos de host de la placa base. Los puertos de host que están incorporados en HIC se denominan puertos de HIC.
Respuesta ICMP PING	El protocolo de mensajes de control de Internet (ICMP) es un protocolo que usan los sistemas operativos de ordenadores conectados a una red para enviar mensajes. Los mensajes ICMP determinan si se puede acceder a un host y cuánto tiempo lleva trasladar paquetes desde o hacia ese host.
Dirección MAC	Ethernet utiliza identificadores de control de acceso de medios (direcciones MAC) para distinguir entre canales lógicos distintos que conectan dos puertos en la misma interfaz de red de transporte físico.

Componente	Descripción
cliente de gestión	Un cliente de gestión es el equipo donde se instala un explorador para acceder a System Manager.
MTU	Una unidad de transmisión máxima (MTU) es el paquete o el marco de mayor tamaño que se pueden enviar en una red.
NTP	El protocolo de tiempo de redes (NTP) es un protocolo de redes para la sincronización del reloj entre los sistemas informáticos en las redes de datos.
Configuraciones simples	Se denomina simple a la configuración de módulos de controladora única en la cabina de almacenamiento. Un sistema simple no ofrece redundancia de la controladora ni de la ruta del disco, pero tiene ventiladores y suministros de alimentación redundantes.
VLAN	Una red de área local virtual (VLAN) es una red lógica que se comporta como si estuviera físicamente separada de otras redes compatibles con los mismos dispositivos (interruptores, enrutadores, etc.).

Términos de unidad:

Componente	Descripción
DA	La garantía de datos (DA) es una función que comprueba y corrige los errores que se pueden producir durante la transferencia de datos a través de las controladoras hasta las unidades. Garantía de datos se puede habilitar en el nivel del pool o grupo de volúmenes, y los hosts pueden utilizar una interfaz de I/o compatible CON DA como, por ejemplo, Fibre Channel.
Función Drive Security	Drive Security es una función de la cabina de almacenamiento que ofrece una capa adicional de seguridad con unidades de cifrado de disco completo (FDE) o unidades de estándar de procesamiento de información federal (FIPS). Cuando estas unidades se usan con la función Drive Security, se requiere una clave de seguridad para acceder a los datos. Cuando se retiran físicamente, las unidades de la cabina no pueden operar hasta que se instalan en otra cabina, instancia en la cual tendrán el estado Security Locked hasta que se proporcione la clave de seguridad correcta.
Bandeja de unidades	Una bandeja de unidades, también denominada bandeja de expansión, consta de un conjunto de unidades y dos módulos de I/o (IOM). Los IOM tienen puertos SAS que permiten conectar una bandeja de unidades a una bandeja de controladoras o a otras bandejas de unidades.
DULBE	Error de bloque lógico no escrito o desasignado (DULBE) es una opción en las unidades NVMe con la que la cabina de almacenamiento EF300 o EF600 puede admitir volúmenes con aprovisionamiento de recursos.
Unidades FDE	Las unidades de cifrado de disco completo (FDE) realizan el cifrado en la unidad de disco en el nivel de hardware. La unidad de disco duro contiene un chip ASIC que cifra los datos durante las escrituras y, a continuación, descifra los datos durante las lecturas.
Unidades FIPS	Las unidades con FIPS utilizan estándares de procesamiento de información federal (FIPS) 140-2 nivel 2. Son esencialmente unidades FDE que cumplen con las normas gubernamentales de los Estados Unidos para garantizar algoritmos y métodos de cifrado sólidos. Las unidades FIPS tienen normas de seguridad más rigurosas que las unidades FDE.
HDD	Las unidades de disco duro (HDD) son dispositivos de almacenamiento de datos que utilizan discos de metal giratorios con un revestimiento magnético.
Unidades de repuesto	Las piezas de repuesto actúan como unidades en espera en los grupos de volúmenes RAID 1, RAID 5 o RAID 6. Son unidades completamente funcionales que no contienen datos. Si se produce un error en una unidad del grupo de volúmenes, la controladora automáticamente reconstruye los datos de la unidad con error en una pieza de repuesto.

Componente	Descripción
NVMe	La memoria no volátil rápida (NVMe) es una interfaz designada para dispositivos de almacenamiento basados en flash, por ejemplo, unidades SSD. NVMe reduce la sobrecarga de I/o e incluye mejoras de rendimiento, en comparación con las interfaces de dispositivos lógicos anteriores.
SAS	SAS es un protocolo en serie de punto a punto que vincula las controladoras directamente con las unidades de disco.
Unidades compatibles con la función de seguridad	Las unidades compatibles con la función de seguridad pueden ser unidades de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS) que cifran datos durante la escritura y descifran datos durante la lectura. Estas unidades se consideran Secure-*capable* porque se pueden usar para obtener más seguridad mediante la función Drive Security. Si está habilitada la función Drive Security para los grupos de volúmenes y pools que se utilizan con estas unidades, las unidades pasan a tener habilitada la función de seguridad-*enabled*.
Unidades con la función de seguridad habilitada	Las unidades con la función de seguridad habilitada se usan con Drive Security. Cuando se habilita la función Drive Security y se aplica Drive Security a un pool o un grupo de volúmenes en unidades_ compatibles con la función de seguridad, las unidades pasan a ser seguras *habilitadas*. El acceso de lectura y escritura solo está disponible a través de una controladora que está configurada con la clave de seguridad correcta. Esta seguridad adicional evita el acceso no autorizado a los datos en una unidad que se quita físicamente de la cabina de almacenamiento.
SSD	Los discos de estado sólido (SSD) son dispositivos de almacenamiento de datos que usan memoria de estado sólido (flash) para almacenar datos en forma persistente. Los SSD emulan las unidades de discos duros convencionales y están disponibles con las mismas interfaces que usan las unidades de disco duro.

Términos de iSCSI:

Duración	Descripción
CHAP	El método de protocolo de autenticación por desafío mutuo (CHAP) valida la identidad de destinos e iniciadores durante el enlace inicial. La autenticación se basa en una clave de seguridad compartida denominada CHAP *secret_*.
Controladora	Una controladora consta de una placa, un firmware y un software. Controla las unidades e implementa las funciones de System Manager.
DHCP	El protocolo de configuración dinámica de hosts (DHCP) es un protocolo que se usa en las redes de protocolo de Internet (IP) para los parámetros de configuración de red de distribución dinámica, como las direcciones IP.
IB	InfiniBand (IB) es una norma de comunicación para la transmisión de datos entre servidores de alto rendimiento y sistemas de almacenamiento.
Respuesta ICMP PING	El protocolo de mensajes de control de Internet (ICMP) es un protocolo que usan los sistemas operativos de ordenadores conectados a una red para enviar mensajes. Los mensajes ICMP determinan si se puede acceder a un host y cuánto tiempo lleva trasladar paquetes desde o hacia ese host.
IQN	Un identificador de nombre completo de iSCSI (IQN) es un nombre único para un iniciador de iSCSI o un destino iSCSI.
Iser	Las extensiones de iSCSI para RDMA (Iser) conforman un protocolo que extiende el protocolo iSCSI para operaciones a través de transporte RDMA, como InfiniBand o Ethernet.
ISNS	El servicio de nombres de almacenamiento de Internet (iSNS) es un protocolo que permite la detección, gestión y configuración automatizada de dispositivos iSCSI y Fibre Channel en redes TCP/IP.
Dirección MAC	Ethernet utiliza identificadores de control de acceso de medios (direcciones MAC) para distinguir entre canales lógicos distintos que conectan dos puertos en la misma interfaz de red de transporte físico.
Cliente de gestión	Un cliente de gestión es el equipo donde se instala un explorador para acceder a System Manager.
MTU	Una unidad de transmisión máxima (MTU) es el paquete o el marco de mayor tamaño que se pueden enviar en una red.
RDMA	El acceso directo a memoria remota (RDMA) es una tecnología que les permite a los equipos en red intercambiar datos en la memoria principal sin la participación del sistema operativo de ninguno de los equipos.

Duración	Descripción
Sesión de detección sin nombre	Cuando se habilita la opción de sesiones de detección sin nombre, no se requiere que los iniciadores de iSCSI especifiquen el IQN objetivo para recuperar la información de la controladora.

Términos de NVMe:

Duración	Descripción
Estructura	InfiniBand (IB) es una norma de comunicación para la transmisión de datos entre servidores de alto rendimiento y sistemas de almacenamiento.
Espacio de nombres	Un espacio de nombres es almacenamiento NVM que se formateó para el acceso en bloque. Es análogo a una unidad lógica en SCSI, que se relaciona con un volumen en la cabina de almacenamiento.
Identificador de espacio de nombres	El ID del espacio de nombres es el identificador único de la controladora NVMe para el espacio de nombres y se puede configurar con un valor entre 1 y 255. Es análogo a un número de unidad lógica (LUN) en SCSI.
NQN	El nombre completo de NVMe (NQN) se utiliza para identificar el destino de almacenamiento remoto (la cabina de almacenamiento).
NVM	La memoria no volátil (NVM) es la memoria persistente utilizada en muchos tipos de dispositivos de almacenamiento.
NVMe	La memoria no volátil rápida (NVMe) es una interfaz designada para dispositivos de almacenamiento basados en flash, por ejemplo, unidades SSD. NVMe reduce la sobrecarga de I/o e incluye mejoras de rendimiento, en comparación con las interfaces de dispositivos lógicos anteriores.
NVMe-of	La memoria no volátil rápida sobre estructuras (NVMe-of) es una especificación que permite el funcionamiento de comandos y la transferencia de datos de NVMe en una red entre un host y el almacenamiento.
Controladora NVMe	Se crea una controladora NVMe durante el proceso de conexión del host. Esta ofrece una ruta de acceso entre un host y los espacios de nombres en la cabina de almacenamiento.
Cola NVMe	Una cola que se utiliza para pasar comandos y mensajes a través de la interfaz de NVMe.
Subsistema NVMe	La cabina de almacenamiento con una conexión NVMe.
RDMA	El acceso remoto a memoria directa (RDMA) permite un movimiento de datos más directo hacia y desde un servidor gracias a la implementación de un protocolo de transporte en el hardware de la tarjeta de interfaz de red (NIC).
Roce	RDMA over Converged Ethernet (roce) es un protocolo de red que permite el acceso remoto a memoria directa (RDMA) sobre una red Ethernet.

Duración	Descripción
SSD	Los discos de estado sólido (SSD) son dispositivos de almacenamiento de datos que usan memoria de estado sólido (flash) para almacenar datos en forma persistente. Los SSD emulan las unidades de discos duros convencionales y están disponibles con las mismas interfaces que usan las unidades de disco duro.

Gestione los componentes de la bandeja

Ver componentes de hardware

La página hardware presenta funciones de ordenación y filtrado que facilitan la búsqueda de componentes.

Pasos

1. Seleccione **hardware**.
2. Use las funciones descritas en la siguiente tabla para ver los componentes de hardware.

Función	Descripción
Vistas de unidades, controladoras y componentes	Para cambiar entre las vistas frontal y trasera de la bandeja, seleccione * Unidades * o * Controladores y componentes * en el extremo derecho (el enlace que aparece depende de la vista actual). La vista **Drives** muestra las unidades y las bahías de unidades vacías. La vista **Controladores y componentes** muestra los controladores y cualquier módulo IOM (ESM), contenedores de alimentación/ventilador o bahías de controlador vacías. En la parte inferior de la página, también puede seleccionar **Mostrar todas las unidades**.
Filtros de vista de unidades	Si la matriz de almacenamiento contiene unidades con diferentes tipos de atributos físicos y lógicos, la página **hardware** incluye filtros de vista de unidades. Estos filtros ayudan a ubicar rápidamente unidades específicas, ya que permiten limitar los tipos de unidades que se muestran en la página. En **Mostrar unidades…**, haga clic en el campo de filtro de la izquierda (de forma predeterminada, muestra **cualquier tipo de unidad**) para ver una lista desplegable de atributos físicos (por ejemplo, capacidad y velocidad). Haga clic en el campo de filtro a la derecha (de forma predeterminada, muestra **en cualquier lugar de la matriz de almacenamiento**) para ver una lista desplegable de atributos lógicos (por ejemplo, asignación de grupo de volúmenes). Es posible usar estos filtros de forma conjunta o por separado. Si la cabina de almacenamiento contiene unidades que comparten todos los mismos atributos físicos, no aparece el campo **cualquier tipo de unidad** de la izquierda. Si todas las unidades están en la misma ubicación lógica, el campo **en cualquier lugar de la matriz de almacenamiento** de la derecha no aparece.

Función	Descripción
Leyenda	Los componentes se muestran en determinados colores para mostrar sus estados de roles. Para expandir y colapsar las descripciones de estos estados, haga clic en **Leyenda**.
Muestra detalles del icono de estado	Los indicadores de estado pueden incluir descripciones de texto para estados de disponibilidad. Haga clic en **Mostrar detalles del icono de estado** para mostrar u ocultar este texto de estado.
Opción Shelf e iconos de bandeja	Cada vista de bandeja proporciona una lista de comandos relacionados, junto con propiedades y Estados. Haga clic en **Bandeja** para ver una lista desplegable de comandos. También es posible seleccionar uno de los iconos en la parte superior para ver el estado y las propiedades de componentes individuales: Controladoras, IOM (ESM), suministros de alimentación, ventiladores, temperatura, Baterías y SFP.
Orden de bandejas	Es posible cambiar el orden de las bandejas en la página hardware. Use las flechas arriba y abajo en la parte superior derecha de cada vista de bandeja para cambiar el orden superior/inferior de las bandejas.

Muestra u oculta el estado de los componentes

Es posible mostrar descripciones de estado para las unidades, las controladoras, los ventiladores y los suministros de alimentación.

Pasos

1. Seleccione **hardware**.
2. Para ver los componentes frontales o posteriores:
   - Si desea ver la controladora y los componentes del contenedor de alimentación/ventilador, aunque se muestren las unidades, haga clic en **Mostrar parte posterior de la bandeja**.
   - Si desea ver las unidades, aunque se muestren la controladora y los componentes del contenedor de alimentación/ventilador, haga clic en **Mostrar frente de la bandeja**.
3. Para ver u ocultar las descripciones de estado emergentes:
   - Si desea ver una descripción emergente de los iconos de estado, haga clic en **Mostrar detalles del icono de estado** en la esquina superior derecha de la vista de bandeja (seleccione la casilla de comprobación).
   - Para ocultar las descripciones emergentes, haga clic en **Mostrar detalles del icono de estado** de nuevo (anule la selección de la casilla de verificación).
4. Si desea ver todos los detalles de estado, seleccione el componente en la vista de bandeja y, a continuación, seleccione **Ver configuración**.
5. Si desea ver las descripciones de los componentes coloreados, seleccione **Leyenda**.

Alternar entre las vistas frontal y trasera

La página hardware puede mostrar la vista frontal o la vista trasera de las bandejas.

Acerca de esta tarea

La vista trasera muestra las controladoras/IOM y los contenedores de alimentación/ventilador. La vista frontal muestra las unidades.

Pasos

1. Seleccione **hardware**.
2. Si el gráfico muestra las unidades, haga clic en **Mostrar parte posterior de la bandeja**.

   El gráfico cambia y muestra las controladoras en lugar de las unidades.

3. Si el gráfico muestra los controladores, haga clic en **Mostrar frente de la bandeja**.

   El gráfico cambia y muestra las unidades en lugar de las controladoras.

4. Opcionalmente, puede seleccionar **Mostrar todo frente** o **Mostrar todo detrás**, ubicado en la parte inferior de la página.

Cambiar el orden de vista de las bandejas

Puede cambiar el orden de las bandejas que se muestran en la página hardware para que coincidan con el orden físico de las bandejas de un armario.

Pasos

1. Seleccione **hardware**.
2. En la parte superior derecha de la vista de una bandeja, seleccione las flechas hacia arriba o hacia abajo para reorganizar el orden de las bandejas que se muestran en la página hardware.

Encienda la luz del localizador de bandejas

Para encontrar la ubicación física de una bandeja que se muestra en la página hardware, es posible encender la luz del localizador de la bandeja.

Pasos

1. Seleccione **hardware**.
2. Seleccione la lista desplegable de Bandeja de controladoras o Bandeja de unidades y, a continuación, seleccione **encender luz localizadora**.

   La luz localizadora de la bandeja se enciende.

3. Cuando haya localizado físicamente el estante, vuelva al cuadro de diálogo y seleccione **Apagar**.

Cambie los ID de bandeja

El ID de bandeja es un número que identifica de forma exclusiva a una bandeja en una cabina de almacenamiento. Las bandejas se numeran consecutivamente, desde 00 o 01, en la parte superior izquierda de cada vista de bandeja.

Acerca de esta tarea

El firmware de la controladora asigna automáticamente el ID de bandeja, pero es posible modificar ese número si desea crear un esquema de ordenamiento diferente.

Pasos

1. Seleccione **hardware**.
2. Seleccione la lista desplegable de Bandeja de controladoras o Bandeja de unidades y, a continuación, seleccione **Cambiar ID**.
3. En el cuadro de diálogo Cambiar ID de bandeja, seleccione la lista desplegable para mostrar los números disponibles.

   En este cuadro de diálogo no se muestran los ID actualmente asignados a las bandejas activas.

4. Seleccione un número disponible y, a continuación, haga clic en **Guardar**.

   Según el número seleccionado, el orden de las bandejas puede reorganizarse en la página hardware. Si lo desea, puede utilizar las flechas arriba/abajo en la parte superior derecha de cada bandeja para volver a ajustar el orden.

Ver el estado y la configuración de componentes de bandejas

En la página hardware, se proporcionan el estado y la configuración para componentes de bandejas, que incluyen suministros de alimentación, ventiladores y baterías.

Acerca de esta tarea

Los componentes disponibles dependen del tipo de bandeja:

- **Bandeja de unidades** — contiene un conjunto de unidades, contenedores de alimentación/ventilador, módulos de entrada/salida (IOM) y otros componentes de soporte en una sola bandeja.
- **Bandeja de controladoras** — contiene un conjunto de unidades, uno o dos contenedores de controladora, contenedores de alimentación/ventilador y otros componentes de soporte en una sola bandeja.

Pasos

1. Seleccione **hardware**.
2. Seleccione la lista desplegable para la bandeja de controladoras o bandeja de unidades y luego seleccione **Ver configuración**.

   Se abre el cuadro de diálogo Configuración de componentes de bandeja, con pestañas en las que se muestran el estado y la configuración relacionados con los componentes de la bandeja. Según el tipo de bandeja seleccionada, es posible que algunas de las pestañas descritas en la tabla no aparezcan.

Pestaña	Descripción
Bandeja	La ficha **Bandeja** muestra las siguientes propiedades: • **ID de bandeja** — identifica de forma exclusiva una bandeja en la cabina de almacenamiento. El firmware de la controladora asigna este número, pero es posible cambiarlo seleccionando MENU:Bandeja[Cambiar ID]. • **Redundancia de ruta de bandeja** — especifica si las conexiones entre la bandeja y el controlador tienen métodos alternativos en su lugar (Sí) o no (no). • **Tipos de unidad actuales** — muestra el tipo de tecnología integrada en las unidades (por ejemplo, una unidad SAS compatible con la función de seguridad). Si hubiera más de un tipo de unidad, se muestran ambas tecnologías. • **Número de serie** — muestra el número de serie del estante.
Iom (ESM)	La ficha **IOM (ESM)** muestra el estado del módulo de entrada/salida (IOM), que también se denomina módulo de servicios ambientales (ESM). Supervisa el estado de los componentes de una bandeja de unidades y funciona como el punto de conexión entre el soporte de unidades y la controladora. El estado puede ser Optimal, Failed, Optimal (Miswire) o sin certificar. Otra información incluye la versión de firmware y la versión de configuración. Seleccione **Mostrar más valores** para ver las velocidades de datos máximas y actuales y el estado de la comunicación de la tarjeta (Sí o no). Para ver este estado, también se puede seleccionar el icono de IOM, Junto a la lista desplegable Bandeja.
Suministros de alimentación	La ficha **fuentes de alimentación** muestra el estado del contenedor de alimentación y de la fuente de alimentación. El estado puede ser Optimal, Failed, Removed o Unknown. También muestra el número de pieza del suministro de alimentación. Para ver este estado, también puede seleccionar el icono de suministro de alimentación, Junto a la lista desplegable Bandeja.
Ventiladores	La ficha **ventiladores** muestra el estado del contenedor de ventilador y del ventilador en sí. El estado puede ser Optimal, Failed, Removed o Unknown. También puede ver este estado seleccionando el icono de ventilador, Junto a la lista desplegable Bandeja.

Pestaña	Descripción
Temperatura	La ficha **temperatura** muestra el estado de temperatura de los componentes de la bandeja, como los sensores, controladores y recipientes de alimentación/ventilador. El estado puede ser Optimal, nominal temperature exceeded, Maximum temperature exceeded o Desconocido. Para ver este estado, también se puede seleccionar el icono temperatura, Junto a la lista desplegable Bandeja.
Pilas	La ficha **baterías** muestra el estado de las baterías del controlador. El estado puede ser Optimal, Failed, Removed o Unknown. Otra información incluye la antigüedad de las baterías, los días restantes hasta el reemplazo, los ciclos de aprendizaje y las semanas entre ciclos de aprendizaje. Para ver este estado, también se puede seleccionar el icono de batería, Junto a la lista desplegable Bandeja.
SFP	En la pestaña **SFP**, se muestra el estado de los transceptores de factor de forma pequeño conectable (SFP) de las controladoras. El estado puede ser Optimal, Failed o Desconocido. Seleccione **Mostrar más ajustes** para ver el número de pieza, el número de serie y el proveedor de SFP. También puede ver este estado seleccionando el icono de SFP, Junto a la lista desplegable Bandeja.

3. Haga clic en **Cerrar**.

Actualice los ciclos de aprendizaje de la batería

Un ciclo de aprendizaje es un ciclo automático para calibrar el indicador de batería inteligente. Los ciclos se programan para comenzar automáticamente, el mismo día y a la misma hora, en intervalos de 8 semanas (por controladora). Si desea configurar un programa distinto, puede ajustar los ciclos de aprendizaje.

Acerca de esta tarea

La actualización de los ciclos de aprendizaje afecta a ambas baterías de la controladora.

Pasos

1. Seleccione **hardware**.
2. Seleccione la lista desplegable para la Bandeja del controlador y, a continuación, seleccione **Ver configuración**.
3. Seleccione la ficha **baterías**.
4. Seleccione **Actualizar ciclos de aprendizaje de la batería**.

   Se abre el cuadro de diálogo Actualizar ciclos de aprendizaje de la batería.

5. Desde las listas desplegables, seleccione un día y una hora nuevos.
6. Haga clic en **Guardar**.

Gestione controladoras

estados de la controladora

Una controladora se puede colocar en tres estados distintos: En línea, sin conexión y modo de servicio.

Estado en línea

El estado en línea es el estado de funcionamiento normal de la controladora. Significa que la controladora funciona con normalidad y está disponible para operaciones de I/O.

Cuando se coloca una controladora en el estado en línea, su estado se configura como Optimal.

Estado sin conexión

Por lo general, el estado sin conexión se usa para preparar una controladora para reemplazarla cuando hay dos controladoras en la cabina de almacenamiento. La controladora puede pasar al estado sin conexión por los siguientes dos motivos: El usuario puede introducir un comando explícito o se puede producir un error en la controladora. Una controladora puede salir del estado sin conexión solo si se emite otro comando explícito o si se reemplaza la controladora que produjo un error. Solo se puede colocar una controladora sin conexión si hay dos controladoras en la cabina de almacenamiento.

Si una controladora se encuentra en un estado sin conexión, es porque se presentaron las siguientes condiciones:

- La controladora no está disponible para I/O.
- No se puede gestionar la cabina de almacenamiento por medio de esa controladora.
- Todos los volúmenes que actualmente pertenecen a esa controladora se mueven a la otra controladora.
- Está deshabilitado el mirroring de la caché y todos los volúmenes se cambian a escritura mediante el modo de caché.

Modo de servicio

El modo de servicio, por lo general, es una condición que solo utiliza el soporte técnico para transferir todos los volúmenes de la cabina de almacenamiento a una controladora a fin de poder efectuar un diagnóstico en la otra controladora. Una controladora se debe colocar manualmente en el modo de servicio y volver a colocarse en línea manualmente una vez que finaliza la operación de mantenimiento.

Si una controladora se encuentra en el modo de servicio, se debe a las siguientes condiciones:

- La controladora no está disponible para I/O.
- El soporte técnico puede acceder a la controladora por medio del puerto serie o la conexión a redes para analizar los problemas potenciales.
- Todos los volúmenes que actualmente pertenecen a esa controladora se mueven a la otra controladora.
- Está deshabilitado el mirroring de la caché y todos los volúmenes se cambian a escritura mediante el modo de caché.

Aspectos que se deben tener en cuenta al asignar direcciones IP

De manera predeterminada, las controladoras se envían con DHCP habilitado en ambos puertos de red. Se pueden asignar direcciones IP estáticas, utilizar direcciones IP estáticas predeterminadas o usar direcciones IP asignadas para DHCP. Además, se puede usar la configuración automática sin estado IPv6.

> IPv6 está deshabilitado de forma predeterminada en las controladoras nuevas, pero se pueden configurar las direcciones IP de puertos de gestión mediante un método alternativo y, luego, habilitar IPv6 en los puertos de gestión por medio de System Manager.

Cuando el puerto de red está en estado de "enlace inactivo", es decir, desconectado de una LAN, el sistema informa su configuración como estática, y se observa una dirección IP de 0.0.0.0 (versiones anteriores) o DHCP habilitado sin dirección IP informada (versiones posteriores). Una vez que el puerto de red pasa al estado de "enlace activo" (es decir, conectado a una LAN) intenta obtener una dirección IP por medio de DHCP.

Si la controladora no puede obtener una dirección DHCP de un puerto de red determinado, revierte a una dirección IP predeterminada que podría demorar 3 minutos. Las direcciones IP predeterminadas son las siguientes:

```
Controller 1 (port 1): IP Address: 192.168.128.101
```

```
Controller 1 (port 2): IP Address: 192.168.129.101
```

```
Controller 2 (port 1): IP Address: 192.168.128.102
```

```
Controller 2 (port 2): IP Address: 192.168.129.102
```

Cuando se asignan direcciones IP:

- Se debe reservar el puerto 2 de las controladoras para que pueda usarlo soporte al cliente. No se debe cambiar la configuración de red predeterminada (DHCP habilitado).
- Para configurar direcciones IP estáticas para las controladoras E2800 y E5700, use SANtricity System Manager. Para configurar direcciones IP estáticas para las controladoras E2700 y E5600, use SANtricity Storage Manager. Una vez que se configura una dirección IP estática, queda configurada durante todos los eventos de enlaces inactivos/activos.
- Para usar DHCP a fin de asignar la dirección IP de la controladora, conecte la controladora a una red que pueda procesar las solicitudes DHCP. Use un arrendamiento DHCP permanente.

> Las direcciones predeterminadas no se mantienen durante los eventos de enlaces inactivos. Cuando se configura un puerto de red para usar DHCP, la controladora intenta obtener una dirección DHCP en cada evento de enlace activo, incluso las conexiones de cables, los reinicios, el apagado y el encendido. Cada vez que falla un intento de DHCP, se usa la dirección IP estática predeterminada para ese puerto.

Configure el puerto de gestión

La controladora incluye un puerto Ethernet que se utiliza para gestionar el sistema. De ser necesario, es posible cambiar los parámetros de transmisión y las direcciones IP.

Acerca de esta tarea

Durante este procedimiento, se selecciona el puerto 1 y después se establecen la velocidad y el método de direccionamiento del puerto. El puerto 1 se conecta a la red en la que el cliente de gestión puede acceder a la controladora y a System Manager.

> No use el puerto 2 en ninguna de las controladoras. El puerto 2 está reservado para uso exclusivo del soporte técnico.

Pasos

1. Seleccione **hardware**.
2. Si el gráfico muestra las unidades, haga clic en **Mostrar parte posterior de la bandeja**.

   El gráfico cambia y muestra las controladoras en lugar de las unidades.

3. Haga clic en la controladora con el puerto de gestión que desea configurar.

   Aparece el menú contextual de la controladora.

4. Seleccione **Configurar puertos de administración**.

   Se abre el cuadro de diálogo Configurar puertos de gestión.

5. Asegúrese de que aparece el puerto 1 y, a continuación, haga clic en **Siguiente**.
6. Seleccione los valores del puerto de configuración y, a continuación, haga clic en **Siguiente**.

   Detalles del campo

Campo	Descripción
Velocidad y modo doble	Conserve la opción de configuración autonegociar si desea que System Manager determine los parámetros de transmisión entre la cabina de almacenamiento y la red; o bien si conoce la velocidad y el modo de la red, seleccione los parámetros de la lista desplegable. En la lista, solamente se muestran la velocidad válida y las combinaciones dobles.
Habilite IPv4/Habilitar IPv6	Seleccione una o ambas opciones para habilitar la compatibilidad con las redes IPv4 e IPv6.

   Si selecciona **Activar IPv4**, se abre un cuadro de diálogo para seleccionar la configuración IPv4 después de hacer clic en **Siguiente**. Si selecciona **Activar IPv6**, se abre un cuadro de diálogo para seleccionar la configuración de IPv6 después de hacer clic en **Siguiente**. Si selecciona ambas opciones, primero se abre el cuadro de diálogo para la configuración de IPv4 y después de hacer clic en **Siguiente**, se abre el cuadro de diálogo para la configuración de IPv6.

7. Configure los valores para IPv4 o IPv6 de forma automática o manual.

Detalles del campo

Campo	Descripción
Obtener automáticamente la configuración del servidor DHCP	Seleccione esta opción para obtener automáticamente la configuración.
Especificar manualmente la configuración estática	Seleccione esta opción y después introduzca la dirección IP de la controladora. (Si lo desea, puede cortar y pegar direcciones en los campos.) En el caso de IPv4, incluya la máscara de subred y la puerta de enlace. En el caso de IPv6, incluya la dirección IP enrutable y la dirección IP del enrutador. Si cambia la configuración de la dirección IP, se pierde la ruta de gestión de la cabina de almacenamiento. Si usa Unified Manager de SANtricity para gestionar globalmente las cabinas en su red, abra la interfaz de usuario y vaya a MENU:gestionar[detectar]. Si usa SANtricity Storage Manager, debe eliminar el dispositivo de Enterprise Management Window (EMW) y volver a añadirlo a EMW. Para hacerlo, seleccione **Edit › Añadir cabina de almacenamiento** e introduzca la nueva dirección IP.

8. Haga clic en **Finalizar**.

Resultados

La configuración del puerto de gestión se muestra en la configuración de la controladora, en la pestaña puertos de gestión.

Configure las direcciones del servidor NTP

Es posible configurar una conexión con el servidor de protocolo de tiempo de redes (NTP) de manera que la controladora consulte periódicamente al servidor NTP para actualizar el reloj interno que señala la hora del día.

Antes de empezar

- Es necesario instalar y configurar un servidor NTP en la red.
- Debe conocer la dirección del servidor NTP primario y un servidor NTP de respaldo opcional. Las direcciones pueden ser nombres de dominio completo, direcciones IPv4 o direcciones IPv6.

Si se introducen uno o más nombres de dominio para los servidores NTP, también se debe configurar un servidor DNS para resolver la dirección del servidor NTP. Es necesario configurar el servidor DNS solamente en aquellas controladoras en las que se haya configurado NTP y provisto un nombre de dominio.

Acerca de esta tarea

NTP permite que la cabina de almacenamiento sincronice automáticamente los relojes de la controladora con

un host externo mediante un protocolo simple de tiempo de redes (SNTP). La controladora consulta periódicamente al servidor NTP configurado, y después utiliza los resultados para actualizar la hora del día en el reloj interno. Si solamente una de las controladoras tiene NTP habilitado, la controladora alternativa sincronizará periódicamente su reloj con el de la controladora que tiene NTP habilitado. Si ninguna de las controladoras tiene NTP habilitado, sincronizarán periódicamente sus relojes entre ellas.

> No es necesario configurar NTP en ambas controladoras, pero, si lo hace, se mejora la capacidad de la cabina de almacenamiento para mantenerse sincronizada durante fallos de hardware o comunicación.

Pasos

1. Seleccione **hardware**.
2. Si el gráfico muestra las unidades, haga clic en **Mostrar parte posterior de la bandeja**.

   El gráfico cambia y muestra las controladoras en lugar de las unidades.

3. Haga clic en la controladora que desea configurar.

   Aparece el menú contextual de la controladora.

4. Seleccione **Configurar servidor NTP**.

   Se abre el cuadro de diálogo Configurar servidor de protocolo de tiempo de redes (NTP).

5. Seleccione **deseo activar NTP en el controlador** (**A** o **B**).

   En el cuadro de diálogo, aparecerán selecciones adicionales.

6. Seleccione una de las siguientes opciones:
   - **Obtener automáticamente las direcciones del servidor NTP desde el servidor DHCP** — se muestran las direcciones detectadas del servidor NTP.

     > Si la cabina de almacenamiento está configurada para usar una dirección NTP estática, no aparecen servidores NTP.

   - **Especificar manualmente las direcciones del servidor NTP** — introducir la dirección primaria del servidor NTP y una dirección del servidor NTP de respaldo. El servidor de respaldo es opcional. (Estos campos de dirección aparecen después de seleccionar el botón de opción.) La dirección del servidor debe ser un nombre de dominio completo, una dirección IPv4 o una dirección IPv6.
7. **Opcional:** Introduzca información del servidor y credenciales de autenticación para un servidor NTP de respaldo.
8. Haga clic en **Guardar**.

Resultados

La configuración del servidor NTP se muestra en la ficha **DNS / NTP** de la configuración de la controladora.

Configurar las direcciones del servidor DNS

El sistema de nombres de dominio (DNS) se utiliza para resolver nombres de dominio completos de las controladoras y un servidor de protocolo de tiempo de redes (NTP). Los puertos de gestión de la cabina de almacenamiento pueden ser compatibles con los

protocolos IPv4 o IPv6 simultáneamente.

Antes de empezar

- Debe haber un servidor DNS instalado y configurado en la red.
- Conoce la dirección del servidor DNS primario y un servidor DNS de respaldo opcional. Las direcciones pueden ser IPv4 o IPv6.

Acerca de esta tarea

En este procedimiento, se describe cómo especificar la dirección de un servidor DNS primario y de respaldo. El servidor DNS de respaldo puede configurarse opcionalmente para utilizarse en caso en que falle el servidor DNS primario.

> Si ya configuró los puertos de gestión de la cabina de almacenamiento con el protocolo de configuración dinámica de hosts (DHCP) y tiene uno o más servidores DNS o NTP asociados con la configuración de DHCP, no necesita configurar manualmente DNS ni NTP. En este caso, la cabina de almacenamiento debería haber obtenido automáticamente las direcciones de los servidores DNS/NTP. De todos modos, debe seguir las instrucciones que se presentan a continuación para abrir el cuadro de diálogo y asegurarse de que se hayan detectado las direcciones correctas.

Pasos

1. Seleccione **hardware**.
2. Si el gráfico muestra las unidades, haga clic en **Mostrar parte posterior de la bandeja**.

   El gráfico cambia y muestra las controladoras en lugar de las unidades.

3. Seleccione la controladora para configurar.

   Aparece el menú contextual de la controladora.

4. Seleccione **Configurar servidor DNS**.

   Se abre el cuadro de diálogo Configurar servidor del sistema de nombres de dominio (DNS).

5. Seleccione una de las siguientes opciones:
   - **Obtener automáticamente las direcciones del servidor DNS desde el servidor DHCP** — se muestran las direcciones del servidor DNS detectadas.

     > Si la cabina de almacenamiento está configurada para usar una dirección DNS estática, no aparecen servidores DNS.

   - **Especificar manualmente las direcciones del servidor DNS** — Introduzca una dirección del servidor DNS primario y una dirección del servidor DNS de respaldo. El servidor de respaldo es opcional. (Estos campos de dirección aparecen después de seleccionar el botón de opción.) Las direcciones pueden ser IPv4 o IPv6.
6. Haga clic en **Guardar**.
7. Repita estos pasos para la otra controladora.

Resultados

La configuración de DNS se muestra en la ficha **DNS / NTP** de la configuración del controlador.

Ver la configuración de la controladora

Es posible ver información sobre una controladora, como el estado de las interfaces del host, de las interfaces de la unidad y de los puertos de gestión.

Pasos

1. Seleccione **hardware**.
2. Si el gráfico muestra las unidades, haga clic en **Mostrar parte posterior de la bandeja**.

   El gráfico cambia y muestra las controladoras en lugar de las unidades.

3. Realice alguna de las siguientes acciones para ver la configuración de la controladora:
   - Haga clic en el controlador para mostrar el menú contextual y, a continuación, seleccione **Ver configuración**.
   - Seleccione el icono del controlador (junto a la lista desplegable **Bandeja**). Para configuraciones dúplex, seleccione **controladora A** o **controladora B** en el cuadro de diálogo y, a continuación, haga clic en **Siguiente**.

     Se abrirá el cuadro de diálogo Configuración de la controladora.

4. Seleccione las pestañas para cambiar de una opción de configuración de propiedad a otra.

   Algunas fichas tienen un enlace para **Mostrar más ajustes** en la parte superior derecha.

Detalles del campo

Pestaña	Descripción
Base	Muestra el estado de la controladora, el nombre del modelo, el número de pieza de repuesto, la versión de firmware actual y la versión de la memoria estática de acceso aleatorio no volátil (NVSRAM).
Almacenamiento en caché	Muestra la configuración de caché de la controladora, que incluye la caché de datos, la caché de procesador y el dispositivo de backup de caché. El dispositivo de backup de caché se usa para crear backups de datos en la caché si la controladora se queda sin energía. Los Estados pueden ser Optimal, Failed, Removed, Unknown, Write Protected, O incompatible.
Interfaces del host	Muestra información de la interfaz del host y el estado del enlace de cada puerto. La interfaz del host es la conexión entre la controladora y el host, como Fibre Channel o iSCSI. La ubicación de la tarjeta de interfaz del host (HIC) puede ser en la placa base o en una ranura (bahía). Si el sistema muestra "Baseboard", significa que los puertos de la HIC están integrados en la controladora. Si el sistema muestra "Slot", significa que los puertos están en la HIC opcional.
Interfaces de unidad	Muestra la información de la interfaz de la unidad y el estado de enlace de cada puerto. La interfaz de la unidad es la conexión entre la controladora y las unidades, como SAS.
Puertos de gestión	Muestra detalles de los puertos de gestión, como el nombre de host que se usa para acceder a la controladora y si se habilitó un inicio de sesión remoto. El puerto de gestión conecta la controladora con el cliente de gestión, que es donde se instala un explorador para acceder a System Manager.
DNS/NTP	Muestra el método de direccionamiento y las direcciones IP del servidor DNS y servidor NTP, si estos servidores se configuraron en System Manager. El sistema de nombres de dominio (DNS) es un sistema de nomenclatura para los dispositivos conectados a Internet o a una red privada. El servidor DNS conserva un directorio de nombres de dominio y los convierte en direcciones de protocolos de Internet (IP). El protocolo de tiempo de redes (NTP) es un protocolo de redes para la sincronización del reloj entre los sistemas informáticos en las redes de datos.

5. Haga clic en **Cerrar**.

Configuración del inicio de sesión remoto (SSH)

Al habilitar el inicio de sesión remoto, permite que los usuarios fuera de la red de área local inicien una sesión SSH y accedan a la configuración en la controladora.

Para las versiones 11.74 y posteriores de SANtricity, también puede configurar la autorización multifactor (MFA) exigiendo a los usuarios que introduzcan una clave SSH o una contraseña de SSH. En las versiones 11.73 y anteriores de SANtricity, esta función *not* incluye una opción para la autorización multifactor con claves y contraseñas SSH.

> **Riesgo de seguridad** — por razones de seguridad, sólo el personal de soporte técnico debe utilizar la función de inicio de sesión remoto.

Pasos

1. Seleccione **hardware**.
2. Si el gráfico muestra las unidades, haga clic en **Mostrar parte posterior de la bandeja**.

   El gráfico cambia y muestra las controladoras en lugar de las unidades.

3. Haga clic en la controladora para la que desea configurar el inicio de sesión remoto.

   Aparece el menú contextual de la controladora.

4. Seleccione **Configurar inicio de sesión remoto (SSH)**. (Para las versiones 11.73 y anteriores de SANtricity, este elemento de menú es **Cambiar inicio de sesión remoto**.)

   Se abre el cuadro de diálogo para habilitar el inicio de sesión remoto.

5. Seleccione la casilla de verificación **Activar inicio de sesión remoto**.

   Esta configuración proporciona el inicio de sesión remoto con tres opciones de autorización:

   - **Sólo contraseña**. Para esta opción, ya ha terminado y puede hacer clic en **Guardar**. Si tiene un sistema doble, puede habilitar el inicio de sesión remoto en la segunda controladora siguiendo los pasos anteriores.
   - **Clave SSH o contraseña**. Para esta opción, continúe con el siguiente paso.
   - **Tanto la contraseña como la clave SSH**. Para esta opción, seleccione la casilla de verificación **requerir clave pública autorizada y contraseña para el inicio de sesión remoto** y continúe con el siguiente paso.

6. Rellene el campo **clave pública autorizada**. Este campo contiene una lista de claves públicas autorizadas, en el formato del archivo OpenSSH **authorized_keys**.

   Al rellenar el campo **clave pública autorizada**, tenga en cuenta las siguientes directrices:

   - El campo **clave pública autorizada** se aplica a ambos controladores y sólo debe configurarse en el primer controlador.
   - El archivo **Authorized_Keys** debe contener sólo una clave por línea. Las líneas que comienzan con # y las líneas vacías se omiten. Para obtener más información acerca del formato de archivo, consulte "Configuración de claves autorizadas para OpenSSH".
   - Un archivo **Authorized_keys** debería tener un aspecto similar al siguiente ejemplo:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDJlG20rYTk4ok+xFjkPHYp/R0LfJqEYDLXA5AJ4
9w3DvAWLrUg+1CpNq76WSqmQBmoG9jgbcAB5ABGdswdeMQZHilJcu29iJ3OKKv6SlCulA
j1tHymwtbdhPuipd2wIDAQAB
```

7. Cuando haya terminado, haga clic en **Guardar**.
8. En el caso de los sistemas dobles, puede habilitar el inicio de sesión remoto en la segunda controladora siguiendo los pasos anteriores. Si está configurando la opción tanto para una contraseña como para una clave SSH, asegúrese de volver a seleccionar la casilla de verificación **requerir clave pública autorizada y contraseña para el inicio de sesión remoto**.
9. Después de que el soporte técnico termine de solucionar problemas, puede desactivar el inicio de sesión remoto volviendo al cuadro de diálogo Configurar inicio de sesión remoto y deseleccionando la casilla de verificación **Activar inicio de sesión remoto**. Si se habilitó el inicio de sesión remoto en una segunda controladora, se abre un cuadro de diálogo de confirmación y se permite deshabilitar el inicio de sesión remoto también en la segunda.

   Al deshabilitar el inicio de sesión remoto, se cierran todas las sesiones SSH vigentes y se rechazan todas las solicitudes de inicio de sesión nuevas.

Coloque una controladora en línea

Si una controladora se encuentra en estado sin conexión o en modo de servicio, es posible colocarla nuevamente en línea.

Pasos

1. Seleccione **hardware**.
2. Si el gráfico muestra las unidades, haga clic en **Mostrar parte posterior de la bandeja**.

   El gráfico cambia y muestra las controladoras en lugar de las unidades.

3. Haga clic en una controladora que se encuentre en estado sin conexión o en modo de servicio.

   Aparece el menú contextual de la controladora.

4. Seleccione **colocar en línea** y confirme que desea realizar la operación.

Resultados

El controlador multivía puede demorar hasta 10 minutos en detectar una ruta de restauración preferida.

Los volúmenes pertenecientes originalmente a esta controladora se moverán automáticamente de vuelta a la controladora a medida que se reciban solicitudes de I/o para cada volumen. En algunos casos, es posible que necesite redistribuir manualmente los volúmenes con el comando **redistribuir volúmenes**.

Coloque una controladora en estado sin conexión

Si se le indica hacerlo, puede colocar una controladora en estado sin conexión.

Antes de empezar

- Una cabina de almacenamiento debe tener dos controladoras. La controladora que no se coloca en estado

sin conexión debe estar en línea (en el estado óptimo).

- Asegúrese de que no existan volúmenes en uso o que exista un controlador multivía instalado en todos los hosts que utilizan estos volúmenes.

Acerca de esta tarea

> No coloque una controladora en estado sin conexión a menos que el soporte técnico o Recovery Guru le indique hacerlo.

Pasos

1. Seleccione **hardware**.
2. Si el gráfico muestra las unidades, haga clic en **Mostrar parte posterior de la bandeja**.

   El gráfico cambia y muestra las controladoras en lugar de las unidades.

3. Haga clic en la controladora que desea colocar en estado sin conexión.

   Aparece el menú contextual de la controladora.

4. Seleccione **colocar fuera de línea** y confirme que desea realizar la operación.

Resultados

Es posible que System Manager demore varios minutos en actualizar el estado de la controladora a sin conexión. No inicie ninguna otra operación hasta que se haya actualizado el estado.

Colocar una controladora en modo de servicio

Si se le indica hacerlo, puede colocar una controladora en modo de servicio.

Antes de empezar

- La cabina de almacenamiento debe tener dos controladoras. La controladora que no se coloca en modo de servicio debe estar en línea (en el estado óptimo).
- Asegúrese de que no existan volúmenes en uso o que exista un controlador multivía instalado en todos los hosts que utilizan estos volúmenes.

> La colocación de una controladora en modo de servicio puede reducir considerablemente el rendimiento. No coloque una controladora en modo de servicio a menos que el soporte técnico le indique hacerlo.

Pasos

1. Seleccione **hardware**.
2. Si el gráfico muestra las unidades, haga clic en **Mostrar parte posterior de la bandeja**.

   El gráfico cambia y muestra las controladoras en lugar de las unidades.

3. Haga clic en la controladora que desea colocar en modo de servicio.

   Aparece el menú contextual de la controladora.

4. Seleccione **colocar en modo de servicio** y confirme que desea realizar la operación.

Restablezca (reinicie) la controladora

Algunos problemas requieren un restablecimiento de la controladora (reinicio). Es posible restablecer la controladora incluso sin tener acceso físico a ella.

Antes de empezar

- La cabina de almacenamiento debe tener dos controladoras. La controladora que no se restablece debe estar en línea (en el estado óptimo).
- Asegúrese de que no existan volúmenes en uso o que exista un controlador multivía instalado en todos los hosts que utilizan estos volúmenes.

Pasos

1. Seleccione **hardware**.
2. Si el gráfico muestra las unidades, haga clic en **Mostrar parte posterior de la bandeja**.

   El gráfico cambia y muestra las controladoras en lugar de las unidades.

3. Haga clic en la controladora que desea restablecer.

   Aparece el menú contextual de la controladora.

4. Seleccione **Restablecer** y confirme que desea realizar la operación.

Gestione los puertos iSCSI

Configure los puertos iSCSI

Si la controladora incluye una conexión de host iSCSI, los ajustes del puerto iSCSI se pueden configurar desde la página hardware.

Antes de empezar

- La controladora debe incluir puertos iSCSI; de lo contrario, la configuración de iSCSI no estará disponible.
- Se debe conocer la velocidad de la red (la tasa de transferencia de datos entre los puertos y el host).

> La configuración y las funciones iSCSI solamente aparecen si la cabina de almacenamiento es compatible con iSCSI.

Pasos

1. Seleccione **hardware**.
2. Si el gráfico muestra las unidades, haga clic en **Mostrar parte posterior de la bandeja**.

   El gráfico cambia y muestra las controladoras en lugar de las unidades.

3. Haga clic en la controladora con los puertos iSCSI que desea configurar.

   Aparece el menú contextual de la controladora.

4. Seleccione **Configurar puertos iSCSI**.

> La opción **Configurar puertos iSCSI** aparece sólo si System Manager detecta puertos iSCSI en la controladora.

Se abre el cuadro de diálogo Configurar puertos iSCSI.

5. En la lista desplegable, seleccione el puerto que desea configurar y, a continuación, haga clic en **Siguiente**.
6. Seleccione los valores del puerto de configuración y, a continuación, haga clic en **Siguiente**.

   Para ver todas las configuraciones de puerto, haga clic en el enlace **Mostrar más opciones de puerto** situado a la derecha del cuadro de diálogo.

Detalles del campo

Opción de configuración de puertos	Descripción
Velocidad del puerto ethernet configurada (aparece solamente en ciertos tipos de tarjetas de interfaz del host)	Seleccione la velocidad que coincida que la capacidad de velocidad del SFP en el puerto.
Modo de corrección de errores de reenvío (FEC) (sólo aparece para determinados tipos de tarjetas de interfaz del sistema principal)	Si lo desea, seleccione uno de los modos FEC para el puerto de host especificado. El modo Reed Solomon no admite la velocidad de puerto de 25 Gbps.
Habilite IPv4/Habilitar IPv6	Seleccione una o ambas opciones para habilitar la compatibilidad con las redes IPv4 e IPv6. Si desea deshabilitar el acceso al puerto, cancele la selección de las dos casillas de comprobación.
Puerto de escucha TCP (disponible haciendo clic en **Mostrar más opciones de puerto**).	De ser necesario, introduzca un nuevo número de puerto. El puerto de escucha es el número de puerto TCP que la controladora utiliza para escuchar inicios de sesión iSCSI de iniciadores iSCSI del host. El puerto de escucha predeterminado es 3260. Debe introducir 3260 o un valor entre 49 49152 y 65 65535.
Tamaño de MTU (disponible haciendo clic en **Mostrar más opciones de puerto**).	De ser necesario, introduzca un nuevo tamaño en bytes para la unidad de transmisión máxima (MTU). El tamaño de MTU predeterminado es de 1500 bytes por trama. Debe introducir un valor entre 1500 y 9000.
Habilite las respuestas PING de ICMP PING	Seleccione esta opción para habilitar el protocolo de mensajes de control de Internet (ICMP). Los sistemas operativos de equipos en red usan ese protocolo para enviar mensajes. Esos mensajes ICMP determinan si es posible acceder a un host y cuánto tiempo debe transcurrir para enviar y recibir los paquetes de ese host.

Si seleccionó **Activar IPv4**, se abre un cuadro de diálogo para seleccionar la configuración IPv4 después de hacer clic en **Siguiente**. Si seleccionó **Activar IPv6**, se abre un cuadro de diálogo para seleccionar la configuración de IPv6 después de hacer clic en **Siguiente**. Si seleccionó ambas opciones, primero se abre el cuadro de diálogo de configuración IPv4 y después de hacer clic en **Siguiente**, se abre el cuadro de diálogo de configuración de IPv6.

7. Configure los valores para IPv4 o IPv6 de forma automática o manual. Para ver todas las opciones de configuración de puertos, haga clic en el enlace **Mostrar más valores** situado a la derecha del cuadro de diálogo.

   Detalles del campo

Opción de configuración de puertos	Descripción
Obtener configuración automáticamente	Seleccione esta opción para obtener automáticamente la configuración.
Especificar manualmente la configuración estática	Seleccione esta opción e introduzca una dirección estática en los campos. (Si lo desea, puede cortar y pegar direcciones en los campos.) En el caso de IPv4, incluya la máscara de subred y la puerta de enlace. En el caso de IPv6, incluya la dirección IP enrutable y la dirección IP del enrutador.
Active la compatibilidad con VLAN (disponible haciendo clic en **Mostrar más opciones**).	Seleccione esta opción para habilitar una VLAN e introducir su ID. Una red de área local virtual (VLAN) es una red lógica que se comporta como si estuviese físicamente separada de otras redes de área local virtuales y físicas (LAN) admitidas por los mismos switches, los mismos enrutadores, o ambos.
Activar prioridad ethernet (disponible haciendo clic en **Mostrar más valores**).	Seleccione esta opción para habilitar el parámetro que determina la prioridad de acceso a la red. Use la barra deslizante para seleccionar una prioridad entre 1 (más baja) y 7 (más alta). En un entorno de red de área local (LAN) compartida, como Ethernet, es posible que muchas estaciones compitan por el acceso a la red. El acceso se otorga por orden de llegada. Es posible que dos estaciones intenten acceder a la red al mismo tiempo, lo que provoca que ambas estaciones se apagen y esperen antes de volver a intentarlo. Este proceso se minimiza para Ethernet con switch, donde existe una sola estación conectada a un puerto del switch.

8. Haga clic en **Finalizar**.

Configure la autenticación iSCSI

Para obtener seguridad adicional en una red iSCSI, se puede establecer la autenticación entre controladoras (objetivos) y hosts (iniciadores).

System Manager usa el método de protocolo de autenticación por desafío mutuo (CHAP), que valida la identidad de los destinos e iniciadores durante el enlace inicial. La autenticación se basa en una clave de seguridad compartida denominada *CHAP Secret*.

Antes de empezar

Es posible establecer el secreto CHAP para los iniciadores (hosts iSCSI) antes o después de haber establecido el secreto CHAP para los objetivos (controladoras). Antes de seguir las instrucciones de esta tarea, primero debe esperar a que los hosts hayan establecido una conexión iSCSI y, a continuación,

configurar el secreto CHAP en los hosts individuales. Una vez realizadas las conexiones, los nombres IQN de los hosts y los secretos CHAP se enumeran en el cuadro de diálogo de autenticación iSCSI (que se describe en esta tarea), y no es necesario introducirlos manualmente.

Acerca de esta tarea

Se puede seleccionar uno de los siguientes métodos de autenticación:

- **Autenticación unidireccional** — Utilice esta opción para permitir que el controlador autentique la identidad de los hosts iSCSI (autenticación unidireccional).
- **Autenticación bidireccional** — Utilice este ajuste para permitir que tanto el controlador como los hosts iSCSI lleven a cabo la autenticación (autenticación bidireccional). Esta opción aporta un segundo nivel de seguridad, ya que permite que la controladora autentique la identidad de los hosts iSCSI y, a su vez, que los hosts iSCSI autentiquen la identidad de la controladora.

> La configuración y las funciones de iSCSI solo aparecen en la página Configuración si la cabina de almacenamiento es compatible con iSCSI.

Pasos

1. Seleccione MENU:Settings[System].
2. En Configuración de iSCSI, haga clic en **Configurar autenticación**.

   Se muestra el cuadro de diálogo Configurar autenticación, donde se indica el método actualmente seleccionado. También muestra si alguno de los hosts tiene secretos CHAP configurados.

3. Seleccione una de las siguientes opciones:
   - **Sin autenticación** — Si no desea que el controlador autentique la identidad de los hosts iSCSI, seleccione esta opción y haga clic en **Finalizar**. El cuadro de diálogo se cierra y la configuración está lista.
   - **Autenticación unidireccional** — para permitir que el controlador autentique la identidad de los hosts iSCSI, seleccione esta opción y haga clic en **Siguiente** para abrir el cuadro de diálogo Configurar CHAP de destino.
   - **Autenticación bidireccional** — para permitir que tanto el controlador como los hosts iSCSI lleven a cabo la autenticación, seleccione esta opción y haga clic en **Siguiente** para abrir el cuadro de diálogo Configurar CHAP de destino.
4. Tanto para la autenticación unidireccional como para la bidireccional, introduzca o confirme el secreto CHAP de la controladora (el objetivo). El secreto CHAP debe tener entre 12 y 57 caracteres ASCII imprimibles.

   > Si el secreto CHAP de la controladora se configuró anteriormente, los caracteres que aparecen en el campo se muestran enmascarados. Si es necesario, puede reemplazar los caracteres existentes (los caracteres nuevos no están enmascarados).

5. Debe realizar una de las siguientes acciones:
   - Si está configurando la autenticación *unidireccional*, haga clic en **Finalizar**. El cuadro de diálogo se cierra y la configuración está lista.
   - Si está configurando la autenticación *bidireccional*, haga clic en **Siguiente** para abrir el cuadro de diálogo Configurar CHAP del iniciador.
6. En el caso de la autenticación bidireccional, introduzca o confirme un secreto CHAP de cualquiera de los hosts iSCSI (los iniciadores), que pueden tener entre 12 y 57 caracteres ASCII imprimibles. Si no desea

configurar la autenticación bidireccional de un host en particular, deje en blanco el campo Secreto CHAP del iniciador.

> Si el secreto CHAP de un host se configuró con anterioridad, los caracteres del campo están enmascarados. Si es necesario, puede reemplazar los caracteres existentes (los caracteres nuevos no están enmascarados).

7. Haga clic en **Finalizar**.

Resultados

La autenticación sucede durante la secuencia de inicio de sesión iSCSI, entre las controladoras y los hosts iSCSI, a menos que no se haya especificado ninguna autenticación.

Habilite la configuración de detección de iSCSI

Es posible habilitar la configuración relacionada con la detección de dispositivos de almacenamiento en una red iSCSI.

La configuración de detección de objetivos permite registrar la información de iSCSI de la cabina de almacenamiento con el protocolo de servicio de nombres de almacenamiento de Internet (iSNS), y también determinar si se deben permitir las sesiones de detección sin nombre.

Antes de empezar

Si el servidor iSNS utiliza una dirección IP estática, esa dirección debe estar disponible para registrarse en iSNS. Se admiten tanto IPv4 como IPv6.

Acerca de esta tarea

Es posible habilitar la siguiente configuración relacionada con la detección de iSCSI:

- **Activar el servidor iSNS para registrar un destino** — cuando está activado, la cabina de almacenamiento registra la información de su nombre completo iSCSI (IQN) y su puerto del servidor iSNS. Esta opción permite la detección de iSNS para que un iniciador pueda recuperar la información de IQN y puerto del servidor iSNS.
- **Activar sesiones de detección sin nombre** — cuando las sesiones de detección sin nombre están habilitadas, el iniciador (host iSCSI) no necesita proporcionar el IQN del destino (controladora) durante la secuencia de inicio de sesión para una conexión de tipo de detección. Cuando se deshabilitan, los hosts deben proporcionar el IQN para establecer una sesión de detección con la controladora. Sin embargo, siempre se requiere el IQN objetivo durante una sesión normal (con I/o). Al deshabilitar esta opción, se puede evitar que los hosts iSCSI no autorizados se conecten a la controladora mediante esta dirección IP solamente.

> La configuración y las funciones de iSCSI solo aparecen en la página Configuración si la cabina de almacenamiento es compatible con iSCSI.

Pasos

1. Seleccione MENU:Settings[System].
2. En **Configuración de iSCSI**, haga clic en **Ver/editar configuración de detección de objetivos**.

   Se muestra el cuadro de diálogo Configuración de detección de objetivos. Debajo del **Activar servidor iSNS**… campo, el cuadro de diálogo indica si la controladora ya está registrada.

3. Para registrar el controlador, seleccione **Activar servidor iSNS para registrar mi destino** y, a continuación, seleccione una de las siguientes opciones:
   - **Obtener automáticamente la configuración del servidor DHCP** — Seleccione esta opción si desea configurar el servidor iSNS usando un servidor DHCP (Dynamic Host Configuration Protocol). Tenga en cuenta que, si usa esta opción, todos los puertos iSCSI en la controladora también deben configurarse para usar DHCP. Si es necesario, actualice el puerto iSCSI de la controladora para habilitar esta opción.

     > Para que el servidor DHCP proporcione la dirección del servidor iSNS, debe configurar el servidor DHCP para que utilice la opción 43 — ""Información específica del proveedor"." Esta opción debe incluir la dirección IPv4 del servidor iSNS en los bytes de datos 0xa-0xd (10-13).

   - **Especificar manualmente la configuración estática** — Seleccione esta opción si desea introducir una dirección IP estática para el servidor iSNS. (Si lo desea, puede cortar y pegar direcciones en los campos.) En el campo, introduzca una dirección IPv4 o IPv6. Si configuró ambas, IPv4 es la predeterminada. Introduzca además un puerto de escucha TCP (utilice 3205, que es el predeterminado, o especifique un valor entre 49 49152 y 65 65535).
4. Para permitir que la cabina de almacenamiento participe en sesiones de detección sin nombre, seleccione **Habilitar sesiones de detección sin nombre**.
   - Cuando se habilita esta opción, no se requiere que los iniciadores de iSCSI especifiquen el IQN objetivo para recuperar la información de la controladora.
   - Cuando se deshabilita, se impiden las sesiones de detección a menos que el iniciador proporcione el IQN objetivo. Al deshabilitar las sesiones de detección sin nombre, se obtiene seguridad adicional.
5. Haga clic en **Guardar**.

Resultados

Se muestra una barra de progreso cuando System Manager intenta registrar la controladora en el servidor iSNS. Este proceso puede llevar hasta cinco minutos.

Ver paquetes de estadísticas de iSCSI

Es posible ver datos sobre las conexiones iSCSI con la cabina de almacenamiento.

Acerca de esta tarea

En System Manager, se muestran los siguientes tipos de estadísticas de iSCSI. Todas las estadísticas son de solo lectura y no pueden configurarse.

- **Estadísticas de MAC Ethernet** — proporciona estadísticas para el control de acceso a medios (MAC). MAC también proporciona un mecanismo de direccionamiento denominado dirección física o dirección MAC. La dirección MAC es una dirección única que se asigna a cada adaptador de red. La dirección MAC ayuda a entregar paquetes de datos a un destino dentro de la subred.
- **Ethernet TCP/IP statistics** — proporciona estadísticas para TCP/IP, que es el Protocolo de control de transmisión (TCP) y el Protocolo de Internet (IP) para el dispositivo iSCSI. Con TCP, las aplicaciones en hosts en red pueden crean conexiones entre sí, mediante las cuales pueden intercambiar datos en paquetes. El IP es un protocolo orientado a datos que comunica datos por una interred conmutada por paquetes. Las estadísticas de IPv4 e IPv6 se muestran por separado.
- **Estadísticas de destino local/iniciador (protocolo)**: Muestra estadísticas para el destino iSCSI, que proporciona acceso a nivel de bloque a sus medios de almacenamiento y muestra las estadísticas de iSCSI para la matriz de almacenamiento cuando se utiliza como iniciador en operaciones de mirroring

asíncrono.

- **Estadísticas de Estados operativos de DCBX** — muestra los estados operativos de las diversas funciones de Data Center Bridging Exchange (DCBX).
- **LLDP TLV statistics** — muestra las estadísticas de tipo-longitud-valor (TLV) del protocolo de detección de nivel de vínculo (LLDP).
- **Estadísticas TLV de DCBX** — muestra la información que identifica los puertos de host de la matriz de almacenamiento en un entorno de protocolo de puente del centro de datos (DCB). Esta información se comparte con los colegas de red para fines de identificación y funcionalidad.

Es posible ver cada una de las estadísticas como estadísticas sin configurar o estadísticas de base. Las estadísticas sin configurar son todas las estadísticas recogidas desde que se iniciaron las controladoras. Las estadísticas de base son las estadísticas de un momento específico que se recogen desde el establecimiento de la hora de la línea de base.

Pasos

1. Seleccione menú:ficha Soporte[Centro de soporte > Diagnóstico].
2. Seleccione **Ver paquetes de estadísticas iSCSI**.
3. Haga clic en una pestaña para ver los diferentes conjuntos de estadísticas.
4. Para establecer la línea de base, haga clic en **establecer nueva línea de base**.

   La configuración de la línea de base establece un nuevo punto de partida para la recogida de estadísticas. La misma línea de base se usa para todas las estadísticas de iSCSI.

Ver sesiones iSCSI

Es posible ver información detallada sobre las conexiones iSCSI a la cabina de almacenamiento. Se pueden realizar sesiones iSCSI con hosts o cabinas de almacenamiento remotas en una relación de reflejo asíncrono.

Pasos

1. Seleccione MENU:Settings[System].
2. Seleccione **Ver/finalizar sesiones iSCSI**.

   Se muestra una lista de las sesiones iSCSI actuales.

3. **Opcional:** para ver información adicional acerca de una sesión iSCSI específica, seleccione una sesión y, a continuación, haga clic en **Ver detalles**.

Detalles del campo

Elemento	Descripción
Identificador de sesión (SSID)	La cadena hexadecimal que identifica una sesión entre un iniciador de iSCSI y un destino iSCSI. El SSID está compuesto por ISID y TPGT.
Identificador de sesión del iniciador (ISID)	La parte del iniciador del identificador de sesión. El iniciador especifica el ISID durante el inicio de sesión.
Grupo de portal de destino	El destino iSCSI.
Etiqueta del grupo de portal de destino (TPGT)	La parte del destino del identificador de sesión. Identificador numérico de 16 bits para un grupo de portales de destino iSCSI.
Nombre iSCSI del iniciador	El nombre WWN único del iniciador.
Etiqueta de iSCSI del iniciador	La etiqueta de usuario configurada en System Manager.
Alias del iniciador de iSCSI	Un nombre que también puede asociarse a un nodo iSCSI. El alias permite a una organización asociar una cadena intuitiva al nombre iSCSI. Sin embargo, el alias no es un sustituto del nombre iSCSI. El alias del iniciador de iSCSI solo puede configurarse en el host, no en System Manager
Host	El servidor que envía entrada y salida a la cabina de almacenamiento.
Identificador de conexión (CID)	Nombre único para una conexión dentro de la sesión entre el iniciador y el destino. El iniciador genera este ID y lo presenta al destino durante las solicitudes de inicio de sesión. El ID de conexión también se presenta durante los cierres de sesión que cierran las conexiones.
Identificador de puerto	El puerto de la controladora asociado a la conexión.
Dirección IP del iniciador	La dirección IP del iniciador.
Parámetros de inicio de sesión negociados	Los parámetros que se negocian durante el inicio de sesión de la sesión iSCSI.
Método de autenticación	La técnica para autenticar usuarios que desean acceder a la red iSCSI. Los valores válidos son **CHAP** y **Ninguno**.

Elemento	Descripción
Método de resumen del encabezado	La técnica para mostrar posibles valores de encabezados para la sesión iSCSI. HeaderDigest y DataDigest pueden ser **None** o **CRC32C**. El valor predeterminado para ambos es **Ninguno**.
Método de resumen de datos	La técnica para mostrar posibles valores de datos para la sesión iSCSI. HeaderDigest y DataDigest pueden ser **None** o **CRC32C**. El valor predeterminado para ambos es **Ninguno**.
Conexiones máximas	El mayor número de conexiones permitidas para la sesión iSCSI. El número máximo de conexiones puede ser de 1 a 4. El valor predeterminado es **1**.
Alias de destino	La etiqueta asociada al destino.
Alias del iniciador	La etiqueta asociada al iniciador.
Dirección IP de destino	La dirección IP del destino para la sesión iSCSI. Los nombres DNS no son compatibles.
R2T inicial	La inicial lista para transferir Estados. El estado puede ser **Sí** o **no**.
Longitud de ráfaga máxima	La carga útil máxima de SCSI en bytes para esta sesión iSCSI. La longitud máxima de ráfaga puede ser de 512 a 262,144 144 (256 KB). El valor predeterminado es **262,144 (256 KB)**.
Longitud de la primera ráfaga	La carga útil de SCSI en bytes para datos no solicitados para esta sesión iSCSI. La longitud de la primera ráfaga puede ser de 512 a 131,072 072 (128 KB). El valor predeterminado es **65,536 (64 KB)**.
Tiempo predeterminado de espera	La cantidad mínima de segundos que se deben esperar para intentar establecer una conexión después de la terminación o el restablecimiento de una conexión. El valor predeterminado de tiempo para esperar puede ser de 0 a 3600. El valor predeterminado es **2**.
Tiempo predeterminado de retención	La cantidad máxima de segundos durante los cuales aún puede establecerse una conexión después de la terminación o el restablecimiento de una conexión. El valor predeterminado de tiempo para retener puede ser de 0 a 3600. El valor predeterminado es **20**.
R2T pendiente máximo	La cantidad máxima de Estados listos para transferencia pendientes para esta sesión iSCSI. El valor máximo de Estados listos para transferencia pendientes puede ser de 1 a 16. El valor predeterminado es **1**.
Nivel de recuperación de errores	El nivel de recuperación de error para esta sesión iSCSI. El valor del nivel de recuperación de errores siempre está establecido en **0**.

Elemento	Descripción
Longitud máxima del segmento de datos de recepción	La cantidad máxima de datos que el iniciador o el destino pueden recibir en cualquier unidad de datos de carga útil de iSCSI (PDU).
Nombre de destino	El nombre oficial del destino (no el alias). El nombre de destino con formato *IQN*.
Nombre del iniciador	El nombre oficial del iniciador (no el alias). El nombre del iniciador que usa formato *IQN* o *eui*.

4. **Opcional:** para guardar el informe en un archivo, haga clic en **Guardar**.

   El archivo se guarda en la carpeta de descargas del explorador con el nombre de archivo `iscsi-session-connections.txt`.

Finalice la sesión iSCSI

Es posible finalizar una sesión iSCSI que no se necesita. Se pueden realizar sesiones iSCSI con hosts o cabinas de almacenamiento remotas en una relación de reflejo asíncrono.

Acerca de esta tarea

Es posible que desee finalizar una sesión iSCSI por los siguientes motivos:

- **Acceso no autorizado** — Si un iniciador iSCSI está conectado y no debe tener acceso, puede finalizar la sesión iSCSI para forzar al iniciador iSCSI fuera de la matriz de almacenamiento. El iniciador de iSCSI puede haber iniciado sesión porque el método de autenticación Ninguno estaba disponible.
- **Tiempo de inactividad del sistema** — Si necesita desconectar una matriz de almacenamiento y observa que los iniciadores iSCSI todavía están conectados, puede finalizar las sesiones iSCSI para sacar los iniciadores iSCSI de la matriz de almacenamiento.

Pasos

1. Seleccione MENU:Settings[System].
2. Seleccione **Ver/finalizar sesiones iSCSI**.

   Se muestra una lista de las sesiones iSCSI actuales.

3. Seleccione la sesión que desea finalizar
4. Haga clic en **Finalizar sesión** y confirme que desea realizar la operación.

Configure los puertos Iser over InfiniBand

Si la controladora tiene un puerto Iser over InfiniBand, se puede configurar la conexión de red al host.

Antes de empezar

- La controladora debe tener un puerto Iser over InfiniBand; de lo contrario, las opciones de Iser over InfiniBand no estarán disponibles en System Manager.
- Se debe conocer la dirección IP de la conexión de host.

Pasos

1. Seleccione **hardware**.
2. Si el gráfico muestra las unidades, haga clic en **Mostrar parte posterior de la bandeja**.

   El gráfico cambia y muestra las controladoras en lugar de las unidades.

3. Haga clic en la controladora que tenga el puerto Iser over InfiniBand que desea configurar.

   Aparece el menú contextual de la controladora.

4. Seleccione **Configurar puertos Iser over InfiniBand**.

   Se muestra el cuadro de diálogo Configurar puertos Iser over InfiniBand.

5. En el menú desplegable, seleccione el puerto HIC que desea configurar y después introduzca la dirección IP del host.
6. Haga clic en **Configurar**.
7. Complete la configuración y, a continuación, restablezca el puerto Iser over InfiniBand haciendo clic en **Sí**.

Ver estadísticas de Iser over InfiniBand

Si la controladora de la cabina de almacenamiento incluye un puerto Iser over InfiniBand, es posible ver datos sobre las conexiones del host.

Acerca de esta tarea

En System Manager, se muestran los siguientes tipos de estadísticas de Iser over InfiniBand. Todas las estadísticas son de solo lectura y no pueden configurarse.

- **Estadísticas de destino local (protocolo)** — proporciona estadísticas para el destino Iser over InfiniBand, que muestra el acceso de nivel de bloque a sus medios de almacenamiento.
- **Estadísticas de la interfaz Iser over InfiniBand** — proporciona estadísticas para todos los puertos Iser en la interfaz InfiniBand, que incluye estadísticas de rendimiento e información de errores de enlace asociados con cada puerto del switch.

Es posible ver cada una de las estadísticas como estadísticas sin configurar o estadísticas de base. Las estadísticas sin configurar son todas las estadísticas recogidas desde que se iniciaron las controladoras. Las estadísticas de base son las estadísticas de un momento específico que se recogen desde el establecimiento de la hora de la línea de base.

Pasos

1. Seleccione MENU:Settings[System].
2. Seleccione **Ver estadísticas de Iser over InfiniBand**.
3. Haga clic en una pestaña para ver los diferentes conjuntos de estadísticas.
4. **Opcional:** para establecer la línea de base, haga clic en **establecer nueva línea de base**.

   La configuración de la línea de base establece un nuevo punto de partida para la recogida de estadísticas.

La misma línea de base se usa para todas las estadísticas de Iser over InfiniBand.

Gestione los puertos NVMe

Información general de NVMe

Algunas controladoras incluyen un puerto para implementar NVMe (memoria no volátil rápida) en estructuras. NVMe permite una comunicación de alto rendimiento entre los hosts y la cabina de almacenamiento.

¿Qué es NVMe?

NVM significa "memoria no volátil", y es una memoria persistente utilizada en muchos tipos de dispositivos de almacenamiento. *NVMe* (NVM Express) es una interfaz o un protocolo estandarizados diseñados específicamente para la comunicación de varias colas de alto rendimiento con dispositivos NVM.

¿Qué es NVMe over Fabrics?

NVMe over Fabrics (NVMe-of) es una especificación de tecnología que permite la transferencia de datos y comandos basados en mensajes de NVMe entre un equipo host y un almacenamiento a través de una red. Un host puede acceder a una cabina de almacenamiento NVMe (que se denomina *SUBSYSTEM*) con una estructura. Los comandos NVMe se habilitan y se encapsulan en capas de abstracción de transporte en el lado del host y del subsistema. Esto extiende la interfaz NVMe integral de alto rendimiento desde el host hasta el almacenamiento, además de estandarizar y simplificar el conjunto de comandos.

El almacenamiento NVMe-of se presenta a un host como dispositivo de almacenamiento basado en bloques local. El volumen (que se denomina *Namespace*) puede montarse en un sistema de archivos, como sucede con cualquier otro dispositivo de almacenamiento en bloques. Es posible usar la API de REST, la SMcli o SANtricity System Manager para aprovisionar el almacenamiento según sea necesario.

¿Qué es un nombre completo de NVMe (NQN)?

El nombre completo de NVMe (NQN) se utiliza para identificar el destino de almacenamiento remoto. El nombre completo de NVMe para la cabina de almacenamiento siempre es una asignación del subsistema que no puede modificarse. Hay un solo nombre completo de NVMe para toda la cabina. El nombre completo de NVMe se limita a 223 caracteres de longitud. Es posible compararlo con un nombre completo de iSCSI.

¿Qué es un espacio de nombres y un identificador de espacio de nombres?

Un espacio de nombres es el equivalente a una unidad lógica en SCSI, que está relacionada con un volumen en la cabina. El identificador de espacio de nombres (NSID) es equivalente a un número de unidad lógica (LUN) en SCSI. Es posible crear el NSID en el momento de la creación del espacio de nombres, y configurarlo con un valor entre 1 y 255.

¿Qué es una controladora NVMe?

Como un SCSI I_T nexus, que representa la ruta desde el iniciador del host hasta el objetivo del sistema de almacenamiento, una controladora NVMe creada durante el proceso de conexión del host ofrece una ruta de acceso entre un host y los espacios de nombres en la cabina de almacenamiento. Un NQN para el host más un identificador de puerto de host identifican de manera única una controladora NVMe. Si bien una controladora NVMe solo puede asociarse con un solo host, puede acceder a varios espacios de nombres.

Es posible configurar los hosts que pueden acceder a determinados espacios de nombres y configurar el identificador de espacio de nombres para el host con SANtricity System Manager. A continuación, cuando se

crea la controladora NVMe, esta puede acceder a la lista de identificadores de espacio de nombres creada y utilizada para configurar las conexiones permitidas.

Configure los puertos NVMe over InfiniBand

Si la controladora incluye una conexión NVMe over InfiniBand, los ajustes del puerto NVMe se pueden configurar desde la página hardware.

Antes de empezar

- La controladora debe incluir un puerto de host NVMe over InfiniBand; de lo contrario, los ajustes de NVMe over InfiniBand no estarán disponibles en System Manager.
- Se debe conocer la dirección IP de la conexión de host.

> La configuración y las funciones de NVMe over InfiniBand aparecen solamente si la controladora de la cabina de almacenamiento contiene un puerto NVMe over InfiniBand.

Pasos

1. Seleccione **hardware**.
2. Si el gráfico muestra las unidades, haga clic en **Mostrar parte posterior de la bandeja**.

   El gráfico cambia y muestra las controladoras en lugar de las unidades.

3. Haga clic en la controladora que tenga el puerto NVMe over InfiniBand que desea configurar.

   Aparece el menú contextual de la controladora.

4. Seleccione **Configurar puertos NVMe over InfiniBand**.

   Se abre el cuadro de diálogo Configurar puertos NVMe over InfiniBand.

5. Seleccione el puerto de HIC que desea configurar de la lista desplegable e introduzca la dirección IP.

   Si desea configurar una cabina de almacenamiento EF600 con una HIC de 200 GB, este cuadro de diálogo muestra dos campos de dirección IP: Uno para un puerto físico (externo) y uno para un puerto virtual (interno). Debe asignar una dirección IP exclusiva a cada puerto. Estos ajustes permiten que el host establezca una ruta entre cada puerto y que la HIC alcance el rendimiento máximo. Si no se asigna una dirección IP al puerto virtual, la HIC se ejecutará a aproximadamente la mitad de su capacidad de velocidad.

6. Haga clic en **Configurar**.
7. Una vez terminada la configuración, haga clic en **Sí** para reiniciar el puerto NVMe over InfiniBand.

Configure los puertos NVMe over roce

Si la controladora incluye una conexión para NVMe over roce (RDMA over Converged Ethernet), es posible configurar las opciones del puerto NVMe desde la página hardware.

Antes de empezar

- La controladora debe incluir un puerto de host NVMe over roce; de lo contrario, los ajustes de NVMe over roce no estarán disponibles en System Manager.
- Se debe conocer la dirección IP de la conexión de host.

Pasos

1. Seleccione **hardware**.
2. Si el gráfico muestra las unidades, haga clic en **Mostrar parte posterior de la bandeja**.

   El gráfico cambia y muestra las controladoras en lugar de las unidades.

3. Haga clic en la controladora que tenga el puerto NVMe over roce que desea configurar.

   Aparece el menú contextual de la controladora.

4. Seleccione **Configurar puertos NVMe over roce**.

   Se abre el cuadro de diálogo Configurar puertos NVMe over roce.

5. En la lista desplegable, seleccione el puerto HIC que desea configurar.
6. Haga clic en **Siguiente**.

   Para ver todas las configuraciones de puerto, haga clic en el enlace **Mostrar más opciones de puerto** situado a la derecha del cuadro de diálogo.

   Detalles del campo

Opción de configuración de puertos	Descripción
Velocidad de puerto ethernet configurada	Seleccione la velocidad que coincida que la capacidad de velocidad del SFP en el puerto.
Habilite IPv4/Habilitar IPv6	Seleccione una o ambas opciones para habilitar la compatibilidad con las redes IPv4 e IPv6. Si desea deshabilitar el acceso al puerto, cancele la selección de las dos casillas de comprobación.
Tamaño de MTU (disponible haciendo clic en **Mostrar más opciones de puerto**).	De ser necesario, introduzca un nuevo tamaño en bytes para la unidad de transmisión máxima (MTU). El tamaño de MTU predeterminado es de 1500 bytes por trama. Debe introducir un valor entre 1500 y 9000.

   Si seleccionó **Activar IPv4**, se abre un cuadro de diálogo para seleccionar la configuración IPv4 después de hacer clic en **Siguiente**. Si seleccionó **Activar IPv6**, se abre un cuadro de diálogo para seleccionar la configuración de IPv6 después de hacer clic en **Siguiente**. Si seleccionó ambas opciones, primero se abre el cuadro de diálogo de configuración IPv4 y después de hacer clic en **Siguiente**, se abre el cuadro de diálogo de configuración de IPv6.

7. Configure los valores para IPv4 o IPv6 de forma automática o manual.

Detalles del campo

Opción de configuración de puertos	Descripción
Obtener configuración automáticamente	Seleccione esta opción para obtener automáticamente la configuración.
Especificar manualmente la configuración estática	Seleccione esta opción e introduzca una dirección estática en los campos. (Si lo desea, puede cortar y pegar direcciones en los campos.) En el caso de IPv4, incluya la máscara de subred y la puerta de enlace. En el caso de IPv6, incluya la dirección IP enrutable y la dirección IP del enrutador. Si desea configurar una cabina de almacenamiento EF600 con una HIC de 200 GB, este cuadro de diálogo muestra dos conjuntos de campos para los parámetros de red: Uno para un puerto físico (externo) y uno para un puerto virtual (interno). Debe asignar parámetros exclusivos a cada puerto. Estos ajustes permiten que el host establezca una ruta entre cada puerto y que la HIC alcance el rendimiento máximo. Si no se asigna una dirección IP al puerto virtual, la HIC se ejecutará a aproximadamente la mitad de su capacidad de velocidad.

8. Haga clic en **Finalizar**.

Ver estadísticas de NVMe over Fabrics

Es posible ver datos acerca de las conexiones NVMe over Fabrics a la cabina de almacenamiento.

Acerca de esta tarea

En System Manager, se muestran los siguientes tipos de estadísticas de NVMe over Fabrics. Todas las estadísticas son de solo lectura y no pueden configurarse.

- **Estadísticas del subsistema NVMe** — muestra estadísticas para la controladora NVMe y su cola. La controladora NVMe ofrece una ruta de acceso entre un host y los espacios de nombres en la cabina de almacenamiento. Es posible revisar las estadísticas del subsistema NVMe para consultar elementos, como errores de conexión, reinicios y apagados.
- **Estadísticas de la interfaz RDMA** — proporciona estadísticas para todos los puertos NVMe over Fabrics de la interfaz RDMA, que incluye estadísticas de rendimiento e información de errores de enlace asociados con cada puerto del switch. Esta pestaña solo se muestra cuando existen puertos NVMe over Fabrics disponibles.

Es posible ver cada una de las estadísticas como estadísticas sin configurar o estadísticas de base. Las estadísticas sin configurar son todas las estadísticas recogidas desde que se iniciaron las controladoras. Las estadísticas de base son las estadísticas de un momento específico que se recogen desde el establecimiento de la hora de la línea de base.

Pasos

1. Seleccione MENU:Settings[System].
2. Seleccione **Ver estadísticas de NVMe over Fabrics**.

3. **Opcional:** para establecer la línea de base, haga clic en **establecer nueva línea de base**.

   La configuración de la línea de base establece un nuevo punto de partida para la recogida de estadísticas. Se usa la misma línea de base para todas las estadísticas de NVMe.

Gestionar unidades

estados de unidad

System Manager informa sobre distintos estados de las unidades.

estados de accesibilidad

Estado	Definición
Omitida	La unidad está presente físicamente, pero la controladora no puede comunicarse con ella en ningún puerto.
Incompatible	Existe una de las siguientes condiciones: • La unidad no está certificada para usar en la cabina de almacenamiento. • La unidad tiene un tamaño de sector diferente. • La unidad tiene datos de configuración inutilizables de una versión de firmware anterior o posterior.
Quitada	La unidad se retiró de manera incorrecta de la cabina de almacenamiento.
Presente	La controladora puede comunicarse con la unidad en ambos puertos.
Sin respuesta	La unidad no responde a los comandos.

estados de roles

Estado	Definición
Asignado	La unidad es miembro de un pool o un grupo de volúmenes.
Pieza de repuesto en uso	La unidad se está usando como reemplazo de otra que tuvo errores. Las piezas de repuesto solo se usan en grupos de volúmenes, no en pools.
Pieza de repuesto en espera	La unidad está lista para usarse como reemplazo de otra que tuvo errores. Las piezas de repuesto solo se usan en grupos de volúmenes, no en pools.
Sin asignar	La unidad no es miembro de un pool ni de un grupo de volúmenes.

estados de disponibilidad

Estado	Definición
Error	La unidad no funciona. Los datos en la unidad no están disponibles.
Fallo inminente	Se detectó que la unidad puede fallar pronto. Los datos en la unidad siguen estando disponibles.
Sin conexión	La unidad no está disponible para almacenar datos, generalmente debido a que forma parte de un grupo de volúmenes que se está exportando o se está sometiendo a una actualización de firmware.
Óptimo	La unidad funciona normalmente.

Discos de estado sólido (SSD)

Los discos de estado sólido (SSD) son dispositivos de almacenamiento de datos que usan memoria de estado sólido (flash) para almacenar datos en forma persistente. Los SSD emulan las unidades de discos duros convencionales y están disponibles con las mismas interfaces que usan las unidades de disco duro.

Ventajas de los discos SSD

Algunas de las ventajas de los discos SSD sobre las unidades de disco duro son:

- Inicio más rápido (sin aumentar velocidad de giro)
- Latencia más baja
- Más operaciones de I/o por segundo (IOPS)
- Más fiabilidad con menos piezas móviles
- Menos consumo de energía
- Menos calor producido y menos refrigeración requerida

Identificación de SSD

En la página hardware, es posible localizar los discos SSD en la vista de la bandeja frontal. Busque las bahías de unidades con un icono de rayo. Esto indica que existe un SSD instalado.

Grupos de volúmenes

Un grupo de volúmenes debe contener unidades de un mismo tipo de medio (todos discos SSD o todas unidades de disco duro). Un grupo de volúmenes no puede contener una combinación de tipos de medios o tipos de interfaces.

Almacenamiento en caché

El almacenamiento en caché de escritura de las controladoras siempre está habilitado para SSD. La caché de escritura aumenta el rendimiento y prolonga la vida útil de los discos SSD.

Además de la caché de la controladora, es posible implementar una caché SSD para mejorar el rendimiento general del sistema. En la caché SSD, se copian datos de volúmenes y se almacenan en dos volúmenes de

RAID internos (uno por controladora).

Limite la vista de unidades

Si la cabina de almacenamiento incluye unidades con diferentes tipos de atributos físicos y lógicos, la página hardware ofrece campos de filtros para limitar la vista de unidades y localizar unidades específicas.

Acerca de esta tarea

Los filtros de unidades pueden limitar la vista a solo ciertos tipos de unidades físicas (por ejemplo, todas las SAS), con ciertos atributos de seguridad (por ejemplo, compatibles con la función de seguridad) en ciertas ubicaciones lógicas (por ejemplo, grupo de volúmenes 1). Es posible usar estos filtros de forma conjunta o por separado.

> Si todas las unidades comparten los mismos atributos físicos, el campo de filtro **Mostrar unidades…** no aparece. Si todas las unidades comparten los mismos atributos lógicos, el campo de filtro **en cualquier lugar de la matriz de almacenamiento** no aparece.

Pasos

1. Seleccione **hardware**.
2. En el primer campo de filtro (en **Mostrar unidades…**), haga clic en la flecha desplegable para mostrar los tipos de unidades y atributos de seguridad disponibles.

   Los tipos de unidades pueden ser los siguientes:

   - Tipo de medio de unidad (unidad de estado sólido, disco duro)
   - Tipo de interfaz de unidad
   - Capacidad de unidad (de la más alta a la más baja)
   - Los atributos de seguridad de velocidad de unidad (de la más alta a la más baja) pueden ser los siguientes:
   - Compatible con la función de seguridad
   - Con la función de seguridad habilitada
   - Compatible con DA (Data Assurance)
   - Conforme a FIPS
   - Conforme a la normativa FIPS (FIPS 140-2)
   - Conforme a FIPS (FIPS 140-3)

     Si todas las unidades comparten algunos de estos atributos, no se mostrarán en la lista desplegable. Por ejemplo, si la cabina de almacenamiento incluye todas las unidades SSD con interfaces SAS y velocidades de 15 15000 RPM, pero algunas unidades SSD poseen diferentes capacidades, la lista desplegable muestra solo las capacidades como opción de filtrado.

   Cuando se selecciona una opción en el campo, las unidades que no coinciden con los criterios del filtro se atenúan en la vista gráfica.

3. En el segundo cuadro de filtro, haga clic en la flecha desplegable para mostrar las ubicaciones lógicas disponibles para las unidades.

Si necesita borrar sus criterios de filtro, seleccione **Borrar** en el extremo derecho de los cuadros de filtro.

Las ubicaciones lógicas pueden ser las siguientes:

- Piscinas
- Grupos de volúmenes
- Pieza de repuesto
- Caché SSD
- Sin asignar

  Cuando se selecciona una opción en el campo, las unidades que no coinciden con los criterios del filtro se atenúan en la vista gráfica.

4. Opcionalmente, puede seleccionar **encender las luces de localización** en el extremo derecho de los campos de filtro para encender las luces de localización de las unidades mostradas.

   Esta acción ayuda a localizar físicamente las unidades en la cabina de almacenamiento.

Encienda la luz localizadora de la unidad

En la página hardware, se puede encender la luz localizadora para encontrar la ubicación física de una unidad en la cabina de almacenamiento.

Acerca de esta tarea

Se pueden localizar unidades únicas o varias unidades que se muestran en la página hardware.

Pasos

1. Seleccione **hardware**.
2. Para localizar una o más unidades, se debe realizar una de las siguientes acciones:
   - **Una sola unidad** — desde el gráfico de estante, encuentre la unidad que desea localizar físicamente en la matriz. (Si el gráfico muestra los controladores, haga clic en **Mostrar frente de la bandeja**.) Haga clic en la unidad para mostrar el menú contextual y, a continuación, seleccione **encender luz de localización**.

     La luz localizadora de la unidad se enciende. Cuando haya localizado físicamente la unidad, vuelva al cuadro de diálogo y seleccione **Apagar**.

   - **Múltiples unidades** — en los campos de filtro, seleccione un tipo de unidad física de la lista desplegable izquierda y un tipo de unidad lógica de la lista desplegable derecha. En el extremo derecho de los campos, se muestra la cantidad de unidades que coincide con sus criterios. A continuación, puede hacer clic en **encender luces de localización** o seleccionar **ubicar todas las unidades filtradas** en el menú contextual. Cuando haya localizado físicamente las unidades, vuelva al cuadro de diálogo y seleccione **Apagar**.

Ver el estado y la configuración de las unidades

Es posible ver el estado y la configuración de las unidades, como el tipo de medios, el tipo de interfaz y la capacidad.

Pasos

1. Seleccione **hardware**.
2. Si el gráfico muestra los controladores, haga clic en **Mostrar frente de la bandeja**.

   El gráfico cambia y muestra las unidades en lugar de las controladoras.

3. Seleccione la unidad para la cual desea ver el estado y la configuración.

   Se abre el menú contextual de la unidad.

4. Seleccione **Ver configuración**.

   Se abrirá el cuadro de diálogo Configuración de la unidad.

5. Para ver todos los ajustes, haga clic en **Mostrar más valores** en la parte superior derecha del cuadro de diálogo.

Detalles del campo

Configuración	Descripción
Estado	Muestra los Estados óptimo, sin conexión, error no crítico y con errores. El estado óptima indica la condición de funcionamiento deseada.
Modo	Muestra los modos Assigned, Unassigned, Hot Spare Standby o pieza de repuesto en uso.
Ubicación	Muestra la bandeja y el número de bahía donde se encuentra la unidad.
Asignado a/puede proteger/Protección	Si la unidad está asignada a un pool, un grupo de volúmenes o una caché SSD, este campo muestra el estado "asignado a". El valor puede ser un nombre de pool, nombre de grupo de volúmenes o nombre de caché SSD. Si la unidad está asignada a una pieza de repuesto y está en modo en espera, este campo muestra "puede proteger". Si la pieza de repuesto puede proteger un grupo de volúmenes o más, se muestra el nombre del grupo de volúmenes. Si no puede proteger un grupo de volúmenes, no se muestra ningún nombre de grupo de volúmenes. Si la unidad está asignada a una pieza de repuesto y está en modo en uso, este campo muestra "Protección". El valor es el nombre del grupo de volúmenes afectado. Si la unidad está sin asignar, este campo no aparece.
Tipo de medios	Muestra el tipo de medio de grabación que utiliza la unidad, que puede ser una unidad de disco duro (HDD) o un disco de estado sólido (SSD).
Porcentaje de resistencia utilizado (solo se muestra si existen unidades SSD)	Muestra la cantidad de datos escritos en la unidad hasta la fecha, divididos por límite de escritura teórico total.
Tipo de interfaz	Muestra el tipo de interfaz que usa la unidad, como SAS.
Redundancia de ruta de unidades	Muestra si las conexiones entre la unidad y la controladora son redundantes o no.
Capacidad (GIB)	Muestra la capacidad utilizable (capacidad configurada total) de la unidad.
Velocidad (RPM)	Muestra la velocidad en RPM (no aparece para SSD).
Tasa de datos actual	Muestra la tasa de transferencia de datos entre la unidad y la cabina de almacenamiento.
Tamaño de sector lógico (bytes)	Muestra el tamaño del sector lógico que usa la unidad.

Configuración	Descripción
Tamaño de sector físico (bytes)	Muestra el tamaño del sector físico que usa la unidad. Por lo general, el tamaño del sector físico es 4096 bytes para unidades de discos duros.
La versión de firmware de la unidad	Muestra el nivel de revisión del firmware de la unidad.
Identificador a nivel mundial	Muestra el identificador hexadecimal único de la unidad.
ID de producto	Muestra el identificador del producto, asignado por el fabricante.
Número de serie	Muestra el número de serie de la unidad.
Fabricante	Muestra el proveedor de la unidad.
Fecha de fabricación	Muestra la fecha en que se fabricó la unidad. No está disponible para unidades NVMe.
Compatible con la función de seguridad	Muestra si la unidad es compatible con la función de seguridad (Sí) o no (no). Las unidades compatibles con la función de seguridad pueden ser unidades de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS) (nivel 140-2 o 140-3) que cifran datos durante la escritura y descifran datos durante la lectura. Estas unidades se consideran Secure-*capable* porque se pueden usar para obtener más seguridad mediante la función Drive Security. Si está habilitada la función Drive Security para los grupos de volúmenes y pools que se utilizan con estas unidades, las unidades pasan a tener habilitada la función de seguridad-*enabled*.
Con la función de seguridad habilitada	Muestra si la unidad tiene la función de seguridad habilitada (Sí) o no (no). Las unidades con la función de seguridad habilitada se usan con Drive Security. Cuando se habilita la función Drive Security y se aplica Drive Security a un pool o un grupo de volúmenes en unidades_ compatibles con la función de seguridad, las unidades pasan a ser seguras-*enabled*. El acceso de lectura y escritura solo está disponible a través de una controladora que está configurada con la clave de seguridad correcta. Esta seguridad adicional evita el acceso no autorizado a los datos en una unidad que se quita físicamente de la cabina de almacenamiento.
Accesibilidad de lectura/escritura	Muestra si la unidad tiene acceso de lectura/escritura (Sí) o no (no).

Configuración	Descripción
Identificador de clave de seguridad de unidad	Muestra la clave de seguridad para unidades con la función de seguridad habilitada. Drive Security es una función de la cabina de almacenamiento que ofrece una capa adicional de seguridad con unidades de cifrado de disco completo (FDE) o unidades de estándar de procesamiento de información federal (FIPS). Cuando estas unidades se usan con la función Drive Security, se requiere una clave de seguridad para acceder a los datos. Cuando se retiran físicamente, las unidades de la cabina no pueden operar hasta que se instalan en otra cabina, instancia en la cual tendrán el estado Security Locked hasta que se proporcione la clave de seguridad correcta.
Compatible con la función de garantía de datos (DA)	Muestra si la función de garantía de datos (DA) está habilitada (Sí) o no (no). La garantía de datos (DA) es una función que comprueba y corrige los errores que se pueden producir durante la transferencia de datos a través de las controladoras hasta las unidades. Garantía de datos se puede habilitar en el nivel del pool o grupo de volúmenes, y los hosts pueden utilizar una interfaz de I/o compatible CON DA como, por ejemplo, Fibre Channel.
Compatible con DULBE	Indica si la opción error de bloque lógico no escrito o desasignado (DULBE) está habilitada (Sí) o no (no). DULBE es una opción en las unidades NVMe con la que la cabina de almacenamiento EF300 o EF600 puede admitir volúmenes con aprovisionamiento de recursos.

6. Haga clic en **Cerrar**.

Reemplace una unidad de forma lógica

Si se produce un error en una unidad o si desea reemplazarla por algún otro motivo, puede reemplazar lógicamente la unidad con error por una unidad sin asignar o una pieza de repuesto totalmente integrada.

Acerca de esta tarea

Cuando se reemplaza una unidad de forma lógica, se asigna y se convierte en miembro permanente del pool o grupo de volúmenes asociados.

La opción de reemplazo lógico se utiliza para reemplazar los siguientes tipos de unidades:

- Unidades con errores
- Unidades ausentes
- Unidades SSD que Recovery Guru notificó como próximas al final de su vida útil
- Unidades de disco duro que Recovery Guru notificó como unidades con un error inminente
- Unidades asignadas (solo disponible para unidades en un grupo de volúmenes, no en un pool)

Antes de empezar

La unidad de reemplazo debe tener las siguientes características:

- En estado óptima
- En estado sin asignar
- Mismos atributos que la unidad que se reemplazará (tipo de medio, tipo de interfaz, etc.)
- Misma capacidad de FDE (se recomienda, no es obligatorio)
- Misma capacidad de DA (se recomienda, no es obligatorio)

Pasos

1. Seleccione **hardware**.
2. Si el gráfico muestra los controladores, haga clic en **Mostrar frente de la bandeja**.

   El gráfico cambia y muestra las unidades en lugar de las controladoras.

3. Haga clic en la unidad que desea reemplazar de forma lógica.

   Aparece el menú contextual de la unidad.

4. Haga clic en **sustituir lógicamente**.
5. **Opcional:** Active la casilla de verificación **fallo de unidad después de su sustitución** para que falle la unidad original después de sustituirla.

   Esta casilla solo se habilita si la unidad asignada original no presenta errores ni se especifica como ausente.

6. En la tabla **Seleccione una unidad de sustitución**, seleccione la unidad de sustitución que desea utilizar.

   La tabla solo contiene las unidades que son compatibles con la unidad que se desea reemplazar. Si es posible, seleccione una unidad con la que se pueda mantener la protección contra pérdida de bandeja y la protección contra pérdida de cajón.

7. Haga clic en **sustituir**.

   Si la unidad original presenta errores o se encuentra ausente, se utiliza la información de paridad para reconstruir los datos en la unidad de reemplazo. Esta reconstrucción se inicia automáticamente. Las luces indicadoras de fallo de la unidad se apagan y las luces indicadoras de actividad de las unidades en el pool o el grupo de volúmenes empiezan a parpadear.

   Si la unidad original no presenta errores ni se especifica como ausente, se copian sus datos a la unidad de reemplazo. La operación de copia se inicia automáticamente. Una vez completada la operación de copia, el sistema transfiere la unidad original al estado sin asignar o, si se seleccionó la casilla correspondiente, al estado con errores.

Reconstruir manualmente una unidad

Normalmente, la reconstrucción de unidades se inicia de forma automática después de reemplazar una unidad. Si la reconstrucción de una unidad no se inicia de forma automática, es posible iniciarla manualmente.

Realice esta operación solo cuando el soporte técnico o Recovery Guru se lo indiquen.

Pasos

1. Seleccione **hardware**.
2. Si el gráfico muestra los controladores, haga clic en **Mostrar frente de la bandeja**.

   El gráfico cambia y muestra las unidades en lugar de las controladoras.

3. Haga clic en la unidad que desea reconstruir manualmente.

   Aparece el menú contextual de la unidad.

4. Seleccione **reconstruir** y confirme que desea realizar la operación.

Inicialice (formatear) una unidad

Si se mueven unidades asignadas de una cabina de almacenamiento a otra, deben inicializarse (formatearse) las unidades para poder utilizarlas en la cabina de almacenamiento nueva.

Acerca de esta tarea

La inicialización elimina la información de configuración previa de una unidad y la devuelve al estado sin asignar. De esa manera, la unidad está disponible para añadirse a un nuevo pool o grupo de volúmenes en la nueva cabina de almacenamiento.

Utilice la operación de inicialización de unidades cuando mueve una sola unidad. No es necesario inicializar unidades si se mueve un grupo de volúmenes entero de una cabina de almacenamiento a otra.

> **Posible pérdida de datos** — cuando se inicializa una unidad, se pierden todos los datos de la unidad. Realice esta operación solo cuando el soporte técnico se lo indique.

Pasos

1. Seleccione **hardware**.
2. Si el gráfico muestra los controladores, haga clic en **Mostrar frente de la bandeja**.

   El gráfico cambia y muestra las unidades en lugar de las controladoras.

3. Haga clic en la unidad que desea inicializar.

   Aparece el menú contextual de la unidad.

4. Seleccione **inicializar** y confirme que desea realizar la operación.

Hacer que una unidad falle

Es posible hacer que una unidad falle de forma manual, si se reciben instrucciones para hacerlo.

Acerca de esta tarea

System Manager supervisa las unidades en la cabina de almacenamiento. Cuando detecta que una unidad está generando muchos errores, Recovery Guru envía una notificación de fallo de unidad inminente. Si sucede esto y existe una unidad de reemplazo disponible, quizás desee hacer que la unidad falle como medida preventiva. Si no tiene una unidad de reemplazo disponible, puede esperar a que la unidad falle por sí misma.

Posible pérdida de acceso a los datos — esta operación podría provocar la pérdida de datos o la pérdida de redundancia de datos. Realice esta operación solo cuando el soporte técnico o Recovery Guru se lo indiquen.

Pasos

1. Seleccione **hardware**.
2. Si el gráfico muestra los controladores, haga clic en **Mostrar frente de la bandeja**.

   El gráfico cambia y muestra las unidades en lugar de las controladoras.

3. Haga clic en la unidad que desea que falle.

   Aparece el menú contextual de la unidad.

4. Seleccione **error**.
5. Mantenga seleccionada la casilla de verificación **Copiar contenido de la unidad antes de la conmutación**.

   La opción de copia aparecerá solo para las unidades asignadas y para los grupos de volúmenes que no poseen una configuración RAID 0.

   Antes de hacer que la unidad falle, asegúrese de copiar su contenido. Según la configuración, es posible que se pierdan potencialmente todos los datos o la redundancia de datos en el pool o el grupo de volúmenes asociado, si primero no se copian los contenidos de la unidad.

   La opción de copia permite una recuperación más rápida de la unidad que la reconstrucción, y reduce la posibilidad de un fallo del volumen si otra unidad presenta errores durante la operación de copia.

6. Confirme que desea que la unidad falle.

   Después de que falle la unidad, espere al menos 30 segundos para quitarla.

Borrar unidades

La opción Borrar se puede usar para preparar una unidad sin asignar y eliminar el sistema. Este procedimiento elimina los datos de forma permanente, asegurándose de que los datos no se pueden leer de nuevo.

Antes de empezar

La unidad debe tener el estado sin asignar.

Acerca de esta tarea

Utilice la opción Borrar solo si desea eliminar de forma permanente todos los datos de una unidad. Si la unidad tiene la función de seguridad habilitada, la opción Borrar ejecuta un borrado criptográfico y restablece los atributos de seguridad de la unidad nuevamente a compatible con la función de seguridad.

La función Borrar no admite algunos modelos de unidad anteriores. Si intenta borrar uno de estos modelos antiguos, aparece un mensaje de error.

Pasos

1. Seleccione **hardware**.

2. Si el gráfico muestra los controladores, haga clic en **Mostrar frente de la bandeja**.

   El gráfico cambia y muestra las unidades en lugar de las controladoras.

3. De manera opcional, se pueden usar los campos de filtro para ver todas las unidades sin asignar de la bandeja. En la lista desplegable **Mostrar unidades que son…**, seleccione **sin asignar**.

   La vista de bandeja muestra solo las unidades no asignadas; el resto aparecen atenuadas.

4. Para abrir el menú contextual de la unidad, haga clic en una unidad que desee borrar. (Si desea seleccionar varias unidades, puede hacerlo en el cuadro de diálogo Borrar unidades).

   Posible pérdida de datos — la operación de borrado no se puede deshacer. Asegúrese de seleccionar las unidades correctas durante el procedimiento.

5. En el menú contextual, seleccione **Borrar**.

   Se abre el cuadro de diálogo Borrar unidades, donde se muestran todas las unidades elegibles para una operación de borrado.

6. Si lo desea, seleccione unidades adicionales de la tabla. No puede seleccionar *All* unidades; asegúrese de que una unidad permanece sin seleccionar.
7. Confirme la operación escribiendo `erase`Y, a continuación, haga clic en **Borrar**.

   Asegúrese de que desea continuar con esta operación. Una vez que haga clic en Sí en el siguiente cuadro de diálogo, la operación no se puede cancelar.

8. En el cuadro de diálogo tiempo estimado de finalización, haga clic en **Sí** para continuar con la operación de borrado.

Resultados

La operación de borrado puede llevar varios minutos o varias horas. Puede ver el estado en MENU:Inicio[Ver operaciones en curso]. Cuando se completa la operación Borrar, las unidades están disponibles para usar en otro grupo de volúmenes o pool de discos, o en otra cabina de almacenamiento.

Después de terminar

Si desea volver a usar la unidad, primero debe inicializarla. Para ello, seleccione **inicializar** en el menú contextual de la unidad.

Desbloquee o restablezca unidades NVMe o FIPS bloqueadas

Si se insertan una o más unidades NVMe o FIPS bloqueadas en una cabina de almacenamiento, es posible desbloquear los datos de la unidad al agregar el archivo de claves de seguridad asociado a las unidades. Si no posee una clave de seguridad, es posible restablecer cada unidad bloqueada; para ello, introduzca el ID de seguridad física (PSID) a fin de restablecer los atributos de seguridad y borrar los datos de la unidad.

Antes de empezar

- Para la opción Desbloquear, asegúrese de que el archivo de claves de seguridad (con la extensión de `.slk`) Está disponible en el cliente de gestión (el sistema con un explorador que se utiliza para acceder a System Manager). También debe conocer la frase de contraseña asociada a la clave.

- Para la opción Restablecer, debe encontrar el PSID en cada unidad que desea restablecer. Para ubicar el PSID, retire físicamente la unidad y ubique la cadena de PSID (máximo de 32 caracteres) en la etiqueta de la unidad y, luego, reinstale la unidad.

Acerca de esta tarea

En esta tarea se describe cómo desbloquear los datos en las unidades NVMe o FIPS mediante la importación de un archivo de clave de seguridad en la cabina de almacenamiento. En caso de que la clave de seguridad no esté disponible, en esta tarea también se describe cómo realizar un restablecimiento de una unidad bloqueada.

> Si la unidad se bloqueó mediante un servidor de gestión de claves externo, seleccione MENU:Configuración[sistema > Gestión de claves de seguridad] en System Manager para configurar la gestión de claves externas y desbloquear la unidad.

Es posible acceder a la función Desbloquear desde la página hardware o desde el menú:Configuración[sistema > Gestión de claves de seguridad]. La tarea siguiente incluye instrucciones en la página hardware.

Pasos

1. Seleccione **hardware**.
2. Si el gráfico muestra los controladores, haga clic en **Mostrar frente de la bandeja**.

   El gráfico cambia y muestra las unidades en lugar de las controladoras.

3. Seleccione la unidad NVMe o FIPS que desea desbloquear o restablecer.

   Se abre el menú contextual de la unidad.

4. Seleccione **Desbloquear** para aplicar el archivo de claves de seguridad o **Restablecer** si no dispone de un archivo de claves de seguridad.

   Estas opciones solo aparecen si selecciona una unidad NVMe o FIPS bloqueada.

   > Durante una operación de restablecimiento, se borran todos los datos. Realice un restablecimiento únicamente si no posee una clave de seguridad. Al restablecer una unidad bloqueada se quitan todos los datos de la unidad y se restablecen los atributos de seguridad a "compatible con la función de seguridad", pero no se habilitan. **Esta operación no es reversible.**

5. Debe realizar una de las siguientes acciones:
   a. **Desbloquear**: En el cuadro de diálogo **Desbloquear unidad segura**, haga clic en **examinar** y, a continuación, seleccione el archivo de clave de seguridad que corresponda a la unidad que desea desbloquear. Luego, introduzca la frase de contraseña y haga clic en **Desbloquear**.
   b. **Restablecer**: En el cuadro de diálogo **Restablecer unidad bloqueada**, introduzca la secuencia de PSID en el campo y, a continuación, escriba `RESET` para confirmar. Haga clic en **Restablecer**.

      Para una operación de desbloqueo, solo es necesario realizar esta operación una vez para desbloquear todas las unidades NVMe o FIPS. Para una operación de restablecimiento, debe seleccionar cada unidad que desea restablecer de forma individual.

Resultados

Ahora la unidad está disponible para usar en otro grupo de volúmenes o pool de discos, o bien en otra cabina de almacenamiento.

Gestionar piezas de repuesto

Información general de la unidad de repuesto

Las piezas de repuesto actúan como unidades en espera en los grupos de volúmenes RAID 1, RAID 5 o RAID 6 de System Manager.

Son unidades completamente funcionales que no contienen datos. Si falla una unidad en el grupo de volúmenes, la controladora reconstruye automáticamente los datos de la unidad con error en una unidad asignada como pieza de repuesto.

Las piezas de repuesto no son unidades dedicadas a grupos de volúmenes específicos. Pueden usarse para cualquier unidad con error en la cabina de almacenamiento siempre que la pieza de repuesto y la unidad compartan estos atributos:

- Igual capacidad (o una pieza de repuesto con mayor capacidad)
- Mismo tipo de medio (por ejemplo, HDD o SSD)
- Mismo tipo de interfaz (por ejemplo, SAS)

Cómo identificar las piezas de repuesto

Es posible asignar piezas de repuesto con el asistente de configuración inicial o en la página hardware. Para determinar si hay piezas de repuesto asignadas, vaya a la página hardware y busque todas las bahías de unidad que aparecen en color rosa.

Cómo funciona la cobertura de piezas de repuesto

La cobertura de piezas de repuesto funciona de la siguiente manera:

- Se reserva una unidad sin asignar como pieza de repuesto para los grupos de volúmenes RAID 1, RAID 5 o RAID 6.

> No pueden usarse piezas de repuesto para pools, ya que estos utilizan un método diferente de protección de datos. En lugar de reservar una unidad adicional, los pools asignan capacidad de reserva (denominada *preservation Capacity*) dentro de cada unidad en el pool. Si falla una unidad dentro del pool, la controladora reconstruye los datos en esa capacidad de reserva.

- Si falla una unidad dentro de un grupo de volúmenes RAID 1, RAID 5 o RAID 6, la controladora utiliza automáticamente datos de redundancia para reconstruir los datos de la unidad con error. La pieza de repuesto sustituye automáticamente la unidad con error sin que se requiera un intercambio físico.
- Luego de reemplazar físicamente la unidad con error, se realiza una operación de copyback de la unidad de repuesto a la unidad reemplazada. Si se designó la unidad de repuesto como miembro permanente de un grupo de volúmenes, no se necesita esa operación.
- La disponibilidad de la protección contra pérdida de soporte y la protección contra pérdida de cajón en un grupo de volúmenes dependen de la ubicación de las unidades que incluye ese grupo de volúmenes. La protección contra pérdida de soporte y la protección contra pérdida de cajón pueden no estar disponibles debido a una unidad con error y a la ubicación de la unidad de repuesto. Para asegurarse de que la protección contra pérdida de soporte y la protección contra pérdida de cajón no se vean afectadas, debe

reemplazar una unidad con error para iniciar el proceso de copyback.

- El volumen de la cabina de almacenamiento permanece en línea y accesible mientras reemplaza la unidad con error, ya que la unidad de repuesto sustituye automáticamente la unidad con error.

Consideraciones sobre la capacidad de la unidad de repuesto

Seleccione una unidad con una capacidad mayor o igual que la capacidad total de la unidad que desea proteger. Por ejemplo, si tiene una unidad de 18 GIB con una capacidad configurada de 8 GIB, puede usar una unidad de 9 GIB o más como pieza de repuesto. Por regla general, no asigne una unidad como pieza de repuesto a menos que su capacidad sea mayor o igual que la capacidad de la unidad más grande en la cabina de almacenamiento.

> Si no hay piezas de repuesto disponibles con la misma capacidad física, puede usarse una unidad de menor capacidad como pieza de repuesto si la "capacidad utilizada" de la unidad es menor o igual a la capacidad de la unidad de repuesto.

Consideraciones sobre tipos de medios e interfaces

La unidad utilizada como pieza de repuesto debe compartir el mismo tipo de medio y tipo de interfaz que las unidades que protegerá. Por ejemplo, una unidad de disco duro no puede actuar como pieza de repuesto de unidades SSD.

Consideraciones sobre unidades compatibles con la función de seguridad

Una unidad compatible con la función de seguridad, como FDE o FIPS, puede actuar como pieza de repuesto para unidades con o sin funcionalidades de seguridad. Sin embargo, una unidad no compatible con la función de seguridad no puede actuar como pieza de repuesto para unidades con funcionalidades de seguridad.

Cuando se selecciona una unidad con la función de seguridad habilitada para usar como pieza de repuesto, System Manager le advierte que ejecute la función Secure Erase antes de continuar. Secure Erase restablece los atributos de seguridad de la unidad para que sea compatible con la función de seguridad, pero no para que tenga la función de seguridad habilitada.

> Cuando se habilita la función Drive Security y se crea un pool o un grupo de volúmenes desde unidades compatibles con la función de seguridad, las unidades pasan a ser *Secure-enabled*. El acceso de lectura y escritura solo está disponible a través de una controladora que está configurada con la clave de seguridad correcta. Esta seguridad adicional evita el acceso no autorizado a los datos en una unidad que se quita físicamente de la cabina de almacenamiento.

Cantidad recomendada de unidades de repuesto

Si utilizó el asistente de configuración inicial para crear automáticamente piezas de repuesto, System Manager crea una pieza de repuesto cada 30 unidades de un tipo de medio y un tipo de interfaz en particular. De lo contrario, puede crear manualmente unidades de repuesto entre los grupos de volúmenes en la cabina de almacenamiento.

Asigne piezas de repuesto

Es posible asignar una pieza de repuesto como unidad en espera para protección de datos adicional en grupos de volúmenes RAID 1, RAID 5 o RAID 6. Si falla una unidad en estos grupos de volúmenes, la controladora reconstruye los datos de la unidad con error en la pieza de repuesto.

Antes de empezar

- Deben crearse grupos de volúmenes RAID 1, RAID 5 o RAID 6. (Las piezas de repuesto no pueden usarse para pools. Un pool utiliza capacidad de reserva dentro de cada unidad para la protección de datos.)
- Debe haber disponible una unidad que cumpla los siguientes criterios:
  - Sin asignar, con estado óptima.
  - El mismo tipo de medio que las unidades del grupo de volúmenes (por ejemplo, SSD).
  - El mismo tipo de interfaz que las unidades del grupo de volúmenes (por ejemplo, SAS).
  - Una capacidad igual o mayor que la capacidad utilizada de las unidades en el grupo de volúmenes.

Acerca de esta tarea

En esta tarea, se describe cómo asignar manualmente una pieza de repuesto en la página hardware. La cobertura recomendada es dos piezas de repuesto por conjunto de unidades.

> Las piezas de repuesto también pueden asignarse desde el asistente de configuración inicial. Para determinar si las piezas de repuesto ya están asignadas, busque las bahías de unidades que se muestran en color rosa en la página hardware.

Pasos

1. Seleccione **hardware**.
2. Si el gráfico muestra los controladores, haga clic en **Mostrar frente de la bandeja**.

   El gráfico cambia y muestra las unidades en lugar de las controladoras.

3. Seleccione una unidad sin asignar (color gris) que desee usar como pieza de repuesto.

   Se abre el menú contextual de la unidad.

4. Seleccione **asignar pieza de repuesto**.

   Si la unidad tiene la función de seguridad habilitada, se abre el cuadro de diálogo secure erase drive? Para usar una unidad con la función de seguridad habilitada como pieza de repuesto, debe ejecutarse la operación Secure Erase, con el fin de eliminar todos sus datos y restablecer sus atributos de seguridad.

   > **Posible pérdida de datos** — Asegúrese de que ha seleccionado la unidad correcta. Una vez finalizada la operación borrado seguro, los datos no se pueden recuperar.

   Si la unidad tiene **no** la función de seguridad habilitada, se abre el cuadro de diálogo Confirmar asignación de unidad de repuesto.

5. Revise el texto en el cuadro de diálogo y confirme la operación.

   La unidad aparece de color rosa en la página hardware, lo que indica que ahora es una pieza de repuesto.

Resultados

Si falla una unidad dentro de un grupo de volúmenes RAID 1, RAID 5 o RAID 6, la controladora utiliza automáticamente datos de redundancia para reconstruir los datos de la unidad con error en la pieza de repuesto.

Anular asignación de piezas de repuesto

Es posible cambiar el estado de una pieza de repuesto a una unidad sin asignar.

Antes de empezar

La pieza de repuesto debe estar en estado óptimo, en espera.

Acerca de esta tarea

No se puede anular la asignación de una pieza de repuesto que esté reemplazando a una unidad con error. Si la pieza de repuesto no está en estado óptimo, siga los procedimientos de Recovery Guru para corregir cualquier problema antes de intentar anular la asignación de la unidad.

Pasos

1. Seleccione **hardware**.
2. Si el gráfico muestra los controladores, haga clic en **Mostrar frente de la bandeja**.

   El gráfico cambia y muestra las unidades en lugar de las controladoras.

3. Seleccione la unidad de la pieza de repuesto (se muestra en rosa) para la cual desea anular la asignación.

   Si existen líneas diagonales en la bahía de unidad rosa, la pieza de repuesto se encuentra en uso y no puede anularse su asignación.

   Se abre el menú contextual de la unidad.

4. Desde la lista desplegable de la unidad, seleccione **Anular asignación de pieza de repuesto**.

   En el cuadro de diálogo, se muestran todos los grupos de volúmenes afectados. Para ello, es necesario quitar esta pieza de repuesto y si otras piezas de repuesto las protegen.

5. Confirme la operación de anulación de asignación.

Resultados

La unidad regresa al estado sin asignar (se muestra en gris).

Preguntas frecuentes sobre las bandejas

¿Qué son la protección contra pérdida de bandeja y la protección contra pérdida de cajón?

La protección contra pérdida de bandeja y de cajón son atributos de los pools y los grupos de volúmenes para mantener el acceso a los datos en caso de fallo de una bandeja o un cajón individuales.

Protección contra pérdida de bandeja

Una bandeja es el compartimento que contiene las unidades o las unidades y la controladora. La protección contra pérdida de bandeja garantiza la accesibilidad a los datos en los volúmenes de un pool o un grupo de volúmenes en caso de pérdida total de comunicación con una bandeja de unidades única. Un ejemplo de pérdida total de comunicación podría ser la pérdida de energía en la bandeja de unidades o el fallo de ambos módulos de I/o (IOM).

> La protección contra pérdida de bandeja no está garantizada si una unidad ya falló en el pool o en el grupo de volúmenes. En este caso, la pérdida de acceso a la bandeja de unidades y, en consecuencia, a otra unidad en el pool o el grupo de volúmenes provoca la pérdida de datos.

El criterio de protección contra pérdida de bandeja depende del método de protección, tal como se describe en la tabla siguiente:

Nivel	Criterios para la protección contra pérdida de bandeja	Cantidad mínima requerida de bandejas
Piscina	El pool debe incluir unidades de al menos cinco bandejas y debe haber la misma cantidad de unidades en cada bandeja. La protección contra pérdida de bandeja no es aplicable a las bandejas de gran capacidad; si el sistema incluye bandejas de gran capacidad, consulte la protección contra pérdida de cajón.	5
RAID 6	El grupo de volúmenes consta de dos unidades como máximo en una sola bandeja.	3
RAID 3 o RAID 5	Cada unidad del grupo de volúmenes se encuentra en una bandeja aparte.	3
RAID 1	Cada unidad de una pareja RAID 1 se debe ubicar en una bandeja aparte.	2
RAID 0	No puede contar con protección contra pérdida de bandeja.	No aplicable

Protección contra pérdida de cajón

Un cajón es uno de los compartimentos de una bandeja que se extrae para acceder a las unidades. Solo las bandejas de gran capacidad poseen cajones. La protección contra pérdida de cajón garantiza la accesibilidad a los datos en los volúmenes de un pool o un grupo de volúmenes en caso de pérdida total de comunicación con un cajón único. Un ejemplo de pérdida total de comunicación podría ser la pérdida de energía en el cajón o el fallo de un componente interno dentro del cajón.

> La protección contra pérdida de cajón no está garantizada si una unidad ya falló en el pool o en el grupo de volúmenes. En este caso, la pérdida de acceso al cajón (y, en consecuencia, a otra unidad en el pool o el grupo de volúmenes) provoca la pérdida de datos.

El criterio de protección contra pérdida de cajón depende del método de protección, tal como se describe en la tabla siguiente:

Nivel	Criterios para la protección contra pérdida de cajón	Cantidad mínima requerida de cajones
Piscina	Los candidatos de pool deben incluir unidades de todos los cajones y debe haber la misma cantidad de unidades por cajón. El pool debe incluir unidades de al menos cinco cajones y debe haber la misma cantidad de unidades por cajón. Una bandeja de 60 unidades puede contar con protección contra pérdida de cajón cuando el pool consta de 15, 20, 25, 30, 35, 40, 45, 50, 55 o 60 unidades. Los incrementos en múltiplos de 5 se pueden agregar al pool después de la creación inicial.	5
RAID 6	El grupo de volúmenes consta de dos unidades como máximo en un solo cajón.	3
RAID 3 o RAID 5	Cada unidad del grupo de volúmenes se encuentra en un cajón aparte.	3
RAID 1	Cada unidad de una pareja reflejada se debe ubicar en un cajón aparte.	2
RAID 0	No puede contar con protección contra pérdida de cajón.	No aplicable

¿Qué son los ciclos de aprendizaje de la batería?

Un ciclo de aprendizaje es un ciclo automático para calibrar el indicador de batería inteligente.

Un ciclo de aprendizaje consta de las siguientes fases:

- Descarga controlada de batería
- Periodo de descanso
- Carga

Las baterías se descargan hasta un umbral predeterminado. Durante esta fase, se calibra el indicador de batería.

Un ciclo de aprendizaje requiere los siguientes parámetros:

- Baterías totalmente cargadas
- Baterías que no estén sobrecalentadas

Los ciclos de aprendizaje para sistemas de controladoras dobles se ejecutan simultáneamente. Para controladoras que tienen alimentación de backup de varias baterías o conjuntos de celdas de batería, los ciclos de aprendizaje se ejecutan secuencialmente.

Los ciclos de aprendizaje se programan para comenzar automáticamente en intervalos regulares, a la misma hora y el mismo día de la semana. El intervalo entre los ciclos se describe en semanas.

Un ciclo de aprendizaje podría demorar varias horas para completarse.

Preguntas frecuentes de la controladora

¿Qué es la negociación automática?

La negociación automática es la capacidad de una interfaz de red para coordinar sus propios parámetros de conexión (velocidad y dúplex) con otra interfaz de red.

Por lo general, la negociación automática es el ajuste preferido para configurar los puertos de gestión; sin embargo, si la negociación falla, los ajustes de la interfaz de red que no coinciden pueden afectar significativamente el rendimiento de la red. En los casos en que esta condición sea inaceptable, debe configurar manualmente las opciones de la interfaz de red con los valores correctos. Los puertos de gestión Ethernet de la controladora son los encargados de realizar la negociación automática. Los adaptadores de bus de host iSCSI no son los encargados de realizar la negociación automática.

Si la negociación automática falla, la controladora intenta establecer una conexión con 10BASE-T, semidúplex, que es el denominador común más bajo.

¿Qué es la configuración automática de direcciones IPv6 sin estado?

Gracias a la configuración automática sin estado, los hosts no obtienen direcciones ni otra información de configuración desde un servidor.

La configuración automática sin estado en IPv6 cuenta con direcciones locales de enlace, multidifusión y protocolo de descubrimiento cercano (ND). La IPv6 puede generar un ID de interfaz de una dirección a partir de la dirección de capa de enlace de datos subyacente.

La configuración automática sin estado y la configuración automática con estado se complementan. Por ejemplo, el host puede utilizar la configuración automática sin estado para configurar sus propias direcciones, pero la configuración automática con estado para obtener otra información. Gracias a la configuración automática con estado, los hosts obtienen direcciones y otra información de configuración desde un servidor. El protocolo de Internet versión 6 (IPv6) también define un método por el cual todas las direcciones IP de una red pueden volver a numerarse de una vez. La IPv6 define un método para que los dispositivos en la red configuren automáticamente su dirección IP y otros parámetros sin la necesidad de un servidor.

Los dispositivos realizan estos pasos cuando utilizan la configuración automática sin estado:

1. **Generar una dirección local de enlace** — el dispositivo genera una dirección local de enlace, que tiene 10 bits, seguida de 54 ceros, y seguido del ID de interfaz de 64 bits.

2. **Pruebe la singularidad de una dirección de enlace local** — el nodo realiza pruebas para asegurarse de que la dirección de enlace local que genera no está ya en uso en la red local. El nodo envía un mensaje de solicitud de cercanía mediante el protocolo ND. En respuesta, la red local escucha un mensaje de anuncio de cercanía, que indica que otro dispositivo ya está usando la dirección de enlace local. Por lo tanto, debe crearse una dirección de enlace local nueva o fallará la configuración automática y deberá utilizarse otro método.
3. **Asignar una dirección de enlace local** — Si el dispositivo supera la prueba de singularidad, el dispositivo asigna la dirección de enlace local a su interfaz IP. La dirección de enlace local se puede utilizar para la comunicación en la red local, pero no en Internet.
4. **Póngase en contacto con el router** — el nodo intenta ponerse en contacto con un router local para obtener más información acerca de cómo continuar la configuración. Este contacto se realiza ya sea escuchando los mensajes de anuncio del enrutador que se envían periódicamente o enviando un mensaje de solicitud al enrutador específico para solicitarle información acerca de cómo continuar.
5. **Proporcionar dirección al nodo** — el router proporciona dirección al nodo acerca de cómo proceder con la configuración automática. Como alternativa, el enrutador le comunica al host cómo determinar la dirección global de Internet.
6. **Configurar la dirección global** — el host se configura con su dirección global única de Internet. Esta dirección por lo general se forma a partir de un prefijo de red que el enrutador proporciona al host.

¿Qué se debe elegir: DHCP o configuración manual?

El método predeterminado de la configuración de red es el protocolo de configuración dinámica de hosts (DHCP). Utilice siempre esta opción, a menos que la red no posea un servidor DHCP.

¿Qué es un servidor DHCP?

El protocolo de configuración dinámica de hosts (DHCP) es un protocolo que automatiza la tarea de asignar una dirección de protocolo de Internet (IP).

Cada dispositivo conectado a una red TCP/IP debe tener asignada una dirección IP única. Estos dispositivos incluyen las controladoras de la cabina de almacenamiento.

Sin DHCP, el administrador de red introduce estas direcciones IP manualmente. Con DHCP, cuando un cliente necesita iniciar operaciones TCP/IP, el cliente transmite una solicitud de información de la dirección. El servidor DHCP recibe la solicitud, asigna una dirección nueva por una cantidad de tiempo específica, que se denomina periodo de concesión, y envía esa dirección al cliente. Con DHCP, un dispositivo puede tener una dirección IP diferente cada vez que se conecta a la red. En algunos sistemas, la dirección IP del dispositivo puede cambiar incluso mientras el dispositivo todavía está conectado.

¿Cómo se configura el servidor DHCP?

Debe configurar un servidor de protocolo de configuración dinámica de hosts (DHCP) para utilizar direcciones de protocolo de Internet (IP) estáticas para las controladoras en la cabina de almacenamiento.

Las direcciones IP que asigna el servidor DHCP generalmente son dinámicas y pueden cambiar debido a que tienen un periodo de concesión que expira. Algunos dispositivos, como los servidores y los enrutadores, deben utilizar direcciones estáticas. Las controladoras en la cabina de almacenamiento también deben utilizar direcciones IP estáticas.

Para obtener información sobre la forma de asignar direcciones estáticas, consulte la documentación del servidor DHCP.

¿Por qué es necesario cambiar la configuración de red de la controladora?

Es necesario configurar la configuración de red para cada controladora—su dirección de protocolo de Internet (IP), máscara de subred y puerta de enlace- cuando se utiliza gestión fuera de banda.

Es posible ajustar la configuración de red a través del servidor de protocolo de configuración dinámica de hosts (DHCP). Si no utiliza un servidor DHCP, debe introducir la configuración de red de forma manual.

¿En dónde se puede obtener la configuración de red?

Es posible obtener del administrador de red la dirección de protocolo de Internet (IP), la máscara de subred y la información de puerta de enlace.

Esta información es necesaria para configurar los puertos de las controladoras.

¿Qué son las respuestas PING de ICMP?

El protocolo de mensajes de control de Internet (ICMP) es uno de los protocolos de la suite TCP/IP.

La `ICMP echo request` y la(`ICMP echo reply` los mensajes suelen denominarse `ping` mensajes. `Ping` es una herramienta para la solución de problemas que usan los administradores del sistema para probar manualmente la conectividad entre dispositivos de red, y también para probar la demora de la red y la pérdida de paquetes. La `ping` el comando envía un `ICMP echo request` a un dispositivo de la red y el dispositivo responde inmediatamente con un(`ICMP echo reply`. A veces, la política de seguridad de red de una empresa requiere `ping` (`ICMP echo reply`) se debe desactivar en todos los dispositivos para que sea más difícil de descubrir personas no autorizadas.

¿Cuándo se debe actualizar la configuración de puertos o el servidor iSNS en el servidor DHCP?

Actualice el servidor DHCP cada vez que se modifique o actualice el servidor y que haya cambiado la información DHCP relevante para la cabina de almacenamiento actual y la cabina de almacenamiento que desea utilizar.

Específicamente, actualice la configuración de puertos o el servidor iSNS desde el servidor DHCP cuando sepa que el servidor DHCP asignará direcciones diferentes.

> La actualización de la configuración de puertos destruye todas las conexiones iSCSI de ese puerto.

¿Qué debo hacer luego de configurar los puertos de gestión?

Si cambió la dirección IP de la cabina de almacenamiento, es posible que desee actualizar la vista de cabina global en Unified Manager.

Para actualizar la vista de cabina global en Unified Manager, abra la interfaz y vaya al menú:gestionar[detectar].

Si todavía utiliza Storage Manager de SANtricity, vaya a Enterprise Management Window (EMW), donde debe eliminar y volver a añadir la nueva dirección IP.

¿Por qué el sistema de almacenamiento se encuentra en el modo no óptimo?

Un sistema de almacenamiento en modo no óptimo se debe a un estado no válido de configuración del sistema. A pesar de este estado, se admite por completo el acceso de I/o normal a los volúmenes existentes; sin embargo, System Manager prohibirá algunas operaciones.

Un sistema de almacenamiento puede realizar una transición a la configuración del sistema no válida por uno de estos motivos:

- La controladora no cumple las normativas, posiblemente porque tiene un código de identificador de submodelo incorrecto (SMID) o superó el límite de funciones premium.
- Hay una operación de servicio interno en curso, como una descarga del firmware de la unidad.
- La controladora superó el umbral de error de paridad y entró en bloqueo.
- Se produjo una condición general de bloqueo.

Preguntas frecuentes sobre iSCSI

¿Qué sucede cuando utilizo un servidor iSNS para el registro?

Cuando se utiliza información del servidor de servicio de nombres de almacenamiento de Internet (iSNS), los hosts (iniciadores) pueden configurarse para consultar el servidor iSNS a fin de recuperar información del objetivo (controladoras).

Este registro proporciona al servidor iSNS la información del puerto y del nombre completo de iSCSI (IQN) de la controladora, y permite consultas entre los iniciadores (hosts iSCSI) y los objetivos (controladoras).

¿Qué métodos de registro se admiten automáticamente para iSCSI?

La implementación de iSCSI es compatible con el método de detección Servicio de nombres de almacenamiento de Internet (iSNS) o con el uso del comando Send Targets.

El método iSNS permite la detección iSNS entre los iniciadores (hosts iSCSI) y los objetivos (controladoras). La controladora objetivo se registra para proporcionar al servidor iSNS la información sobre el puerto y el nombre completo de iSCSI (IQN) de la controladora.

Si no se configura iSNS, el host iSCSI puede enviar el comando Send Targets durante una sesión de detección iSCSI. En respuesta, la controladora devuelve la información del puerto (por ejemplo, el IQN objetivo, la dirección IP del puerto, el puerto de escucha y el grupo de puertos de destino). Este método de detección no es necesario si utiliza iSNS, dado que el iniciador del host puede recuperar las IP objetivo del servidor iSNS.

¿Cómo se interpretan las estadísticas de Iser over InfiniBand?

El cuadro de diálogo Ver estadísticas de Iser over InfiniBand muestra las estadísticas de destino local (protocolo) y las estadísticas de la interfaz Iser over InfiniBand (IB). Todas las estadísticas son de solo lectura y no pueden configurarse.

- **Estadísticas de destino local (protocolo)** — proporciona estadísticas para el destino Iser over InfiniBand, que muestra el acceso de nivel de bloque a sus medios de almacenamiento.
- **Estadísticas de la interfaz Iser over InfiniBand** — proporciona estadísticas para todos los puertos Iser over InfiniBand en la interfaz InfiniBand, que incluye estadísticas de rendimiento e información de errores de enlace asociados con cada puerto del switch.

Es posible ver cada una de las estadísticas como estadísticas sin configurar o estadísticas de base. Las estadísticas sin configurar son todas las estadísticas recogidas desde que se iniciaron las controladoras. Las estadísticas de base son las estadísticas de un momento específico que se recogen desde el establecimiento de la hora de la línea de base.

¿Qué más debo hacer para configurar o diagnosticar Iser over InfiniBand?

En la tabla a continuación, se enumeran las funciones de System Manager que se pueden utilizar para configurar y gestionar sesiones Iser over InfiniBand.

> La configuración de Iser over InfiniBand solo está disponible si la controladora de la cabina de almacenamiento incluye un puerto de gestión de hosts Iser over InfiniBand.

Acción	Ubicación
Configure los puertos Iser over InfiniBand	1. Seleccione **hardware**. 2. Seleccione **Mostrar parte posterior de la bandeja**. 3. Seleccione una controladora. 4. Seleccione **Configurar puertos Iser over InfiniBand**. o. 1. Seleccione MENU:Settings[System]. 2. Desplácese hasta **Configuración de Iser over InfiniBand** y seleccione **Configurar puertos Iser over InfiniBand**.
Ver estadísticas de Iser over InfiniBand	1. Seleccione MENU:Settings[System]. 2. Desplácese hasta **Configuración de Iser over InfiniBand** y seleccione **Ver estadísticas de Iser over InfiniBand**.

¿Qué más debo hacer para configurar o diagnosticar iSCSI?

Se pueden realizar sesiones iSCSI con hosts o cabinas de almacenamiento remotas en una relación de reflejo asíncrono. En las tablas a continuación, se enumeran las funciones de System Manager que se pueden utilizar para configurar y gestionar estas sesiones iSCSI.

> La configuración de iSCSI solo se encuentra disponible si la cabina de almacenamiento es compatible con iSCSI.

Configure iSCSI

Acción	Ubicación
Gestionar configuración de iSCSI	1. Seleccione MENU:Settings[System]. 2. Desplácese hasta **Ajustes iSCSI** para ver todas las funciones de administración.
Configure los puertos iSCSI	1. Seleccione **hardware**. 2. Seleccione **Mostrar parte posterior de la bandeja**. 3. Seleccione una controladora. 4. Seleccione **Configurar puertos iSCSI**.
Establezca el secreto CHAP del host	1. Seleccione MENU:Settings[System]. 2. Desplácese hasta **Configuración de iSCSI** y seleccione **Configurar autenticación**. o. 1. Seleccione MENU:Storage[hosts]. 2. Seleccione un miembro del host. 3. Haga clic en menú:ficha Ver/editar configuración[puertos de host].

Diagnosticar iSCSI

Acción	Ubicación
Ver o finalizar sesiones iSCSI	1. Seleccione MENU:Settings[System]. 2. Desplácese hasta **Configuración iSCSI** y seleccione **Ver/finalizar sesiones iSCSI**. o. 1. Seleccione menú:ficha Soporte[Centro de soporte > Diagnóstico]. 2. Seleccione **Ver/finalizar sesiones iSCSI**.

Acción	Ubicación
Ver estadísticas de iSCSI	1. Seleccione MENU:Settings[System]. 2. Desplácese hasta **Configuración de iSCSI** y seleccione **Ver paquetes de estadísticas de iSCSI**. o. 1. Seleccione menú:ficha Soporte[Centro de soporte > Diagnóstico]. 2. Seleccione **Ver paquetes de estadísticas iSCSI**.

Preguntas frecuentes de NVMe

¿Cómo se interpretan las estadísticas de NVMe over Fabrics?

El cuadro de diálogo Ver estadísticas de NVMe over Fabrics muestra estadísticas para el subsistema NVMe y la interfaz RDMA. Todas las estadísticas son de solo lectura y no pueden configurarse.

- **Estadísticas del subsistema NVMe** — muestra estadísticas para la controladora NVMe y su cola. La controladora NVMe ofrece una ruta de acceso entre un host y los espacios de nombres en la cabina de almacenamiento. Es posible revisar las estadísticas del subsistema NVMe para consultar elementos, como errores de conexión, reinicios y apagados. Para obtener más información sobre estas estadísticas, haga clic en **Ver leyenda de encabezados de tabla**.
- **Estadísticas de la interfaz RDMA** — proporciona estadísticas para todos los puertos NVMe over Fabrics de la interfaz RDMA, que incluye estadísticas de rendimiento e información de errores de enlace asociados con cada puerto del switch. Esta pestaña solo se muestra cuando existen puertos NVMe over Fabrics disponibles. Para obtener más información sobre las estadísticas, haga clic en **Ver leyenda de encabezados de tabla**.

Es posible ver cada una de las estadísticas como estadísticas sin configurar o estadísticas de base. Las estadísticas sin configurar son todas las estadísticas recogidas desde que se iniciaron las controladoras. Las estadísticas de base son las estadísticas de un momento específico que se recogen desde el establecimiento de la hora de la línea de base.

¿Qué más debo hacer para configurar o diagnosticar NVMe over InfiniBand?

En la tabla a continuación, se enumeran las funciones de System Manager que se pueden utilizar para configurar y gestionar sesiones NVMe over InfiniBand.

> La configuración de NVMe over InfiniBand solo está disponible si la controladora de la cabina de almacenamiento incluye un puerto NVMe over InfiniBand.

Acción	Ubicación
Configure los puertos NVMe over InfiniBand	1. Seleccione **hardware**. 2. Seleccione **Mostrar parte posterior de la bandeja**. 3. Seleccione una controladora. 4. Seleccione **Configurar puertos NVMe over InfiniBand**. o. 1. Seleccione MENU:Settings[System]. 2. Desplácese hasta **Configuración de NVMe over InfiniBand** y seleccione **Configurar puertos NVMe over InfiniBand**.
Ver estadísticas de NVMe over InfiniBand	1. Seleccione MENU:Settings[System]. 2. Desplácese hasta **Configuración de NVMe over InfiniBand** y seleccione **Ver estadísticas de NVMe over Fabrics**.

¿Qué más debo hacer para configurar o diagnosticar NVMe over roce?

Es posible configurar y gestionar NVMe over roce desde las páginas hardware y Configuración.

> La configuración de NVMe over roce solo está disponible si la controladora de la cabina de almacenamiento incluye un puerto NVMe over roce.

Acción	Ubicación
Configure los puertos NVMe over roce	1. Seleccione **hardware**. 2. Seleccione **Mostrar parte posterior de la bandeja**. 3. Seleccione una controladora. 4. Seleccione **Configurar puertos NVMe over roce**. o. 1. Seleccione MENU:Settings[System]. 2. Desplácese hasta **Configuración de NVMe over roce** y seleccione **Configurar puertos NVMe over roce**.
Ver estadísticas de NVMe over Fabrics	1. Seleccione MENU:Settings[System]. 2. Desplácese hasta **Configuración de NVMe over roce** y seleccione **Ver estadísticas de NVMe over Fabrics**.

¿Por qué existen dos direcciones IP para un puerto físico?

La cabina de almacenamiento EF600 puede incluir dos HIC: Una externa y una interna.

En esta configuración, la HIC externa se encuentra conectada a una HIC interna auxiliar. Cada puerto físico al que se puede obtener acceso desde la HIC externa tiene un puerto virtual asociado desde la HIC interna.

Para alcanzar el rendimiento máximo de 200 GB, es necesario asignar una dirección IP exclusiva a los puertos físico y virtual para que el host pueda establecer conexiones a ambos. Si no se asigna una dirección IP al puerto virtual, la HIC se ejecutará a aproximadamente la mitad de su capacidad de velocidad.

¿Por qué existen dos conjuntos de parámetros para un puerto físico?

La cabina de almacenamiento EF600 puede incluir dos HIC: Una externa y una interna.

En esta configuración, la HIC externa se encuentra conectada a una HIC interna auxiliar. Cada puerto físico al que se puede obtener acceso desde la HIC externa tiene un puerto virtual asociado desde la HIC interna.

Para alcanzar el rendimiento máximo de 200 GB, es necesario asignar parámetros a los puertos físico y virtual para que el host pueda establecer conexiones a ambos. Si no se asignan parámetros al puerto virtual, la HIC se ejecutará a aproximadamente la mitad de su capacidad de velocidad.

Preguntas frecuentes de unidades

¿Qué es una unidad de repuesto?

Las piezas de repuesto actúan como unidades en espera en los grupos de volúmenes RAID 1, RAID 5 o RAID 6. Son unidades completamente funcionales que no contienen datos. Si se produce un error en una unidad del grupo de volúmenes, la controladora automáticamente reconstruye los datos de la unidad con error en una pieza de repuesto.

Si se produce un error en una unidad de la cabina de almacenamiento, la unidad de repuesto automáticamente sustituye a la unidad con error sin necesidad de realizar un cambio físico. Si la unidad de repuesto está disponible cuando se produce un error en una unidad, la controladora utiliza datos de redundancia para reconstruir los datos de la unidad con error en la unidad de repuesto.

Una unidad de repuesto no está dedicada a un grupo de volúmenes específico. Sino que se puede usar la unidad de repuesto en lugar de cualquier unidad con error de la cabina de almacenamiento con la misma capacidad o una menor. Una unidad de repuesto debe ser del mismo tipo de medio (HDD o SSD) que las unidades que protege.

> Las unidades de repuesto no son compatibles con los pools. En lugar de las unidades de repuesto, los pools utilizan la capacidad de conservación dentro de cada unidad que compone el pool.

¿Qué es la capacidad de conservación?

La capacidad de conservación es la cantidad de capacidad (cantidad de unidades) que se reserva en un pool para admitir fallos de unidad potenciales.

Cuando se crea un pool, el sistema reserva automáticamente una cantidad predeterminada de capacidad de conservación según el número de unidades del pool.

Los pools utilizan la capacidad de conservación durante la reconstrucción, mientras que los grupos de volúmenes utilizan unidades de pieza de repuesto con el mismo fin. El método de capacidad de conservación es una mejora con respecto a las unidades de pieza de repuesto, dado que permite realizar la reconstrucción

con mayor rapidez. La capacidad de conservación se distribuye en varias unidades del pool, en lugar de en una unidad como en el caso de la unidad de repuesto, por lo que la velocidad o disponibilidad de una unidad no representan una limitación.

¿Por qué debería reemplazar lógicamente una unidad?

Si se produce un error en una unidad o si desea reemplazarla por algún otro motivo y tiene una unidad sin asignar en la cabina de almacenamiento, puede reemplazar lógicamente la unidad con error por la unidad sin asignar. Si no tiene una unidad sin asignar, puede optar por reemplazar físicamente la unidad.

Los datos de la unidad original se copian o reconstruyen en la unidad de reemplazo.

¿Dónde se puede ver el estado de una unidad sujeta a reconstrucción?

Se puede ver el estado de reconstrucción de la unidad desde la consola Operaciones en curso.

En la página Inicio, haga clic en el enlace **Ver operaciones en curso** de la parte superior derecha.

Según la unidad, es posible que la reconstrucción completa demore bastante. Si se modificó la propiedad de un volumen, es posible que se realice la reconstrucción completa en lugar de la rápida.

Alertas

Información general sobre las alertas

Es posible configurar System Manager para que envíe alertas de cabina de almacenamiento por correo electrónico, capturas SNMP y mensajes de syslog.

¿Qué son las alertas?

Alerts notifica a los administradores sobre eventos importantes que se producen en la cabina de almacenamiento. Los eventos pueden incluir problemas como un fallo de batería, un componente que pasa de estado óptimo a sin conexión o errores de redundancia en la controladora. Se considera que todos los eventos críticos generan alertas, junto con algunos eventos informativos y de advertencia.

Obtenga más información:

- "¿Cómo funcionan las alertas"
- "Terminología de alertas"

¿Cómo se configuran las alertas?

Es posible configurar las alertas que se enviarán como mensaje a una o varias direcciones de correo electrónico, como una captura SNMP a un servidor SNMP, o como un mensaje a un servidor de syslog. La configuración de alertas está disponible en MENU:Settings[Alerts].

Obtenga más información:

- "Configurar servidores de correo y destinatarios para las alertas"

- "Configurar el servidor de syslog para las alertas"
- "Configurar las alertas SNMP"

Información relacionada

Más información sobre conceptos relacionados con las alertas:

- "Información general sobre el registro de eventos"
- "Marcas de tiempo incoherentes"

Conceptos

¿Cómo funcionan las alertas

Las alertas notifican a los administradores sobre eventos importantes que se producen en la cabina de almacenamiento. Las alertas se pueden enviar por correo electrónico, capturas SNMP y syslog.

El proceso de las alertas funciona de la siguiente manera:

1. Un administrador configura uno o varios de los siguientes métodos de alerta en System Manager:
   - **Correo electrónico** — los mensajes se envían a direcciones de correo electrónico.
   - **SNMP** — las capturas SNMP se envían a un servidor SNMP.
   - **Syslog** — los mensajes se envían a un servidor syslog.
2. Cuando el monitor de eventos de la cabina de almacenamiento detecta un problema, escribe información sobre ese problema en el registro de eventos (disponible en **Support › Event Log**). Por ejemplo, los problemas pueden incluir eventos como un fallo de la batería, un componente que pasa del estado óptimo a sin conexión, o bien errores de redundancia en la controladora.
3. Si el monitor de eventos determina que el evento genera alertas, envía una notificación con los métodos de alerta configurados (correo electrónico, SNMP o syslog). Se considera que todos los eventos críticos generan alertas, junto con algunos eventos informativos y de advertencia.

Configuración de alertas

Es posible configurar alertas en el asistente de configuración inicial (solo para alertas de correo electrónico) o en la página Alertas. Para comprobar la configuración actual, vaya a MENU:Settings[Alerts].

El icono Alertas muestra la configuración de las alertas, que puede ser una de las siguientes:

- No configurado.
- Configurado; se ha configurado al menos un método de alerta. Para determinar qué métodos de alertas están configurados, apunte el cursor al icono.

Información sobre alertas

Las alertas pueden incluir los siguientes tipos de información:

- Nombre de la cabina de almacenamiento.
- Tipo de error de evento relacionado con una entrada del registro de eventos.

- La fecha y la hora en que ocurrió el evento.
- Una breve descripción del evento.

Las alertas de syslog siguen el estándar de mensajería de RFC 5424.

Terminología de alertas

Conozca la forma en que los términos de alertas se aplican a su cabina de almacenamiento.

Componente	Descripción
Monitor de eventos	El monitor de eventos reside en la cabina de almacenamiento y se ejecuta como una tarea en segundo plano. Cuando el monitor de eventos detecta anomalías en la cabina de almacenamiento, escribe información acerca de los problemas en el registro de eventos. Los problemas pueden incluir eventos como un fallo de batería, un componente que pasa de estado óptimo a sin conexión o errores de redundancia en la controladora. Si el monitor de eventos determina que el evento genera alertas, envía una notificación con los métodos de alerta configurados (correo electrónico, SNMP o syslog). Se considera que todos los eventos críticos generan alertas, junto con algunos eventos informativos y de advertencia.
Servidor de correo	El servidor de correo se usa para enviar y recibir alertas de correo electrónico. El servidor utiliza un protocolo para la transferencia simple de correo electrónico (SMTP).
SNMP	El protocolo simple de gestión de redes (SNMP) es un protocolo estándar de Internet que se usa para gestionar y compartir información entre dispositivos en redes de IP.
Captura SNMP	Una captura SNMP es una notificación que se envía a un servidor SNMP. La captura tiene información acerca de problemas importantes en la cabina de almacenamiento.
Destino de capturas SNMP	El destino de una captura SNMP es la dirección IPv4 o IPv6 del servidor que ejecuta un servicio SNMP.
Nombre de comunidad	Un nombre de comunidad es una cadena que actúa como contraseña para el servidor de red en un entorno SNMP.
Archivo MIB	El archivo de base de datos de información de gestión (MIB) define los datos que se están supervisando y gestionando en la cabina de almacenamiento. Se debe copiar y compilar en el servidor mediante la aplicación de servicio SNMP. El archivo MIB está disponible en el software System Manager del sitio de soporte.
Variables MIB	Las variables de la base de datos de información de gestión (MIB) pueden mostrar valores, como el nombre de cabina de almacenamiento, la ubicación de la cabina y una persona de contacto, en respuesta a las solicitudes SNMP GetRequests.

Componente	Descripción
Syslog	Syslog es un protocolo que utilizan los dispositivos de red para enviar mensajes de eventos a un servidor de registro.
UDP	El protocolo de datagramas de usuario (UDP) es un protocolo de capa de transporte que especifica un número de puerto de origen y de destino en los encabezados de paquete.

Gestionar alertas por correo electrónico

Configurar servidores de correo y destinatarios para las alertas

Para configurar las alertas por correo electrónico, debe indicar una dirección de correo electrónico del servidor y las direcciones de correo electrónico de los destinatarios de las alertas. Está permitido introducir hasta 20 direcciones de correo electrónico.

Antes de empezar

- La dirección del servidor de correo debe estar disponible. La dirección puede ser IPv4 o IPv6, o bien un nombre de dominio completo.

  Para usar un nombre de dominio completo, debe configurar un servidor DNS en ambas controladoras. Es posible configurar un servidor DNS desde la página hardware.

- La dirección de correo electrónico que se usará como remitente de alertas debe estar disponible. Esta es la dirección que aparece en el campo "From" del mensaje de alerta. Es necesario contar con una dirección de remitente en el protocolo SMTP; sin esa dirección, se produce un error.
- Las direcciones de correo electrónico de los destinatarios de alertas deben estar disponibles. Por lo general, el destinatario tiene la dirección de un administrador de red o de almacenamiento. Es posible introducir hasta 20 direcciones de correo electrónico.

Acerca de esta tarea

En esta tarea, se describe cómo configurar el servidor de correo, introducir las direcciones de correo electrónico del remitente y de los destinatarios, y analizar todas las direcciones de correo electrónico introducidas desde la página Alertas.

Las alertas por correo electrónico también pueden configurarse en el asistente de configuración inicial.

Pasos

1. Seleccione MENU:Settings[Alerts].
2. Seleccione la ficha **correo electrónico**.

   Si aún no se configuró ningún servidor de correo, la pestaña correo electrónico muestra "Configure Mail Server".

3. Seleccione **Configurar el servidor de correo**.

   Se abre el cuadro de diálogo Configurar el servidor de correo.

4. Introduzca la información del servidor de correo y, a continuación, haga clic en **Guardar**.
   - **Dirección del servidor de correo** — Introduzca un nombre de dominio completo, una dirección IPv4 o una dirección IPv6 del servidor de correo.

     > Para usar un nombre de dominio completo, debe configurar un servidor DNS en ambas controladoras. Es posible configurar un servidor DNS desde la página hardware.

   - **Dirección del remitente de correo electrónico** — Introduzca una dirección de correo electrónico válida que se utilizará como remitente del correo electrónico. Esta dirección aparece en el campo "de" del mensaje de correo electrónico.
   - **Cifrado** — Si desea cifrar mensajes, seleccione **SMTPS** o **STARTTLS** para el tipo de cifrado y, a continuación, seleccione el número de puerto para los mensajes cifrados. De lo contrario, seleccione **Ninguno**.
   - **Nombre de usuario y contraseña** — Si es necesario, introduzca un nombre de usuario y una contraseña para la autenticación con el remitente saliente y el servidor de correo.
   - **Incluir información de contacto en el correo electrónico** — para incluir la información de contacto del remitente con el mensaje de alerta, seleccione esta opción e introduzca un nombre y un número de teléfono.

     Después de hacer clic en **Guardar**, las direcciones de correo electrónico aparecerán en la ficha correo electrónico de la página Alertas.

5. Seleccione **Añadir correos electrónicos**.

   Se abre el cuadro de diálogo Añadir correos electrónicos.

6. Introduzca una o más direcciones de correo electrónico para los destinatarios de alertas y, a continuación, haga clic en **Agregar**.

   Las direcciones de correo electrónico aparecerán en la página Alertas.

7. Si desea asegurarse de que las direcciones de correo electrónico son válidas, haga clic en **probar todos los correos electrónicos** para enviar mensajes de prueba a los destinatarios.

Resultados

Después de configurar las alertas por correo electrónico, el monitor de eventos envía mensajes de correo electrónico a los destinatarios especificados cada vez que se produce un evento que genera alertas.

Editar direcciones de correo electrónico para alertas

Es posible cambiar las direcciones de correo electrónico de los destinatarios que recibieron alertas por correo electrónico.

Antes de empezar

Las direcciones de correo electrónico que pretende editar deben estar definidas en la pestaña correo electrónico de la página Alertas.

Pasos

1. Seleccione MENU:Settings[Alerts].
2. Seleccione la ficha **correo electrónico**.

3. En la tabla **Dirección de correo electrónico**, seleccione la dirección que desea cambiar y, a continuación, haga clic en el icono **Edición** (lápiz) situado en el extremo derecho.

   La fila se convierte en un campo editable.

4. Introduzca una dirección nueva y, a continuación, haga clic en el icono **Guardar** (Marca de verificación).

   Si desea cancelar los cambios, seleccione el icono **Cancelar** (X).

Resultados

La pestaña correo electrónico de la página Alertas muestra las direcciones de correo electrónico actualizadas.

Añadir direcciones de correo electrónico para alertas

Es posible añadir hasta 20 destinatarios para alertas por correo electrónico.

Pasos

1. Seleccione MENU:Settings[Alerts].
2. Seleccione la ficha **correo electrónico**.
3. Seleccione **Añadir correos electrónicos**.

   Se abre el cuadro de diálogo Añadir correos electrónicos.

4. En el campo vacío, introduzca una nueva dirección de correo electrónico. Si desea agregar más de una dirección, seleccione **Agregar otro correo electrónico** para abrir otro campo.
5. Haga clic en **Agregar**.

Resultados

La pestaña correo electrónico de la página Alertas muestra las nuevas direcciones de correo electrónico.

Eliminar servidor de correo o direcciones de correo electrónico para las alertas

Es posible eliminar el servidor de correo definido previamente para que no se envíen alertas a las direcciones de correo electrónico, o eliminar direcciones de correo electrónico individuales.

Pasos

1. Seleccione MENU:Settings[Alerts].
2. Seleccione la ficha **correo electrónico**.
3. Desde la tabla, realice una de las siguientes acciones:
   - Para eliminar un servidor de correo de modo que no se envíen alertas a las direcciones de correo electrónico, seleccione la fila del servidor de correo.
   - Para eliminar una dirección de correo electrónico y no enviar alertas a esta dirección, seleccione la fila de la dirección de correo electrónico que desea eliminar. El botón **Eliminar** de la parte superior derecha de la tabla está disponible para su selección.
4. Haga clic en **Eliminar** y confirme la operación.

Editar servidor de correo para alertas

Es posible cambiar la dirección del servidor de correo y la dirección del remitente de correo utilizada para las alertas por correo electrónico.

Antes de empezar

La dirección del servidor de correo que desea cambiar debe estar disponible. La dirección puede ser IPv4 o IPv6, o bien un nombre de dominio completo.

> Para usar un nombre de dominio completo, debe configurar un servidor DNS en ambas controladoras. Es posible configurar un servidor DNS desde la página hardware.

Pasos

1. Seleccione MENU:Settings[Alerts].
2. Seleccione la ficha **correo electrónico**.
3. Seleccione **Configurar el servidor de correo**.

   Se abre el cuadro de diálogo Configurar el servidor de correo.

4. Edite la dirección del servidor de correo, la información del remitente y la información de contacto.
   - **Dirección del servidor de correo** — edite el nombre de dominio completo, la dirección IPv4 o la dirección IPv6 del servidor de correo.

     > Para usar un nombre de dominio completo, debe configurar un servidor DNS en ambas controladoras. Es posible configurar un servidor DNS desde la página hardware.

   - **Dirección del remitente de correo electrónico** — edite la dirección de correo electrónico que se utilizará como remitente del correo electrónico. Esta dirección aparece en el campo "de" del mensaje de correo electrónico.
   - **Incluir información de contacto en el correo electrónico** — para editar la información de contacto del remitente, seleccione esta opción y, a continuación, edite el nombre y el número de teléfono.
5. Haga clic en **Guardar**.

Gestionar alertas SNMP

Configurar las alertas SNMP

Para configurar alertas del protocolo simple de gestión de redes (SNMP) se debe identificar al menos un servidor en el que el monitor de eventos de la cabina de almacenamiento pueda enviar capturas SNMP. La configuración requiere un nombre de comunidad o nombre de usuario y una dirección IP para el servidor.

Antes de empezar

- Debe configurarse un servidor de red con una aplicación de servicio SNMP. Es necesario tener la dirección de red de este servidor (ya sea una dirección IPv4 o IPv6), de manera que el monitor de eventos pueda enviar mensajes de captura a esa dirección. Es posible usar más de un servidor (se permiten hasta 10 servidores).
- El archivo de base de datos de información de gestión (MIB) se copió y compiló en el servidor con la aplicación de servicio SNMP. Este archivo MIB define los datos que se están supervisando y gestionando.

Si no tiene el archivo MIB, puede obtenerlo en el sitio de soporte de NetApp:

- Vaya a. "Soporte de NetApp".
- Haga clic en la ficha **Descargas** y seleccione **Descargas**.
- Haga clic en **E-Series SANtricity OS Controller Software**.
- Seleccione **Descargar la última versión**.
- Inicie sesión.
- Acepte la declaración de precaución y el acuerdo de licencia.
- Desplácese hacia abajo hasta que vea el archivo MIB para el tipo de controladora y haga clic en el enlace para descargar el archivo.

Acerca de esta tarea

En esta tarea, se describe cómo identificar el servidor SNMP para el destino de capturas y, a continuación, poner a prueba la configuración.

Pasos

1. Seleccione MENU:Settings[Alerts].
2. Seleccione la ficha **SNMP**.

   En la primera configuración, la pestaña SNMP muestra "Configure Communities/Users".

3. Seleccione **Configurar comunidades/usuarios**.

   Se abre el cuadro de diálogo Seleccionar versión de SNMP.

4. Seleccione la versión SNMP para las alertas, ya sea **SNMPv2c** o **SNMPv3**.

   En función de lo que seleccione, se abrirá el cuadro de diálogo Configurar comunidades o el cuadro de diálogo Configurar usuarios SNMPv3.

5. Siga las instrucciones adecuadas para SNMPv2c (comunidades) o SNMPv3 (usuarios):
   - **SNMPv2c (comunidades)** — en el diálogo Configurar comunidades, introduzca una o más cadenas de comunidad para los servidores de red. Un nombre de comunidad es una cadena que identifica un conjunto conocido de estaciones de gestión y que normalmente lo crea un administrador de red. Está compuesto solo por caracteres ASCII que se pueden imprimir. Puede añadir hasta 256 comunidades. Cuando haya terminado, haga clic en **Guardar**.
   - **SNMPv3 (usuarios)** — en el cuadro de diálogo Configurar usuarios de SNMPv3, haga clic en **Agregar** e introduzca la siguiente información:
     - **Nombre de usuario** — Introduzca un nombre para identificar al usuario, que puede tener hasta 31 caracteres.
     - **ID del motor** — Seleccione el ID del motor, que se utiliza para generar claves de autenticación y cifrado para los mensajes, y debe ser único en el dominio administrativo. En la mayoría de los casos, debe seleccionar **local**. Si tiene una configuración no estándar, seleccione **personalizado**; aparece otro campo en el que debe introducir el ID de motor autorizado como una cadena hexadecimal, con un número par de caracteres de entre 10 y 32 caracteres de longitud.
     - **Credenciales de autenticación** — Seleccione un protocolo de autenticación que garantice la identidad de los usuarios. A continuación, introduzca una contraseña de autenticación, que es obligatoria cuando se defina el protocolo de autenticación o se modifique. La contraseña debe tener entre 8 y 128 caracteres.

- **Credenciales de privacidad** — Seleccione un protocolo de privacidad que se utiliza para cifrar el contenido de los mensajes. A continuación, introduzca una contraseña de privacidad, que es necesaria cuando se establece o cambia el protocolo de privacidad. La contraseña debe tener entre 8 y 128 caracteres. Cuando haya terminado, haga clic en **Agregar** y, a continuación, haga clic en **Cerrar**.

6. En la página Alertas con la ficha SNMP seleccionada, haga clic en **Añadir destinos de captura**.

   Se abre el cuadro de diálogo Añadir destinos de captura.

7. Introduzca uno o más destinos de captura, seleccione sus nombres de comunidad o de usuario asociados y, a continuación, haga clic en **Agregar**.
   - **Destino de captura** — Introduzca una dirección IPv4 o IPv6 del servidor que ejecuta un servicio SNMP.
   - **Nombre de comunidad o Nombre de usuario** — en el menú desplegable, seleccione el nombre de comunidad (SNMPv2c) o el nombre de usuario (SNMPv3) para este destino de captura. (Si ha definido sólo uno, el nombre ya aparecerá en este campo.)
   - **Enviar captura de fallo de autenticación** — Seleccione esta opción (la casilla de verificación) si desea alertar al destino de la captura cada vez que se rechace una solicitud SNMP debido a un nombre de comunidad o de usuario no reconocido. Después de hacer clic en **Agregar**, los destinos de captura y los nombres asociados aparecen en la ficha **SNMP** de la página **Alertas**.
8. Para asegurarse de que una captura es válida, seleccione un destino de captura de la tabla y, a continuación, haga clic en **probar destino de captura** para enviar una captura de prueba a la dirección configurada.

Resultados

El monitor de eventos envía capturas SNMP a los servidores cada vez que ocurre un evento que genera alertas.

Añadir destinos de capturas para alertas SNMP

Es posible añadir hasta 10 servidores para enviar capturas SNMP.

Antes de empezar

- El servidor de red que desea añadir debe estar configurado con una aplicación de servicio SNMP. Es necesario tener la dirección de red de este servidor (ya sea una dirección IPv4 o IPv6), de manera que el monitor de eventos pueda enviar mensajes de captura a esa dirección. Es posible usar más de un servidor (se permiten hasta 10 servidores).
- El archivo de base de datos de información de gestión (MIB) se copió y compiló en el servidor con la aplicación de servicio SNMP. Este archivo MIB define los datos que se están supervisando y gestionando.

  Si no tiene el archivo MIB, puede obtenerlo en el sitio de soporte de NetApp:

  - Vaya a. "Soporte de NetApp".
  - Haga clic en **Descargas** y, a continuación, seleccione **Descargas**.
  - Haga clic en **E-Series SANtricity OS Controller Software**.
  - Seleccione **Descargar la última versión**.
  - Inicie sesión.
  - Acepte la declaración de precaución y el acuerdo de licencia.

- Desplácese hacia abajo hasta que vea el archivo MIB para el tipo de controladora y haga clic en el enlace para descargar el archivo.

Pasos

1. Seleccione MENU:Settings[Alerts].
2. Seleccione la ficha **SNMP**.

   Los destinos de capturas definidos actualmente se muestran en la tabla.

3. Seleccione **Agregar destinos de captura**.

   Se abre el cuadro de diálogo Añadir destinos de captura.

4. Introduzca uno o más destinos de captura, seleccione sus nombres de comunidad o de usuario asociados y, a continuación, haga clic en **Agregar**.
   - **Destino de captura** — Introduzca una dirección IPv4 o IPv6 del servidor que ejecuta un servicio SNMP.
   - **Nombre de comunidad o Nombre de usuario** — en el menú desplegable, seleccione el nombre de comunidad (SNMPv2c) o el nombre de usuario (SNMPv3) para este destino de captura. (Si ha definido sólo uno, el nombre ya aparecerá en este campo.)
   - **Enviar captura de fallo de autenticación** — Seleccione esta opción (la casilla de verificación) si desea alertar al destino de la captura cada vez que se rechace una solicitud SNMP debido a un nombre de comunidad o de usuario no reconocido. Después de hacer clic en **Agregar**, los destinos de captura y los nombres de comunidad o de usuario asociados aparecen en la tabla.
5. Para asegurarse de que una captura es válida, seleccione un destino de captura de la tabla y, a continuación, haga clic en **probar destino de captura** para enviar una captura de prueba a la dirección configurada.

Resultados

El monitor de eventos envía capturas SNMP a los servidores cada vez que ocurre un evento que genera alertas.

Configure las variables MIB de SNMP

En el caso de las alertas SNMP, tiene la opción de configurar las variables de la base de datos de información de gestión (MIB) que se muestran en las excepciones SNMP. Estas variables pueden mostrar el nombre de la cabina de almacenamiento, su ubicación y una persona de contacto.

Antes de empezar

El archivo MIB debe copiarse y compilarse en el servidor con la aplicación de servicio SNMP.

Si no tiene un archivo MIB, puede obtenerlo del siguiente modo:

- Vaya a. "Soporte de NetApp".
- Haga clic en **Descargas** y, a continuación, seleccione **Descargas**.
- Haga clic en **E-Series SANtricity OS Controller Software**.
- Seleccione **Descargar la última versión**.
- Inicie sesión.

- Acepte la declaración de precaución y el acuerdo de licencia.
- Desplácese hacia abajo hasta que vea el archivo MIB para el tipo de controladora y haga clic en el enlace para descargar el archivo.

Acerca de esta tarea

En esta tarea, se describe cómo definir variables MIB para excepciones SNMP. Estas variables pueden mostrar los siguientes valores, en respuesta a los mensajes GetRequests de SNMP:

- `sysName` (nombre para la cabina de almacenamiento)
- `sysLocation` (ubicación de la cabina de almacenamiento)
- `sysContact` (nombre de un administrador)

Pasos

1. Seleccione MENU:Settings[Alerts].
2. Seleccione la ficha **SNMP**.
3. Seleccione **Configurar variables MIB de SNMP**.

   Se muestra el cuadro de diálogo Configurar variables MIB de SNMP.

4. Introduzca uno o más de los siguientes valores y, a continuación, haga clic en **Guardar**.
   - **Nombre** — el valor de la variable MIB `sysName`. Por ejemplo, introduzca un nombre para la cabina de almacenamiento.
   - **Ubicación** — el valor de la variable MIB `sysLocation`. Por ejemplo, introduzca la ubicación de la cabina de almacenamiento.
   - **Contacto** — el valor de la variable MIB `sysContact`. Por ejemplo, introduzca un administrador que sea responsable de la cabina de almacenamiento.

Resultados

Estos valores se muestran en los mensajes de captura SNMP en las alertas de la cabina de almacenamiento.

Editar comunidades para capturas SNMPv2c

Puede editar nombres de comunidad para capturas SNMPv2c.

Antes de empezar

Se debe crear un nombre de comunidad.

Pasos

1. Seleccione MENU:Setting[Alerts].
2. Seleccione la ficha **SNMP**.

   Los destinos de capturas y los nombres de comunidad aparecen en la tabla.

3. Seleccione **Configurar comunidades**.
4. Introduzca el nuevo nombre de comunidad y haga clic en **Guardar**. Los nombres de comunidades deben consistir únicamente en caracteres ASCII imprimibles.

Resultados

La pestaña SNMP de la página Alertas muestra el nombre actualizado de la comunidad.

Edite la configuración de usuario de las capturas SNMPv3

Puede editar definiciones de usuario para solapamientos SNMPv3.

Antes de empezar

Se debe crear un usuario para la captura SNMPv3.

Pasos

1. Seleccione MENU:Settings[Alerts].
2. Seleccione la ficha **SNMP**.

   Los destinos de capturas y los nombres de usuario aparecen en la tabla.

3. Para editar una definición de usuario, seleccione el usuario en la tabla y, a continuación, haga clic en **Configurar usuarios**.
4. En el cuadro de diálogo, haga clic en **Ver/editar configuración**.
5. Edite la siguiente información:
   - **Nombre de usuario** — cambie el nombre que identifica al usuario, que puede tener hasta 31 caracteres.
   - **ID del motor** — Seleccione el ID del motor, que se utiliza para generar claves de autenticación y cifrado para los mensajes, y debe ser único en el dominio administrativo. En la mayoría de los casos, debe seleccionar **local**. Si tiene una configuración no estándar, seleccione **personalizado**; aparece otro campo en el que debe introducir el ID de motor autorizado como una cadena hexadecimal, con un número par de caracteres de entre 10 y 32 caracteres de longitud.
   - **Credenciales de autenticación** — Seleccione un protocolo de autenticación que garantice la identidad de los usuarios. A continuación, introduzca una contraseña de autenticación, que es obligatoria cuando se defina el protocolo de autenticación o se modifique. La contraseña debe tener entre 8 y 128 caracteres.
   - **Credenciales de privacidad** — Seleccione un protocolo de privacidad que se utiliza para cifrar el contenido de los mensajes. A continuación, introduzca una contraseña de privacidad, que es necesaria cuando se establece o cambia el protocolo de privacidad. La contraseña debe tener entre 8 y 128 caracteres.

Resultados

La pestaña SNMP de la página Alertas muestra la configuración actualizada.

Añada comunidades para las trampas SNMPv2c

Puede agregar hasta 256 nombres de comunidad para las trampas SNMPv2c.

Pasos

1. Seleccione MENU:Settings[Alerts].
2. Seleccione la ficha **SNMP**.

   Los destinos de capturas y los nombres de comunidad aparecen en la tabla.

3. Seleccione **Configurar comunidades**.

Se abre el cuadro de diálogo Configurar comunidades.

4. Seleccione **Añadir otra comunidad**.
5. Introduzca el nuevo nombre de comunidad y haga clic en **Guardar**.

Resultados

El nuevo nombre de la comunidad se muestra en la pestaña SNMP de la página Alertas.

Agregue usuarios para capturas SNMPv3

Puede agregar hasta 256 usuarios para capturas SNMPv3.

Pasos

1. Seleccione MENU:Settings[Alerts].
2. Seleccione la ficha **SNMP**.

   Los destinos de capturas y los nombres de usuario aparecen en la tabla.

3. Seleccione **Configurar usuarios**.

   Se abre el cuadro de diálogo Configurar usuarios de SNMPv3.

4. Seleccione **Agregar**.
5. Introduzca la siguiente información y, a continuación, haga clic en **Agregar**.
   - **Nombre de usuario** — Introduzca un nombre para identificar al usuario, que puede tener hasta 31 caracteres.
   - **ID del motor** — Seleccione el ID del motor, que se utiliza para generar claves de autenticación y cifrado para los mensajes, y debe ser único en el dominio administrativo. En la mayoría de los casos, debe seleccionar **local**. Si tiene una configuración no estándar, seleccione **personalizado**; aparece otro campo en el que debe introducir el ID de motor autorizado como una cadena hexadecimal, con un número par de caracteres de entre 10 y 32 caracteres de longitud.
   - **Credenciales de autenticación** — Seleccione un protocolo de autenticación que garantice la identidad de los usuarios. A continuación, introduzca una contraseña de autenticación, que es obligatoria cuando se defina el protocolo de autenticación o se modifique. La contraseña debe tener entre 8 y 128 caracteres.
   - **Credenciales de privacidad** — Seleccione un protocolo de privacidad que se utiliza para cifrar el contenido de los mensajes. A continuación, introduzca una contraseña de privacidad, que es necesaria cuando se establece o cambia el protocolo de privacidad. La contraseña debe tener entre 8 y 128 caracteres.

Quitar comunidades de las trampas SNMPv2c

Puede eliminar un nombre de comunidad de las trampas SNMPv2c.

Pasos

1. Seleccione MENU:Settings[Alerts].
2. Seleccione la ficha **SNMP**.

   Los destinos de captura y los nombres de comunidad aparecen en la página **Alertas**.

3. Seleccione **Configurar comunidades**.

   Se abre el cuadro de diálogo Configurar comunidades.

4. Seleccione el nombre de comunidad que desea eliminar y, a continuación, haga clic en el icono **Quitar** (X) situado en el extremo derecho.

   Si existen destinos de captura asociados con este nombre de comunidad, el cuadro de diálogo Confirmar eliminación de comunidad muestra las direcciones de los destinos de captura afectados.

5. Confirme la operación y haga clic en **Quitar**.

Resultados

El nombre de comunidad y el destino de captura asociado se eliminan de la página Alertas.

Eliminar usuarios para solapamientos SNMPv3

Puede eliminar un usuario para capturas SNMPv3.

Pasos

1. Seleccione MENU:Settings[Alerts].
2. Seleccione la ficha **SNMP**.

   Los nombres de usuario y los destinos de captura se muestran en la página Alertas.

3. Seleccione **Configurar usuarios**.

   Se abre el cuadro de diálogo Configurar usuarios de SNMPv3.

4. Seleccione el nombre de usuario que desea eliminar y, a continuación, haga clic en **Eliminar**.
5. Confirme la operación y haga clic en **Eliminar**.

Resultados

El nombre de usuario y el destino de captura asociado se eliminan de la página Alertas.

Eliminar destinos de capturas

Es posible eliminar una dirección de destino de captura para que el monitor de eventos de la cabina de almacenamiento ya no envíe capturas SNMP a esa dirección.

Pasos

1. Seleccione MENU:Settings[Alerts].
2. Seleccione la ficha **SNMP**.

   Las direcciones de los destinos de captura se muestran en la tabla.

3. Seleccione un destino de captura y, a continuación, haga clic en **Eliminar** en la esquina superior derecha de la página.
4. Confirme la operación y haga clic en **Eliminar**.

   La dirección de destino ya no aparece en la página Alertas.

Resultados

El destino de captura eliminado ya no recibe capturas SNMP del monitor de eventos de la cabina de almacenamiento.

Gestionar alertas de syslog

Configurar el servidor de syslog para las alertas

Para configurar alertas de syslog, debe introducir una dirección de servidor de syslog y un puerto UDP. Se permiten hasta cinco servidores de syslog.

Antes de empezar

- Debe estar disponible la dirección del servidor de syslog. La dirección debe ser un nombre de dominio completo o una dirección IPv4 o IPv6.
- El número de puerto UDP del servidor de syslog debe estar disponible. Por lo general, se trata del puerto 514.

Acerca de esta tarea

En esta tarea, se describe cómo introducir la dirección y el puerto de un servidor de syslog, y después probar la dirección introducida.

Pasos

1. Seleccione MENU:Settings[Alerts].
2. Seleccione la ficha **Syslog**.

   Si aún no hay ningún servidor de syslog definido, la página Alertas muestra "Add Syslog Servers".

3. Haga clic en **Agregar servidores de syslog**.

   Se abre el cuadro de diálogo Añadir servidor de syslog.

4. Introduzca información para uno o más servidores de syslog (hasta un máximo de cinco) y, a continuación, haga clic en **Agregar**.
   - **Dirección del servidor** — Introduzca un nombre de dominio completo, una dirección IPv4 o una dirección IPv6.
   - **Puerto UDP** — por lo general, el puerto UDP para syslog es 514. En la tabla, se presentan los servidores de syslog configurados.
5. Para enviar una alerta de prueba a las direcciones del servidor, seleccione **probar todos los servidores de syslog**.

Resultados

El monitor de eventos envía alertas al servidor de syslog cada vez que ocurre un evento que genera alertas. Para seguir configurando los ajustes de syslog para los registros de auditoría, consulte "Configurar servidores de syslog para registros de auditoría".

Edite los servidores de syslog para las alertas

Es posible editar la dirección de servidor utilizada para recibir alertas de syslog.

Pasos

1. Seleccione MENU:Settings[Alerts].
2. Seleccione la ficha **Syslog**.
3. En la tabla, seleccione una dirección de servidor de syslog y, a continuación, haga clic en el icono **Editar** (lápiz) situado en el extremo derecho.

   La fila se convierte en un campo editable.

4. Edite la dirección de servidor y el número de puerto UDP y, a continuación, haga clic en el icono **Guardar** (Marca de verificación).

Resultados

La dirección actualizada del servidor se muestra en la tabla.

Añada servidores de syslog para alertas

Es posible añadir un máximo de cinco servidores para las alertas de syslog.

Antes de empezar

- Debe estar disponible la dirección del servidor de syslog. La dirección debe ser un nombre de dominio completo o una dirección IPv4 o IPv6.
- Debe estar disponible el número de puerto UDP del servidor de syslog. Por lo general, se trata del puerto 514.

Pasos

1. Seleccione MENU:Settings[Alerts].
2. Seleccione la ficha **Syslog**.
3. Seleccione **Agregar servidores de syslog**.

   Se abre el cuadro de diálogo Añadir servidor de syslog.

4. Seleccione **Añadir otro servidor de syslog**.
5. Introduzca información para el servidor syslog y, a continuación, haga clic en **Agregar**.
   - **Dirección del servidor Syslog** — Introduzca un nombre de dominio completo, una dirección IPv4 o una dirección IPv6.
   - **Puerto UDP** — por lo general, el puerto UDP para syslog es 514.

   Es posible configurar hasta cinco servidores de syslog.

Resultados

Las direcciones del servidor de syslog aparecen en la tabla.

Elimine los servidores de syslog para las alertas

Es posible eliminar un servidor de syslog para que no siga recibiendo alertas.

Pasos

1. Seleccione MENU:Settings[Alerts].
2. Seleccione la ficha **Syslog**.

3. Seleccione una dirección de servidor de syslog y haga clic en **Quitar** en la parte superior derecha.

   Se abrirá el cuadro de diálogo Confirmar eliminación de servidor de syslog.

4. Confirme la operación y haga clic en **Eliminar**.

Resultados

El servidor que ha eliminado ya no recibe alertas del monitor de eventos.

Preguntas frecuentes

¿Qué sucede si se deshabilitan las alertas?

Si desea que los administradores reciban notificaciones sobre eventos importantes que suceden en la cabina de almacenamiento, se debe configurar un método de alerta.

Para las cabinas de almacenamiento gestionadas con SANtricity System Manager, es posible configurar alertas desde la página Alertas. Las notificaciones de alerta se pueden enviar por correo electrónico, capturas SNMP o mensajes de syslog. Además, las alertas por correo electrónico pueden configurarse desde el asistente de configuración inicial.

¿Cómo se configuran las alertas de SNMP o syslog?

Además de las alertas por correo electrónico, es posible configurar el envío de alertas mediante capturas de protocolo simple de gestión de redes (SNMP) o mensajes de syslog.

Para configurar las alertas de SNMP o syslog, vaya a MENU:Configuración[Alertas].

¿Por qué las marcas de tiempo no son consistentes entre la cabina y las alertas?

Cuando la cabina de almacenamiento envía alertas, no corrige la zona horaria según el host o servidor de destino que recibe las alertas. En cambio, la cabina de almacenamiento utiliza la hora local (GMT) para crear la Marca de tiempo que se utiliza para el registro de alertas. Como resultado, es posible que se observen inconsistencias entre las marcas de tiempo de la cabina de almacenamiento y el servidor o host que recibe una alerta.

Debido a que la cabina de almacenamiento no corrige la zona horaria cuando envía alertas, la Marca de tiempo de las alertas está en horario GMT, que tiene un valor cero de desfase de zona horaria. Para calcular una Marca de tiempo adecuada para su zona horaria local, debe determinar el desfase de su zona horaria respecto a GMT y sumar o restar ese valor a las marcas de tiempo.

Configuración de cabina

Información general de la configuración

Puede configurar System Manager para algunas opciones de cabina generales y funciones complementarias.

¿Qué ajustes puedo configurar?

La configuración de cabina incluye:

- "Rendimiento y configuración de la caché"
- "Equilibrio de carga automático"
- "Funciones complementarias"
- "Impulse la seguridad"

Tareas relacionadas

Obtenga más información acerca de las tareas relacionadas con la configuración del sistema:

- "Descargar la interfaz de línea de comandos (CLI)"
- "Cree una clave de seguridad interna"
- "Cree una clave de seguridad externa"
- "Configure los puertos iSCSI"
- "Configure los puertos NVME over IB"
- "Configure los puertos NVMe over roce"

Conceptos

Rendimiento y configuración de la caché

La memoria caché es un área de almacenamiento volátil temporal en la controladora que tiene un tiempo de acceso menor que los medios con unidades.

Con el almacenamiento en caché, es posible aumentar el rendimiento de I/o de la siguiente manera:

- Los datos solicitados desde el host para una lectura pueden estar ya en la caché debido a una operación anterior. Esto elimina la necesidad de acceder a la unidad.
- Los datos de escritura se escriben primero en la caché. Esto permite que la aplicación avance sin esperar que los datos se escriban en la unidad.

La configuración predeterminada de la caché cumple con los requisitos de la mayoría de los entornos, pero es posible modificarla si es necesario.

Configuración de la caché de la cabina de almacenamiento

Es posible especificar los siguientes valores en la página sistema para todos los volúmenes de la cabina de almacenamiento:

- **Iniciar valor para vaciar** — el porcentaje de datos no escritos en la caché que activan un vaciado de caché (escribir en disco). Cuando la caché alberga el porcentaje de inicio especificado de datos sin escribir, se activa un vaciado. De forma predeterminada, la controladora inicia el vaciado de la caché cuando la caché se encuentra un 80 % llena.
- **Tamaño de bloque de caché** — el tamaño máximo de cada bloque de caché, que es una unidad organizativa para la administración de caché. De forma predeterminada, el tamaño de bloque de caché es 8 KiB, pero se puede establecer en 4, 8, 16 o 32 KiB. Lo ideal es establecer el tamaño de bloque de caché

en el tamaño de I/o predominante de las aplicaciones. Por lo general, los sistemas de archivos o las aplicaciones de bases de datos utilizan tamaños menores. Se recomiendan tamaños mayores para las aplicaciones de grandes transferencias de datos o I/o secuenciales

Configuración de la caché del volumen

Es posible especificar los siguientes valores en la página volúmenes para volúmenes individuales de la cabina de almacenamiento (menú:almacenamiento[volúmenes]):

- **Caché de lectura** — la caché de lectura es un búfer que almacena datos que se han leído desde las unidades. Es posible que los datos de una operación de lectura ya deban estar en la caché debido a una operación anterior, por lo tanto, no es necesario acceder a las unidades. Los datos se conservan en la caché de lectura hasta que esta se vacía.
  - **Captura previa de caché de lectura dinámica**: La captura previa de lectura de caché dinámica permite a la controladora copiar otros bloques de datos secuenciales en la caché mientras lee bloques de datos de una unidad en la caché. Ese almacenamiento en caché aumenta la posibilidad de que se puedan cumplir futuras solicitudes de datos de la caché. La captura previa de lectura de la caché dinámica es importante para las aplicaciones multimedia que utilizan I/o secuencial La cantidad y la velocidad de las capturas previas de los datos en la caché se ajustan automáticamente según la velocidad y el tamaño de solicitud de las lecturas del host. El acceso aleatorio no provoca la captura previa de los datos en la caché. Esta función no se aplica cuando el almacenamiento en caché de lectura está deshabilitado.
- **Almacenamiento en caché de escritura** — la caché de escritura es un búfer que almacena datos del host que todavía no se han escrito en las unidades. Los datos permanecen en la caché de escritura hasta que se escriben en las unidades. El almacenamiento en caché de escritura puede aumentar el rendimiento de I/O.

> **Posible pérdida de datos** — Si activa la opción **almacenamiento en caché de escritura sin baterías** y no dispone de una fuente de alimentación universal de protección, podría perder datos. Además, puede perder datos si no tiene baterías de controlador y activa la opción **almacenamiento en caché de escritura sin baterías**.

  - **Almacenamiento en caché de escritura sin baterías** — la configuración de almacenamiento en caché de escritura sin baterías permite que el almacenamiento en caché de escritura continúe incluso cuando las baterías faltan, fallan, están completamente descargadas o no están totalmente cargadas. Por lo general, no se recomienda elegir el almacenamiento en caché de escritura sin baterías porque se pueden perder los datos en caso de interrupción del suministro eléctrico. Comúnmente, la controladora desactiva en forma temporal el almacenamiento en caché de escritura hasta que se cargan las baterías o se reemplaza una batería con errores.
  - **Almacenamiento en caché de escritura con duplicación** — el almacenamiento en caché de escritura con duplicación se produce cuando los datos escritos en la memoria caché de un controlador también se escriben en la memoria caché del otro controlador. Por lo tanto, si una controladora falla, la otra puede completar todas las operaciones de escritura pendientes. El mirroring de la caché de escritura está disponible solo si el almacenamiento en caché de escritura está habilitado y existen dos controladoras. El almacenamiento en caché de escritura con mirroring es la configuración predeterminada cuando se crea un volumen.

Información general sobre equilibrio de carga automático

La función Automatic Load Balancing ofrece una gestión de recursos de I/o mejorada, ya que reacciona dinámicamente a los cambios de carga con el tiempo y ajusta automáticamente la propiedad de la controladora de volumen para corregir cualquier

problema de desequilibrio de carga cuando las cargas de trabajo son distintas de una controladora a otra.

La carga de trabajo de cada controladora se supervisa continuamente y, con la colaboración de los controladores multivía instalados en los hosts, es posible establecer automáticamente el equilibrio cada vez que sea necesario. Una vez que la carga de trabajo se vuelve a equilibrar de forma automática en todas las controladoras, el administrador de almacenamiento queda liberado de la carga que supone ajustar manualmente la propiedad de la controladora de volumen para admitir cambios de carga en la cabina de almacenamiento.

Cuando la función Automatic Load Balancing está habilitada, ejecuta las siguientes funciones:

- Supervisa y equilibra automáticamente la utilización de recursos de la controladora.
- Ajusta automáticamente la propiedad de la controladora de volumen cuando es necesario y así, optimiza el ancho de banda de I/o entre los hosts y la cabina de almacenamiento.

Habilitar y deshabilitar Automatic Load Balancing

La función Automatic Load Balancing está habilitada de forma predeterminada en todas las cabinas de almacenamiento.

Puede ser conveniente deshabilitar Automatic Load Balancing en la cabina de almacenamiento por las siguientes razones:

- No se desea cambiar automáticamente la propiedad de una controladora de volumen para equilibrar la carga de trabajo.
- Se trabaja en un entorno altamente optimizado donde la distribución de carga se configura intencionalmente para lograr una distribución específica entre las controladoras.

Los tipos de hosts compatibles con la función Automatic Load Balancing

Aunque la función Automatic Load Balancing está habilitada en el nivel de la cabina de almacenamiento, el tipo de host que se selecciona para un host o clúster de hosts tiene una influencia directa sobre la forma en que opera la función.

Cuando se equilibra la carga de trabajo de la cabina de almacenamiento en varias controladoras, la función Automatic Load Balancing intenta mover volúmenes a los que pueden acceder ambas controladoras y que solo se asignan a un host o clúster de hosts compatible con la función Automatic Load Balancing.

Este comportamiento evita que un host pierda acceso a un volumen debido al proceso de equilibrio de carga; sin embargo, la presencia de volúmenes asignados a hosts no compatibles con Automatic Load Balancing afecta a la capacidad para equilibrar la carga de trabajo que posee la cabina de almacenamiento. Para que Automatic Load Balancing equilibre la carga de trabajo, el controlador multivía debe ser compatible con TPGS, y debe incluirse el tipo de host en la siguiente tabla.

> Para que un clúster de hosts se considere compatible con Automatic Load Balancing, todos los hosts de ese grupo deben ser compatibles con Automatic Load Balancing.

Tipo de host compatible con Automatic Load Balancing	Con este controlador multivía
Windows o Windows almacenado en clúster	MPIO con DSM E-Series de NetApp

Tipo de host compatible con Automatic Load Balancing	Con este controlador multivía
Linux DM-MP (Kernel 3.10 o posterior)	DM-MP con `scsi_dh_alua` controlador de dispositivos
VMware	Complemento nativo multivía (NMP) con `VMW_SATP_ALUA Storage Array Type` plugin

> Salvo excepciones menores, los tipos de hosts no compatibles con Automatic Load Balancing siguen funcionando normalmente más allá de que la función esté habilitada o no. Una excepción es cuando un sistema conmuta al nodo de respaldo y las cabinas de almacenamiento mueven volúmenes sin asignar nuevamente a la controladora a la que pertenecen cuando la ruta de datos regresa. No se mueve ninguno de los volúmenes asignados a hosts no compatibles con Automatic Load Balancing.

Consulte "Herramienta de matriz de interoperabilidad" Para acceder a información de compatibilidad para controladores multivía específicos, nivel de sistema operativo y compatibilidad con soportes de controladoras-unidades.

Comprobación de la compatibilidad del sistema operativo con la función Automatic Load Balancing

Compruebe la compatibilidad del sistema operativo con la función Automatic Load Balancing antes de configurar un sistema nuevo o migrar uno existente.

1. Vaya a la "Herramienta de matriz de interoperabilidad" para encontrar la solución y verificar la compatibilidad.

   Si el sistema operativo es Red Hat Enterprise Linux 6 o SUSE Linux Enterprise Server 11, póngase en contacto con el servicio de asistencia técnica.

2. Actualice y configure el `/etc/multipath.conf file`.
3. Asegúrese de que ambos `retain_attached_device_handler` y.. `detect_prio` se establecen en `yes` para el proveedor y el producto correspondientes, o utilice la configuración predeterminada.

Configure las opciones de cabina

Edite el nombre de la cabina de almacenamiento

Es posible cambiar el nombre de la cabina de almacenamiento que aparece en la barra de título de SANtricity System Manager.

Pasos

1. Seleccione MENU:Settings[System].
2. En **General**, busque el campo **Nombre:**.

   Si no se definió un nombre de cabina de almacenamiento, este campo muestra el texto "Unknown".

3. Haga clic en el icono **Editar** (lápiz) ubicado junto al nombre de la cabina de almacenamiento.

   Ahora el campo puede editarse.

4. Introduzca un nombre nuevo.

   Un nombre puede contener letras, números y los caracteres especiales subrayado (_), guión (-) y signo numeral (#). Un nombre no puede contener espacios. Un nombre puede contener un máximo de 30 caracteres. El nombre debe ser único.

5. Haga clic en el icono **Guardar** (Marca de verificación).

   Si desea cerrar el campo editable sin realizar cambios, haga clic en el icono **Cancelar** (X).

Resultados

El nuevo nombre aparecerá en la barra de título de SANtricity System Manager.

Encender luces de localización en cabina de almacenamiento

Para encontrar la ubicación física de una cabina de almacenamiento en un armario, se pueden encender las luces (LED) localizadoras.

Pasos

1. Seleccione MENU:Settings[System].
2. En **General**, haga clic en **encender las luces localizadoras de la matriz de almacenamiento**.

   Se abre el cuadro de diálogo encender las luces localizadoras de la cabina de almacenamiento y se encienden las luces localizadoras de la cabina de almacenamiento correspondiente.

3. Cuando haya localizado físicamente la cabina de almacenamiento, regrese al cuadro de diálogo y seleccione **Apagar**.

Resultados

Las luces localizadoras se apagan y el cuadro de diálogo se cierra.

Sincronice los relojes de la cabina de almacenamiento

Si el protocolo de tiempo de redes (NTP) no está habilitado, los relojes de las controladoras se pueden configurar manualmente, de manera que queden sincronizados con el cliente de gestión (el sistema que se utiliza para ejecutar el explorador que accede a System Manager).

Acerca de esta tarea

La sincronización garantiza que las marcas de tiempo del evento del registro de eventos coincidan con las marcas de tiempo escritas en los archivos de registro del host. Durante el proceso de sincronización, las controladoras siguen estando disponibles y siguen siendo operativas.

Si la opción NTP se encuentra habilitada en System Manager, no se debe usar esta opción para sincronizar los relojes. En cambio, NTP sincroniza automáticamente los relojes con un host externo que utiliza el protocolo de tiempo de redes simple (SNTP).

> Una vez que se realiza la sincronización, se puede observar que las estadísticas de rendimiento se pierden o se alteran, las programaciones se ven afectadas (ASUP, snapshots, etc.) y las marcas de tiempo de los datos de registro se alteran. Para evitar este problema, se puede usar NTP.

Pasos

1. Seleccione MENU:Settings[System].
2. En **General**, haga clic en **Sincronizar relojes de cabinas de almacenamiento**.

   Se abre el cuadro de diálogo Sincronizar relojes de cabinas de almacenamiento. Muestra la fecha y hora actuales de la controladora y el equipo que se usa como cliente de gestión.

   > Para las cabinas de almacenamiento simples, solo se muestra una controladora.

3. Si las horas que aparecen en el cuadro de diálogo no coinciden, haga clic en **Sincronizar**.

Resultados

Una vez que la sincronización se haya realizado correctamente, las marcas de tiempo del evento serán las mismas para el registro de eventos y los registros de host.

Guarde la configuración de la cabina de almacenamiento

Es posible guardar la información de configuración de una cabina de almacenamiento en un archivo de script para ahorrar tiempo al configurar cabinas de almacenamiento adicionales con las mismas opciones.

Antes de empezar

La cabina de almacenamiento no debe estar sujeta a ninguna operación por la que se modifique su configuración lógica. Algunos ejemplos de estas operaciones son crear o eliminar volúmenes, descargar firmware de controladora, asignar o modificar unidades de repuesto, o añadir capacidad (unidades) a un grupo de volúmenes.

Acerca de esta tarea

Al guardar la configuración de una cabina de almacenamiento, se genera un script de interfaz de línea de comandos (CLI) con las opciones de la cabina de almacenamiento, la configuración de los volúmenes, la configuración de los hosts o las asignaciones de host a volumen para la cabina de almacenamiento. Se puede usar este script de CLI generado para replicar una configuración a otra cabina de almacenamiento con la misma configuración de hardware.

No obstante, no se debe usar este script de CLI para la recuperación ante desastres. En lugar de eso, para restaurar el sistema, utilice el archivo de backup de base de datos de configuración que creó manualmente o póngase en contacto con el soporte técnico para obtener estos datos de los datos de AutoSupport más recientes.

Esta operación *not* guarda estos valores:

- Duración de la batería
- Hora del día de la controladora
- Opciones de la memoria estática de acceso aleatorio no volátil (NVSRAM)
- Funciones excepcionales

- Contraseña de la cabina de almacenamiento
- Estado operativo y estados de los componentes de hardware
- Estado operativo (excepto que sea óptimo) y estados de los grupos de volúmenes
- Servicios de copia, como el mirroring y la copia de volumen

> **Riesgo de errores en la aplicación** — no utilice esta opción si la matriz de almacenamiento está sufriendo una operación que cambiará cualquier configuración lógica. Algunos ejemplos de estas operaciones son crear o eliminar volúmenes, descargar firmware de controladora, asignar o modificar unidades de repuesto, o añadir capacidad (unidades) a un grupo de volúmenes.

Pasos

1. Seleccione MENU:Settings[System].
2. Seleccione **Guardar configuración de la matriz de almacenamiento**.
3. Seleccione los elementos de la configuración que desea guardar:
   - Configuración de cabina de almacenamiento
   - Configuración de volúmenes
   - Configuración de hosts
   - Asignaciones de host a volumen

   > Si selecciona el elemento **asignaciones de host a volumen**, el elemento **Configuración de volumen** y el elemento **Configuración de host** también se seleccionan de forma predeterminada. No puede guardar "asignaciones de hosts a volúmenes" sin guardar también "Configuración del volumen" y "Configuración de host".

4. Haga clic en **Guardar**.

   El archivo se guarda en la carpeta de descargas del explorador con el nombre `storage-array-configuration.cfg`.

Después de terminar

Para cargar la configuración guardada de una cabina de almacenamiento en otra cabina de almacenamiento, utilice la interfaz de línea de comandos de SANtricity (SMcli) con el `-f` para aplicar la `.cfg` archivo.

> También puede cargar la configuración guardada de una cabina de almacenamiento en otras cabinas de almacenamiento mediante la interfaz de Unified Manager (seleccione MENU:gestionar[Importar configuración]).

Borrar la configuración de la cabina de almacenamiento

Use la operación Clear Configuration cuando desee eliminar todos los pools, los grupos de volúmenes, los volúmenes, las definiciones de hosts y las asignaciones de hosts de la cabina de almacenamiento.

Antes de empezar

Antes de borrar la configuración de la cabina de almacenamiento, realice un backup de los datos.

Acerca de esta tarea

Clear Storage Array Configuration contiene dos opciones:

- **Volumen**: Normalmente, puede utilizar la opción volumen para volver a configurar una matriz de almacenamiento de prueba como una matriz de almacenamiento de producción. Por ejemplo, puede configurar una cabina de almacenamiento para pruebas y después, una vez terminadas las pruebas, eliminar la configuración de prueba y configurar la cabina de almacenamiento para un entorno de producción.
- **Storage Array**: Normalmente, puede utilizar la opción Storage Array para mover una matriz de almacenamiento a otro departamento o grupo. Por ejemplo, puede que utilice una cabina de almacenamiento en Engineering y ahora Engineering consigue una nueva cabina de almacenamiento, por lo que desea mover la cabina de almacenamiento actual a Administración para volver a configurarla.

  La opción cabina de almacenamiento elimina algunas opciones de configuración adicionales.

	Volumen	**Cabina de almacenamiento**
Elimina pools y grupos de volúmenes	X	X
Elimina volúmenes	X	X
Elimina hosts y clústeres de hosts	X	X
Elimina asignaciones de hosts	X	X
Elimina el nombre de la cabina de almacenamiento		X
Restablece la configuración de caché de la cabina de almacenamiento a su valor predeterminado		X

Riesgo de pérdida de datos — esta operación elimina todos los datos de la matriz de almacenamiento. (No ejecuta un borrado seguro.) No es posible cancelar esta operación una vez que se inicia. Realice esta operación solo cuando el soporte técnico se lo indique.

Pasos

1. Seleccione MENU:Settings[System].
2. Seleccione **Borrar configuración de la matriz de almacenamiento**.
3. En la lista desplegable, seleccione **volumen** o **matriz de almacenamiento**.
4. **Opcional:** Si desea guardar la configuración (no los datos), utilice los vínculos del cuadro de diálogo.
5. Confirme que desea llevar a cabo la operación.

Resultados

- La configuración actual se elimina y se destruyen todos los datos existentes de la cabina de almacenamiento.

- Todas las unidades quedan sin asignar.

Modifique la configuración de caché para la cabina de almacenamiento

Se puede ajustar la configuración de la memoria caché para el vaciado y el tamaño del bloque de todos los volúmenes de la cabina de almacenamiento.

Acerca de esta tarea

La memoria caché es un área de almacenamiento volátil temporal en la controladora que tiene un tiempo de acceso más rápido que la unidad. Para ajustar el rendimiento de la caché, se pueden modificar las siguientes opciones de configuración:

Configuración de caché	Descripción
Inicio de vaciado de caché bajo demanda	La opción Iniciar purga de caché según demanda especifica el porcentaje de datos sin escribir de la caché que activan el vaciado de caché (escritura en disco). De forma predeterminada, el vaciado de caché comienza cuando los datos sin escribir alcanzan un 80 % de la capacidad. Un porcentaje mayor es una buena opción en entornos que tienen principalmente operaciones de escritura, de manera que las solicitudes de escritura nuevas se pueden procesar mediante la caché sin tener que ir al disco. Los valores de configuración más bajos son mejores para los entornos con operaciones de I/o erráticas (con ráfagas de datos), de manera que el sistema vacía la caché con frecuencia entre las ráfagas de datos. No obstante, un porcentaje inicial inferior al 80 % puede disminuir el rendimiento.
Tamaño del bloque de caché	El tamaño de bloque de la caché determina el tamaño máximo de cada bloque de la caché, que es una unidad organizativa para la gestión de la caché. De manera predeterminada, el tamaño de bloque es de 32 KiB. El sistema permite un tamaño de bloque de caché de 4, 8, 16 o 32 KiBs. Las aplicaciones utilizan distintos tamaños de bloques, que pueden afectar al rendimiento del almacenamiento. Un tamaño menor es una buena opción para los sistemas de archivos o las aplicaciones de bases de datos. Un tamaño mayor es ideal para aplicaciones que generan operaciones de I/o secuenciales, por ejemplo, multimedia.

Pasos

1. Seleccione MENU:Settings[System].
2. Desplácese hacia abajo hasta **Configuración adicional** y, a continuación, haga clic en **Cambiar configuración de caché**.

   Se abre el cuadro de diálogo Cambiar configuración de caché.

3. Ajuste los siguientes valores:
   - **Iniciar purga de caché de demanda** — Seleccione un porcentaje que sea apropiado para la E/S utilizada en su entorno. Si elige un valor inferior a 80 %, es posible que note una disminución de rendimiento.
   - **Tamaño de bloque de caché —** Elija un tamaño que sea apropiado para sus aplicaciones.
4. Haga clic en **Guardar**.

Establecer equilibrio de carga automático

La función Automatic Load Balancing garantiza que el tráfico de I/o entrante de los hosts se gestione dinámicamente y se equilibre entre ambas controladoras. Esta función está habilitada de forma predeterminada, pero se puede deshabilitar desde System Manager.

Acerca de esta tarea

Cuando la función Automatic Load Balancing está habilitada, ejecuta las siguientes funciones:

- Supervisa y equilibra automáticamente la utilización de recursos de la controladora.
- Ajusta automáticamente la propiedad de la controladora de volumen cuando es necesario y así, optimiza el ancho de banda de I/o entre los hosts y la cabina de almacenamiento.

Puede ser conveniente deshabilitar Automatic Load Balancing en la cabina de almacenamiento por las siguientes razones:

- No se desea cambiar automáticamente la propiedad de una controladora de volumen para equilibrar la carga de trabajo.
- Se trabaja en un entorno altamente optimizado donde la distribución de carga se configura intencionalmente para lograr una distribución específica entre las controladoras.

Pasos

1. Seleccione MENU:Settings[System].
2. Desplácese hasta **Configuración adicional** y, a continuación, haga clic en **Habilitar/deshabilitar equilibrio de carga automático**.

   El texto debajo de esta opción indica si la función se encuentra habilitada o deshabilitada.

   Se abre un cuadro de diálogo de confirmación.

3. Confirme haciendo clic en **Sí** para continuar.

   Al seleccionar esta opción, es posible alternar entre habilitar o deshabilitar la función.

   > Cuando esta función pasa de estar deshabilitada a habilitada, también se habilita la función Host Connectivity Reporting.

Habilitar o deshabilitar la interfaz de gestión heredada

Es posible habilitar o deshabilitar la interfaz de gestión heredada (Symbol), que es un método de comunicación entre la cabina de almacenamiento y el cliente de gestión.

Acerca de esta tarea

De manera predeterminada, la interfaz de gestión heredada está activada. Si se desactiva, la cabina de almacenamiento y su cliente de gestión utilizan un método más seguro de comunicación (API DE REST a través de https); sin embargo, ciertas herramientas y tareas pueden verse afectadas si se deshabilita la cabina.

> Para el sistema de almacenamiento EF600, esta función está deshabilitada de manera predeterminada.

La configuración afecta a las operaciones de la siguiente manera:

- **Activado** (predeterminado) — Configuración necesaria para configurar la duplicación con la CLI y otras herramientas, como el adaptador OCI.
- **Off** — Configuración requerida para reforzar la confidencialidad en las comunicaciones entre la matriz de almacenamiento y el cliente de administración, y para acceder a herramientas externas. Opción recomendada para configurar un servidor de directorio (LDAP).

Pasos

1. Seleccione MENU:Settings[System].
2. Desplácese hacia abajo hasta **Configuración adicional** y, a continuación, haga clic en **Cambiar interfaz de administración**.
3. En el cuadro de diálogo, haga clic en **Sí** para continuar.

Configure las funciones complementarias

Cómo trabajar con las funciones complementarias

Las funciones adicionales son las que no se incluyen en la configuración estándar de System Manager y pueden requerir una clave para su habilitación. Una función complementaria puede ser una sola función excepcional o un paquete de funciones agrupadas.

Los siguientes pasos proporcionan información general sobre cómo habilitar una función excepcional o un paquete de funciones:

1. Obtenga la siguiente información:
    - El número de serie del chasis y el identificador de habilitación de la función, el cual identifica la cabina de almacenamiento para la función que se instalará. Estos elementos están disponibles en System Manager.
    - El código de activación de la función, que está disponible en el sitio de soporte al adquirir la función.
2. Obtenga la clave de función. Para ello, póngase en contacto con el proveedor de almacenamiento o acceda al sitio de activación de funciones prémium. Proporcione el número de serie del chasis, el identificador de habilitación y el código de función para la activación.
3. En System Manager, habilite la función excepcional o el paquete de funciones con el archivo de claves de función.

Terminología de la función complementaria

Conozca la forma en que los términos de las funciones complementarias se aplican a su cabina de almacenamiento.

Duración	Descripción
Identificador de habilitación de la función	Un identificador de habilitación de la función es una cadena única que identifica una cabina de almacenamiento específica. Este identificador garantiza que cuando se obtiene la función excepcional, esta se asocie únicamente con una cabina de almacenamiento en particular. Esta cadena aparece en la sección funciones adicionales de la página sistema.
Archivo de claves de función	Un archivo de claves de función es un archivo que se recibe para desbloquear y habilitar una función excepcional o un paquete de funciones.
Paquete de funciones	Un paquete de funciones es un paquete que cambia los atributos de la cabina de almacenamiento (por ejemplo, cambiar el protocolo Fibre Channel a iSCSI). Los paquetes de funciones requieren una clave especial para habilitarlos.
Función excepcional	Una función prémium es una opción adicional que requiere una clave para habilitarla. No se incluye en la configuración estándar de System Manager.

Obtener un archivo de claves de función

Para habilitar una función excepcional o un paquete de funciones en una cabina de almacenamiento, primero es necesario obtener un archivo de claves de función. Una clave se asociada con una sola cabina de almacenamiento.

Acerca de esta tarea

En esta tarea, se describe cómo obtener la información requerida para la función y, a continuación, enviar una solicitud para un archivo de claves de función. Entre la información requerida se encuentra la siguiente:

- Número de serie del chasis
- Identificador de habilitación de la función
- Código de activación de la función

Pasos

1. En System Manager, busque y registre el número de serie del chasis. Para ver este número de serie, debe pasar el ratón por el icono Centro de soporte.
2. En System Manager, busque Identificador de habilitación de funciones. Vaya a MENU:Settings[System] y, a continuación, desplácese hacia abajo hasta **Add-ons**. Busque **Identificador de habilitación de funciones**. Registre el número de la opción Identificador de habilitación de funciones.
3. Busque y registre el código para la activación de la función. Para paquetes de funciones, este código se proporciona en las instrucciones correspondientes para realizar la conversión.

   Es posible acceder a las instrucciones de NetApp en "Centro de documentación para sistemas E-Series y EF-Series de NetApp".

   Para funciones excepcionales, es posible acceder al código de activación en el sitio de soporte de la siguiente manera:

   a. Inicie sesión en "Soporte de NetApp".
   b. Vaya a **licencias de software** para su producto.

c. Introduzca el número de serie del chasis de la cabina de almacenamiento y, a continuación, haga clic en **Ir**.

d. Busque los códigos de activación de la función en la columna **clave de licencia**.

e. Registre el contenido de la opción Feature Activation Code de la función deseada.

4. Para solicitar un archivo de claves de función, envíe un correo electrónico o un documento de texto al proveedor de almacenamiento con la siguiente información: Número de serie del chasis, el identificador de habilitación y el código para la activación de la función.

   También puede ir a. "Activación de licencias de NetApp: Activación de funciones prémium de matriz de almacenamiento" e introduzca la información requerida para obtener la función o el paquete de funciones. (Las instrucciones en este sitio son para funciones excepcionales, no paquetes de funciones.)

Después de terminar

Una vez que tenga el archivo de claves de la función, podrá habilitar la función excepcional o el paquete de funciones.

Habilite una función excepcional

Una función prémium es una opción adicional que requiere una clave para habilitarla.

Antes de empezar

- Obtuvo una clave de función. Si es necesario, comuníquese con soporte técnico para obtener una clave.
- Cargó el archivo de claves en el cliente de gestión (el sistema con un explorador para acceder a System Manager).

Acerca de esta tarea

En esta tarea, se describe cómo usar System Manager para habilitar una función excepcional.

> Si desea deshabilitar una función excepcional, debe utilizar el comando Deshabilitar función de cabina de almacenamiento (`disable storageArray) (featurePack | feature=featureAttributeList`) En la interfaz de línea de comandos (CLI).

Pasos

1. Seleccione MENU:Settings[System].
2. En **Complementos**, seleccione **Activar característica Premium**.

   Se abre el cuadro de diálogo Habilitar una función prémium.

3. Haga clic en **examinar** y, a continuación, seleccione el archivo de claves.

   El nombre del archivo aparece en el cuadro de diálogo.

4. Haga clic en **Activar**.

Habilite el paquete de funciones

Un paquete de funciones es un paquete que cambia los atributos de la cabina de almacenamiento (por ejemplo, cambiar el protocolo Fibre Channel a iSCSI). Para habilitar paquetes de funciones, se requiere una clave especial.

Antes de empezar

- Siguió las instrucciones adecuadas donde se describen la conversión y la preparación de los nuevos atributos de la cabina de almacenamiento. Para obtener instrucciones sobre la conversión de protocolos de host, consulte la guía de mantenimiento de hardware para su modelo de controladora.
- La cabina de almacenamiento está sin conexión, por lo que ningún host ni aplicación accede a la cabina.
- Existen backups de todos los datos.
- Obtuvo un archivo de paquete de funciones.

  El paquete de funciones está cargado en el cliente de gestión (el sistema con un explorador para acceder a System Manager).

> Debe programar una ventana de mantenimiento de tiempo de inactividad y detener todas las operaciones de I/o entre el host y las controladoras. Además, tenga en cuenta que no podrá acceder a los datos en la cabina de almacenamiento hasta después de completar correctamente la conversión.

Acerca de esta tarea

En esta tarea, se describe cómo usar System Manager para habilitar un paquete de funciones. Al finalizar, debe reiniciar la cabina de almacenamiento.

Pasos

1. Seleccione MENU:Settings[System].
2. En **Complementos**, seleccione **Cambiar paquete de funciones**.
3. Haga clic en **examinar** y, a continuación, seleccione el archivo de claves.

   El nombre del archivo aparece en el cuadro de diálogo.

4. Tipo `change` en el campo.
5. Haga clic en **Cambiar**.

   Comienza la migración del paquete de funciones y se reinician las controladoras. Se eliminan los datos no escritos en la caché, lo que garantiza que no exista actividad de I/O. Las dos controladoras se reinician automáticamente para que el nuevo paquete de funciones entre en vigencia. La cabina de almacenamiento vuelve a responder cuando se completa el reinicio.

Descargar la interfaz de línea de comandos (CLI)

En System Manager, es posible descargar el paquete de la CLI.

La CLI proporciona un método a partir de texto para la configuración y supervisión de cabinas. Se comunica mediante https y utiliza la misma sintaxis que la CLI que está disponible en el paquete de software de gestión instalado de forma externa. Para descargar la CLI, no se requiere ninguna clave.

Antes de empezar

Debe haber disponible un entorno Java Runtime Environment (JRE), versión 8 y superior en el sistema de administración en el que planea ejecutar los comandos de la CLI.

Pasos

1. Seleccione MENU:Settings[System].

2. En **Complementos**, seleccione **interfaz de línea de comandos**.

   El paquete ZIP se descargará en el explorador.

3. Guarde el archivo ZIP en el sistema de gestión donde tenga pensado ejecutar los comandos de la CLI para la cabina de almacenamiento y, a continuación, extraiga el archivo.

   Ahora puede ejecutar los comandos de la CLI a partir de una solicitud del sistema operativo, como dos C: Prompt. Encontrará una referencia de comandos de la CLI en el menú Ayuda, en la parte superior derecha de la interfaz de usuario de System Manager.

Preguntas frecuentes

¿Qué es el equilibrio de carga automático?

La función Automatic Load Balancing proporciona equilibrio de I/o automatizado y garantiza que el tráfico de I/o entrante de los hosts se gestione dinámicamente y se equilibre en ambas controladoras.

La función Automatic Load Balancing ofrece una gestión de recursos de I/o mejorada, ya que reacciona dinámicamente a los cambios de carga con el tiempo y ajusta automáticamente la propiedad de la controladora de volumen para corregir cualquier problema de desequilibrio de carga cuando las cargas de trabajo son distintas de una controladora a otra.

La carga de trabajo de cada controladora se supervisa continuamente y, con la colaboración de los controladores multivía instalados en los hosts, es posible establecer automáticamente el equilibrio cada vez que sea necesario. Una vez que la carga de trabajo se vuelve a equilibrar de forma automática en todas las controladoras, el administrador de almacenamiento queda liberado de la carga que supone ajustar manualmente la propiedad de la controladora de volumen para admitir cambios de carga en la cabina de almacenamiento.

Cuando la función Automatic Load Balancing está habilitada, ejecuta las siguientes funciones:

- Supervisa y equilibra automáticamente la utilización de recursos de la controladora.
- Ajusta automáticamente la propiedad de la controladora de volumen cuando es necesario y así, optimiza el ancho de banda de I/o entre los hosts y la cabina de almacenamiento.

> Cualquier volumen asignado para utilizar una caché SSD de una controladora no es elegible para una transferencia de equilibrio de carga automática.

¿Qué es la caché de la controladora?

La caché de la controladora es un espacio de memoria física que optimiza dos tipos de operaciones de I/o (entrada/salida): Entre las controladoras y los hosts, y entre las controladoras y los discos.

En el caso de las transferencias de datos de lectura y escritura, los hosts y las controladoras se comunican a través de conexiones de alta velocidad. Sin embargo, la comunicación del back-end de la controladora a los discos es más lenta debido a que los discos son dispositivos relativamente lentos.

Cuando la caché de la controladora recibe los datos, la controladora reconoce qué aplicaciones host son las que ahora tienen los datos. De este modo, las aplicaciones host no necesitan esperar a que se escriban las

operaciones de I/o en el disco. En cambio, las aplicaciones pueden continuar con sus operaciones. Los datos en caché también están a disposición de las aplicaciones de servidor, lo que elimina la necesidad de lecturas adicionales del disco para acceder a los datos.

La caché de la controladora afecta al rendimiento general de la cabina de almacenamiento de diversas maneras:

- La caché actúa como un búfer, de modo que las transferencias de datos entre disco y host no necesitan sincronizarse.
- Los datos de una operación de escritura o lectura del host pueden estar en caché desde una operación anterior, lo que elimina la necesidad de acceder al disco.
- Si se utiliza el almacenamiento en caché de escritura, el host puede enviar comandos de escritura posteriores antes de que los datos de una operación de escritura anterior se escriban en el disco.
- Si la captura previa de caché está habilitada, el acceso de lectura secuencial se optimiza. La captura previa de caché hace que una operación de lectura tenga más probabilidades de encontrar los datos en la caché, en lugar de leer los datos del disco.

Posible pérdida de datos — Si activa la opción **almacenamiento en caché de escritura sin baterías** y no dispone de una fuente de alimentación universal de protección, podría perder datos. Además, puede perder datos si no tiene baterías de controlador y activa la opción **almacenamiento en caché de escritura sin baterías**.

¿Qué es el vaciado de la caché?

Cuando la cantidad de datos no guardados que se encuentra en la caché llega a cierto nivel, la controladora guarda periódicamente en una unidad los datos en caché. Este proceso de guardado se denomina "vaciado".

La controladora utiliza dos algoritmos para vaciar la caché: En función de la demanda y en función de la antigüedad. La controladora utiliza un algoritmo en función de la demanda hasta que la cantidad de datos en caché desciende por debajo del umbral de vaciado de caché. De manera predeterminada, un vaciado comienza cuando está en uso el 80 % de la caché.

En System Manager, puede configurar el umbral «Iniciar purga de caché a demanda» para que admita mejor el tipo de I/o utilizado en su entorno. En un entorno principalmente compuesto por operaciones de escritura, debe establecer un porcentaje alto de «Iniciar purga de caché de demanda» para aumentar la probabilidad de que cualquier solicitud de escritura nueva se pueda procesar mediante la caché sin tener que ir al disco. La configuración de un porcentaje alto limita la cantidad de vaciados de caché a fin de que más datos permanezcan en la caché, lo que aumenta la posibilidad de más aciertos en caché.

En un entorno en el que las operaciones de I/o son erráticas (con picos de datos), es posible utilizar un vaciado de caché bajo para que el sistema vacíe la caché con frecuencia entre los picos de datos. En un entorno diverso de operaciones de I/o que procesa diferentes cargas, o cuando se desconoce el tipo de cargas, se puede configurar un umbral del 50 % como un buen punto de partida intermedio. Tenga en cuenta que, si selecciona un porcentaje de inicio inferior al 80 %, es posible que disminuya el rendimiento, ya que los datos necesarios para la lectura del host pueden no estar disponibles. Además, un porcentaje más bajo también aumenta la cantidad de escrituras de disco necesarias para mantener el nivel de caché, lo que aumenta la sobrecarga del sistema.

El algoritmo en función de la antigüedad especifica el periodo durante el cual los datos de escritura pueden permanecer en la caché antes de calificar para el vaciamiento a los discos. Las controladoras utilizan el algoritmo en función de la antigüedad hasta que se alcanza el umbral de vaciado de caché. El valor

predeterminado es de 10 segundos, pero este lapso se considera solo en periodos de inactividad. No puede modificar el tiempo de vaciado en System Manager; en su lugar, debe utilizar el comando **Set Storage Array** en la interfaz de línea de comandos (CLI).

> **Posible pérdida de datos** — Si activa la opción **almacenamiento en caché de escritura sin baterías** y no dispone de una fuente de alimentación universal de protección, podría perder datos. Además, puede perder datos si no tiene baterías de controlador y activa la opción **almacenamiento en caché de escritura sin baterías**.

¿Qué es el tamaño de bloque de caché?

La controladora de la cabina de almacenamiento organiza su caché en "bloques", que son fragmentos de memoria que pueden tener un tamaño de 8, 16 o 32 KiB. Todos los volúmenes del sistema de almacenamiento comparten el mismo espacio de caché; por lo tanto, los volúmenes solo pueden tener un tamaño de bloque de caché.

Las aplicaciones utilizan diferentes tamaños de bloque, lo que puede afectar el rendimiento del almacenamiento. De manera predeterminada, el tamaño de bloque en System Manager es de 32 KiB, pero se puede modificar el valor a 8, 16 o 32 KiB. Un tamaño menor es una buena opción para los sistemas de archivos o las aplicaciones de bases de datos. Un tamaño mayor es una buena opción para aplicaciones que requieren grandes transferencias de datos, operaciones de I/o secuenciales o alto ancho de banda, como las aplicaciones multimedia.

¿Cuándo se deben sincronizar los relojes de la cabina de almacenamiento?

Se deben sincronizar manualmente los relojes de las controladoras en la cabina de almacenamiento si se observa que las marcas de tiempo que se muestran en System Manager no están alineadas con las marcas de tiempo del cliente de gestión (el ordenador que accede a System Manager por medio del explorador). Esta tarea es necesaria solo si no se habilitó el protocolo de tiempo de redes (NTP) en System Manager.

> Se recomienda enfáticamente utilizar un servidor NTP en lugar de sincronizar manualmente los relojes. NTP sincroniza automáticamente los relojes con un servidor externo que utiliza el protocolo de tiempo de redes simple (SNTP).

Se puede comprobar el estado de sincronización desde el cuadro de diálogo Sincronizar relojes de cabinas de almacenamiento, que se encuentra disponible en la página sistema. Si las horas que aparecen en el cuadro de diálogo no coinciden, ejecute una sincronización. Puede ver este cuadro de diálogo periódicamente y verificar si las horas que muestran los relojes de las controladoras se distanciaron y ya no están sincronizadas.

Impulse la seguridad

Información general de Drive Security

Es posible configurar Drive Security y la gestión de claves desde la página Gestión de claves de seguridad.

¿Qué es Drive Security?

Drive Security es una función que evita el acceso no autorizado a datos almacenados en unidades con la función de seguridad habilitada cuando la unidad se quita de la cabina de almacenamiento. Estas unidades pueden ser unidades de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS). Cuando se retiran físicamente, las unidades FDE o FIPS de la cabina no pueden operar hasta que se instalan en otra cabina, instancia en la cual las unidades tendrán el estado Security Locked hasta que se proporcione la clave de seguridad correcta. Un *Security Key* es una cadena de caracteres que se comparte entre estos tipos de unidades y las controladoras en una cabina de almacenamiento.

Obtenga más información:

- "Cómo opera la función Drive Security"
- "Cómo funciona la gestión de claves de seguridad"
- "Terminología de Drive Security"

¿Cómo se configura la gestión de claves?

Para implementar Drive Security, debe tener instaladas unidades FDE o FIPS en la cabina. Para configurar la gestión de claves para estas unidades, vaya a menú:Configuración[sistema > Gestión de claves de seguridad] donde se puede crear una clave interna desde la memoria persistente de la controladora o una clave externa desde un servidor de gestión de claves. Por último, si desea habilitar Drive Security para pools y grupos de volúmenes, seleccione la opción "compatible con la función de seguridad" en la configuración del volumen.

Obtenga más información:

- "Cree una clave de seguridad interna"
- "Cree una clave de seguridad externa"
- "Crear un pool manualmente"
- "Crear grupos de volúmenes"

¿Cómo se desbloquearán unidades?

Si se configuró la gestión de claves y luego se mueven unidades con la función de seguridad habilitada de una cabina de almacenamiento a otra, se debe volver a asignar la clave de seguridad a la nueva cabina de almacenamiento para acceder a los datos cifrados en las unidades.

Obtenga más información:

- "Desbloquear unidades al utilizar la gestión de claves internas"
- "Desbloquear unidades al utilizar gestión de claves externas"

Información relacionada

Obtenga más información sobre tareas relacionadas con la gestión de claves:

- "Use certificados firmados por CA para la autenticación con un servidor de gestión de claves"
- "Realice un backup de la clave de seguridad"

Conceptos

Cómo opera la función Drive Security

Drive Security es una función de la cabina de almacenamiento que ofrece una capa adicional de seguridad con unidades de cifrado de disco completo (FDE) o unidades de estándar de procesamiento de información federal (FIPS).

Cuando estas unidades se usan con la función Drive Security, se requiere una clave de seguridad para acceder a los datos. Cuando se retiran físicamente, las unidades de la cabina no pueden operar hasta que se instalan en otra cabina, instancia en la cual tendrán el estado Security Locked hasta que se proporcione la clave de seguridad correcta.

Cómo implementar Drive Security

Para implementar Drive Security, siga estos pasos.

1. Equipe la cabina de almacenamiento con unidades compatibles con la función de seguridad, ya sea con unidades FDE o FIPS. (Para los volúmenes que requieren compatibilidad con FIPS, debe utilizar únicamente unidades FIPS. Si se mezclan unidades FIPS y FDE en un grupo de volúmenes o un pool, todas las unidades se tratarán como unidades FDE. Además, una unidad FDE no puede añadirse a ni usarse como pieza de repuesto en un grupo de volúmenes o un pool completamente FIPS.)
2. Cree una clave de seguridad, que es una cadena de caracteres compartida por la controladora y las unidades para acceso de lectura/escritura. Es posible crear una clave interna desde la memoria persistente de la controladora o una clave externa desde un servidor de gestión de claves. Para la gestión de claves externas, debe establecerse una autenticación con el servidor de gestión de claves.
3. Habilite Drive Security para pools y grupos de volúmenes:
   - Cree un pool o grupo de volúmenes (busque **Sí** en la columna **compatible con la función de seguridad** de la tabla candidatos).
   - Seleccione un pool o grupo de volúmenes cuando cree un volumen nuevo (busque **Sí** junto a **compatible con la función de seguridad** en la tabla de candidatos de pools y grupos de volúmenes).

Cómo funciona Drive Security en el nivel de unidad

Una unidad compatible con la función de seguridad, FDE o FIPS, cifra los datos durante la escritura y descifra los datos durante la lectura. Estas operaciones de cifrado y descifrado no afectan al rendimiento ni al flujo de trabajo del usuario. Cada unidad tiene su propia clave de cifrado, que jamás puede transferirse de la unidad.

La función Drive Security ofrece una capa adicional de protección en unidades compatibles con la función de seguridad. Cuando se seleccionan grupos de volúmenes o pools en estas unidades para Drive Security, las unidades buscan una clave de seguridad antes de permitir el acceso a los datos. Es posible habilitar Drive Security para pools y grupos de volúmenes en cualquier momento sin afectar a los datos existentes en la unidad. Sin embargo, no es posible deshabilitar Drive Security sin borrar todos los datos en la unidad.

Cómo funciona Drive Security en el nivel de cabina de almacenamiento

Con la función Drive Security, se crea una clave de seguridad que se comparte entre las unidades con la función de seguridad habilitada y las controladoras en una cabina de almacenamiento. Siempre que se encienden y se apagan las unidades, las unidades con la función de seguridad habilitada cambian al estado Security Locked hasta que la controladora aplica la clave de seguridad.

Si se quita una unidad con la función de seguridad habilitada de la cabina de almacenamiento y se vuelve a

instalar en otra, la unidad tendrá el estado Security Locked. La unidad reubicada busca la clave de seguridad para que pueda volver a accederse a los datos. Para desbloquear los datos, debe aplicar la clave de seguridad desde la cabina de almacenamiento de origen. Después de un proceso de desbloqueo correcto, la unidad reubicada utilizará la clave de seguridad ubicada en la cabina de almacenamiento objetivo, y el archivo de claves de seguridad importado ya no será necesario.

> Para la gestión de claves internas, la clave de seguridad se almacena en una ubicación inaccesible de la controladora. No está en formato legible, y el usuario no puede acceder a ella.

Cómo funciona Drive Security en el nivel de volumen

Al crear un pool o un grupo de volúmenes desde unidades compatibles con la función de seguridad, también es posible habilitar Drive Security para estos pools o grupos de volúmenes. La opción Drive Security permite que las unidades y los pools y los grupos de volúmenes asociados tengan la función de seguridad-*enabled*.

Tenga en cuenta las siguientes directrices antes de crear pools y grupos de volúmenes con la función de seguridad habilitada:

- Los grupos de volúmenes y los pools deben estar compuestos en su totalidad por unidades compatibles con la función de seguridad. (Para los volúmenes que requieren compatibilidad con FIPS, debe utilizar únicamente unidades FIPS. Si se mezclan unidades FIPS y FDE en un grupo de volúmenes o un pool, todas las unidades se tratarán como unidades FDE. Además, una unidad FDE no puede añadirse a ni usarse como pieza de repuesto en un grupo de volúmenes o un pool completamente FIPS.)
- Los grupos de volúmenes y los pools deben tener el estado Optimal.

Cómo funciona la gestión de claves de seguridad

Cuando se implementa la función Drive Security, las unidades con la función de seguridad habilitada (FIPS o FDE) requieren una clave de seguridad para acceder a los datos. Una clave de seguridad es una cadena de caracteres que se comparte entre estos tipos de unidades y las controladoras en una cabina de almacenamiento.

Siempre que se encienden y se apagan las unidades, las unidades con la función de seguridad habilitada cambian al estado Security Locked hasta que la controladora aplica la clave de seguridad. Si se elimina una unidad habilitada para seguridad de la cabina de almacenamiento, se bloquean los datos de esa unidad. Cuando se vuelve a instalar la unidad en otra cabina de almacenamiento, se busca la clave de seguridad para que pueda volver a accederse a los datos. Para desbloquear los datos, debe aplicar la clave de seguridad original.

Puede crear y gestionar claves de seguridad mediante uno de los siguientes métodos:

- Gestión de claves internas en la memoria persistente de la controladora.
- Gestión de claves externas en un servidor de gestión de claves externo.

Gestión de claves internas

Se mantienen las claves internas y se «"ocultan"» en una ubicación sin acceso en la memoria persistente de la controladora. Para implementar la gestión de claves internas, siga estos pasos:

1. Instale unidades compatibles con la función de seguridad en la cabina de almacenamiento. Estas unidades pueden ser de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS).

2. Asegúrese de que la función Drive Security esté habilitada. Si fuera necesario, comuníquese con el proveedor de almacenamiento para pedir indicaciones sobre cómo habilitar la función Drive Security.
3. Cree una clave de seguridad interna, que implica definir un identificador y una frase de contraseña. El identificador es una frase que está asociada con la clave de seguridad, y se almacena en la controladora y en todas las unidades asociadas con la clave. La frase de contraseña se utiliza para cifrar la clave de seguridad con fines de backup. Para crear una clave interna, vaya a menú:Configuración[sistema > Gestión de claves de seguridad > Crear clave interna].

La clave de seguridad se almacena en una ubicación oculta a la que no se puede acceder. Es posible crear grupos de volúmenes o pools con la función de seguridad habilitada, o bien habilitar la seguridad en grupos de volúmenes o pools existentes.

Gestión de claves externas

Las claves externas se mantienen en un servidor de gestión de claves individual mediante un protocolo de interoperabilidad de gestión de claves (KMIP). Para implementar la gestión de claves externas, siga estos pasos:

1. Instale unidades compatibles con la función de seguridad en la cabina de almacenamiento. Estas unidades pueden ser de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS).
2. Asegúrese de que la función Drive Security esté habilitada. Si fuera necesario, comuníquese con el proveedor de almacenamiento para pedir indicaciones sobre cómo habilitar la función Drive Security.
3. Obtener un archivo de certificado de cliente firmado. Un certificado de cliente valida las controladoras de la cabina de almacenamiento para que el servidor de gestión de claves pueda confiar en sus solicitudes KMIP.
   a. En primer lugar, complete y descargue una solicitud de firma de certificación (CSR) de cliente. Vaya a menú:Configuración[certificados > Gestión de claves > completar CSR].
   b. A continuación, se solicita un certificado de cliente firmado de una CA de confianza para el servidor de gestión de claves. (También se puede crear y descargar un certificado de cliente desde el servidor de gestión de claves con el archivo CSR).
   c. Una vez que tenga un archivo de certificado de cliente, copie ese archivo en el host en el que accede a System Manager.
4. Recupere un archivo de certificado del servidor de gestión de claves y copie ese archivo en el host donde accede a System Manager. Un certificado de servidor de gestión de claves valida el servidor de gestión de claves para que la cabina de almacenamiento pueda confiar en su dirección IP. Es posible usar un certificado raíz, intermedio o de servidor para el servidor de gestión de claves.
5. Cree una clave externa, que implica definir la dirección IP del servidor de gestión de claves y el número de puerto utilizado para comunicaciones KMIP. Durante este proceso, también debe cargar los archivos de certificado. Para crear una clave externa, vaya a menú:Configuración[sistema > Gestión de claves de seguridad > Crear clave externa].

El sistema se conecta al servidor de gestión de claves con las credenciales introducidas. Es posible crear grupos de volúmenes o pools con la función de seguridad habilitada, o bien habilitar la seguridad en grupos de volúmenes o pools existentes.

Terminología de Drive Security

Conozca la forma en que los términos de Drive Security se aplican a su cabina de almacenamiento.

Duración	Descripción
Función Drive Security	Drive Security es una función de la cabina de almacenamiento que ofrece una capa adicional de seguridad con unidades de cifrado de disco completo (FDE) o unidades de estándar de procesamiento de información federal (FIPS). Cuando estas unidades se usan con la función Drive Security, se requiere una clave de seguridad para acceder a los datos. Cuando se retiran físicamente, las unidades de la cabina no pueden operar hasta que se instalan en otra cabina, instancia en la cual tendrán el estado Security Locked hasta que se proporcione la clave de seguridad correcta.
Unidades FDE	Las unidades de cifrado de disco completo (FDE) realizan el cifrado en la unidad de disco en el nivel de hardware. La unidad de disco duro contiene un chip ASIC que cifra los datos durante las escrituras y, a continuación, descifra los datos durante las lecturas.
Unidades FIPS	Las unidades con FIPS utilizan estándares de procesamiento de información federal (FIPS) 140-2 nivel 2. Son esencialmente unidades FDE que cumplen con las normas gubernamentales de los Estados Unidos para garantizar algoritmos y métodos de cifrado sólidos. Las unidades FIPS tienen normas de seguridad más rigurosas que las unidades FDE.
Cliente de gestión	Un sistema local (equipo, tablet, etc.) que incluye un explorador para acceder a System Manager.
Frase de contraseña	La frase de contraseña se utiliza para cifrar la clave de seguridad con fines de backup. La misma frase de contraseña utilizada para cifrar la clave de seguridad debe incluirse cuando se importa la clave de seguridad como resultado de una migración de unidad o un cambio de cabezal. La frase de contraseña puede tener entre 8 y 32 caracteres. La frase de contraseña de Drive Security es independiente de la contraseña de administrador de la cabina de almacenamiento.
Unidades compatibles con la función de seguridad	Las unidades compatibles con la función de seguridad pueden ser unidades de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS) que cifran datos durante la escritura y descifran datos durante la lectura. Estas unidades se consideran Secure-*capable* porque se pueden usar para obtener más seguridad mediante la función Drive Security. Si está habilitada la función Drive Security para los grupos de volúmenes y pools que se utilizan con estas unidades, las unidades pasan a tener habilitada la función de seguridad-*enabled*.

Duración	Descripción
Unidades con la función de seguridad habilitada	Las unidades con la función de seguridad habilitada se usan con Drive Security. Cuando se habilita la función Drive Security y se aplica Drive Security a un pool o un grupo de volúmenes en unidades_ compatibles con la función de seguridad, las unidades pasan a ser seguras *habilitadas*. El acceso de lectura y escritura solo está disponible a través de una controladora que está configurada con la clave de seguridad correcta. Esta seguridad adicional evita el acceso no autorizado a los datos en una unidad que se quita físicamente de la cabina de almacenamiento.
Clave de seguridad	Una clave de seguridad es una cadena de caracteres que se comparte entre las unidades habilitadas para seguridad y las controladoras en una cabina de almacenamiento. Siempre que se encienden y se apagan las unidades, las unidades con la función de seguridad habilitada cambian al estado Security Locked hasta que la controladora aplica la clave de seguridad. Si se elimina una unidad habilitada para seguridad de la cabina de almacenamiento, se bloquean los datos de esa unidad. Cuando se vuelve a instalar la unidad en otra cabina de almacenamiento, se busca la clave de seguridad para que pueda volver a accederse a los datos. Para desbloquear los datos, debe aplicar la clave de seguridad original. Puede crear y gestionar claves de seguridad mediante uno de los siguientes métodos: • Gestión de claves internas: Crea y mantiene claves de seguridad en la memoria persistente de la controladora. • Gestión de claves externas: Crea y mantiene claves de seguridad en un servidor de gestión de claves externo.
Identificador de clave de seguridad	El identificador de clave de seguridad es una cadena asociada con la clave de seguridad durante su creación. El identificador se almacena en la controladora y en todas las unidades asociadas con la clave de seguridad.

Configure las claves de seguridad

Cree una clave de seguridad interna

Para usar la función Drive Security, se puede crear una clave de seguridad interna que compartan las controladoras y las unidades compatibles con la función de seguridad de la cabina de almacenamiento. Las claves internas se conservan en la memoria persistente de la controladora.

Antes de empezar

- Se deben instalar unidades compatibles con la función de seguridad en la cabina de almacenamiento. Estas unidades pueden ser de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS).
- Se debe habilitar la función Drive Security. De lo contrario, se abre el cuadro de diálogo no puede crearse una clave de seguridad durante esta tarea. Si fuera necesario, comuníquese con el proveedor de almacenamiento para pedir indicaciones sobre cómo habilitar la función Drive Security.

> Si se instalan unidades FDE y FIPS en la cabina de almacenamiento, ambas compartirán la misma clave de seguridad.

Acerca de esta tarea

En esta tarea, se deben definir un identificador y una frase de contraseña para asociarlos con la clave de seguridad interna.

> La frase de contraseña de Drive Security es independiente de la contraseña de administrador de la cabina de almacenamiento.

Pasos

1. Seleccione MENU:Settings[System].
2. En **Gestión de claves de seguridad**, seleccione **Crear clave interna**.

   Si todavía no generó una clave de seguridad, se abre el cuadro de diálogo Crear clave de seguridad.

3. Introduzca información en los siguientes campos:

   - **Definir un identificador de claves de seguridad**: Puede aceptar el valor predeterminado (Marca de tiempo y nombre de la cabina de almacenamiento, que genera el firmware de la controladora) o introducir el valor deseado. Puede introducir hasta 189 caracteres alfanuméricos sin espacios, puntuación ni símbolos.

     > Se generarán otros caracteres automáticamente, incorporados a ambos extremos de la cadena que introdujo. Los caracteres generados garantizan que el identificador sea único.

   - **Definir una frase de contraseña/Volver a introducir la frase de contraseña** — Introduzca y confirme una frase de contraseña. El valor puede tener entre 8 y 32 caracteres, y debe incluir uno de los siguientes caracteres:
     - Una letra mayúscula (o varias). Se debe tener en cuenta que la frase de contraseña distingue mayúsculas de minúsculas.
     - Un número (o varios).
     - Un carácter no alfanumérico, como !, *, @ (o varios).

     > **Asegúrese de grabar sus entradas para un uso posterior**. Si se necesita transferir una unidad con la función de seguridad habilitada de la cabina de almacenamiento, se deben conocer el identificador y la frase de contraseña para desbloquear los datos de la unidad.

4. Haga clic en **Crear**.

   La clave de seguridad se almacena en una ubicación inaccesible de la controladora. Además de la clave real, se descarga un archivo de claves cifrado del explorador.

   > La ruta del archivo descargado podría depender de la ubicación predeterminada de las descargas del explorador.

5. Anote el identificador de claves, la frase de la contraseña y la ubicación del archivo de claves descargado y, a continuación, haga clic en **Cerrar**.

Resultados

Ahora se pueden crear grupos de volúmenes o pools con la función de seguridad habilitada o puede habilitar la seguridad en los grupos de volúmenes y pools existentes.

> Cada vez que se apagan y se vuelven a encender las unidades, todas las unidades con la función de seguridad habilitada cambian al estado Security Locked. En este estado, no se puede acceder a los datos hasta que la controladora aplica la clave de seguridad correcta durante la inicialización de la unidad. Si alguien quita físicamente la unidad bloqueada y la instala en otro sistema, el estado Security Locked evita el acceso no autorizado de los datos.

Después de terminar

Debe validar la clave de seguridad para asegurarse de que no se haya dañado el archivo de claves.

Cree una clave de seguridad externa

Para usar la función Drive Security con un servidor de gestión de claves, se debe crear una clave externa que se compartirá con el servidor de gestión de claves y las unidades compatibles con la función de seguridad de la cabina de almacenamiento.

Antes de empezar

- Se deben instalar unidades compatibles con la función de seguridad en la cabina. Estas unidades pueden ser de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS).

  > Si se instalan unidades FDE y FIPS en la cabina de almacenamiento, ambas compartirán la misma clave de seguridad.

- Se debe habilitar la función Drive Security. De lo contrario, se abre el cuadro de diálogo no puede crearse una clave de seguridad durante esta tarea. Si fuera necesario, comuníquese con el proveedor de almacenamiento para pedir indicaciones sobre cómo habilitar la función Drive Security.
- Posee un archivo de certificado de cliente firmado para las controladoras de la cabina de almacenamiento y copió ese archivo en el host donde se accede a System Manager. Un certificado de cliente valida las controladoras de la cabina de almacenamiento para que el servidor de gestión de claves pueda confiar en sus solicitudes de protocolo de interoperabilidad de gestión de claves (KMIP).
- Debe recuperar un archivo de certificado del servidor de gestión de claves y, a continuación, copiar ese archivo en el host donde va a acceder a System Manager. Un certificado de servidor de gestión de claves valida el servidor de gestión de claves para que la cabina de almacenamiento pueda confiar en su dirección IP. Es posible usar un certificado raíz, intermedio o de servidor para el servidor de gestión de claves.

  > Si desea obtener más información sobre el certificado de servidor, consulte la documentación del servidor de gestión de claves.

Acerca de esta tarea

En esta tarea, se deben definir la dirección IP del servidor de gestión de claves y el número de puerto que utiliza y, luego, cargar los certificados para la gestión de claves externas.

Pasos

1. Seleccione MENU:Settings[System].
2. En **Gestión de claves de seguridad**, seleccione **Crear clave externa**.

> Si está configurada actualmente la gestión de claves internas, se muestra un cuadro de diálogo para solicitar la confirmación de que se desea cambiar a la gestión de claves externas.

Se abre el cuadro de diálogo Crear clave de seguridad externa.

3. En **conectar con el servidor de claves**, introduzca información en los siguientes campos.
   - **Dirección del servidor de administración de claves** — Introduzca el nombre de dominio completo o la dirección IP (IPv4 o IPv6) del servidor utilizado para la administración de claves.
   - **Número de puerto de administración de claves** — Introduzca el número de puerto utilizado para las comunicaciones KMIP. El número de puerto más común que se usa para la comunicación del servidor de gestión de claves es 5696.

     Opcional: Si desea configurar un servidor de claves de copia de seguridad, haga clic en **Agregar servidor de claves** y, a continuación, escriba la información de ese servidor. Si no puede establecerse acceso al servidor de claves primario, se utilizará el segundo servidor de claves. Asegúrese de que cada servidor de claves tenga acceso a la misma base de datos de las claves; de lo contrario, la cabina publicará errores y no podrá utilizar el servidor de backup.

     > Solo se utiliza un servidor de claves individual a la vez. Si la cabina de almacenamiento no puede alcanzar el servidor de claves primario, la cabina se pondrá en contacto con el servidor de claves de backup. Tenga en cuenta que debe mantener la paridad en ambos servidores; de lo contrario, se pueden producir errores.

   - **Seleccionar certificado de cliente** — haga clic en el primer botón **examinar** para seleccionar el archivo de certificado para los controladores de la matriz de almacenamiento.
   - **Seleccione el certificado del servidor de administración de claves** — haga clic en el segundo botón **examinar** para seleccionar el archivo de certificado del servidor de administración de claves. Es posible elegir un certificado raíz, intermedio o de servidor para el servidor de gestión de claves.
4. Haga clic en **Siguiente**.
5. En **Crear/realizar copia de seguridad de la clave**, puede crear una clave de copia de seguridad con fines de seguridad.
   - (Recomendado) para crear una clave de backup, mantenga seleccionada la casilla de comprobación y, a continuación, introduzca y confirme una frase de contraseña. El valor puede tener entre 8 y 32 caracteres, y debe incluir uno de los siguientes caracteres:
     - Una letra mayúscula (o varias). Se debe tener en cuenta que la frase de contraseña distingue mayúsculas de minúsculas.
     - Un número (o varios).
     - Un carácter no alfanumérico, como !, *, @ (o varios).

     > **Asegúrese de grabar sus entradas para un uso posterior**. Si se necesita transferir una unidad con la función de seguridad habilitada de la cabina de almacenamiento, se debe conocer la frase de contraseña para desbloquear los datos de la unidad.

+

   - Si no desea crear una clave de backup, anule la selección de la casilla de comprobación.

> Tenga en cuenta que, si se pierde el acceso al servidor de claves externo y no existe una clave de backup, se perderá el acceso a los datos en las unidades si se migran a otra cabina de almacenamiento. Esta opción es el único método para crear una clave de backup en System Manager.

6. Haga clic en **Finalizar**.

   El sistema se conecta al servidor de gestión de claves con las credenciales introducidas. Luego, se almacena una copia de la clave de seguridad en el sistema local.

   > La ruta del archivo descargado podría depender de la ubicación predeterminada de las descargas del explorador.

7. Anote la frase de contraseña y la ubicación del archivo de claves descargado y, a continuación, haga clic en **Cerrar**.

   En la página, se muestra el siguiente mensaje con enlaces adicionales para la gestión de claves externas.

   ```
   Current key management method: External
   ```

8. Pruebe la conexión entre la cabina de almacenamiento y el servidor de gestión de claves. Para ello, seleccione **probar comunicación**.

   Los resultados de la prueba se muestran en el cuadro de diálogo.

Resultados

Cuando se habilita la gestión de claves externas, se pueden crear grupos de volúmenes o pools con la función de seguridad habilitada, o bien se puede habilitar la función de seguridad en los grupos de volúmenes y pools existentes.

> Cada vez que se apagan y se vuelven a encender las unidades, todas las unidades con la función de seguridad habilitada cambian al estado Security Locked. En este estado, no se puede acceder a los datos hasta que la controladora aplica la clave de seguridad correcta durante la inicialización de la unidad. Si alguien quita físicamente la unidad bloqueada y la instala en otro sistema, el estado Security Locked evita el acceso no autorizado de los datos.

Después de terminar

Debe validar la clave de seguridad para asegurarse de que no se haya dañado el archivo de claves.

Gestionar claves de seguridad

Cambiar clave de seguridad

Es posible reemplazar una clave de seguridad por una nueva en cualquier momento. Puede resultar necesario cambiar una clave de seguridad en aquellos casos en los que potencialmente se haya comprometido la seguridad en la empresa y en los que se desee garantizar que personal no autorizado no pueda acceder a los datos de las unidades.

Pasos

1. Seleccione MENU:Settings[System].

2. En **Gestión de claves de seguridad**, seleccione **Cambiar clave**.

   Se abre el cuadro de diálogo Cambiar clave de seguridad.

3. Introduzca información en los siguientes campos.
   - **Definir un identificador de clave de seguridad** — (sólo para claves de seguridad internas). Acepte el valor predeterminado (Marca de tiempo y nombre de la cabina de almacenamiento, que genera el firmware de la controladora) o introduzca un valor personalizado. Puede introducir hasta 189 caracteres alfanuméricos sin espacios, puntuación ni símbolos.

     > Se generan automáticamente caracteres adicionales y se agregan a ambos extremos de la cadena que introduce. Los caracteres generados ayudan a garantizar que el identificador sea único.

   - **Definir una frase de contraseña/Volver a introducir la frase de contraseña** — en cada uno de estos campos, introduzca la frase de contraseña. El valor puede tener entre 8 y 32 caracteres, y debe incluir uno de los siguientes caracteres:
     - Una letra mayúscula (o varias). Se debe tener en cuenta que la frase de contraseña distingue mayúsculas de minúsculas.
     - Un número (o varios).
     - Un carácter no alfanumérico, como !, *, @ (o varios).
4. Para las claves de seguridad externas, si desea eliminar la clave de seguridad antigua cuando se crea la nueva, seleccione la opción "Delete current Security key…" en la parte inferior del cuadro de diálogo.

   > **Asegúrese de registrar las entradas para uso posterior** — Si necesita mover una unidad con la función de seguridad habilitada de la cabina de almacenamiento, debe conocer el identificador y la frase de contraseña para desbloquear los datos de la unidad.

5. Haga clic en **Cambiar**.

   La clave de seguridad nueva sobrescribe la clave anterior, que ya no es válida.

   > La ruta del archivo descargado podría depender de la ubicación predeterminada de las descargas del explorador.

6. Anote el identificador de claves, la frase de la contraseña y la ubicación del archivo de claves descargado y, a continuación, haga clic en **Cerrar**.

Después de terminar

Debe validar la clave de seguridad para asegurarse de que no se haya dañado el archivo de claves.

Alternar de gestión de claves internas a externas

Se puede modificar el método de gestión de Drive Security de un servidor de claves externo a un método interno utilizado por la cabina de almacenamiento. La clave de seguridad definida previamente para la gestión de claves externas luego se utiliza para la gestión de claves internas.

Acerca de esta tarea

En esta tarea, se deshabilita la gestión de claves externas y se descarga una nueva copia de backup en el host local. La clave existente se sigue usando para Drive Security, pero se gestionará internamente en la cabina de almacenamiento.

Pasos

1. Seleccione MENU:Settings[System].
2. En **Gestión de claves de seguridad**, seleccione **Desactivar administración de claves externa**.

   Se abre el cuadro de diálogo Deshabilitar gestión de claves externa.

3. En **definir una frase de contraseña/Volver a introducir la frase de contraseña**, introduzca y confirme una frase de contraseña para el backup de la clave. El valor puede tener entre 8 y 32 caracteres, y debe incluir uno de los siguientes caracteres:

   - Una letra mayúscula (o varias). Se debe tener en cuenta que la frase de contraseña distingue mayúsculas de minúsculas.
   - Un número (o varios).
   - Un carácter no alfanumérico, como !, *, @ (o varios).

   > *Asegúrese de registrar las entradas para uso futuro*. Si se necesita transferir una unidad con la función de seguridad habilitada de la cabina de almacenamiento, se deben conocer el identificador y la frase de contraseña para desbloquear los datos de la unidad.

4. Haga clic en **Desactivar**.

   La clave de backup se descarga en el host local.

5. Anote el identificador de claves, la frase de la contraseña y la ubicación del archivo de claves descargado y, a continuación, haga clic en **Cerrar**.

Resultados

Drive Security ahora se gestiona internamente mediante la cabina de almacenamiento.

Después de terminar

Debe validar la clave de seguridad para asegurarse de que no se haya dañado el archivo de claves.

Editar configuración del servidor de gestión de claves

Si configuró la gestión de claves externas, es posible ver y editar los ajustes del servidor de gestión de claves en cualquier momento.

Pasos

1. Seleccione MENU:Settings[System].
2. En **Gestión de claves de seguridad**, seleccione **Ver/editar configuración del servidor de administración de claves**.
3. Edite la información en los siguientes campos:

   - **Dirección del servidor de administración de claves** — Introduzca el nombre de dominio completo o la dirección IP (IPv4 o IPv6) del servidor utilizado para la administración de claves.
   - **Número de puerto de administración de claves** — Introduzca el número de puerto utilizado para las comunicaciones del Protocolo de interoperabilidad de administración de claves (KMIP).

Opcional: puede incluir otro servidor de claves haciendo clic en **Agregar servidor de claves**.

4. Haga clic en **Guardar**.

Realice un backup de la clave de seguridad

Después de crear o de cambiar una clave de seguridad, es posible crear una copia de backup del archivo de claves en caso de que el original se dañe.

Acerca de esta tarea

En esta tarea, se describe cómo realizar un backup de la clave de seguridad creada previamente. Durante este procedimiento, es posible crear una nueva frase de contraseña para el backup. No es necesario que esta frase de contraseña coincida con la utilizada cuando se creó o se modificó por última vez la clave original. La frase de contraseña se aplica solo al backup que se va a crear.

Pasos

1. Seleccione MENU:Settings[System].
2. En **Gestión de claves de seguridad**, seleccione **clave de copia de seguridad**.

   Se abre el cuadro de diálogo realizar backup de la clave de seguridad.

3. En los campos **define a pass phrase/Re-enter pass phrase**, introduzca y confirme una frase de contraseña para este backup.

   El valor puede tener entre 8 y 32 caracteres, y debe incluir uno de los siguientes caracteres:

   - Una letra mayúscula (o varias)
   - Un número (o varios).
   - Un carácter no alfanumérico, como !, *, @ (o varios).

   Asegúrese de grabar su entrada para uso posterior. Necesita la frase de contraseña para acceder al backup de esta clave de seguridad.

4. Haga clic en **copia de seguridad**.

   Se descarga una copia de seguridad de la clave de seguridad en el host local y, a continuación, se abre el cuadro de diálogo **Confirmar/registrar copia de seguridad de la clave**.

   La ruta del archivo de claves de seguridad descargado puede depender de la ubicación de descarga predeterminada del explorador.

5. Registre la frase de contraseña en un lugar seguro y, a continuación, haga clic en **Cerrar**.

Después de terminar

Debe validar la clave de seguridad de backup.

Valide la clave de seguridad

Es posible validar la clave de seguridad para asegurarse de que no se haya dañado y verificar que tenga una frase de contraseña correcta.

Acerca de esta tarea

Esta tarea describe cómo validar la clave de seguridad que se creó anteriormente. Este es un paso importante para asegurarse de que el archivo de claves no esté dañado y que la frase de contraseña sea correcta. Esto permite acceder a datos de la unidad más adelante si se mueve una unidad con la función de seguridad habilitada de una cabina de almacenamiento a otra.

Pasos

1. Seleccione MENU:Settings[System].
2. En **Gestión de claves de seguridad**, seleccione **Validar clave**.

   Se abre el cuadro de diálogo Validar clave de seguridad.

3. Haga clic en **examinar** y, a continuación, seleccione el archivo de claves (por ejemplo, `drivesecurity.slk`).
4. Introduzca la frase de contraseña asociada con la clave que seleccionó.

   Al seleccionar un archivo de claves válido y una frase de contraseña, el botón **Validar** se vuelve disponible.

5. Haga clic en **Validar**.

   Los resultados de la validación se muestran en el cuadro de diálogo.

6. Si los resultados muestran que la clave de seguridad se validó correctamente, haga clic en **Cerrar**. Si aparece un mensaje de error, siga las instrucciones sugeridas que se muestran en el cuadro de diálogo.

Desbloquear unidades al utilizar la gestión de claves internas

Si se configuró la gestión de claves internas y luego se mueven unidades con la función de seguridad habilitada de una cabina de almacenamiento a otra, se debe volver a asignar la clave de seguridad a la nueva cabina de almacenamiento para acceder a los datos cifrados en las unidades.

Antes de empezar

- En la cabina de origen (la cabina donde se quitan las unidades), se exportaron los grupos de volúmenes y se quitaron las unidades. En la cabina objetivo, se deben volver a instalar las unidades.

  > La función Export/Import no se admite en la interfaz de usuario de System Manager. Se debe usar la interfaz de línea de comandos (CLI) para exportar o importar un grupo de volúmenes a otra cabina de almacenamiento.

  En la, se proporcionan instrucciones detalladas para migrar un grupo de volúmenes "Base de conocimientos de NetApp". Asegúrese de seguir las instrucciones adecuadas para las cabinas más recientes gestionadas por System Manager o para sistemas heredados.

- Se debe habilitar la función Drive Security. De lo contrario, se abre el cuadro de diálogo no puede crearse una clave de seguridad durante esta tarea. Si fuera necesario, comuníquese con el proveedor de almacenamiento para pedir indicaciones sobre cómo habilitar la función Drive Security.
- Debe conocer la clave de seguridad asociada con las unidades que desea desbloquear.
- El archivo de claves de seguridad está disponible en el cliente de gestión (el sistema con un explorador que se utilizó para acceder a System Manager). Si mueve las unidades a una cabina de almacenamiento

gestionada por otro sistema, debe mover el archivo de claves de seguridad a ese cliente de gestión.

Acerca de esta tarea

Cuando se utiliza la gestión de claves internas, la clave de seguridad se almacena de forma local en la cabina de almacenamiento. Una clave de seguridad es una cadena de caracteres que comparte la controladora y las unidades para acceso de lectura/escritura. Cuando las unidades se retiran físicamente de la cabina e instalan en otra, no pueden operar hasta que se ofrece la clave de seguridad correcta.

> Es posible crear una clave interna desde la memoria persistente de la controladora o una clave externa desde un servidor de gestión de claves. En este tema se describe cómo desbloquear datos cuando se utiliza la gestión de claves *internal*. Si utilizó *external* gestión de claves, consulte "Desbloquear unidades al utilizar gestión de claves externas". Si va a realizar una actualización de la controladora y va a intercambiar todas las controladoras por el hardware más reciente, debe seguir los pasos distintos que se describen en el centro de documentación de E-Series y SANtricity, en "Desbloquear unidades".

Una vez que se vuelven a instalar las unidades con la función de seguridad habilitada en otra cabina, esa cabina detecta las unidades y muestra la condición "Needs Attention" junto con el estado "Security Key Needed". Para desbloquear los datos de la unidad, se selecciona el archivo de claves de seguridad y se introduce la frase de contraseña para la clave. (Esta frase de contraseña no es la misma que la contraseña de administrador de la cabina de almacenamiento.)

Si se instalan otras unidades con la función de seguridad habilitada en la nueva cabina de almacenamiento, estas podrían usar una clave de seguridad distinta de la que se está importando. Durante el proceso de importación, la clave de seguridad antigua se usa únicamente para desbloquear los datos de las unidades que se instalan. Cuando el proceso de desbloqueo se realiza correctamente, se vuelve a asignar una clave de seguridad de cabina de almacenamiento de destino a las unidades recién instaladas.

Pasos

1. Seleccione MENU:Settings[System].
2. En **Gestión de claves de seguridad**, seleccione **Desbloquear unidades seguras**.

   Se abre el cuadro de diálogo Desbloquear unidades seguras. Todas las unidades que requieren una clave de seguridad se muestran en la tabla.

3. **Opcional:** pase el ratón sobre un número de unidad para ver la ubicación de la unidad (número de bandeja y número de bahía).
4. Haga clic en **examinar** y, a continuación, seleccione el archivo de claves de seguridad correspondiente a la unidad que desea desbloquear.

   El archivo de claves seleccionado aparece en el cuadro de diálogo.

5. Introduzca la frase de contraseña asociada con este archivo de claves.

   Los caracteres introducidos están enmascarados.

6. Haga clic en **Desbloquear**.

   Si la operación de desbloqueo se realiza correctamente, en el cuadro de diálogo se muestra un mensaje que indica que se desbloquearon las unidades seguras asociadas.

Resultados

Cuando todas las unidades se bloquean y después se desbloquean, se reinicia cada controladora de la cabina

de almacenamiento. Sin embargo, si ya existen algunas unidades desbloqueadas en la cabina de almacenamiento de destino, las controladoras no se reinician.

Después de terminar

En la cabina de destino (la cabina con las unidades recién instaladas), ahora es posible importar grupos de volúmenes.

> La función Export/Import no se admite en la interfaz de usuario de System Manager. Se debe usar la interfaz de línea de comandos (CLI) para exportar o importar un grupo de volúmenes a otra cabina de almacenamiento.

En la, se proporcionan instrucciones detalladas para migrar un grupo de volúmenes "Base de conocimientos de NetApp".

Desbloquear unidades al utilizar gestión de claves externas

Si se configuró la gestión de claves externas y luego se mueven unidades con la función de seguridad habilitada de una cabina de almacenamiento a otra, se debe volver a asignar la clave de seguridad a la nueva cabina de almacenamiento para acceder a los datos cifrados en las unidades.

Antes de empezar

- En la cabina de origen (la cabina donde se quitan las unidades), se exportaron los grupos de volúmenes y se quitaron las unidades. En la cabina objetivo, se deben volver a instalar las unidades.

  > La función Export/Import no se admite en la interfaz de usuario de System Manager. Se debe usar la interfaz de línea de comandos (CLI) para exportar o importar un grupo de volúmenes a otra cabina de almacenamiento.

  En la, se proporcionan instrucciones detalladas para migrar un grupo de volúmenes "Base de conocimientos de NetApp". Asegúrese de seguir las instrucciones adecuadas para las cabinas más recientes gestionadas por System Manager o para sistemas heredados.

- Se debe habilitar la función Drive Security. De lo contrario, se abre el cuadro de diálogo no puede crearse una clave de seguridad durante esta tarea. Si fuera necesario, comuníquese con el proveedor de almacenamiento para pedir indicaciones sobre cómo habilitar la función Drive Security.
- Debe conocer la dirección IP y el número de puerto del servidor de gestión de claves.
- Posee un archivo de certificado de cliente firmado para las controladoras de la cabina de almacenamiento y copió ese archivo en el host donde se accede a System Manager. Un certificado de cliente valida las controladoras de la cabina de almacenamiento para que el servidor de gestión de claves pueda confiar en sus solicitudes de protocolo de interoperabilidad de gestión de claves (KMIP).
- Debe recuperar un archivo de certificado del servidor de gestión de claves y, a continuación, copiar ese archivo en el host donde va a acceder a System Manager. Un certificado de servidor de gestión de claves valida el servidor de gestión de claves para que la cabina de almacenamiento pueda confiar en su dirección IP. Es posible usar un certificado raíz, intermedio o de servidor para el servidor de gestión de claves.

> Si desea obtener más información sobre el certificado de servidor, consulte la documentación del servidor de gestión de claves.

Acerca de esta tarea

Cuando se utiliza gestión de claves externas, la clave de seguridad se almacena externamente en un servidor diseñado para proteger claves de seguridad. Una clave de seguridad es una cadena de caracteres que comparte la controladora y las unidades para acceso de lectura/escritura. Cuando las unidades se retiran físicamente de la cabina e instalan en otra, no pueden operar hasta que se ofrece la clave de seguridad correcta.

> Es posible crear una clave interna desde la memoria persistente de la controladora o una clave externa desde un servidor de gestión de claves. En este tema se describe cómo desbloquear datos cuando se utiliza la gestión de claves *external*. Si utilizó la gestión de claves *interno*, consulte "Desbloquear unidades al utilizar la gestión de claves internas". Si va a realizar una actualización de la controladora y va a intercambiar todas las controladoras por el hardware más reciente, debe seguir los pasos distintos que se describen en el centro de documentación de E-Series y SANtricity, en "Desbloquear unidades".

Una vez que se vuelven a instalar las unidades con la función de seguridad habilitada en otra cabina, esa cabina detecta las unidades y muestra la condición "Needs Attention" junto con el estado "Security Key Needed". Para desbloquear los datos de la unidad, se debe importar el archivo de claves de seguridad y introducir la frase de contraseña para la clave. (Esta frase de contraseña no es la misma que la contraseña de administrador de la cabina de almacenamiento.) Durante este proceso, es posible configurar la cabina de almacenamiento para que use un servidor de gestión de claves externo y, luego, será posible acceder a la clave segura. Se requiere proporcionar información de contacto del servidor para que la cabina de almacenamiento pueda conectarse y recuperar la clave de seguridad.

Si se instalan otras unidades con la función de seguridad habilitada en la nueva cabina de almacenamiento, estas podrían usar una clave de seguridad distinta de la que se está importando. Durante el proceso de importación, la clave de seguridad antigua se usa únicamente para desbloquear los datos de las unidades que se instalan. Cuando el proceso de desbloqueo se realiza correctamente, se vuelve a asignar una clave de seguridad de cabina de almacenamiento de destino a las unidades recién instaladas.

Pasos

1. Seleccione MENU:Settings[System].
2. En **Gestión de claves de seguridad**, seleccione **Crear clave externa**.
3. Complete el asistente con la información de conexión de requisitos previos y los certificados.
4. Haga clic en **probar comunicación** para garantizar el acceso al servidor de administración de claves externo.
5. Seleccione **Desbloquear unidades seguras**.

   Se abre el cuadro de diálogo Desbloquear unidades seguras. Todas las unidades que requieren una clave de seguridad se muestran en la tabla.

6. **Opcional:** pase el ratón sobre un número de unidad para ver la ubicación de la unidad (número de bandeja y número de bahía).
7. Haga clic en **examinar** y, a continuación, seleccione el archivo de claves de seguridad correspondiente a la unidad que desea desbloquear.

   El archivo de claves seleccionado aparece en el cuadro de diálogo.

8. Introduzca la frase de contraseña asociada con este archivo de claves.

   Los caracteres introducidos están enmascarados.

9. Haga clic en **Desbloquear**.

   Si la operación de desbloqueo se realiza correctamente, en el cuadro de diálogo se muestra un mensaje que indica que se desbloquearon las unidades seguras asociadas.

Resultados

Cuando todas las unidades se bloquean y después se desbloquean, se reinicia cada controladora de la cabina de almacenamiento. Sin embargo, si ya existen algunas unidades desbloqueadas en la cabina de almacenamiento de destino, las controladoras no se reinician.

Después de terminar

En la cabina de destino (la cabina con las unidades recién instaladas), ahora es posible importar grupos de volúmenes.

> La función Export/Import no se admite en la interfaz de usuario de System Manager. Se debe usar la interfaz de línea de comandos (CLI) para exportar o importar un grupo de volúmenes a otra cabina de almacenamiento.

En la, se proporcionan instrucciones detalladas para migrar un grupo de volúmenes "Base de conocimientos de NetApp".

Preguntas frecuentes

¿Qué debo saber antes de crear una clave de seguridad?

Las controladoras y unidades con seguridad habilitada comparten una clave de seguridad dentro de una cabina de almacenamiento. Si se quita una unidad con la función de seguridad habilitada de la cabina de almacenamiento, la clave de seguridad protege los datos de un acceso no autorizado.

Puede crear y gestionar claves de seguridad mediante uno de los siguientes métodos:

- Gestión de claves internas en la memoria persistente de la controladora.
- Gestión de claves externas en un servidor de gestión de claves externo.

Gestión de claves internas

Se mantienen las claves internas y se «"ocultan"» en una ubicación sin acceso en la memoria persistente de la controladora. Antes de crear una clave de seguridad interna, debe hacer lo siguiente:

1. Instale unidades compatibles con la función de seguridad en la cabina de almacenamiento. Estas unidades pueden ser de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS).
2. Asegúrese de que la función Drive Security esté habilitada. Si fuera necesario, comuníquese con el proveedor de almacenamiento para pedir indicaciones sobre cómo habilitar la función Drive Security.

Luego, podrá crear una clave de seguridad interna, lo que implica definir un identificador y una frase de contraseña. El identificador es una frase que está asociada con la clave de seguridad, y se almacena en la controladora y en todas las unidades asociadas con la clave. La frase de contraseña se utiliza para cifrar la clave de seguridad con fines de backup. Una vez que haya terminado, la clave de seguridad se almacena en una ubicación no accesible de la controladora. Es posible crear grupos de volúmenes o pools con la función

de seguridad habilitada, o bien habilitar la seguridad en grupos de volúmenes o pools existentes.

Gestión de claves externas

Las claves externas se mantienen en un servidor de gestión de claves individual mediante un protocolo de interoperabilidad de gestión de claves (KMIP). Antes de crear una clave de seguridad externa, debe hacer lo siguiente:

1. Instale unidades compatibles con la función de seguridad en la cabina de almacenamiento. Estas unidades pueden ser de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS).
2. Asegúrese de que la función Drive Security esté habilitada. Si fuera necesario, comuníquese con el proveedor de almacenamiento para pedir indicaciones sobre cómo habilitar la función Drive Security.
3. Obtener un archivo de certificado de cliente firmado. Un certificado de cliente valida las controladoras de la cabina de almacenamiento para que el servidor de gestión de claves pueda confiar en sus solicitudes KMIP.
   a. En primer lugar, complete y descargue una solicitud de firma de certificación (CSR) de cliente. Vaya a menú:Configuración[certificados > Gestión de claves > completar CSR].
   b. A continuación, se solicita un certificado de cliente firmado de una CA de confianza para el servidor de gestión de claves. (También se puede crear y descargar un certificado de cliente desde el servidor de gestión de claves con el archivo CSR descargado).
   c. Una vez que tenga un archivo de certificado de cliente, copie ese archivo en el host en el que accede a System Manager.
4. Recupere un archivo de certificado del servidor de gestión de claves y copie ese archivo en el host donde accede a System Manager. Un certificado de servidor de gestión de claves valida el servidor de gestión de claves para que la cabina de almacenamiento pueda confiar en su dirección IP. Es posible usar un certificado raíz, intermedio o de servidor para el servidor de gestión de claves.

Luego, podrá crear una clave externa, lo que implica definir la dirección IP del servidor de gestión de claves y el número de puerto para las comunicaciones KMIP. Durante este proceso, también debe cargar los archivos de certificado. Una vez que haya terminado, el sistema se conecta al servidor de gestión de claves con las credenciales introducidas. Es posible crear grupos de volúmenes o pools con la función de seguridad habilitada, o bien habilitar la seguridad en grupos de volúmenes o pools existentes.

¿Por qué debo definir una frase de contraseña?

La frase de contraseña se utiliza para cifrar y descifrar el archivo de claves de seguridad almacenado en el cliente de gestión local. Sin la frase de contraseña, la clave de seguridad no se puede descifrar y utilizar para desbloquear datos de una unidad con la función de seguridad habilitada, si se la reinstala en otra cabina de almacenamiento.

¿Por qué es importante registrar la información de claves de seguridad?

Si pierde la información de la clave de seguridad y no cuenta con un backup, podría perder los datos al reubicar las unidades con la función de seguridad habilitada o actualizar una controladora. La clave de seguridad es necesaria para desbloquear los datos en las unidades.

Asegúrese de registrar el identificador de la clave de seguridad, la frase de contraseña asociada y la ubicación en el host local en donde se guardó el archivo de claves de seguridad.

¿Qué debo saber antes de realizar un backup de una clave de seguridad?

Si la clave de seguridad original se daña y no existe un backup, se perderá el acceso a los datos de las unidades al migrarlas de una cabina de almacenamiento a otra.

Antes de realizar el backup de una clave de seguridad, tenga en cuenta las siguientes directrices:

- Asegúrese de conocer el identificador de claves de seguridad y la frase de contraseña del archivo de claves original.

> Solo las claves internas usan identificadores. Cuando se crea el identificador, se crean caracteres adicionales que se anexan automáticamente a ambos extremos de la cadena del identificador. Los caracteres generados garantizan que el identificador sea único.

- Es posible crear una frase de contraseña nueva para el backup. No es necesario que esta frase de contraseña coincida con la utilizada cuando se creó o se modificó por última vez la clave original. La frase de contraseña solo se aplica al backup que se crea.

> La frase de contraseña para Drive Security no debería confundirse con la contraseña del administrador de la cabina de almacenamiento. La frase de contraseña para Drive Security protege los backups de una clave de seguridad. La contraseña del administrador protege toda la cabina de almacenamiento de un acceso no autorizado.

- El archivo de claves de seguridad de backup se descarga en el cliente de gestión. La ruta del archivo descargado podría depender de la ubicación predeterminada de las descargas del explorador. Asegúrese de registrar dónde se almacena la información de la clave de seguridad.

¿Qué debo saber antes de desbloquear unidades seguras?

Para desbloquear los datos de una unidad con la función de seguridad habilitada, se debe importar la clave de seguridad.

Antes de desbloquear unidades con la función de seguridad habilitada, recuerde las siguientes directrices:

- La cabina de almacenamiento ya debe tener una clave de seguridad. Las unidades migradas se volverán a asignar una clave a la cabina de almacenamiento objetivo.
- Para las unidades que se van a migrar, se deben conocer el identificador de la clave de seguridad y la frase de contraseña que corresponden al archivo de claves de seguridad.
- El archivo de claves de seguridad debe estar disponible en el cliente de gestión (el sistema con un explorador que se utilizó para acceder a System Manager).
- Si va a restablecer una unidad NVMe bloqueada, debe introducir el identificador de seguridad de la unidad. Para ubicarlo, retire físicamente la unidad y busque la cadena de PSID (máximo de 32 caracteres) en la etiqueta de la unidad. Asegúrese de reinstalar la unidad antes de iniciar la operación.

¿Qué es la accesibilidad de lectura/escritura?

La ventana Configuración de la unidad incluye información acerca de los atributos de seguridad de la unidad. "Read/Write Accessible" es uno de los atributos que se muestran si se bloquearon los datos de una unidad.

Para ver los atributos de Drive Security, vaya a la página hardware. Seleccione una unidad, haga clic en **Ver**

configuración y, a continuación, haga clic en **Mostrar más valores**. En la parte inferior de la página, el valor del atributo Accesibilidad de lectura/escritura será **Sí** cuando la unidad esté desbloqueada. El valor del atributo Accesibilidad de lectura/escritura es **no, clave de seguridad no válida** cuando la unidad está bloqueada. Si desea desbloquear una unidad segura, importe una clave de seguridad (vaya a menú:Configuración[sistema > Desbloquear unidades seguras]).

¿Qué debo saber acerca de la validación de la clave de seguridad?

Después de crear una clave de seguridad, se debe validar el archivo de claves para garantizar que no esté dañado.

Si la validación falla, haga lo siguiente:

- Si el identificador de claves de seguridad no coincide con el identificador de la controladora, busque el archivo de claves de seguridad correcto y vuelva a intentar hacer la validación.
- Si la controladora no puede descifrar la clave de seguridad para la validación, es posible que haya introducido incorrectamente la frase de contraseña. Haga doble clic en la frase de contraseña, vuelva a introducirla si fuera necesario y vuelva a intentar hacer la validación. Si vuelve a aparecer el mensaje de error, seleccione un backup del archivo de claves (si estuviera disponible) y vuelva a intentar hacer la validación.
- Si aún no puede validar la clave de seguridad, es posible que el archivo original esté dañado. Cree un backup nuevo de la clave y valide esa copia.

¿Cuál es la diferencia entre la gestión de claves de seguridad interna y de claves de seguridad externa?

Cuando se implementa la función Drive Security, es posible utilizar una clave de seguridad interna o una clave de seguridad externa para bloquear los datos cuando se quita una unidad con la función de seguridad habilitada de la cabina de almacenamiento.

Una clave de seguridad es una cadena de caracteres, que se comparte entre las unidades y controladoras con la función de seguridad habilitada en una cabina de almacenamiento. Las claves internas se conservan en la memoria persistente de la controladora. Las claves externas se mantienen en un servidor de gestión de claves individual mediante un protocolo de interoperabilidad de gestión de claves (KMIP).

Gestión del acceso

Información general de Access Management

Access Management es un método para establecer la autenticación de usuario en System Manager.

¿Qué métodos de autenticación están disponibles?

Los métodos de autenticación incluyen el control de acceso basado en roles (RBAC), los servicios de directorio y el lenguaje de marcado de aserción de seguridad (SAML):

- **RBAC/roles de usuario local** — la autenticación se gestiona a través de capacidades RBAC aplicadas en la cabina de almacenamiento. Los roles de usuario local incluyen perfiles de usuario predefinidos con permisos de acceso específicos.
- **Servicios de directorio** — la autenticación se administra a través de un servidor LDAP (protocolo ligero

de acceso a directorios) y servicios de directorio, como Active Directory de Microsoft.

- **SAML** — la autenticación se gestiona a través de un proveedor de identidades (IDP) que utiliza SAML 2.0.

Obtenga más información:

- "Cómo funciona Access Management"
- "Terminología de Access Management"
- "Permisos para roles asignados"
- "Roles de usuario local"
- "Servicios de directorio"
- "SAML"

¿Cómo se configura la autenticación?

La cabina de almacenamiento está preconfigurada para utilizar roles de usuario local, que son una implementación de capacidades RBAC. Si desea configurar un método diferente, vaya al menú:Configuración[Access Management].

Obtenga más información:

- "Añadir servidor de directorio LDAP"
- "Configure SAML"

Información relacionada

Obtenga más información sobre tareas relacionadas con la gestión del acceso:

- "Cambiar contraseñas"
- "Ver actividad de registro de auditoría"
- "Configurar servidores de syslog para registros de auditoría"

Conceptos

Cómo funciona Access Management

Access Management es un método para establecer la autenticación de usuario en System Manager.

La configuración y la autenticación de usuarios funcionan de la siguiente manera:

1. Un administrador inicia sesión en System Manager con un perfil de usuario que incluye permisos de administración de seguridad.

   > La primera vez que se inicia sesión, el nombre de usuario `admin` se muestra automáticamente y no se puede cambiar. La `admin` el usuario tiene acceso completo a todas las funciones del sistema.

2. El administrador navega hasta Access Management en la interfaz de usuario. La cabina de almacenamiento está preconfigurada para utilizar roles de usuario local, que son una implementación de

capacidades RBAC (control de acceso basado en roles).

3. El administrador configura uno o varios de los siguientes métodos de autenticación:
   - **Roles de usuario local** — la autenticación se gestiona a través de capacidades RBAC aplicadas en la cabina de almacenamiento. Los roles de usuario local incluyen perfiles de usuario predefinidos con permisos de acceso específicos. Los administradores pueden usar estos roles de usuario local como el único método de autenticación o usarlos en combinación con un servicio de directorio. No hace falta configurar nada más allá de las contraseñas de los usuarios.
   - **Servicios de directorio** — la autenticación se administra a través de un servidor LDAP (protocolo ligero de acceso a directorios) y un servicio de directorio, como Active Directory de Microsoft. Un administrador se conecta con el servidor LDAP y luego asigna los usuarios LDAP a los roles de usuario local integrados en la cabina de almacenamiento.
   - **SAML** — la autenticación se gestiona a través de un proveedor de identidades (IDP) utilizando el lenguaje de marcado de aserción de seguridad (SAML) 2.0. Un administrador establece comunicación entre el sistema IDP y la cabina de almacenamiento, y luego asigna los usuarios IDP a los roles de usuario local integrados en la cabina de almacenamiento.
4. El administrador ofrece credenciales de inicio de sesión en System Manager para los usuarios.
5. Los usuarios inician sesión en el sistema con sus credenciales.

   > Si la autenticación se gestiona con SAML y un SSO (inicio de sesión único), el sistema puede omitir el diálogo de inicio de sesión de System Manager.

   Durante el inicio de sesión, el sistema realiza las siguientes tareas en segundo plano:

   - Autentica el nombre de usuario y la contraseña en relación con la cuenta de usuario.
   - Determina los permisos del usuario según los roles asignados.
   - Ofrece acceso al usuario a las tareas en la interfaz de usuario.
   - Muestra el nombre de usuario en la esquina superior derecha de la interfaz.

Tareas disponibles en System Manager

El acceso a las tareas depende de los roles asignados a un usuario, entre los cuales se encuentran los siguientes:

- **Storage admin** — acceso completo de lectura/escritura a los objetos de almacenamiento (por ejemplo, volúmenes y pools de discos), pero sin acceso a la configuración de seguridad.
- **Administración de seguridad** — acceso a la configuración de seguridad en Access Management, administración de certificados, administración de registros de auditoría y la capacidad de activar o desactivar la interfaz de administración heredada (Symbol).
- **Support admin** — acceso a todos los recursos de hardware en la cabina de almacenamiento, datos de fallos, eventos MEL y actualizaciones del firmware de la controladora. No brinda acceso a los objetos de almacenamiento ni a la configuración de seguridad.
- **Monitor** — acceso de sólo lectura a todos los objetos de almacenamiento, pero sin acceso a la configuración de seguridad.

Una tarea no disponible está atenuada o no aparece en la interfaz de usuario. Por ejemplo, un usuario con el rol de supervisión puede ver toda la información sobre los volúmenes, pero no puede acceder a funciones para modificarlos. Las pestañas para funciones como **Servicios de copia** y **Agregar a carga de trabajo** estarán atenuadas; sólo **Ver/Editar configuración** está disponible.

Limitaciones en Unified Manager y Storage Manager

Si se configura SAML para una cabina de almacenamiento, los usuarios no pueden detectar ni gestionar el almacenamiento de esa cabina desde las interfaces de Unified Manager o heredada de Storage Manager.

Cuando se configuran los roles de usuario local y los servicios de directorio, los usuarios deben introducir credenciales para poder realizar cualquiera de las siguientes funciones:

- Cambiar el nombre de la cabina de almacenamiento
- Actualizar el firmware de la controladora
- Cargar una configuración de la cabina de almacenamiento
- Ejecutar un script
- Intentar realizar una operación activa cuando se agotó el tiempo de espera de una sesión no utilizada

Terminología de Access Management

Conozca la forma en que los términos de Access Management se aplican a su cabina de almacenamiento.

Duración	Descripción
Token de acceso	Los tokens de acceso se utilizan para la autenticación con la API DE REST o la interfaz de línea de comandos (CLI) en lugar de un nombre de usuario y una contraseña. Los tokens están asociados a un usuario específico (incluidos los usuarios LDAP) e incluyen un conjunto de permisos y una caducidad.
Active Directory	Active Directory (AD) es un servicio de directorio de Microsoft en el que se utiliza LDAP para redes de dominio de Windows.
Vinculación	Las operaciones de vinculación se usan para autenticar clientes en el servidor de directorio. Por lo general, la vinculación requiere credenciales de cuenta y contraseña, pero algunos servidores aceptan operaciones de vinculación anónimas.
APROX	Una entidad de certificación (CA) es una entidad de confianza que emite documentos electrónicos, denominados certificados digitales, para la seguridad de Internet. Estos certificados identifican a los propietarios de sitios web y, de esta manera, permiten conexiones seguras entre clientes y servidores.
Certificado	Un certificado identifica al propietario de un sitio con el fin de brindar seguridad, para evitar que atacantes se hagan pasar por los propietarios del sitio. El certificado tiene información acerca del propietario del sitio y la identidad de la entidad de confianza que certifica (firma) esta información.
IDP	Un proveedor de identidades (IDP) es un sistema externo que se usa para solicitar credenciales a un usuario y para determinar si el usuario se autentica correctamente. El IDP se puede configurar para ofrecer autenticación multifactor y para usar cualquier base de datos de usuario, como Active Directory. El equipo de seguridad es responsable de mantener el IDP.

Duración	Descripción
LDAP	El protocolo ligero de acceso a directorios (LDAP) es un protocolo de aplicación para acceder a servicios distribuidos de información de directorio y mantenerlos. Este protocolo permite que varias aplicaciones y servicios se conecten con el servidor LDAP para validar usuarios.
RBAC	El control de acceso basado en funciones (RBAC) es un método para regular el acceso a los recursos informáticos o de red en función de las funciones de los usuarios individuales. Los controles de RBAC se aplican en la cabina de almacenamiento y se componen de roles predefinidos.
SAML	El lenguaje de marcado de aserción de seguridad (SAML) es un estándar basado en XML para fines de autenticación y autorización entre dos entidades. SAML permite utilizar la autenticación multifactor, en la cual los usuarios deben introducir dos o más elementos para validar su identidad (por ejemplo, una contraseña y una huella digital). La función de SAML integrada de la cabina de almacenamiento es compatible con SAML2.0 para autenticación, autorización y confirmación de identidades.
SP	Un proveedor de servicios (SP) es un sistema que controla la autenticación y el acceso de usuario. Cuando se configura Access Management con SAML, la cabina de almacenamiento actúa como proveedor de servicios, ya que solicita la autenticación del proveedor de identidades.
SSO	El inicio de sesión único (SSO) es un servicio de autenticación que permite el uso de un conjunto de credenciales de inicio de sesión para acceder a varias aplicaciones.

Permisos para roles asignados

Las capacidades de RBAC (control de acceso basado en roles) presentes en la cabina de almacenamiento incluyen perfiles de usuario predefinidos con uno o varios roles asignados. Cada rol incluye permisos para acceder a tareas en System Manager.

Puede accederse a los perfiles de usuario y a los roles asignados desde el menú:Configuración[Access Management > roles de usuario local] desde la interfaz de usuario de cualquier System Manager.

Los roles permiten que los usuarios accedan a tareas de la siguiente manera:

- **Storage admin** — acceso completo de lectura/escritura a los objetos de almacenamiento (por ejemplo, volúmenes y pools de discos), pero sin acceso a la configuración de seguridad.
- **Administración de seguridad** — acceso a la configuración de seguridad en Access Management, administración de certificados, administración de registros de auditoría y la capacidad de activar o desactivar la interfaz de administración heredada (Symbol).
- **Support admin** — acceso a todos los recursos de hardware en la cabina de almacenamiento, datos de fallos, eventos MEL y actualizaciones del firmware de la controladora. No brinda acceso a los objetos de almacenamiento ni a la configuración de seguridad.
- **Monitor** — acceso de sólo lectura a todos los objetos de almacenamiento, pero sin acceso a la configuración de seguridad.

Si un usuario no tiene permisos para determinada tarea, la tarea aparece atenuada o directamente no aparece en la interfaz de usuario.

Access Management con roles de usuario local

Para Access Management, los administradores pueden usar las capacidades RBAC (control de acceso basado en roles) aplicadas en la cabina de almacenamiento. Estas capacidades se denominan "roles de usuario local".

Flujo de trabajo de configuración

Los roles de usuario local están preconfigurados para la cabina de almacenamiento. Para usar roles de usuario local con fines de autenticación, los administradores pueden hacer lo siguiente:

1. Un administrador inicia sesión en System Manager con un perfil de usuario que incluye permisos de administración de seguridad.

   La `admin` el usuario tiene acceso completo a todas las funciones del sistema.

2. Un administrador revisa los perfiles de usuario, que están predefinidos y no pueden modificarse.
3. De manera opcional, el administrador asigna nuevas contraseñas para cada perfil de usuario.
4. Los usuarios inician sesión en el sistema con las credenciales asignadas.

Gestión

Al utilizar solamente los roles de usuario local para la autenticación, los administradores pueden realizar las siguientes tareas de gestión:

- Cambiar contraseñas.
- Configurar la longitud mínima de las contraseñas.
- Permitir que los usuarios inicien sesión sin contraseñas.

Access Management con servicios de directorio

Para Access Management, los administradores puede usar un servidor LDAP (protocolo ligero de acceso a directorios) y un servicio de directorios, como Active Directory de Microsoft.

Flujo de trabajo de configuración

Si se utilizan un servidor LDAP y un servicio de directorio en la red, la configuración opera de la siguiente manera:

1. Un administrador inicia sesión en System Manager con un perfil de usuario que incluye permisos de administración de seguridad.

   La `admin` el usuario tiene acceso completo a todas las funciones del sistema.

2. El administrador introduce los ajustes de configuración del servidor LDAP. Entre ellas se encuentran el nombre de dominio, la URL y la información de la cuenta vinculada.

3. Si el servidor LDAP utiliza un protocolo seguro (LDAPS), el administrador carga una cadena de certificados de Certificate Authority (CA) para la autenticación entre el servidor LDAP y la cabina de almacenamiento.
4. Después de establecer la conexión del servidor, el administrador asigna los grupos de usuarios a los roles de la cabina de almacenamiento. Estos roles están predefinidos y no pueden modificarse.
5. El administrador prueba la conexión entre el servidor LDAP y la cabina de almacenamiento.
6. Los usuarios inician sesión en el sistema con las credenciales de LDAP/servicios de directorio asignadas.

Gestión

Al utilizar los servicios de directorio para la autenticación, los administradores pueden realizar las siguientes tareas de gestión:

- Añadir servidor de directorio.
- Editar la configuración del servidor de directorio.
- Asignar usuarios LDAP a roles de usuario local.
- Quitar un servidor de directorio.

Access Management con SAML

Para Access Management, los administradores pueden usar las funcionalidades de lenguaje de marcado de aserción de seguridad (SAML) 2.0 que están integradas en la cabina.

Flujo de trabajo de configuración

La configuración de SAML funciona de la siguiente manera:

1. Un administrador inicia sesión en System Manager con un perfil de usuario que incluye permisos de administración de seguridad.

   > La `admin` El usuario tiene acceso completo a todas las funciones en System Manager.

2. El administrador se dirige a la ficha **SAML** de Access Management.
3. Un administrador configura las comunicaciones con el proveedor de identidades (IDP). Un IDP es un sistema externo que se usa para solicitar credenciales a un usuario y determinar si el usuario se autentica correctamente. Para configurar las comunicaciones con la cabina de almacenamiento, el administrador descarga el archivo de metadatos de IDP desde el sistema IDP y luego usa System Manager para cargarlo a la cabina de almacenamiento.
4. Un administrador establece una relación de confianza entre el proveedor de servicios y el IDP. Un proveedor de servicios controla la autorización de usuarios; en este caso, la controladora en la cabina de almacenamiento actúa como proveedor de servicios. Para configurar las comunicaciones, el administrador usa System Manager para exportar el archivo de metadatos del proveedor de servicios en cada controladora. Desde el sistema IDP, el administrador importa estos archivos de metadatos al IDP.

   > Los administradores también deben asegurarse de que el IDP admite la capacidad para obtener un ID de nombre en el momento de la autenticación.

5. El administrador asigna los roles de la cabina de almacenamiento a los atributos de usuario definidos en el

IDP. Para hacerlo, el administrador usa System Manager y crea las asignaciones.

6. El administrador prueba el inicio de sesión de SSO en la URL del IDP. Esta prueba garantiza que la cabina de almacenamiento y el IDP puedan comunicarse.

> Una vez que se habilita SAML, _no se puede deshabilitar desde la interfaz de usuario, tampoco se puede editar desde la configuración de IDP. Si necesita deshabilitar o editar la configuración de SAML, comuníquese con el soporte técnico para obtener ayuda.

7. En System Manager, el administrador del sistema habilita SAML para la cabina de almacenamiento.
8. Los usuarios inician sesión en el sistema con sus credenciales de SSO.

Gestión

Cuando se usa SAML con fines de autenticación, los administradores pueden realizar las siguientes tareas de administración:

- Modifique o cree nuevas asignaciones de roles
- Exporte los archivos del proveedor de servicios

Restricciones de acceso

Cuando se habilita SAML, los usuarios no pueden detectar ni gestionar el almacenamiento de esa cabina desde Unified Manager o la interfaz de Storage Manager heredada.

Además, los siguientes clientes no pueden obtener acceso a los recursos y los servicios de la cabina de almacenamiento:

- Enterprise Management Window (EMW)
- Interfaz de línea de comandos (CLI)
- Clientes de kits de desarrollo de software (SDK)
- Clientes en banda
- Clientes HTTP de la API de REST de autenticación básica
- Inicio de sesión mediante extremo estándar de la API de REST

Tokens de acceso

Los tokens de acceso proporcionan un método de autenticación con la API REST o la interfaz de línea de comandos (CLI), sin exponer los nombres de usuario ni las contraseñas. Un token está asociado a un usuario específico (incluidos los usuarios LDAP) e incluye un conjunto de permisos y una caducidad.

Acceso al token web SAML y JSON

De manera predeterminada, un sistema con SAML habilitado no permite el acceso a herramientas de línea de comandos tradicionales. La API REST y la interfaz de línea de comandos se tornan inoperables porque el flujo de trabajo de la MFA requiere un redireccionamiento a un servidor de proveedor de identidades para la autenticación. Por lo tanto, debe generar tokens en System Manager, que obliga a los usuarios a autenticarse a través de MFA.

No es necesario habilitar SAML para usar tokens web, pero SAML se recomienda para el nivel más alto de seguridad.

Flujo de trabajo para crear y utilizar tokens

1. Cree un token en System Manager y determine su vencimiento.
2. Copie el texto del token en el portapapeles o descárguelo en un archivo y, a continuación, guarde el texto del token en una ubicación segura.
3. Utilice el token de la siguiente manera:
   - **API REST**: Para utilizar un token en una solicitud de API REST, agregue un encabezado HTTP a sus solicitudes. Por ejemplo:
     `Authorization: Bearer <access-token-value>`
   - **Secure CLI**: Para utilizar un token en la CLI, agregue el valor de token en la línea de comandos o utilice la ruta de acceso a un archivo que contenga el valor de token. Por ejemplo:
     - Valor de token en la línea de comandos: `-t access-token-value`
     - Ruta de acceso a un archivo que contiene el valor de token: `-T access-token-file`

Obtenga más información:

- "Cree tokens de acceso"
- "Edite los tokens de acceso"
- "Revocar tokens de acceso"

Use los roles de usuario local

Ver los roles de usuario local

Desde la pestaña roles de usuario local, es posible ver las asignaciones de los perfiles de usuario a los roles predeterminados. Estas asignaciones forman parte de los controles de acceso basados en roles (RBAC) aplicados en la cabina de almacenamiento.

Antes de empezar

Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.

Acerca de esta tarea

Los perfiles de usuario y las asignaciones no pueden cambiarse. Solo las contraseñas pueden modificarse.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la ficha **roles de usuario local**.

   Los perfiles de usuario se muestran en la tabla:

   - **Administrador raíz** (admin) — Super administrador que tiene acceso a todas las funciones del sistema. Este perfil de usuario incluye todos los roles.

- **Administrador de almacenamiento** (almacenamiento) — el administrador responsable de todo el aprovisionamiento de almacenamiento. Este perfil de usuario incluye los siguientes roles: Administrador de almacenamiento, administrador de soporte y Supervisión.
- **Administración de seguridad** (seguridad): El usuario responsable de la configuración de seguridad, incluidas la administración de acceso, la administración de certificados y las funciones de unidad con seguridad habilitada. Este perfil de usuario incluye los siguientes roles: Administrador de seguridad y Supervisión.
- **Support admin** (asistencia técnica) — el usuario responsable de recursos de hardware, datos de fallos y actualizaciones de firmware. Este perfil de usuario incluye los siguientes roles: Support Admin y Supervisión.
- **Monitor** (monitor) — un usuario con acceso de sólo lectura al sistema. Este perfil de usuario incluye únicamente el rol Supervisión.

Cambiar contraseñas

Es posible cambiar las contraseñas de usuario de cada perfil de usuario desde Access Management.

Antes de empezar

- Inició sesión como administrador local, lo que incluye permisos de administrador raíz.
- Debe conocer la contraseña de administrador local.

Acerca de esta tarea

Tenga en cuenta estas directrices al elegir una contraseña:

- Todas las contraseñas de usuarios locales nuevas deben alcanzar o superar la configuración de longitud mínima actual de la contraseña (en Ver/editar configuración).
- Las contraseñas distinguen mayúsculas de minúsculas.
- Los espacios al final de la contraseña no se eliminan, si se los utiliza. Procure incluir espacios si se incluyeron en la contraseña.
- Para mayor seguridad, use al menos 15 caracteres alfanuméricos y cambie la contraseña con frecuencia.

> Cuando se cambia la contraseña en System Manager también se modifica en la interfaz de línea de comandos (CLI). Además, los cambios de contraseña provocan el cierre de la sesión activa del usuario.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la ficha **roles de usuario local**.
3. Seleccione un usuario de la tabla.

   Se habilita el botón Cambiar contraseña.

4. Seleccione **Cambiar contraseña**.

   Se abre el cuadro de diálogo Cambiar contraseña.

5. Si no se estableció una longitud de contraseña mínima para las contraseñas de usuario local, se puede marcar la casilla para solicitar que el usuario seleccionado introduzca una contraseña para acceder a la

cabina de almacenamiento y, a continuación, se puede escribir la contraseña nueva para el usuario seleccionado.

6. Introduzca su contraseña de administrador local y, a continuación, haga clic en **Cambiar**.

Resultados

Si el usuario está conectado, el cambio de contraseña provocará el cierre de la sesión activa del usuario.

Cambie la configuración de contraseña de usuario local

Es posible configurar la longitud mínima requerida para todas las contraseñas de usuario locales nuevas o actualizadas de la cabina de almacenamiento. También es posible permitir a los usuarios locales acceder a la cabina de almacenamiento sin introducir una contraseña.

Antes de empezar

Inició sesión como administrador local, lo que incluye permisos de administrador raíz.

Acerca de esta tarea

Recuerde estas directrices cuando configure la longitud mínima para las contraseñas de usuario local:

- Los cambios en la configuración no afectan a las contraseñas existentes de usuarios locales.
- La configuración de la longitud mínima requerida para las contraseñas de usuario local debe tener entre 0 y 30 caracteres.
- Todas las contraseñas de usuario local nuevas deben alcanzar o superar la configuración de longitud mínima actual.
- No configure una longitud mínima para la contraseña si no desea que usuarios locales accedan a la cabina de almacenamiento sin introducir una contraseña.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la ficha **roles de usuario local**.
3. Seleccione el botón **Ver/editar configuración**.

   Se abre el cuadro de diálogo Configuración de contraseña de usuario local.

4. Debe realizar una de las siguientes acciones:
   - Para permitir a los usuarios locales acceder a la cabina de almacenamiento *sin* introducir una contraseña, desactive la casilla de comprobación "require all local user passwords to be at least".
   - Para configurar una longitud mínima de contraseña para todas las contraseñas de usuarios locales, active la casilla de comprobación "require all local user passwords to be at least" y luego use el cuadro de desplazamiento para configurar la longitud mínima requerida para todas las contraseñas de usuarios locales.

     Todas las contraseñas de usuario local nuevas deben alcanzar o superar la configuración actual.

5. Haga clic en **Guardar**.

Uso de los servicios de directorio

Añadir servidor de directorio LDAP

Para configurar la autenticación de Access Management, se pueden establecer comunicaciones entre la cabina de almacenamiento y un servidor LDAP, y luego asignar los grupos de usuarios LDAP a los roles predefinidos de la cabina.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- Debe haber grupos de usuarios definidos en el servicio de directorio.
- Deben estar disponibles las credenciales del servidor LDAP, incluidos el nombre de dominio y la URL del servidor y, de manera opcional, el nombre de usuario y la contraseña de la cuenta de enlace.
- En el caso de los servidores LDAPS que utilizan un protocolo seguro, se debe instalar la cadena de certificados del servidor LDAP en la máquina local.

Acerca de esta tarea

La adición de un servidor de directorio es un proceso que consta de dos pasos. Primero, se debe introducir la URL y el nombre de dominio. Si el servidor utiliza un protocolo seguro, se debe cargar además un certificado de CA para autenticación, si no está firmado por una entidad de firma estándar. Si se poseen credenciales de una cuenta de enlace, también es posible introducir el nombre de cuenta de usuario y la contraseña. Luego, se deben asignar los grupos de usuarios del servidor LDAP a los roles predefinidos de la cabina de almacenamiento.

> Durante el procedimiento para añadir un servidor LDAP, se deshabilitará la interfaz de gestión heredada. La interfaz de gestión heredada (Symbol) es un método de comunicación entre la cabina de almacenamiento y el cliente de gestión. Cuando se encuentra deshabilitada, la cabina de almacenamiento y el cliente de gestión utilizan un método de comunicación más seguro (API DE REST por https).

Pasos

1. Seleccione MENU:Settings[Access Management].
2. En la ficha Servicios de directorio, seleccione **Agregar servidor de directorio**.

   Se abre el cuadro de diálogo Añadir servidor de directorio.

3. En la pestaña Configuración del servidor, introduzca las credenciales del servidor LDAP.

Detalles del campo

Ajuste	Descripción
Ajustes de configuración	Dominios
Introduzca el nombre de dominio del servidor LDAP. Si desea introducir varios dominios, escríbalos en una lista separada por comas. El nombre de dominio se utiliza en el inicio de sesión (*username@domain*) para especificar con qué servidor de directorio debe realizarse la autenticación.	URL del servidor
Introduzca la URL para acceder al servidor LDAP con el formato de `ldap[s]://host:*port*`.	Cargar certificado (opcional)

Ajuste	Descripción
Este campo aparece solo si se especific a un protocolo LDAPS en el campo URL del servidor arriba. Haga clic en **examinar** y seleccione un certificado de CA para cargar. Este es el certificado o la cadena de certificados de confianza utilizado para autenticar el servidor LDAP.	Enlazar cuenta (opcional)
Introduzca una cuenta de usuario de solo lectura para realizar consultas de búsqueda en el servidor LDAP y para buscar dentro de los grupos. Introduzca el nombre de cuenta con formato tipo LDAP. Por ejemplo, si el usuario de enlace se denomina "bindacct", puede introducir un valor como el siguiente: "CN=bindacct,CN=Users,DC=cpoc,DC=local".	Enlazar contraseña (opcional)

Ajuste	Descripción
Este campo aparece cuando introduce una cuenta de enlace arriba. Introduzca la contraseña de la cuenta de enlace.	Probar conexión del servidor antes de añadir
Seleccione esta casilla de comprobación si desea asegurarse de que la cabina de almacenamiento pueda comunicarse con la configuración de servidor LDAP que introdujo. La prueba se produce después de hacer clic en **Agregar** en la parte inferior del cuadro de diálogo. Si esta casilla de comprobación está seleccionada y la prueba falla, no se añadirá la configuración. Debe resolver el error o anular la selección de la casilla de comprobación para omitir la comprobación y añadir la configuración.	**Ajustes de privilegios**
DN base de búsqueda	Introduzca el contexto de LDAP para buscar usuarios, generalmente con el formato de `CN=Users, DC=cpoc, DC=local`.
Atributo de nombre de usuario	Introduzca el atributo vinculado al ID de usuario para los fines de autenticación. Por ejemplo: `sAMAccountName`.

Ajuste	Descripción
Atributos de grupo\(s\)	Introduzca una lista de atributos de grupo en el usuario, que se utilizará para la asignación de grupos a roles. Por ejemplo: `memberOf, managedObjects`.

4. Haga clic en la ficha **asignación de roles**.
5. Asigne grupos LDAP a los roles predefinidos. Un grupo puede tener varios roles asignados.

Detalles del campo

Ajuste	Descripción
Asignaciones	DN de grupo
Especifique el nombre distintivo (DN) del grupo correspondiente al grupo de usuarios LDAP que se asignará. Se admiten expresiones regulares. Estos caracteres especiales de expresión regular deben escaparse con una barra invertida (`\`) si no forman parte de un patrón de expresión regular: \.[]{}()<>*+-=	Funciones

El rol de supervisión se requiere para todos los usuarios, incluido el administrador. System Manager no funcionará correctamente para los usuarios que no tengan el rol de supervisión.

6. Si lo desea, haga clic en **Agregar otra asignación** para introducir más asignaciones de grupo a rol.
7. Cuando termine de asignar, haga clic en **Agregar**.

   El sistema realiza una validación y se asegura de que la cabina de almacenamiento y el servidor LDAP pueden comunicarse. Si aparece un mensaje de error, compruebe las credenciales que introdujo en el cuadro de diálogo y vuelva a introducir la información, de ser necesario.

Editar ajustes y asignaciones de roles del servidor de directorios

Si anteriormente configuró un servidor de directorio en Access Management, es posible cambiar sus ajustes en cualquier momento. Entre estos ajustes se encuentran la información de conexión del servidor y las asignaciones de grupos a roles.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- Debe definirse un servidor de directorio.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la ficha **Servicios de directorio**.
3. Si se define más de un servidor, seleccione el servidor que desea editar en la tabla.
4. Seleccione **Ver/editar configuración**.

   Se abre el cuadro de diálogo Configuración del servidor de directorio.

5. En la pestaña Configuración del servidor, cambie la configuración que desea.

Detalles del campo

Ajuste	Descripción
Ajustes de configuración	Dominios
Los nombres de dominio de los servidores LDAP. Si desea introducir varios dominios, escríbalos en una lista separada por comas. El nombre de dominio se utiliza en el inicio de sesión (*username@domain*) para especificar con qué servidor de directorio debe realizarse la autenticación.	URL del servidor
La URL para acceder al servidor LDAP con el formato de `ldap[s]://host:port`.	Enlazar cuenta (opcional)
La cuenta de usuario de solo lectura para realizar consultas en el servidor LDAP y buscar dentro de grupo.	Enlazar contraseña (opcional)
La contraseña de la cuenta vinculada. (Este campo se muestra cuando se introduce una cuenta vinculada.)	Probar conexión del servidor antes de guardar

Ajuste	Descripción
Comprueba que la cabina de almacenamiento pueda comunicarse con la configuración del servidor LDAP. La prueba se produce después de hacer clic en **Guardar** en la parte inferior del cuadro de diálogo. Si se selecciona esta casilla de comprobación y la prueba falla, no se modifica la configuración. Debe resolver el error o cancelar la selección de la casilla de comprobación para omitir la prueba y volver a editar la configuración.	**Configuración de privilegios**
DN base de búsqueda	El contexto de LDAP para buscar usuarios, normalmente en la forma de `CN=Users, DC=cpoc, DC=local`.
Atributo de nombre de usuario	El atributo que está vinculado al ID de usuario para la autenticación. Por ejemplo: `sAMAccountName`.
Atributos de grupo	Lista de atributos de grupo en el usuario, que se utiliza para la asignación de grupos a roles. Por ejemplo: `memberOf, managedObjects`.

6. En la pestaña asignación de roles, cambie la asignación deseada.

Detalles del campo

Ajuste	Descripción
Asignaciones	DN de grupo
El nombre de dominio para asignar el grupo de usuarios LDAP. Se admiten expresiones regulares. Estos caracteres especiales de expresión regular deben escaparse con una barra invertida (\) si no forman parte de un patrón de expresión regular: \.[]{}()<>*+-=	Funciones

El rol de supervisión se requiere para todos los usuarios, incluido el administrador. System Manager no funcionará correctamente para los usuarios que no tengan el rol de supervisión.

7. Si lo desea, haga clic en **Agregar otra asignación** para introducir más asignaciones de grupo a rol.
8. Haga clic en **Guardar**.

Resultados

Una vez finalizada esta tarea, se finalizarán todas las sesiones de usuario activas. Solo se mantiene la sesión de usuario actual.

Quitar un servidor de directorio

Para interrumpir la conexión entre un servidor de directorio y la cabina de almacenamiento, es posible eliminar la información del servidor de la página Access Management. Se recomienda ejecutar esta tarea si se configuró un servidor nuevo y se desea eliminar el anterior.

Antes de empezar

Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.

Acerca de esta tarea

Una vez finalizada esta tarea, se finalizarán todas las sesiones de usuario activas. Solo se mantiene la sesión de usuario actual.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la ficha **Servicios de directorio**.

3. Seleccione el servidor de directorio que desea eliminar de la lista.
4. Haga clic en **Quitar**.

   Se abrirá el cuadro de diálogo Quitar servidor de directorio.

5. Tipo `remove` En el campo y, a continuación, haga clic en **Quitar**.

   Se eliminará la configuración del servidor de directorio, la configuración de privilegios y las asignaciones de roles. Los usuarios ya no podrán iniciar sesión con las credenciales de este servidor.

Use SAML

Configure SAML

Para configurar la autenticación de Access Management, puede usar las funcionalidades de lenguaje de marcado de aserción de seguridad (SAML) que están integradas en la cabina de almacenamiento. Esta configuración establece una conexión entre un proveedor de identidades y el proveedor de almacenamiento.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- Debe conocer la dirección IP o el nombre de dominio de cada controladora de la cabina de almacenamiento.
- Un administrador de IDP configuró un sistema IDP.
- Un administrador de IDP comprobó que el IDP admite la capacidad para obtener un ID de nombre en el momento de la autenticación.
- Un administrador comprobó que los relojes del servidor de IDP y de la controladora están sincronizados (ya sea mediante un servidor NTP o mediante el ajuste de la configuración del reloj de la controladora).
- Se descargó un archivo de metadatos de IDP del sistema de IDP y ese archivo está disponible en el sistema local que se usa para acceder a System Manager.

Acerca de esta tarea

Un proveedor de identidades (IDP) es un sistema externo que se usa para solicitar credenciales a un usuario y para determinar si el usuario se autentica correctamente. El IDP se puede configurar para ofrecer autenticación multifactor y para usar cualquier base de datos de usuario, como Active Directory. El equipo de seguridad es responsable de mantener el IDP. Un proveedor de servicios (SP) es un sistema que controla la autenticación y el acceso de usuario. Cuando se configura Access Management con SAML, la cabina de almacenamiento actúa como proveedor de servicios, ya que solicita la autenticación del proveedor de identidades. Para establecer una conexión entre el IDP y la cabina de almacenamiento, se deben compartir archivos de metadatos entre estas dos entidades. A continuación, se deben asignar las entidades de usuario de IDP con los roles de la cabina de almacenamiento. Y, finalmente, se debe probar la conexión y los inicios de sesión SSO antes de habilitar SAML.

> **SAML y Directory Services**. Si SAML se habilita cuando Directory Services está configurado como método de autenticación, SAML sustituye a Directory Services en System Manager. Si se deshabilita SAML posteriormente, la configuración de Directory Services se establece en los valores anteriores.

Edición y desactivación. una vez que SAML está habilitado, *no puede* desactivarlo a través de la interfaz de usuario, ni puede editar la configuración de IDP. Si necesita deshabilitar o editar la configuración de SAML, comuníquese con el soporte técnico para obtener ayuda.

La configuración de la autenticación SAML es un procedimiento de varios pasos.

Paso 1: Cargue el archivo de metadatos de IDP

Para brindar información de conexión de IDP a la cabina de almacenamiento, se deben importar los metadatos de IDP en System Manager. El sistema IDP necesita los metadatos para redirigir las solicitudes de autenticación a la URL correcta y validar las respuestas recibidas. Solamente es necesario cargar un solo archivo de metadatos para la cabina de almacenamiento, incluso si hay dos controladoras.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la pestaña **SAML**.

   La página muestra información general de los pasos de configuración.

3. Haga clic en el enlace **Import Identity Provider (IDP) file**.

   Se abre el cuadro de diálogo Importar archivo del proveedor de identidades.

4. Haga clic en **examinar** para seleccionar y cargar el archivo de metadatos IDP que copió en el sistema local.

   Una vez seleccionado el archivo, se muestra el ID de entidad IDP.

5. Haga clic en **Importar**.

Paso 2: Exporte los archivos del proveedor de servicios

Para establecer una relación de confianza entre IDP y la cabina de almacenamiento, se deben importar los metadatos del proveedor de servicios en IDP. IDP necesita estos metadatos para establecer una relación de confianza con las controladoras y procesar las solicitudes de autorización. El archivo incluye información, como el nombre de dominio de la controladora o la dirección IP, por lo que IDP se puede comunicar con los proveedores de servicios.

Pasos

1. Haga clic en el enlace **Exportar archivos del proveedor de servicios**.

   Se abre el cuadro de diálogo Exportar archivos del proveedor de servicios.

2. Introduzca la dirección IP del controlador o el nombre DNS en el campo **controladora A** y, a continuación, haga clic en **Exportar** para guardar el archivo de metadatos en el sistema local. Si la matriz de almacenamiento incluye dos controladoras, repita este paso con la segunda controladora en el campo **controladora B**.

   Después de hacer clic en **Exportar**, los metadatos del proveedor de servicios se descargan en el sistema local. Anote en qué lugar se almacena el archivo.

3. Desde el sistema local, busque los archivos de metadatos del proveedor de servicios que exportó.

   Hay un archivo con formato XML por controladora.

4. Desde el servidor IDP, importe los archivos de metadatos del proveedor de servicios para establecer la relación de confianza. Es posible importar los archivos directamente o bien introducir manualmente la información de la controladora desde los archivos.

Paso 3: Asignar roles

Para proporcionar autorización y acceso a System Manager a los usuarios, se deben asignar los atributos de usuario IDP y las membresías de grupo a los roles predefinidos de la cabina de almacenamiento.

Antes de empezar

- Un administrador IDP configuró los atributos del usuario y la pertenencia al grupo en el sistema IDP.
- Se importó el archivo de metadatos de IDP a System Manager.
- Para la relación de confianza, se importó un archivo de metadatos del proveedor de servicios para cada controladora en el sistema IDP.

Pasos

1. Haga clic en el vínculo para **asignación de roles de System Manager**.

   Se abre el cuadro de diálogo asignación de roles.

2. Asigne los grupos y atributos de usuario IDP a los roles predefinidos. Un grupo puede tener varios roles asignados.

   Detalles del campo

Ajuste	Descripción
Asignaciones	Atributo de usuario
Especifique un atributo (por ejemplo, "miembro de") para el grupo SAML que será asignado.	Valor de atributo
Especifique el valor de atributo para el grupo que será asignado. Se admiten expresiones regulares. Estos caracteres especiales de expresión regular deben escaparse con una barra invertida (\) si no forman parte de un patrón de expresión regular: \.[]{}()<>*+-=	Funciones

> El rol de supervisión se requiere para todos los usuarios, incluido el administrador. System Manager no funcionará correctamente para los usuarios que no tengan el rol de supervisión.

3. Si lo desea, haga clic en **Agregar otra asignación** para introducir más asignaciones de grupo a rol.

> Es posible modificar las asignaciones de roles después de haber habilitado SAML.

4. Cuando termine de asignar, haga clic en **Guardar**.

Paso 4: Probar el inicio de sesión SSO

Para garantizar la comunicación entre el sistema IDP y la cabina de almacenamiento, de manera opcional, se puede probar un inicio de sesión SSO. Esa prueba también se puede llevar a cabo durante el paso final para habilitar SAML.

Antes de empezar

- Se importó el archivo de metadatos de IDP a System Manager.
- Para la relación de confianza, se importó un archivo de metadatos del proveedor de servicios para cada controladora en el sistema IDP.

Pasos

1. Seleccione el enlace **probar inicio de sesión SSO**.

   Se abre un cuadro de diálogo para introducir las credenciales de SSO.

2. Introduzca las credenciales de inicio de sesión para un usuario, tanto con permisos de administración de seguridad como de supervisión.

   Se abre un cuadro de diálogo mientras el sistema prueba el inicio de sesión.

3. Busque el mensaje Test Successful. Si el análisis se realiza correctamente, vaya al siguiente paso para habilitar SAML.

   Si el análisis no se realiza correctamente, se muestra un mensaje de error con más información. Asegúrese de que:

   - El usuario pertenezca a un grupo con permisos de administración de seguridad y supervisión.
   - Los metadatos cargados para el servidor IDP sean correctos.
   - Las direcciones de las controladoras en los archivos de metadatos de SP sean correctas.

Paso 5: Habilite SAML

El paso final es completar la configuración de SAML para la autenticación de usuarios. Durante este proceso, el sistema también le indica que pruebe un inicio de sesión SSO. El proceso de prueba de inicio de sesión con SSO se describe en el paso anterior.

Antes de empezar

- Se importó el archivo de metadatos de IDP a System Manager.
- Para la relación de confianza, se importó un archivo de metadatos del proveedor de servicios para cada controladora en el sistema IDP.

- Se debe configurar al menos una asignación de rol de administración de seguridad y una de rol de supervisión.

> **Edición y desactivación.** una vez que SAML está habilitado, *no puede* desactivarlo a través de la interfaz de usuario, ni puede editar la configuración de IDP. Si necesita deshabilitar o editar la configuración de SAML, comuníquese con el soporte técnico para obtener ayuda.

Pasos

1. En la ficha **SAML**, seleccione el enlace **Habilitar SAML**.

   Se abre el cuadro de diálogo Confirmar acción de habilitar SAML.

2. Tipo `enable`Y, a continuación, haga clic en **Activar**.
3. Introduzca las credenciales de usuario para llevar a cabo una prueba de inicio de sesión SSO.

Resultados

Una vez que el sistema habilita SAML, se cierran todas las sesiones activas y se inicia la autenticación de usuarios a través de SAML.

Cambiar las asignaciones de roles SAML

Si anteriormente configuró SAML para Access Management, puede cambiar las asignaciones de roles entre los grupos IDP y los roles predefinidos de la cabina de almacenamiento.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- Un administrador IDP configuró los atributos del usuario y la pertenencia al grupo en el sistema IDP.
- SAML debe estar configurado y habilitado.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la pestaña **SAML**.
3. Seleccione **asignación de roles**.

   Se abre el cuadro de diálogo asignación de roles.

4. Asigne los grupos y atributos de usuario IDP a los roles predefinidos. Un grupo puede tener varios roles asignados.

   > Tenga cuidado de no quitar los permisos mientras SAML está habilitado; de lo contrario, perderá el acceso a System Manager.

Detalles del campo

Ajuste	Descripción
Asignaciones	Atributo de usuario
Especifique un atributo (por ejemplo, "miembro de") para el grupo SAML que será asignado.	Valor de atributo
Especifique el valor de atributo para el grupo que será asignado.	Funciones

> El rol de supervisión se requiere para todos los usuarios, incluido el administrador. System Manager no funcionará correctamente para los usuarios que no tengan el rol de supervisión.

5. Opcionalmente, haga clic en **Agregar otra asignación** para introducir más asignaciones de grupo a rol.
6. Haga clic en **Guardar**.

Resultados

Una vez finalizada esta tarea, se finalizarán todas las sesiones de usuario activas. Solo se mantiene la sesión de usuario actual.

Exporte los archivos de proveedor de servicios SAML

Si es necesario, se pueden exportar metadatos de proveedor de servicios para la cabina de almacenamiento y volver a importar los archivos en el sistema del proveedor de identidades (IDP).

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- SAML debe estar configurado y habilitado.

Acerca de esta tarea

En esta tarea, es posible exportar metadatos de las controladoras (un archivo para cada controladora). IDP necesita estos metadatos para establecer una relación de confianza con las controladoras y procesar solicitudes de autenticación. El archivo incluye información, como el nombre de dominio o la dirección IP de la controladora, que IDP puede usar para enviar solicitudes.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la pestaña **SAML**.

3. Seleccione **Exportar**.

   Se abre el cuadro de diálogo Exportar archivos del proveedor de servicios.

4. Para cada controlador, haga clic en **Exportar** para guardar el archivo de metadatos en el sistema local.

   > Los campos de nombre de dominio para cada controladora son de solo lectura.

   Anote en qué lugar se almacena el archivo.

5. Desde el sistema local, busque los archivos de metadatos del proveedor de servicios que exportó.

   Hay un archivo con formato XML por controladora.

6. Desde el servidor IDP, importe los archivos de metadatos del proveedor de servicios. Puede importar los archivos directamente o introducir manualmente la información de la controladora incluida en ellos.
7. Haga clic en **Cerrar**.

Utilice tokens de acceso

Cree tokens de acceso

Puede crear un token de acceso para la autenticación con la API DE REST o la interfaz de línea de comandos (CLI) en lugar de un nombre de usuario y una contraseña.

> Los tokens no tienen contraseñas, por lo que debe administrarlas con cuidado.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la ficha **tokens de acceso**.
3. Seleccione **Ver/editar configuración de token de acceso**. En el cuadro de diálogo, asegúrese de que la casilla de verificación **Habilitar tokens de acceso** está activada. Haga clic en **Guardar** para cerrar el cuadro de diálogo.
4. Seleccione **Crear símbolo de acceso**.
5. En el cuadro de diálogo, seleccione la duración del token que será válido.

   > Cuando caduque el token, se producirá un error en los intentos de autenticación del usuario.

6. Haga clic en **Crear.**
7. En el cuadro de diálogo, seleccione una de las siguientes opciones:
   - **Copiar** para guardar el texto del token en el portapapeles.
   - **Descargar** para guardar el texto del token en un archivo.

     > Asegúrese de guardar el texto del token. Esta es la única oportunidad para ver el texto antes de cerrar el diálogo.

8. Haga clic en **Cerrar**.

9. Utilice el token de la siguiente manera:
   - **API REST**: Para utilizar un token en una solicitud de API REST, agregue un encabezado HTTP a sus solicitudes. Por ejemplo:
     `Authorization: Bearer <access-token-value>`
   - **Secure CLI**: Para utilizar un token en la CLI, agregue el valor de token en la línea de comandos o utilice la ruta de acceso a un archivo que contenga el valor de token. Por ejemplo:
     - Valor de token en la línea de comandos: `-t access-token-value`
     - Ruta de acceso a un archivo que contiene el valor de token: `-T access-token-file`

> La interfaz de línea de comandos solicita al usuario un valor de token de acceso en la línea de comandos si no se especifica ningún nombre de usuario, contraseña ni token.

Edite la configuración del token de acceso

Puede editar la configuración de los tokens de acceso, lo que incluye los tiempos de caducidad y la capacidad de crear nuevos tokens.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la ficha **tokens de acceso**.
3. Seleccione **Ver/editar configuración de token de acceso**.
4. En el cuadro de diálogo, puede realizar una o ambas tareas:
   - Activar o desactivar la creación de token.
   - Cambiar la caducidad de los tokens existentes.

> Al anular la selección del valor **Habilitar tokens de acceso**, se evita tanto la creación de token como la autenticación de token. Si vuelve a activar esta configuración más tarde, se pueden volver a utilizar tokens no vencidos. Si desea revocar permanentemente todos los tokens existentes, consulte "Revocar tokens de acceso".

5. Haga clic en **Guardar**.

Revocar tokens de acceso

Puede revocar todos los tokens de acceso si determina que se ha comprometido un token o si desea realizar una rotación manual de claves criptográficas para las claves de acceso utilizadas para firmar y validar los tokens de acceso.

Esta operación regenera las claves utilizadas para firmar los tokens. Una vez restablecidos las claves, los tokens *All* emitidos se invalidan inmediatamente. Como la cabina de almacenamiento no realiza un seguimiento de tokens, no pueden revocarse tokens individuales.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la ficha **tokens de acceso**.

3. Seleccione **revocar todos los tokens de acceso**.
4. En el cuadro de diálogo, haga clic en **Sí**.

Después de revocar todos los tokens, puede crear nuevos tokens y utilizarlos inmediatamente.

Gestionar syslog

Ver actividad de registro de auditoría

Al ver los registros de auditoría, los usuarios que tienen permisos de administrador de seguridad pueden supervisar acciones de usuarios, fallos de autenticación, intentos de inicio de sesión no válidos y la vida útil de la sesión de usuario.

Antes de empezar

Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la ficha **Registro de auditoría**.

   La actividad de registro de auditoría aparece en una tabla de resultados, que incluye las siguientes columnas de información:

   - **Fecha/Hora** — Marca de hora del momento en que la matriz de almacenamiento detectó el evento (en GMT).
   - **Nombre de usuario** — el nombre de usuario asociado al evento. Para cualquier acción sin autenticar en la cabina de almacenamiento, aparece "N/A" como nombre de usuario. El proxy interno o algún otro mecanismo podrían activar acciones sin autenticar.
   - **Código de estado** — Código de estado HTTP de la operación (200, 400, etc.) y texto descriptivo asociado al evento.
   - **URL visitada** — URL completa (incluido el host) y cadena de consulta.
   - **Dirección IP del cliente** — Dirección IP del cliente asociado al evento.
   - **Source** — origen de registro asociado al evento, que puede ser System Manager, CLI, Web Services o Support Shell.
   - **Descripción** — Información adicional sobre el evento, si corresponde.
3. Use las selecciones de la página Registro de auditoría para ver y gestionar eventos.

Detalles de selección

Selección	Descripción
Mostrar eventos de…	Eventos de límite mostrados por rango de fechas (últimas 24 horas, últimos 7 días, últimos 30 días o un rango de fechas personalizado).
Filtro	Eventos de límite mostrados por los caracteres introducidos en el campo. Utilice comillas ("") para una coincidencia exacta de palabras, introduzca `OR` para devolver una o más palabras, o introduzca un guión (—) para omitir palabras.
Actualice	Seleccione **Actualizar** para actualizar la página a los eventos más recientes.
Ver/editar configuración	Seleccione **Ver/editar configuración** para abrir un cuadro de diálogo que permite especificar una política de registro completo y el nivel de acciones que se registrarán.
Eliminar eventos	Seleccione **Eliminar** para abrir un cuadro de diálogo que le permite eliminar eventos antiguos de la página.
Mostrar/ocultar columnas	Haga clic en el icono de la columna **Mostrar/Ocultar** para seleccionar columnas adicionales para mostrar en la tabla. Las columnas adicionales incluyen: • **Método** — el método HTTP (POR ejemplo, POST, GET, DELETE, etc.). • **Comando CLI ejecutado** — el comando CLI (gramática) ejecutado para solicitudes Secure CLI. • **Estado de devolución de CLI** — un código de estado de CLI o una solicitud de archivos de entrada del cliente. • **Procedimiento de Symbol** — procedimiento de Symbol ejecutado. • **Tipo de evento SSH** — Tipo de eventos Secure Shell (SSH), como inicio de sesión, cierre de sesión y login_fail. • **PID de sesión SSH** — número de ID de proceso de la sesión SSH. • **Duración(s) de sesión de SSH** — el número de segundos en los que el usuario estuvo conectado. • **Tipo de autenticación** — los tipos pueden incluir Usuario local, LDAP, SAML y token de acceso. • **ID de autenticación** — ID de la sesión autenticada.
Alternar filtros de columnas	Haga clic en el icono **alternar** para abrir los campos de filtrado de cada columna. Introduzca los caracteres en un campo de columna para limitar los eventos que se muestran con esos caracteres. Vuelva a hacer clic en el icono para cerrar los campos de filtrado.

Selección	Descripción
Deshacer cambios	Haga clic en el icono **Deshacer** para devolver la tabla a la configuración predeterminada.
Exportar	Haga clic en **Exportar** para guardar los datos de la tabla en un archivo de valores separados por comas (CSV).

Defina políticas de registro de auditoría

Es posible cambiar la política de sobrescritura y los tipos de eventos registrados en el registro de auditoría.

Antes de empezar

Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.

Acerca de esta tarea

En esta tarea, se describe la forma de cambiar la configuración del registro de auditoría, lo que incluye la política para sobrescribir eventos anteriores y la política para registrar tipos de eventos.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la ficha **Registro de auditoría**.
3. Seleccione **Ver/editar configuración**.

   Se abrirá el cuadro de diálogo Configuración del registro de auditoría.

4. Cambie la política de sobrescritura o los tipos de eventos registrados.

Detalles del campo

Ajuste	Descripción
Política de sobrescritura	Determine la política para sobrescribir eventos antiguos cuando se alcanza la capacidad máxima: • **Permitir que los eventos más antiguos del registro de auditoría se sobrescriban cuando el registro de auditoría está lleno** — sobrescribe los eventos antiguos cuando el registro de auditoría llega a 50,000 registros. • **Requerir que se eliminen manualmente los eventos del registro de auditoría** — especifica que los eventos no se eliminarán automáticamente; en su lugar, aparecerá una advertencia de umbral en el porcentaje establecido. Los eventos deben eliminarse manualmente. Si se deshabilita la política de sobrescritura y las entradas del registro de auditoría llegan al límite máximo, se deniega el acceso a System Manager para usuarios sin permisos de Administrador de seguridad. Para restaurar el acceso al sistema para usuarios sin permisos de Administrador de seguridad, un usuario asignado al rol Security Admin debe eliminar los registros de eventos anteriores. Las políticas de sobrescritura no se aplican si un servidor de syslog está configurado para archivar registros de auditoría.
Nivel de acciones que se registrarán	Determina los tipos de eventos que deben registrarse: • **Grabar sólo eventos de modificación** — muestra sólo los eventos en los que una acción del usuario implica realizar un cambio en el sistema. • **Grabar todos los eventos de modificación y sólo lectura** — muestra todos los eventos, incluyendo una acción del usuario que implica leer o descargar información.

5. Haga clic en **Guardar**.

Elimine eventos del registro de auditoría

Es posible borrar los eventos antiguos del registro de auditoría para que la búsqueda de eventos sea más sencilla. Tiene la opción de guardar los eventos antiguos en un archivo CSV (valores separados por comas) después de su eliminación.

Antes de empezar

Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo

contrario, no se mostrarán las funciones de Access Management.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la ficha **Registro de auditoría**.
3. Seleccione **Eliminar**.

   Se abre el cuadro de diálogo Eliminar registro de auditoría.

4. Seleccione o escriba el número de eventos antiguos que desea eliminar.
5. Si desea exportar los eventos eliminados a un archivo CSV (recomendado), mantenga seleccionada la casilla de comprobación. Se le pedirá que introduzca un nombre de archivo y una ubicación al hacer clic en **Eliminar** en el paso siguiente. De lo contrario, si no desea guardar eventos en un archivo CSV, haga clic en la casilla de comprobación para cancelar la selección.
6. Haga clic en **Eliminar**.

   Se abre un cuadro de diálogo de confirmación.

7. Tipo `delete` En el campo y, a continuación, haga clic en **Eliminar**.

   Los eventos más antiguos se eliminarán de la página Registro de auditoría.

Configurar servidores de syslog para registros de auditoría

Si desea archivar registros de auditoría en un servidor de syslog externo, puede configurar las comunicaciones entre ese servidor y la cabina de almacenamiento. Una vez que se establece la conexión, los registros de auditoría se guardan automáticamente en el servidor de syslog.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- La dirección, el protocolo y el número de puerto del servidor de syslog deben estar disponibles. La dirección del servidor debe ser un nombre de dominio completo, una dirección IPv4 o una dirección IPv6.
- Si el servidor usa un protocolo seguro (por ejemplo, TLS), debe haber disponible un certificado de entidad de certificación (CA) en el sistema local. Los certificados DE CA identifican propietarios de sitios web para lograr conexiones seguras entre servidores y clientes.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. En la ficha Registro de auditoría, seleccione **Configurar servidores de syslog**.

   Se abre el cuadro de diálogo Configurar servidores de syslog.

3. Haga clic en **Agregar**.

   Se abre el cuadro de diálogo Añadir servidor de syslog.

4. Introduzca la información del servidor y, a continuación, haga clic en **Agregar**.

- **Dirección del servidor** — Introduzca un nombre de dominio completo, una dirección IPv4 o una dirección IPv6.
- **Protocolo** — Seleccione un protocolo de la lista desplegable (por ejemplo, TLS, UDP o TCP).
- **Cargar certificado (opcional)** — Si ha seleccionado el protocolo TLS y todavía no ha cargado un certificado de CA firmado, haga clic en **examinar** para cargar un archivo de certificado. Los registros de auditoría no se archivan en un servidor de syslog si no cuentan con un certificado de confianza.

> Si la certificación ya no es válida en el futuro, el apretón de manos de TSL fallará. Como resultado, se publica un mensaje de error en el registro de auditoría y ya no se envían mensajes al servidor de syslog. Para resolver este problema, debe corregir la certificación en el servidor de syslog y, a continuación, ir a menú:Configuración[Registro de auditoría > Configurar servidores de syslog > probar todo].

- **Puerto** — Introduzca el número de puerto para el receptor de syslog. Después de hacer clic en **Agregar**, se abre el cuadro de diálogo Configurar servidores de syslog y se muestra el servidor de syslog configurado en la página.

5. Para probar la conexión del servidor con la matriz de almacenamiento, seleccione **probar todo**.

Resultados

Después de la configuración, se envían todos los registros de auditoría nuevos al servidor de syslog. Los registros anteriores no se transfieren. Para seguir configurando los ajustes de syslog de las alertas, consulte "Configurar el servidor de syslog para las alertas".

Editar la configuración del servidor de syslog para los registros de auditoría

Es posible modificar la configuración del servidor de syslog utilizada para archivar registros de auditoría, y también cargar un nuevo certificado de una entidad de certificación (CA) para el servidor.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- La dirección, el protocolo y el número de puerto del servidor de syslog deben estar disponibles. La dirección del servidor debe ser un nombre de dominio completo, una dirección IPv4 o una dirección IPv6.
- Si va a cargar un nuevo certificado de CA, el certificado debe estar disponible en el sistema local.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. En la ficha Registro de auditoría, seleccione **Configurar servidores de syslog**.

   Los servidores de syslog configurados se muestran en la página.

3. Para editar la información del servidor, seleccione el icono **Editar** (lápiz) situado a la derecha del nombre del servidor y, a continuación, realice los cambios deseados en los siguientes campos:
   - **Dirección del servidor** — Introduzca un nombre de dominio completo, una dirección IPv4 o una dirección IPv6.
   - **Protocolo** — Seleccione un protocolo de la lista desplegable (por ejemplo, TLS, UDP o TCP).
   - **Puerto** — Introduzca el número de puerto para el receptor de syslog.

4. Si cambió el protocolo al protocolo TLS seguro (desde UDP o TCP), haga clic en **Importar certificado de confianza** para cargar un certificado de CA.
5. Para probar la nueva conexión con la matriz de almacenamiento, seleccione **probar todo**.

Resultados

Después de la configuración, se envían todos los registros de auditoría nuevos al servidor de syslog. Los registros anteriores no se transfieren.

Preguntas frecuentes

¿Por qué no puedo iniciar sesión?

Si recibe un error al intentar iniciar sesión en System Manager, revise estas causas posibles.

Los errores de inicio de sesión en System Manager pueden ocurrir por uno de estos motivos:

- Introdujo un nombre de usuario o contraseña incorrectos.
- No tiene privilegios suficientes.
- El servidor de directorio (si está configurado) puede no estar disponible. Si este es el caso, intente iniciar sesión con un rol de usuario local.
- Intentó iniciar sesión reiteradamente sin éxito y se activó el modo de bloqueo. Aguarde 10 minutos y vuelva a intentarlo.
- Se activó la condición de bloqueo y es posible que el registro de auditoría esté completo. Vaya a Access Management y elimine los eventos anteriores del registro de auditoría.
- La autenticación SAML está habilitada. Actualice el explorador para iniciar sesión.

Los errores de inicio de sesión en una cabina de almacenamiento remota para tareas de mirroring pueden ocurrir por uno de estos motivos:

- Introdujo una contraseña incorrecta.
- Intentó iniciar sesión reiteradamente sin éxito y se activó el modo de bloqueo. Aguarde 10 minutos para volver a iniciar sesión.
- Se alcanzó la cantidad máxima de conexiones de clientes en la controladora. Busque clientes o usuarios múltiples.

¿Qué debo saber antes de añadir un servidor de directorio?

Antes de añadir un servidor de directorio en Access Management, asegúrese de cumplir con los siguientes requisitos.

- Debe haber grupos de usuarios definidos en el servicio de directorio.
- Deben estar disponibles las credenciales del servidor LDAP, incluidos el nombre de dominio y la URL del servidor y, de manera opcional, el nombre de usuario y la contraseña de la cuenta de enlace.
- En el caso de los servidores LDAPS que utilizan un protocolo seguro, se debe instalar la cadena de certificados del servidor LDAP en la máquina local.

¿Qué debo saber acerca de la asignación de roles de la cabina de almacenamiento?

Antes de asignar grupos a roles, revise las siguientes directrices.

Las funcionalidades de control de acceso basado en roles (RBAC) incorporadas en la cabina de almacenamiento incluyen los siguientes roles:

- **Storage admin** — acceso completo de lectura/escritura a los objetos de almacenamiento (por ejemplo, volúmenes y pools de discos), pero sin acceso a la configuración de seguridad.
- **Administración de seguridad** — acceso a la configuración de seguridad en Access Management, administración de certificados, administración de registros de auditoría y la capacidad de activar o desactivar la interfaz de administración heredada (Symbol).
- **Support admin** — acceso a todos los recursos de hardware en la cabina de almacenamiento, datos de fallos, eventos MEL y actualizaciones del firmware de la controladora. No brinda acceso a los objetos de almacenamiento ni a la configuración de seguridad.
- **Monitor** — acceso de sólo lectura a todos los objetos de almacenamiento, pero sin acceso a la configuración de seguridad.

Servicios de directorio

Si usa un servidor de protocolo ligero de acceso a directorios (LDAP) y servicios de directorio, asegúrese de que:

- Un administrador haya definido grupos de usuarios en el servicio de directorio.
- Conoce los nombres de dominio de los grupos de usuarios LDAP. Se admiten expresiones regulares. Estos caracteres especiales de expresión regular deben escaparse con una barra invertida (`\`) si no forman parte de un patrón de expresión regular:

  ```
  \.[]{}()<>*+-=!?^$|
  ```

- El rol de supervisión se requiere para todos los usuarios, incluido el administrador. System Manager no funcionará correctamente para los usuarios que no tengan el rol de supervisión.

SAML

Si usa las funcionalidades de lenguaje de marcado de aserción de seguridad (SAML) incorporadas en la cabina de almacenamiento, asegúrese de que:

- Un administrador de proveedor de identidades (IDP) haya configurado atributos de usuario y pertenencia a grupos en el sistema del IDP.
- Conoce los nombres de pertenencia a grupos.
- Conoce el valor de atributo para el grupo que será asignado. Se admiten expresiones regulares. Estos caracteres especiales de expresión regular deben escaparse con una barra invertida (`\`) si no forman parte de un patrón de expresión regular:

  ```
  \.[]{}()<>*+-=!?^$|
  ```

- El rol de supervisión se requiere para todos los usuarios, incluido el administrador. System Manager no funcionará correctamente para los usuarios que no tengan el rol de supervisión.

¿A cuáles herramientas de gestión externas puede afectar este cambio?

Cuando se realizan ciertos cambios en System Manager, como el cambio de la interfaz de gestión o el uso de SAML como método de autenticación, puede restringirse el uso de algunas herramientas y funciones externas.

Interfaz de gestión

Las herramientas que se comunican directamente con la interfaz de gestión heredada (Symbol), como SANtricity SMI-S Provider u OnCommand Insight (OCI), no funcionan a menos que la configuración interfaz de gestión heredada esté habilitada. Además, no es posible utilizar comandos de la CLI heredados ni realizar operaciones de mirroring si dicha configuración está deshabilitada.

Póngase en contacto con el soporte técnico para obtener más información.

Autenticación SAML

Cuando se habilita SAML, los siguientes clientes no pueden acceder a los recursos y los servicios de la cabina de almacenamiento:

- Enterprise Management Window (EMW)
- Interfaz de línea de comandos (CLI)
- Clientes de kits de desarrollo de software (SDK)
- Clientes en banda
- Clientes HTTP de la API de REST de autenticación básica
- Inicio de sesión mediante extremo estándar de la API de REST

Póngase en contacto con el soporte técnico para obtener más información.

¿Qué debo saber antes de configurar y habilitar SAML?

Antes de configurar y habilitar las funcionalidades de lenguaje de marcado de aserción de seguridad (SAML) para la autenticación, asegúrese de cumplir con los siguientes requisitos y comprender las restricciones de SAML.

Requisitos

Antes de comenzar, compruebe lo siguiente:

- Se configuró un proveedor de identidades (IDP) en la red. Un IDP es un sistema externo que se usa para solicitar credenciales a un usuario y determinar si el usuario se autentica correctamente. El equipo de seguridad es responsable de mantener el IDP.
- Un administrador IDP configuró los atributos y los grupos del usuario en el sistema IDP.
- Un administrador de IDP comprobó que el IDP admite la capacidad para obtener un ID de nombre en el momento de la autenticación.
- Un administrador comprobó que los relojes del servidor de IDP y de la controladora están sincronizados (ya sea mediante un servidor NTP o mediante el ajuste de la configuración del reloj de la controladora).
- Se descargó un archivo de metadatos de IDP del sistema de IDP y ese archivo está disponible en el sistema local que se usa para acceder a System Manager.

- Conoce la dirección IP o el nombre de dominio de cada controladora de la cabina de almacenamiento.

Restricciones

Además de los requisitos mencionados más arriba, asegúrese de comprender las siguientes restricciones:

- Una vez que se habilita SAML, _no se puede deshabilitar desde la interfaz de usuario, tampoco se puede editar desde la configuración de IDP. Si necesita deshabilitar o editar la configuración de SAML, comuníquese con el soporte técnico para obtener ayuda. Se recomienda que pruebe los inicios de sesión SSO para poder habilitar SAML en el paso final de la configuración. (El sistema también hace una prueba de inicio de sesión SSO antes de habilitar SAML.)
- Si deshabilita SAML en el futuro, el sistema restaura automáticamente la configuración anterior (local User roles o Directory Services).
- Si Directory Services está actualmente configurado para la autenticación de usuario, SAML anula esa configuración.
- Cuando se configura SAML, los siguientes clientes no pueden acceder a los recursos de la cabina de almacenamiento:
  - Enterprise Management Window (EMW)
  - Interfaz de línea de comandos (CLI)
  - Clientes de kits de desarrollo de software (SDK)
  - Clientes en banda
  - Clientes HTTP de la API de REST de autenticación básica
  - Inicio de sesión mediante extremo estándar de la API de REST

¿Qué tipo de eventos se registran en el registro de auditoría?

El registro de auditoría puede incluir eventos de modificación, o bien tanto eventos de modificación como de solo lectura.

Según la configuración de la política, se muestran los siguientes tipos de eventos:

- **Eventos de modificación** — acciones del usuario desde System Manager que involucran cambios en el sistema, como el aprovisionamiento de almacenamiento.
- **Eventos de modificación y de sólo lectura** — acciones del usuario que involucran cambios en el sistema, así como eventos que involucran la visualización o descarga de información, como la visualización de asignaciones de volumen.

¿Qué debo saber antes de configurar un servidor de syslog?

Es posible archivar registros de auditoría en un servidor de syslog externo.

Antes de configurar un servidor de syslog, tenga en cuenta las siguientes directrices.

- Asegúrese de conocer la dirección, el protocolo y el número de puerto del servidor. La dirección del servidor debe ser un nombre de dominio completo, una dirección IPv4 o una dirección IPv6.
- Si el servidor usa un protocolo seguro (por ejemplo, TLS), debe haber disponible un certificado de entidad de certificación (CA) en el sistema local. Los certificados DE CA identifican propietarios de sitios web para lograr conexiones seguras entre servidores y clientes.

- Después de la configuración, se envían todos los registros de auditoría nuevos al servidor de syslog. Los registros anteriores no se transfieren.
- La configuración de la política de sobrescritura (disponible en **View/Edit Settings**) no afecta a la forma en que se gestionan los registros con una configuración de servidor syslog.
- Los registros de auditoría tienen el formato de mensajería RFC 5424.

El servidor de syslog ya no recibe registros de auditoría. ¿Qué debo hacer?

Si configuró un servidor de syslog con un protocolo TLS, el servidor no puede recibir mensajes si la certificación no es válida por algún motivo. Se envía un mensaje de error sobre el certificado no válido al registro de auditoría.

Para resolver este problema, debe corregir la certificación para el servidor de syslog. Una vez que haya una cadena de certificados válida vigente, vaya a menú:Configuración[Registro de auditoría > Configurar servidores de syslog > probar todo].

Certificados

Información general sobre certificados

Es posible utilizar System Manager para crear solicitudes de firma de certificados (CSR), importar certificados y gestionar certificados existentes.

¿Qué son los certificados?

Certificates son archivos digitales que identifican entidades en línea, como sitios web y servidores, para comunicaciones seguras en Internet. Existen dos tipos de certificados: Un *certificado firmado* es validado por una entidad de certificación (CA) y un *certificado autofirmado* es validado por el propietario de la entidad en lugar de por un tercero.

Obtenga más información:

- "Cómo funcionan los certificados"
- "Terminología de certificados"

¿Cómo se configuran los certificados firmados?

Primero, se genera una solicitud de firma desde System Manager y, a continuación, se envía el archivo a una CA. Una vez que la CA devuelve los archivos de certificado, se deben importar mediante System Manager.

Obtenga más información:

- "Use certificados firmados por CA para las controladoras"
- "Use certificados firmados por CA para la autenticación con un servidor de gestión de claves"

Información relacionada

Obtenga más información acerca de las tareas relacionadas con los certificados:

- "Vea información de certificaciones importadas"

- "Habilite la comprobación de revocación de certificados"

Conceptos

Cómo funcionan los certificados

Los certificados son archivos digitales que identifican entidades en línea, como sitios web y servidores, para poder establecer comunicaciones seguras en Internet.

Los certificados garantizan que solo se transmitan comunicaciones web en formato cifrado, de forma privada y sin alternaciones, entre el servidor especificado y el cliente. Con System Manager, puede gestionar los certificados entre el explorador en un sistema de gestión host (que actúa como cliente) y las controladoras en un sistema de almacenamiento (que actúan como servidores).

Un certificado puede estar firmado por una autoridad de confianza o puede ser autofirmado. La firma simplemente implica que alguien validó la identidad del propietario y determinó que sus dispositivos son de confianza. Las cabinas de almacenamiento se entregan con un certificado autofirmado generado automáticamente en cada controladora. Puede continuar usando el certificado autofirmado o puede obtener certificados firmados por CA para establecer conexiones más seguras entre las controladoras y los sistemas host.

> Si bien los certificados firmados por CA aumentan la protección de seguridad (por ejemplo, evitan los ataques de tipo "man in the middle"), también aplican tarifas que pueden ser costosas si la red es extensa. En cambio, los certificados autofirmados son menos seguros, pero son gratuitos. Por lo tanto, los certificados autofirmados se utilizan con mayor frecuencia para entornos de prueba internos, no en entornos de producción.

Certificados firmados

Un certificado firmado es validado por una entidad de certificación (CA), que es una organización de terceros de confianza. Los certificados firmados incluyen detalles sobre el propietario de la entidad (generalmente, un servidor o sitio web), la fecha de emisión y de vencimiento del certificado, los dominios válidos de la entidad, y una firma digital compuesta por letras y números.

Al abrir un explorador y escribir una dirección web, el sistema ejecuta un proceso de comprobación de certificados en segundo plano para determinar si el usuario se está conectando a un sitio web que incluye un certificado válido firmado por una CA. Generalmente, un sitio que está protegido con un certificado firmado incluye un icono de candado y una designación https en la dirección. Si el usuario intenta conectarse a un sitio web que no contiene un certificado firmado por CA, el explorador mostrará una advertencia para indicar que el sitio no es seguro.

La CA toma las medidas necesarias para verificar las identidades durante el proceso de solicitud. La entidad puede enviar un correo electrónico a la empresa registrada, verificar la dirección empresarial, y realizar una verificación de HTTP o DNS. Una vez completado el proceso de solicitud, la CA envía los archivos digitales para cargar en el sistema de gestión host. Normalmente, estos archivos contienen una cadena de confianza como la siguiente:

- **Raíz** — en la parte superior de la jerarquía está el certificado raíz, que contiene una clave privada utilizada para firmar otros certificados. El certificado raíz identifica una organización de CA determinada. Si utiliza la misma CA para todos los dispositivos de red, solo necesita un certificado raíz.
- **Intermediate** — ramificándose desde la raíz son los certificados intermedios. La CA emite uno o varios certificados intermedios para actuar como intermediarios entre un certificado raíz y los certificados de servidor protegidos.

- **Servidor** — en la parte inferior de la cadena se encuentra el certificado de servidor, que identifica su entidad específica, como un sitio web u otro dispositivo. Cada controladora de una cabina de almacenamiento requiere un certificado de servidor aparte.

Certificados autofirmados

Cada controladora de la cabina de almacenamiento incluye un certificado autofirmado preinstalado. Un certificado autofirmado es similar a un certificado firmado por CA, excepto que es validado por el propietario de la entidad y no por un tercero. Al igual que un certificado firmado por CA, un certificado autofirmado contiene su propia clave privada, y también garantiza que los datos se cifren y se envíen a través de una conexión HTTPS entre un servidor y un cliente. Sin embargo, un certificado autofirmado no utiliza la misma cadena de confianza que un certificado firmado por CA.

Los certificados autofirmados no son «'de confianza'» por parte de los navegadores. Cada vez que intente conectarse a un sitio web que solo contiene un certificado autofirmado, el explorador mostrará un mensaje de advertencia. Deberá hacer clic en un enlace del mensaje de advertencia para continuar al sitio web; al hacer eso, estará aceptando básicamente el certificado autofirmado.

Certificados usados para el servidor de gestión de claves

Si usa un servidor de gestión de claves externo con la función Drive Security, también puede gestionar los certificados para la autenticación entre ese servidor y las controladoras.

Terminología de certificados

Los siguientes términos se utilizan en la gestión de certificados.

Duración	Descripción
APROX	Una entidad de certificación (CA) es una entidad de confianza que emite documentos electrónicos, denominados certificados digitales, para la seguridad de Internet. Estos certificados identifican a los propietarios de sitios web y, de esta manera, permiten conexiones seguras entre clientes y servidores.
CSR	Una solicitud de firma de certificación (CSR) es un mensaje que envía un solicitante a una entidad de certificación (CA). La CSR valida la información que requiere la CA para emitir un certificado.
Certificado	Un certificado identifica al propietario de un sitio con el fin de brindar seguridad, para evitar que atacantes se hagan pasar por los propietarios del sitio. El certificado tiene información acerca del propietario del sitio y la identidad de la entidad de confianza que certifica (firma) esta información.
Cadena de certificados	La cadena de certificados es una jerarquía de archivos que suma una capa de seguridad a los certificados. Normalmente, la cadena incluye un certificado raíz en la parte superior de la jerarquía, uno o varios certificados intermedios y los certificados de servidor que identifican a las entidades.
Certificado de cliente	En la gestión de claves de seguridad, un certificado de cliente valida las controladoras de la cabina de almacenamiento a fin de que el servidor de gestión de claves pueda confiar en sus direcciones IP.

Duración	Descripción
Certificado intermedio	Uno o varios certificados intermedios se extienden como una rama del certificado raíz en la cadena de certificados. La CA emite uno o varios certificados intermedios para actuar como intermediarios entre un certificado raíz y los certificados de servidor protegidos.
Certificado de servidor de gestión de claves	En la gestión de claves de seguridad, un certificado de servidor de gestión de claves valida el servidor a fin de que la cabina de almacenamiento pueda confiar en su dirección IP.
Almacén de claves	Un almacén de claves es un repositorio en el sistema de gestión host que contiene claves privadas, junto con sus correspondientes claves públicas y certificados. Estas claves y certificados identifican a las entidades propias como, por ejemplo, las controladoras.
Servidor OCSP	El servidor de protocolo de estado de certificado en línea (OCSP) determina si la entidad de certificación (CA) ha revocado algún certificado antes de su fecha de vencimiento programada y bloquea el acceso del usuario a un servidor si se ha revocado el certificado.
Certificado raíz	El certificado raíz se encuentra en la parte superior de la jerarquía de la cadena de certificados y contiene una clave privada que se utiliza para firmar otros certificados. El certificado raíz identifica una organización de CA determinada. Si utiliza la misma CA para todos los dispositivos de red, solo necesita un certificado raíz.
Certificado firmado	Un certificado que ha validado una entidad de certificación (CA). Este archivo de datos contiene una clave privada, y garantiza que los datos se envíen en formato cifrado entre un servidor y un cliente a través de una conexión HTTPS. Además, un certificado firmado incluye detalles sobre el propietario de la entidad (normalmente, un servidor o sitio web) y una firma digital compuesta por letras y números. Un certificado firmado usa una cadena de certificados y, por consiguiente, se utiliza con mayor frecuencia en los entornos de producción. También se conoce como "certificado firmado por CA" o "certificado de gestión".
Certificado autofirmado	Un certificado autofirmado es validado por el propietario de la entidad. Este archivo de datos contiene una clave privada, y garantiza que los datos se envíen en formato cifrado entre un servidor y un cliente a través de una conexión HTTPS. También incluye una firma digital compuesta por letras y números. Un certificado autofirmado no usa la misma cadena de confianza que un certificado firmado por CA y, por consiguiente, se utiliza con mayor frecuencia en los entornos de prueba. También se conoce como certificado "preinstalado".
Certificado de servidor	El certificado de servidor se encuentra en la parte inferior de la cadena de certificados. Este certificado identifica la entidad específica del usuario, por ejemplo, un sitio web u otro dispositivo. Cada controladora de un sistema de almacenamiento requiere un certificado de servidor aparte.

Usar certificados

Use certificados firmados por CA para las controladoras

Es posible obtener certificados firmados por CA para establecer comunicaciones seguras entre las controladoras y el explorador que se utiliza para acceder a System Manager.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de certificación.
- Debe conocer la dirección IP o los nombres DNS de cada controladora.

Acerca de esta tarea

El uso de certificados firmados por CA implica un procedimiento de tres pasos.

Paso 1: Completar los CSR para las controladoras

Primero, es necesario generar un archivo de solicitud de firma de certificación (CSR) para cada controladora de la cabina de almacenamiento.

Acerca de esta tarea

En esta tarea, se describe cómo generar un archivo CSR desde System Manager. La CSR proporciona información sobre la organización y la dirección IP o el nombre DNS de la controladora. Durante esta tarea, se genera un archivo CSR si la cabina de almacenamiento tiene una controladora y dos archivos CSR si posee dos controladoras.

> También puede generar un archivo CSR con una herramienta como OpenSSL y puede saltar a. Paso 2: Envíe los archivos CSR.

Pasos

1. Seleccione MENU:Settings[Certificates].
2. En la ficha Administración de matrices, seleccione **completar CSR**.

   > Si aparece un cuadro de diálogo que le pide que acepte un certificado autofirmado para el segundo controlador, haga clic en **Aceptar certificado autofirmado** para continuar.

3. Introduzca la siguiente información y, a continuación, haga clic en **Siguiente**:
   - **Organización** — el nombre completo y legal de su empresa u organización. Incluya sufijos, como Inc. O Corp
   - **Unidad organizativa (opcional)** — la división de su organización que maneja el certificado.
   - **Ciudad/localidad** — Ciudad en la que se encuentra la matriz de almacenamiento o el negocio.
   - **Estado/Región (opcional)** — el estado o región donde está ubicada la matriz de almacenamiento o el negocio.
   - **Código ISO de país**: Código ISO (Organización Internacional de Normalización) de dos dígitos de su país, por ejemplo, US.

> Algunos campos pueden autocompletarse con la información adecuada, como la dirección IP de la controladora. No cambie los valores autocompletados a menos que esté seguro de que son incorrectos. Por ejemplo, si todavía no ha completado una CSR, la dirección IP de la controladora se establecerá en "'localhost'". En ese caso, deberá cambiar «'localhost'» por el nombre DNS o la dirección IP del controlador.

4. Verifique o introduzca la siguiente información acerca de la controladora A en su cabina de almacenamiento:
   - **Controller un nombre común** — la dirección IP o el nombre DNS del controlador A se muestran de manera predeterminada. Compruebe que la dirección sea correcta; debe coincidir exactamente con lo que escribe para acceder a System Manager en el explorador. El nombre DNS no puede comenzar con un comodín.
   - **Controller a Alternate IP address** — Si el nombre común es una dirección IP, puede opcionalmente escribir cualquier dirección IP adicional o alias para el controlador A. Si va a introducir varios datos, use un formato delimitado por comas.
   - **Nombre DNS alternativo del controlador a** — Si el nombre común es un nombre DNS, introduzca cualquier nombre DNS adicional para el controlador A. Si va a introducir varios datos, use un formato delimitado por comas. Si no hay nombres DNS alternativos, pero especificó un nombre DNS en el primer campo, copie ese nombre aquí. El nombre DNS no puede comenzar con un comodín. Si la cabina de almacenamiento sólo tiene una controladora, el botón **Finalizar** estará disponible.

     Si la cabina de almacenamiento tiene dos controladores, el botón **Siguiente** estará disponible.

> No haga clic en el enlace **Omitir este paso** cuando cree inicialmente una solicitud CSR. El enlace se proporciona para situaciones de recuperación de errores. En raras ocasiones, una solicitud CSR puede generar errores en una controladora, pero no en la otra. Este enlace permite omitir el paso para crear una solicitud CSR en la controladora A si ya está definida, y continuar hacia el siguiente paso para volver a crear una solicitud CSR en la controladora B.

5. Si sólo hay un controlador, haga clic en **Finalizar**. Si hay dos controladores, haga clic en **Siguiente** para introducir información para el controlador B (igual que el anterior) y, a continuación, haga clic en **Finalizar**.

   Para una sola controladora, se descarga un archivo CSR en el sistema local. Para controladoras dobles, se descargan dos archivos CSR. La ubicación de la carpeta de la descarga depende del explorador.

6. Vaya a. Paso 2: Envíe los archivos CSR.

Paso 2: Envíe los archivos CSR

Después de crear los archivos de solicitud de firma de certificación (CSR), envíe los archivos a una CA. Los sistemas E-Series requieren el formato PEM (codificación ASCII Base64) para certificados firmados, que incluye los siguientes tipos de archivo: pem, .crt, .cer o .key.

Pasos

1. Busque los archivos CSR descargados.
2. Envíe los archivos CSR a una CA (por ejemplo, VeriSign o DigiCert) y solicite certificados firmados en formato PEM.

Después de enviar un archivo CSR a la CA, NO vuelva a generar otro archivo CSR. cada vez que genere una CSR, el sistema creará un par de claves pública y privada. La clave pública se incluye en la CSR, mientras que la clave privada se conserva en el almacén de claves del sistema. Cuando recibe los certificados firmados e importarlos, el sistema se asegura de que las claves pública y privada sean la pareja original. Si las claves no coinciden, los certificados firmados no funcionarán y debe solicitar certificados nuevos de la CA.

3. Cuando la CA devuelva los certificados firmados, vaya a. Paso 3: Importar certificados firmados para las controladoras.

Paso 3: Importar certificados firmados para las controladoras

Después de recibir los certificados firmados de la entidad de certificación (CA), importe los archivos para las controladoras.

Antes de empezar

- La CA devolvió archivos de certificado firmados. Estos archivos incluyen el certificado raíz, uno o varios certificados intermedios y los certificados de servidor.
- Si la CA proporcionó un archivo de certificado encadenado (por ejemplo, un archivo .p7b), debe desempaquetar el archivo encadenado en archivos individuales: El certificado raíz, el o los certificados intermedios y los certificados de servidor que identifican a las controladoras. Puede utilizar Windows `certmgr` Utilidad para desempaquetar los archivos (haga clic con el botón derecho y seleccione MENU:todas las tareas[Exportar]). Se recomienda la codificación base-64. Una vez completadas las exportaciones, se mostrará un archivo CER para cada archivo de certificado de la cadena.
- Copió los archivos de certificado en el sistema host donde se accede a System Manager.

Pasos

1. Seleccionar menú:Configuración[certificados]
2. En la ficha Administración de matrices, seleccione **Importar**.

   Se abre un cuadro de diálogo para importar los archivos de certificado.

3. Haga clic en los botones **examinar** para seleccionar primero los archivos de certificado raíz e intermedio y, a continuación, seleccionar cada certificado de servidor para los controladores. El archivo raíz y los archivos intermedios son los mismos para ambas controladoras. Solo los certificados de servidor son únicos para cada controladora. Si generó la CSR desde una herramienta externa, también debe importar el archivo de claves privadas que se creó junto con la CSR.

   Se muestran los nombres de los archivos en el cuadro de diálogo.

4. Haga clic en **Importar**.

   Los archivos se cargan y validan.

Resultado

La sesión finaliza automáticamente. Debe volver a iniciar sesión para que los certificados entren en vigencia. Cuando inicia sesión nuevamente, se utilizan los nuevos certificados firmados por la CA en la sesión.

Restablezca los certificados de gestión

Es posible revertir los certificados que se usan en las controladoras de los certificados firmados por CA a los certificados autofirmados de fábrica.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de certificación.
- Se deben importar de forma previa los certificados firmados por CA.

Acerca de esta tarea

La función Restablecer elimina los archivos de certificados firmados por CA actuales de cada controladora. A continuación, las controladoras revierten al uso de certificados autofirmados.

Pasos

1. Seleccione MENU:Settings[Certificates].
2. En la ficha Administración de matrices, seleccione **Restablecer**.

   Se abre el cuadro de diálogo Confirmar restablecimiento de certificados de gestión.

3. Tipo `reset` En el campo y, a continuación, haga clic en **Restablecer**.

   Una vez que se actualiza el explorador, es posible que el explorador bloquee el acceso al sitio de destino e informe de que el sitio utiliza HTTP estricto Transport Security. Esta condición surge cuando se cambia a certificados autofirmados. Para borrar la condición que bloquea el acceso al destino, debe borrar los datos de navegación del explorador.

Resultados

Las controladoras revierten al uso de certificados autofirmados. Como resultado, el sistema solicita a los usuarios que acepten manualmente el certificado autofirmado para sus sesiones.

Vea información de certificaciones importadas

Desde la página certificados, es posible ver el tipo de certificado, la entidad emisora y el rango válido de fechas de los certificados para la cabina de almacenamiento.

Antes de empezar

Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de certificación.

Pasos

1. Seleccione MENU:Settings[Certificates].
2. Seleccione una de las pestañas para ver información sobre los certificados.

Pestaña	Descripción
Gestión de cabinas	Vea información sobre los certificados firmados por CA importados para cada controladora, incluido el archivo raíz, los archivos intermedios y los archivos de servidor.

Pestaña	Descripción
De confianza	Vea información sobre los otros tipos de certificados importados para las controladoras. Utilice el campo de filtro en **Mostrar certificados…** para ver certificados instalados por el usuario o instalados previamente. • **Instalado por el usuario** — certificados que un usuario cargó en la cabina de almacenamiento, los cuales pueden incluir certificados de confianza cuando la controladora funciona como cliente (en lugar de servidor), certificados LDAPS y certificados de la Federación de identidades. • **Preinstalado** — certificados autofirmados incluidos con la cabina de almacenamiento.
Gestión de claves	Vea información sobre los certificados firmados por CA importados para un servidor de gestión de claves externo.

Importar certificados para las controladoras cuando funcionan como clientes

Si la controladora rechaza una conexión debido a que no puede validar la cadena de confianza de un servidor de red, es posible importar un certificado de la pestaña de confianza con el que la controladora (actuando como cliente) pueda aceptar comunicaciones de ese servidor.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de certificación.
- Los archivos de certificado están instalados en el sistema local.

Acerca de esta tarea

Es posible que sea necesario importar certificados de la pestaña de confianza para permitir que otro servidor se comunique con las controladoras (por ejemplo, un servidor de syslog o un servidor LDAP que utiliza TLS).

Pasos

1. Seleccione MENU:Settings[Certificates].
2. En la ficha Trusted, seleccione **Importar**.

   Se abre un cuadro de diálogo para importar los archivos de certificado de confianza.

3. Haga clic en **examinar** para seleccionar los archivos de certificado para los controladores.

   Se muestran los nombres de los archivos en el cuadro de diálogo.

4. Haga clic en **Importar**.

Resultados

Los archivos se cargan y validan.

Habilite la comprobación de revocación de certificados

Es posible habilitar comprobaciones automáticas de certificados revocados para que el servidor de protocolo de estado de certificado en línea (OCSP) bloquee los usuarios y no permita que realicen conexiones no seguras.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de certificación.
- Existe un servidor DNS configurado en las dos controladoras, lo que permite usar un nombre de dominio completo para el servidor OCSP. Esta tarea está disponible en la página hardware.
- Si desea especificar su propio servidor OCSP, debe conocer la URL de ese servidor.

Acerca de esta tarea

La comprobación de revocación automática es útil cuando la CA emite de manera incorrecta un certificado o cuando la clave privada está en riesgo.

Durante esta tarea, es posible configurar un servidor OCSP o usar el servidor especificado en el archivo de certificado. El servidor OCSP determina si la CA revocó algún certificado antes de su fecha de vencimiento programada y, a continuación, bloquea al usuario para que no acceda al sitio si se ha revocado el certificado.

Pasos

1. Seleccione MENU:Settings[Certificates].
2. Seleccione la ficha **Trusted**.

   ⓘ También puede habilitar la comprobación de revocación en la ficha **Gestión de claves**.

3. Haga clic en **tareas no comunes** y seleccione **Activar comprobación de revocación** en el menú desplegable.
4. Seleccione **deseo habilitar la comprobación de revocación**, de modo que aparezca una Marca de verificación en la casilla de verificación y aparecerán campos adicionales en el cuadro de diálogo.
5. En el campo **Dirección de respondedor OCSP**, puede especificar opcionalmente una URL para un servidor de respuesta OCSP. Si no se especifica ninguna dirección, el sistema utiliza la URL del servidor OCSP incluida en el archivo de certificado.
6. Haga clic en **Dirección de prueba** para asegurarse de que el sistema pueda abrir una conexión a la URL especificada.
7. Haga clic en **Guardar**.

Resultados

Si la cabina de almacenamiento intenta conectarse a un servidor que posee un certificado revocado, la conexión se rechaza y se registra un evento.

Elimine certificados de confianza

Es posible eliminar los certificados instalados por el usuario que se importaron anteriormente desde la pestaña de confianza.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De

lo contrario, no se mostrarán las funciones de certificación.

- Si actualiza a una nueva versión de certificado de confianza, el certificado actualizado debe importarse antes de eliminar el anterior.

> Si elimina un certificado que se utiliza para autenticar las controladoras y otro servidor, como un servidor LDAP, antes de importar un certificado de reemplazo, puede perder el acceso al sistema.

Acerca de esta tarea

En esta tarea, se describe la manera de eliminar certificados instalados por el usuario. No se pueden eliminar los certificados autofirmados preinstalados.

Pasos

1. Seleccione MENU:Settings[Certificates].
2. Seleccione la ficha **Trusted**.

   En la tabla, se muestran los certificados de confianza de la cabina de almacenamiento.

3. En la tabla, seleccione el certificado que desea eliminar.
4. Haga clic en menú:tareas no comunes[Eliminar].

   Se abrirá el cuadro de diálogo Confirmar eliminación de certificado de confianza.

5. Tipo `delete` En el campo y, a continuación, haga clic en **Eliminar**.

Use certificados firmados por CA para la autenticación con un servidor de gestión de claves

Para establecer comunicaciones seguras entre un servidor de gestión de claves y las controladoras de la cabina de almacenamiento, debe configurar los conjuntos de certificados adecuados.

Antes de empezar

Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de certificación.

Acerca de esta tarea

La autenticación entre las controladoras y un servidor de gestión de claves es un procedimiento de dos pasos.

Paso 1: Complete y envíe una CSR para la autenticación con un servidor de gestión de claves

Primero, debe generar un archivo de solicitud de firma de certificación (CSR) y utilizar la CSR para solicitar un certificado de cliente firmado de una entidad de certificación (CA) que confía en el servidor de gestión de claves. También es posible crear y descargar un certificado de cliente desde el servidor de gestión de claves con el archivo CSR descargado. Un certificado de cliente valida las controladoras de la cabina de almacenamiento para que el servidor de gestión de claves pueda confiar en sus solicitudes de protocolo de interoperabilidad de gestión de claves (KMIP).

Pasos

1. Seleccione MENU:Settings[Certificates].
2. En la ficha Gestión de claves, seleccione **completar CSR**.

3. Introduzca la siguiente información:
   - **Nombre común** — un nombre que identifica a esta CSR, como el nombre de la matriz de almacenamiento, que se mostrará en los archivos de certificado.
   - **Organización** — el nombre completo y legal de su empresa u organización. Incluya sufijos, como Inc. O Corp
   - **Unidad organizativa (opcional)** — la división de su organización que maneja el certificado.
   - **Ciudad/localidad** — la ciudad o localidad donde está ubicada su organización.
   - **Estado/Región (opcional)** — el estado o región donde está ubicada su organización.
   - **Código ISO de país** — el código ISO (Organización Internacional de Normalización) de dos dígitos, como US, en el que se encuentra su organización.
4. Haga clic en **Descargar**.

   Se guardará un archivo CSR en el sistema local.

5. Solicite un certificado de cliente firmado de una CA a la que confíe el servidor de gestión de claves.
6. Cuando tenga un certificado de cliente, vaya a. Paso 2: Importar certificados para el servidor de gestión de claves.

Paso 2: Importar certificados para el servidor de gestión de claves

Como paso siguiente, debe importar certificados para la autenticación entre la cabina de almacenamiento y el servidor de gestión de claves. Existen dos tipos de certificados: El certificado de cliente valida las controladoras de la cabina de almacenamiento, mientras que el certificado de servidor de gestión de claves valida al servidor. Debe cargar tanto el archivo de certificado de cliente para las controladoras como el archivo de certificado de servidor para el servidor de gestión de claves.

Antes de empezar

- Tiene un archivo de certificado de cliente firmado (consulte Paso 1: Complete y envíe una CSR para la autenticación con un servidor de gestión de claves), y copió ese archivo en el host donde se accede a System Manager. Un certificado de cliente valida las controladoras de la cabina de almacenamiento para que el servidor de gestión de claves pueda confiar en sus solicitudes de protocolo de interoperabilidad de gestión de claves (KMIP).
- Debe recuperar un archivo de certificado del servidor de gestión de claves y, a continuación, copiar ese archivo en el host donde va a acceder a System Manager. Un certificado de servidor de gestión de claves valida el servidor de gestión de claves para que la cabina de almacenamiento pueda confiar en su dirección IP. Es posible usar un certificado raíz, intermedio o de servidor para el servidor de gestión de claves.

> Si desea obtener más información sobre el certificado de servidor, consulte la documentación del servidor de gestión de claves.

Pasos

1. Seleccione MENU:Settings[Certificates].
2. En la ficha Gestión de claves, seleccione **Importar**.

   Se abre un cuadro de diálogo para importar los archivos de certificado.

3. Junto a **Seleccionar certificado de cliente**, haga clic en el botón **examinar** para seleccionar el archivo de certificado de cliente para los controladores de la matriz de almacenamiento.

Se muestra el nombre del archivo en el cuadro de diálogo.

4. Junto a **Seleccionar certificado de servidor del servidor de administración de claves**, haga clic en el botón **examinar** para seleccionar el archivo de certificado de servidor del servidor de administración de claves. Es posible elegir un certificado raíz, intermedio o de servidor para el servidor de gestión de claves.

   Se muestra el nombre del archivo en el cuadro de diálogo.

5. Haga clic en **Importar**.

   Los archivos se cargan y validan.

Exportar certificados del servidor de gestión de claves

Es posible guardar un certificado para un servidor de gestión de claves en una máquina local.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de certificación.
- Los certificados deben haberse importado previamente.

Pasos

1. Seleccione MENU:Settings[Certificates].
2. Seleccione la ficha **Gestión de claves**.
3. En la tabla, seleccione el certificado que desea exportar y, a continuación, haga clic en **Exportar**.

   Se abre el cuadro de diálogo Guardar.

4. Introduzca un nombre de archivo y haga clic en **Guardar**.

Preguntas frecuentes

¿Por qué se muestra el cuadro de diálogo no se puede acceder a otra controladora?

Cuando se realizan ciertas operaciones relacionadas con los certificados de CA (por ejemplo, la importación de un certificado), es posible que aparezca un cuadro de diálogo que le solicite aceptar un certificado autofirmado para la segunda controladora.

En las cabinas de almacenamiento con dos controladoras (configuraciones dúplex), este cuadro de diálogo aparece en ocasiones si System Manager de SANtricity no puede comunicarse con la segunda controladora, o bien si el explorador no puede aceptar el certificado durante un determinado punto en una operación.

Si se abre este cuadro de diálogo, haga clic en **Aceptar certificado autofirmado** para continuar. Si otro cuadro de diálogo le solicita una contraseña, introduzca la contraseña de administrador que utiliza para acceder a System Manager.

En caso de que este cuadro de diálogo se muestre nuevamente y no pueda completar una tarea de certificado, intente uno de los procedimientos a continuación:

- Utilice un tipo de explorador diferente para acceder a esta controladora, acepte el certificado y continúe.

- Acceda a la segunda controladora con System Manager, acepte el certificado autofirmado y luego regrese a la primera controladora y continúe.

¿Cómo saber qué certificados deben cargarse en System Manager para la gestión de claves externas?

Para la gestión de claves externas, debe importar dos tipos de certificados para la autenticación entre la cabina de almacenamiento y el servidor de gestión de claves, de forma tal que exista confianza mutua entre las dos entidades.

Un certificado de cliente valida las controladoras de la cabina de almacenamiento para que el servidor de gestión de claves pueda confiar en sus solicitudes de protocolo de interoperabilidad de gestión de claves (KMIP). Para obtener un certificado de cliente, se usa System Manager para completar una CSR para la cabina de almacenamiento. Luego, puede cargar la CSR en un servidor de gestión de claves y generar un certificado de cliente a partir de ese punto. Una vez que tenga un certificado de cliente, copie ese archivo en el host donde acceda a System Manager.

Un certificado de servidor de gestión de claves valida el servidor de gestión de claves para que la cabina de almacenamiento pueda confiar en su dirección IP. Recupere el archivo de certificado de servidor del servidor de gestión de claves y copie ese archivo en el host donde va a acceder a System Manager.

¿Qué debo saber acerca de la comprobación de revocación de certificados?

System Manager permite verificar certificados revocados mediante un servidor de protocolo de estado de certificado en línea (OCSP), en lugar de cargar listas de revocación de certificados (CRL).

Los certificados revocados ya no deberán considerarse de confianza. Un certificado puede ser revocado por varios motivos; por ejemplo, si la entidad de certificación (CA) emitió el certificado incorrectamente, una clave privada quedó en riesgo o la entidad identificada no cumplió con los requisitos de la política.

Después de establecer una conexión con un servidor OCSP en System Manager, la cabina de almacenamiento realiza la verificación de revocación cada vez que se conecta a un servidor de AutoSupport, un servidor de gestión de claves externo (EKMS), un servidor de protocolo ligero de acceso a directorios por SSL (LDAPS) o un servidor de syslog. La cabina de almacenamiento intenta validar los certificados de tales servidores para asegurarse de que no se hayan revocado. A continuación, el servidor obtiene los valores "good", "revoked" o "unknown" para ese certificado. Si el certificado se revoca o la cabina no puede conectarse al servidor de OCSP, la conexión se rechaza.

> La especificación de una dirección de respuesta de OCSP en System Manager o en la interfaz de línea de comandos (CLI) anula la dirección de OCSP que se encontró en el archivo de certificado.

¿Para qué tipos de servidores se habilitará la comprobación de revocación?

La cabina de almacenamiento realiza la verificación de revocación cada vez que se conecta a un servidor AutoSupport, un servidor de gestión de claves externo (EKMS), un servidor de protocolo ligero de acceso a directorios por SSL (LDAPS) o un servidor de syslog.

Soporte técnico

Información general del soporte

La página Soporte proporciona acceso a recursos de soporte técnico.

¿Qué tareas de soporte hay disponibles?

En Support, es posible ver contactos de soporte técnico, realizar diagnósticos, configurar AutoSupport, ver el registro de eventos y realizar actualizaciones de software.

Obtenga más información:

- "Información general sobre la función AutoSupport"
- "Información general sobre el registro de eventos"
- "Información general del centro de actualización"

¿Cómo puedo ponerme en contacto con el soporte técnico?

En la página principal, haga clic en MENU:Support[Support Center > Support Resources tab]. La información de contacto del soporte técnico se incluye en la esquina superior derecha de la interfaz.

Ver información y diagnóstico

Ver el perfil de la cabina de almacenamiento

El perfil de la cabina de almacenamiento proporciona una descripción de todos los componentes y las propiedades de la cabina de almacenamiento.

Acerca de esta tarea

Es posible usar el perfil de la cabina de almacenamiento a modo de ayuda durante la recuperación o como información general de la configuración actual de la cabina de almacenamiento. Puede ser conveniente guardar una copia del perfil de la cabina de almacenamiento en el cliente de gestión y conservar una copia impresa del perfil de la cabina de almacenamiento con la cabina de almacenamiento. Cree una nueva copia del perfil de la cabina de almacenamiento si cambia la configuración.

Pasos

1. Seleccione menú:ficha Soporte[Centro de soporte > Recursos de soporte].
2. Desplácese hasta **Iniciar información detallada de la matriz de almacenamiento** y, a continuación, seleccione **Perfil de la matriz de almacenamiento**.

   Se muestra el informe en la pantalla.

Detalles del campo

Sección	Descripción
Cabina de almacenamiento	Se muestran todas las opciones que se pueden configurar y las opciones estáticas del sistema para la cabina de almacenamiento. Estas opciones incluyen la cantidad de controladoras, bandejas de unidades, unidades, pools de discos, grupos de volúmenes, Volúmenes y unidades de repuesto; la cantidad máxima de bandejas de unidades, unidades, discos de estado sólido (SSD) y volúmenes permitidos; la cantidad de grupos Snapshot, imágenes Snapshot, volúmenes Snapshot y grupos de coherencia; información sobre funciones; información sobre versiones de firmware; información sobre el número de serie del chasis; estado de AutoSupport e información de programación de AutoSupport; La configuración para la recogida automática de datos de soporte y la recogida programada de datos de soporte, el identificador a nivel mundial (WWID) de la cabina de almacenamiento y la configuración de análisis de medios y caché.
Reducida	Se muestra una lista de todos los dispositivos de almacenamiento de la cabina de almacenamiento. Según la configuración de la cabina de almacenamiento, en la sección de almacenamiento, podrían mostrarse las siguientes subsecciones. • **Disk Pools** — muestra una lista de todos los grupos de discos en la matriz de almacenamiento. • **Grupos de volúmenes** — muestra una lista de todos los grupos de volúmenes de la cabina de almacenamiento. Los volúmenes y la capacidad libre se enumeran en el orden en que se crearon. • **Volumes** — muestra una lista de todos los volúmenes de la matriz de almacenamiento. La información descrita incluye el nombre del volumen, el estado del volumen, la capacidad, el nivel de RAID, el grupo de volúmenes o pool de discos, el tipo de unidad y detalles adicionales. • **Volúmenes faltantes** — muestra una lista de todos los volúmenes de la matriz de almacenamiento que actualmente tienen un estado faltante. La información descrita incluye el identificador a nivel mundial (WWID) para cada volumen faltante.

Sección	Descripción
Servicios de copia	Se muestra una lista de todos los servicios de copias que se usan para la cabina de almacenamiento. Según la configuración de la cabina de almacenamiento, en la sección de servicios de copias, podrían mostrarse las siguientes subsecciones: • **Copias de volumen** — muestra una lista de todos los pares de copias en la matriz de almacenamiento. La información descrita incluye el número de copias, los nombres de las parejas de copias, el estado, la Marca de hora de inicio y detalles adicionales. • **Grupos Snapshot** — muestra una lista de todos los grupos de instantáneas de la matriz de almacenamiento. • **Imágenes Snapshot** — muestra una lista de todas las instantáneas de la matriz de almacenamiento. • **Volúmenes Snapshot** — muestra una lista de todos los volúmenes Snapshot de la matriz de almacenamiento. • **Grupos de consistencia** — muestra una lista de todos los grupos de consistencia de la matriz de almacenamiento. • **Volúmenes miembro** — muestra una lista de todos los volúmenes miembro de grupo de coherencia de la cabina de almacenamiento. • * Grupos de duplicación* — muestra una lista de todos los volúmenes duplicados. • **Capacidad reservada**: Se muestra una lista de todos los volúmenes de capacidad reservada de la cabina de almacenamiento.
Asignaciones de host	Se muestra una lista de las asignaciones de hosts de la cabina de almacenamiento. La información descrita incluye el nombre del volumen, el número de unidad lógica (LUN), el ID de la controladora, el nombre de host o el nombre del clúster de hosts y el estado del volumen. La información adicional enumerada incluye definiciones de topología y definiciones de tipos de hosts.

Sección	Descripción
Hardware subyacente	Se muestra una lista de todo el hardware de la cabina de almacenamiento. Según la configuración de la cabina de almacenamiento, en la sección de hardware, podrían mostrarse las siguientes subsecciones. • **Controladores** — muestra una lista de todas las controladoras de la matriz de almacenamiento e incluye la ubicación, el estado y la configuración del controlador. Además, se incluye información del canal de unidades, información del canal de hosts e información del puerto Ethernet. • **Drives** — muestra una lista de todas las unidades de la matriz de almacenamiento. Las unidades se enumeran por orden de ID de bandeja, ID de cajón e ID de ranura. La información descrita incluye el ID de bandeja, el ID de cajón, el ID de ranura, el estado, la capacidad bruta, El tipo de medio, el tipo de interfaz, la tasa de datos actual, el ID de producto y la versión de firmware de cada unidad. En la sección de la unidad, también se incluye información del canal de unidades, información de cobertura de piezas de repuesto e información sobre deterioro (solo para unidades SSD). La información sobre deterioro incluye el porcentaje de resistencia usado, que es la cantidad de datos escritos en la unidad SSD hasta la fecha, dividida por el límite de escritura teórico total para las unidades. • **Canales de unidad** — muestra información de todos los canales de unidad de la matriz de almacenamiento. La información descrita incluye el estado de los canales, el estado de los enlaces (si corresponde), el número de unidades y el número acumulativo de errores. • **Bandejas** — muestra información de todas las estanterías de la matriz de almacenamiento. La información descrita incluye los tipos de unidades y la información de estado de cada componente de la bandeja. Es posible que los componentes de la bandeja incluyan paquetes de batería, transceptores de factor de forma pequeño conectable (SFP), contenedores de alimentación/ventilador o contenedores de módulos de entrada/salida (IOM). En la sección de hardware, también se muestra el identificador de clave de seguridad si la cabina de almacenamiento usa una clave de seguridad.
Funciones	Se muestra una lista de los paquetes de funciones instalados y la cantidad máxima permitida de grupos Snapshot, snapshots (heredadas) y volúmenes por host o clúster de hosts. La información de la sección funciones también incluye datos sobre seguridad de unidades; es decir, si la cabina de almacenamiento tiene la función de seguridad habilitada o deshabilitada.

3. Para buscar en el perfil de la matriz de almacenamiento, escriba un término de búsqueda en el cuadro de texto **Buscar** y haga clic en **Buscar**.

   Se destacan todos los términos que coinciden. Para desplazarse por todos los resultados, uno a la vez, haga clic en **Buscar**.

4. Para guardar el perfil de la matriz de almacenamiento, haga clic en **Guardar**.

   El archivo se guarda en la carpeta de descargas del explorador con el nombre `storage-array-profile.txt`.

Ver el inventario de software y firmware

En el inventario de software y firmware, se enumeran las versiones de firmware para cada componente de la cabina de almacenamiento.

Acerca de esta tarea

Una cabina de almacenamiento está compuesta por muchos componentes, que pueden incluir controladoras, unidades, cajones y módulos de entrada/salida (IOM). Cada uno de estos componentes contiene firmware. Algunas versiones de firmware dependen de otras versiones de firmware. Para captar información sobre todas las versiones de firmware de la cabina de almacenamiento, se debe ver el inventario de software y firmware. El soporte técnico puede analizar el inventario de software y firmware para detectar incoherencias de firmware.

Pasos

1. Seleccione menú:ficha Soporte[Centro de soporte > Recursos de soporte].
2. Desplácese hasta **Iniciar información detallada de la matriz de almacenamiento** y, a continuación, seleccione **Inventario de software y firmware**.

   En la pantalla, se muestra el informe Inventario de software y firmware.

3. Para guardar el inventario de software y firmware, haga clic en **Guardar**.

   El archivo se guarda en la carpeta de descargas del explorador con el nombre de archivo `firmware-inventory.txt`.

4. Siga las instrucciones del soporte técnico para enviar el archivo.

Recopilar datos de diagnóstico

Recopilar manualmente datos de soporte

Es posible recopilar distintas clases de inventario, Estados y datos de rendimiento acerca de la cabina de almacenamiento en un único archivo. El soporte técnico puede utilizar el archivo para la solución de problemas y un análisis más profundo.

Acerca de esta tarea

> Si la función AutoSupport está activada, también puede recopilar estos datos en la ficha **AutoSupport** y seleccionando **Enviar envío AutoSupport**.

Solo se puede ejecutar una operación de recogida a la vez. Si intenta iniciar otra operación, recibirá un mensaje de error.

> Realice esta operación solo cuando el soporte técnico se lo indique.

Pasos

1. Seleccione menú:ficha Soporte[Centro de soporte > Diagnóstico].
2. Seleccione **recopilar datos de soporte**.
3. Haga clic en **recoger**.

   El archivo se guarda en la carpeta de descargas del explorador con el nombre `support-data.7z`. Si la bandeja tiene cajones, los datos diagnósticos de esa bandeja se archivan en otro archivo comprimido con el nombre `tray-component-state-capture.7z`.

4. Siga las instrucciones del soporte técnico para enviar el archivo.

Recopilar datos de configuración

Es posible guardar datos de configuración RAID de la controladora, que incluye todos los datos de los grupos de volúmenes y pools de discos. Luego, puede ponerse en contacto con el soporte técnico para obtener ayuda con la restauración de los datos.

Acerca de esta tarea

En esta tarea, se describe cómo guardar el estado actual de la base de datos de configuración de RAID. Estos datos se recuperan de la ubicación de la memoria RPA de la controladora.

> La función recoger datos de configuración guarda la misma información que el comando de la CLI para `save storageArray dbmDatabase`.

Solo debe realizar esta tarea cuando se lo indique una operación de Recovery Guru o el soporte técnico.

Pasos

1. Seleccione menú:ficha Soporte[Centro de soporte > Diagnóstico].
2. Seleccione **recopilar datos de configuración**.
3. En el cuadro de diálogo, haga clic en **recopilar**.

   El archivo, `configurationData-<arrayName>-<dateTime>.7z`, Se guarda en la carpeta de descargas del explorador.

4. Póngase en contacto con el soporte técnico para obtener más información sobre cómo enviar el archivo y para cargar los datos de nuevo en el sistema.

Recupere los archivos de soporte de recuperación

El soporte técnico puede utilizar archivos de soporte de recuperación para solucionar problemas. System Manager guarda automáticamente estos archivos.

Antes de empezar

El soporte técnico solicitó el envío de archivos adicionales para la solución de problemas.

Acerca de esta tarea

Los archivos de soporte de recuperación incluyen los siguientes tipos de archivo:

- Archivos de datos de soporte

- Historia de AutoSupport
- Registro de AutoSupport
- Archivos de diagnóstico SAS/RLS
- Datos de perfil de recuperación
- Archivos de captura de base de datos

Pasos

1. Seleccione menú:ficha Soporte[Centro de soporte > Diagnóstico].
2. Seleccione **recuperar archivos de soporte de recuperación**.

   Se muestra un cuadro de diálogo con todos los archivos de soporte de recuperación recogidos por la cabina de almacenamiento. Para buscar archivos específicos, puede ordenar cualquiera de las columnas o escribir caracteres en el cuadro **filtro**.

3. Seleccione un archivo y, a continuación, haga clic en **Descargar**.

   El archivo se guarda en la carpeta de descargas del explorador.

4. Si necesita guardar más archivos, repita el paso anterior.
5. Haga clic en **Cerrar**.
6. Siga las instrucciones del soporte técnico para enviar el archivo.

Recuperar búferes de seguimiento

Es posible recuperar los búferes de seguimiento de las controladoras y enviar el archivo al soporte técnico para su análisis.

Acerca de esta tarea

El firmware utiliza los búferes de seguimiento para registrar el procesamiento, especialmente las condiciones de excepción, que pueden ser de utilidad para la depuración. Es posible recuperar búferes de seguimiento sin interrupciones en el funcionamiento de la cabina de almacenamiento y con efectos mínimos sobre el rendimiento.

> Realice esta operación solo cuando el soporte técnico se lo indique.

Pasos

1. Seleccione menú:ficha Soporte[Centro de soporte > Diagnóstico].
2. Seleccione **recuperar búferes de seguimiento**.
3. Seleccione la casilla junto a cada controladora para la que desee recuperar búferes de seguimiento.

   Puede seleccionar una o dos controladoras. Si el mensaje de estado de la controladora a la derecha de la casilla es con errores o Deshabilitado, la casilla estará deshabilitada.

4. Haga clic en **Sí**.

   El archivo se guarda en la carpeta de descargas del explorador con el nombre de archivo `trace-buffers.7z`.

5. Siga las instrucciones del soporte técnico para enviar el archivo.

Recoja estadísticas de rutas de I/O.

Puede guardar el archivo de estadísticas de la ruta de I/o y enviarlo al soporte técnico para su análisis.

Acerca de esta tarea

El soporte técnico utiliza las estadísticas de la ruta de I/o para ayudar a diagnosticar problemas de rendimiento. Los problemas de rendimiento de la aplicación pueden producirse por la utilización de memoria, utilización de CPU, latencia de red, latencia de I/o u otros problemas. Las estadísticas de la ruta de I/o se obtienen automáticamente durante la recogida de datos de soporte, o bien es posible recogerlas manualmente. Además, si AutoSupport está activado, las estadísticas de la ruta de I/o se recopilan automáticamente y se envían a soporte técnico.

Los contadores de estadísticas de la ruta de I/o vuelven a cero una vez que el usuario confirma que desea recoger las estadísticas de la ruta de I/O. Los contadores vuelven a cero incluso si después se cancela la operación. Además, los contadores también vuelven a cero cuando la controladora se restablece (reinicia).

Realice esta operación solo cuando el soporte técnico se lo indique.

Pasos

1. Seleccione menú:ficha Soporte[Centro de soporte > Diagnóstico].
2. Seleccione **recoger estadísticas de ruta de E/S**.
3. Para confirmar que desea llevar a cabo la operación, escriba `collect`Y, a continuación, haga clic en **recopilar**.

   El archivo se guarda en la carpeta de descargas del explorador con el nombre de archivo `io-path-statistics.7z`.

4. Siga las instrucciones del soporte técnico para enviar el archivo.

Recuperar una imagen de estado

Es posible revisar la imagen de estado de una controladora. Una imagen de estado es un volcado de datos sin formato de la memoria del procesador de la controladora que el soporte técnico puede utilizar para diagnosticar un problema con una controladora.

Acerca de esta tarea

El firmware genera automáticamente una imagen de estado cuando detecta ciertos errores. Después de que se genera una imagen de estado, se reinicia la controladora con el error y se registra un evento en el registro de eventos.

Si se activó AutoSupport, la imagen de estado se envía automáticamente al soporte técnico. Si no se activó AutoSupport, es necesario ponerse en contacto con el soporte técnico para obtener instrucciones sobre la forma de recuperar la imagen de estado y enviarla al soporte para su análisis.

Realice esta operación solo cuando el soporte técnico se lo indique.

Pasos

1. Seleccione menú:ficha Soporte[Centro de soporte > Diagnóstico].
2. Seleccione **recuperar imagen médica**.

Puede revisar la sección de detalles para ver el tamaño de la imagen de estado antes de descargar el archivo.

3. Haga clic en **recoger**.

   El archivo se guarda en la carpeta de descargas del explorador con el nombre `health-image.7z`.

4. Siga las instrucciones del soporte técnico para enviar el archivo.

Realizar acciones de recuperación

Ver el registro de sectores ilegibles

Es posible guardar el registro de sectores ilegibles y enviar el archivo al soporte técnico para el análisis.

Acerca de esta tarea

El registro de sectores ilegibles contiene registros detallados de sectores ilegibles causados por los informes de errores irrecuperables de medios que generan las unidades. Los sectores ilegibles se detectan durante operaciones normales de I/o y de modificación, como reconstrucciones. Cuando se detectan sectores ilegibles en una cabina de almacenamiento, aparece una alerta que indica que se requiere atención para la cabina de almacenamiento. Recovery Guru distingue qué condición de sector ilegible necesita atención. No se pueden recuperar los datos contenidos en un sector ilegible y estos datos deben considerarse perdidos.

El registro de sectores ilegibles puede almacenar hasta 1,000 sectores ilegibles. Cuando el registro de sectores ilegibles alcanza las 1,000 entradas, se aplican las siguientes condiciones:

- Si se detectan sectores ilegibles nuevos durante la reconstrucción, esta última falla y no se registra ninguna entrada.
- Para los sectores ilegibles nuevos detectados durante las operaciones de I/o, fallan las I/o y no se registra ninguna entrada.

> Estas acciones incluyen escrituras RAID 5 y RAID 6 que se habrían realizado correctamente antes del desbordamiento.

> **Posible pérdida de datos** — la recuperación de sectores ilegibles es un procedimiento complicado que puede implicar varios métodos diferentes. Realice esta operación solo cuando el soporte técnico se lo indique.

Pasos

1. Seleccione menú:ficha Soporte[Centro de soporte > Diagnóstico].
2. Seleccione **Ver/borrar sectores ilegibles**.
3. Para guardar el registro de sectores ilegibles:

   a. En la primera columna de la tabla, es posible seleccionar los volúmenes individuales para los cuales se desea guardar el registro de sectores ilegibles (haga clic en la casilla de comprobación junto a cada volumen) o es posible seleccionar todos los volúmenes (seleccione la casilla de comprobación del encabezado de la tabla).

      Para buscar volúmenes específicos, puede ordenar cualquiera de las columnas o escribir caracteres en el cuadro **filtro**.

b. Haga clic en **Guardar**.

El archivo se guarda en la carpeta de descargas del explorador con el nombre `unreadable-sectors.txt`.

4. Si el soporte técnico le indica que borre el registro de sectores ilegibles, siga los siguientes pasos:
   a. En la primera columna de la tabla, es posible seleccionar los volúmenes individuales para los cuales se desea borrar el registro de sectores ilegibles (haga clic en la casilla de comprobación junto a cada volumen) o es posible seleccionar todos los volúmenes (seleccione la casilla de comprobación del encabezado de la tabla).
   b. Haga clic en **Borrar** y confirme que desea realizar la operación.

Vuelva a habilitar puertos de unidad

Es posible indicar a la controladora que se ha tomado esa acción correctiva para recuperar el sistema de una condición de conexión incorrecta.

Pasos

1. Seleccione menú:ficha Soporte[Centro de soporte > Diagnóstico].
2. Seleccione **Volver a habilitar puertos de unidad** y confirme que desea realizar la operación.

   Esta opción solo se muestra cuando la cabina de almacenamiento contiene puertos de unidad deshabilitados.

   La controladora vuelve a habilitar los puertos SAS que se deshabilitaron al detectar una conexión incorrecta.

Desactivar el modo de recuperación

Después de restaurar la configuración de una cabina de almacenamiento, use la operación Clear Recovery Mode para reanudar las operaciones de I/o en la cabina de almacenamiento y restablecer las operaciones normales.

Antes de empezar

- Si desea que la cabina de almacenamiento regrese a una configuración previa, debe restaurar la configuración desde backup antes de desactivar el modo de recuperación.
- Debe efectuar comprobaciones de validación o corroborar con el soporte técnico para asegurarse de que la restauración se haya realizado correctamente. Una vez que se determina que la restauración se realizó correctamente, se puede desactivar el modo de recuperación.

Acerca de esta tarea

La cabina de almacenamiento contiene una base de datos de configuración que incluye un registro de la configuración lógica (pools, grupo de volúmenes, volúmenes, etc). Si elimina intencionalmente la configuración de la cabina de almacenamiento o si se daña la base de datos de configuración, la cabina de almacenamiento entra en modo de recuperación. El modo de recuperación detiene las operaciones de I/o y congela la base de datos de configuración, lo que da tiempo para llevar a cabo una de las siguientes acciones:

- Restaure la configuración desde la función de backup automático almacenada en los dispositivos flash de la controladora. Debe comunicarse con el soporte técnico para hacerlo.
- Restaure la configuración desde una operación Save Configuration Database anterior. Las operaciones

Save Configuration Database se llevan a cabo a través de la interfaz de línea de comandos (CLI).

- Vuelva a configurar la cabina de almacenamiento desde cero.

Una vez que se pudo restaurar o redefinir la configuración de la cabina de almacenamiento y se pudo verificar que todo funciona bien, se debe desactivar manualmente el modo de recuperación.

> Una vez que se inicia, no es posible cancelar la operación Clear Recovery Mode. Esta operación puede llevar mucho tiempo. Realice esta operación solo cuando el soporte técnico se lo indique.

Pasos

1. Seleccione menú:ficha Soporte[Centro de soporte > Diagnóstico].
2. Seleccione **Desactivar modo de recuperación** y confirme que desea realizar esta operación.

   La opción aparece solamente si la cabina de almacenamiento se encuentra en modo de recuperación.

Gestione AutoSupport

Información general sobre la función AutoSupport

La función AutoSupport supervisa el estado de una cabina de almacenamiento y envía mensajes automáticos al soporte técnico.

El soporte técnico utiliza los datos de AutoSupport de manera reactiva para acelerar el diagnóstico y la resolución de problemas del cliente, y de manera proactiva para detectar y evitar potenciales problemas.

Los datos de AutoSupport incluyen información sobre la configuración, el estado, el rendimiento y los eventos del sistema de una cabina de almacenamiento. Los datos de AutoSupport no incluyen datos de usuario. Los mensajes pueden enviarse inmediatamente o según una programación (diaria y semanal).

Ventajas clave

Algunas de las ventajas clave de la función AutoSupport son las siguientes:

- Resolución de incidencias más rápida
- Supervisión sofisticada para gestionar los incidentes de forma más rápida
- Informes automatizados de acuerdo con una programación, además de generación de informes automatizada sobre eventos críticos
- Solicitudes de reemplazo de hardware automatizadas para ciertos componentes, como unidades
- Alertas no intrusivas para notificar problemas y ofrecer información para que el soporte técnico tome acciones correctivas
- Herramientas de análisis de AutoSupport que supervisan los mensajes por si surgen problemas de configuración conocidos

Funciones individuales de AutoSupport

La función AutoSupport cuenta con tres funciones individuales que se habilitan por separado.

- **Basic AutoSupport** — permite que la cabina de almacenamiento recopile y envíe datos al soporte técnico automáticamente.

- **AutoSupport OnDemand** — permite al soporte técnico solicitar la retransmisión de un envío anterior de AutoSupport cuando se necesita solucionar un problema. Todas las transmisiones se inician en la cabina de almacenamiento, no en el servidor de AutoSupport. La cabina de almacenamiento realiza comprobaciones periódicas con el servidor de AutoSupport para determinar si existen solicitudes de retransmisión pendientes y responde de manera acorde.
- **Diagnóstico remoto** — permite al soporte técnico solicitar un nuevo mensaje de AutoSupport actualizado cuando se necesita para solucionar un problema. Todas las transmisiones se inician en la cabina de almacenamiento, no en el servidor de AutoSupport. La cabina de almacenamiento realiza comprobaciones periódicas con el servidor de AutoSupport para determinar si existen solicitudes nuevas pendientes y responde de manera acorde.

Diferencia entre AutoSupport y recoger datos de soporte

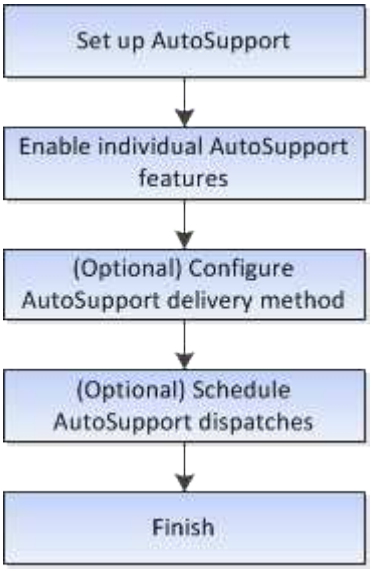
Existen dos métodos para recoger datos de soporte en la cabina de almacenamiento:

- **Función AutoSupport** — los datos se recopilan automáticamente.
- **Opción de recopilar datos de soporte** — los datos deben recopilarse y enviarse manualmente.

La función AutoSupport es más fácil de usar, ya que los datos se recogen y se envían automáticamente. Los datos de AutoSupport pueden utilizarse proactivamente para evitar problemas antes de que sucedan. La función AutoSupport acelera la solución de problemas, ya que el soporte técnico ya tiene acceso a los datos. Por estos motivos, la función AutoSupport es el método de recogida de datos preferido.

Flujo de trabajo de la función AutoSupport

En System Manager, puede configurar la función AutoSupport siguiendo estos pasos.



Habilitar o deshabilitar funciones de AutoSupport

Es posible habilitar la función AutoSupport y las funciones individuales de AutoSupport durante la configuración inicial, o bien es posible habilitarlas o deshabilitarlas más adelante.

Antes de empezar

Si desea habilitar AutoSupport OnDemand o Remote Diagnostics, el método de entrega de AutoSupport debe

configurarse en HTTPS.

Acerca de esta tarea

Es posible deshabilitar la función AutoSupport en cualquier momento, pero se recomienda especialmente dejarla habilitada. Habilitar la función AutoSupport puede acelerar significativamente la detección y resolución de problemas cuando se producen fallos en la cabina de almacenamiento.

La función AutoSupport cuenta con tres funciones individuales que se habilitan por separado.

- **Basic AutoSupport** — permite que la cabina de almacenamiento recopile y envíe datos al soporte técnico automáticamente.
- **AutoSupport OnDemand** — permite al soporte técnico solicitar la retransmisión de un envío anterior de AutoSupport cuando se necesita solucionar un problema. Todas las transmisiones se inician en la cabina de almacenamiento, no en el servidor de AutoSupport. La cabina de almacenamiento realiza comprobaciones periódicas con el servidor de AutoSupport para determinar si existen solicitudes de retransmisión pendientes y responde de manera acorde.
- **Diagnóstico remoto** — permite al soporte técnico solicitar un nuevo mensaje de AutoSupport actualizado cuando se necesita para solucionar un problema. Todas las transmisiones se inician en la cabina de almacenamiento, no en el servidor de AutoSupport. La cabina de almacenamiento realiza comprobaciones periódicas con el servidor de AutoSupport para determinar si existen solicitudes nuevas pendientes y responde de manera acorde.

Pasos

1. Seleccione menú:ficha Soporte[Centro de soporte > AutoSupport].
2. Seleccione **Activar/desactivar funciones de AutoSupport**.
3. Seleccione las casillas ubicadas junto a las funciones de AutoSupport que desea habilitar.

   Las funciones dependen una de otra, como lo indican las marcas de los elementos en el cuadro de diálogo. Por ejemplo, debe habilitar AutoSupport OnDemand para poder habilitar Remote Diagnostics.

4. Haga clic en **Guardar**.

   Si deshabilita AutoSupport, se muestra una notificación en la página Inicio. Puede descartar la notificación haciendo clic en **Ignorar**.

Configurar el método de entrega de AutoSupport

La función AutoSupport admite los protocolos HTTPS, HTTP y SMTP para entregar informes al soporte técnico.

Antes de empezar

- Se debe habilitar la función AutoSupport. Puede comprobar si está habilitada en la página AutoSupport.
- Debe haber un servidor DNS instalado y configurado en la red. La dirección del servidor DNS debe configurarse en System Manager (esta tarea está disponible en la página hardware).

Acerca de esta tarea

Revise los diferentes protocolos:

- **HTTPS** — le permite conectarse directamente al servidor de soporte técnico de destino mediante HTTPS. Si desea habilitar AutoSupport OnDemand o Remote Diagnostics, el método de entrega de AutoSupport debe configurarse en HTTPS.

- **HTTP** — le permite conectarse directamente al servidor de soporte técnico de destino mediante HTTP.
- **Correo electrónico** — le permite utilizar un servidor de correo electrónico como método de entrega para enviar mensajes AutoSupport.

> **Diferencias entre los métodos HTTPS/HTTP y Email**. El método de entrega por correo electrónico, que utiliza SMTP, tiene algunas diferencias importantes con los métodos de entrega mediante HTTPS y HTTP. Primero, el tamaño de los mensajes para el método de correo electrónico se limita a 5 MB, lo cual significa que algunas recogidas de datos ASUP no se enviarán. Segundo, la función AutoSupport OnDemand solo está disponible en los métodos de entrega mediante HTPP y HTTPS.

Pasos

1. Seleccione menú:ficha Soporte[Centro de soporte > AutoSupport].
2. Seleccione **Configurar método de entrega de AutoSupport**.

   Se muestra un cuadro de diálogo con una lista de los métodos de entrega de mensajes.

3. Seleccione el método de entrega deseado y los parámetros para ese método. Debe realizar una de las siguientes acciones:
   - Si eligió HTTPS o HTTP, seleccione uno de los siguientes parámetros de entrega:
     - **Directamente** — este parámetro de entrega es la selección predeterminada. Esta opción permite la conexión directa con el sistema de soporte técnico de destino mediante el protocolo HTTPS o HTTP.
     - **Via Proxy Server** — elegir esta opción le permite especificar los detalles del servidor proxy HTTP necesarios para establecer la conexión con el sistema de soporte técnico de destino. Es necesario especificar la dirección y el número de puerto del host. No obstante, solo se deben introducir los detalles de autenticación del host (nombre de usuario y contraseña) si así se requiere.
     - **Secuencia de comandos de configuración automática vía Proxy (PAC)**: Especifique la ubicación de un archivo de secuencia de comandos de configuración automática de proxy (PAC). Un archivo de PAC permite al sistema seleccionar automáticamente el servidor proxy adecuado para establecer una conexión con el sistema de soporte técnico de destino.
   - Si seleccionó correo electrónico, introduzca la siguiente información:
     - La dirección del servidor de correo como un nombre de dominio completo, una dirección IPv4 o una dirección IPv6.
     - La dirección de correo electrónico que aparece en el campo de del correo electrónico de envío de AutoSupport.
     - **Opcional; si desea realizar una prueba de configuración**: La dirección de correo electrónico donde se envía una confirmación cuando el sistema AutoSupport recibe el mensaje de prueba.
     - Si desea cifrar mensajes, seleccione **SMTPS** o **STARTTLS** para el tipo de cifrado y, a continuación, seleccione el número de puerto para los mensajes cifrados. De lo contrario, seleccione **Ninguno**.
     - Si es necesario, introduzca un nombre de usuario y una contraseña para la autenticación con el remitente saliente y el servidor de correo.
4. Si tiene un firewall que bloquea la entrega de estas entregas de ASUP, añada la siguiente URL a la lista blanca: `https://support.netapp.com/put/AsupPut/`
5. Haga clic en **Configuración de prueba** para probar la conexión al servidor de soporte técnico utilizando los parámetros de entrega especificados. Si habilitó la función AutoSupport bajo demanda, el sistema

también probará la conexión para la entrega de mensajes de AutoSupport OnDemand.

Si la prueba de configuración falla, compruebe los ajustes de configuración y vuelva a ejecutar la prueba. Si la prueba sigue fallando, póngase en contacto con el soporte técnico.

6. Haga clic en **Guardar**.

Programar mensajes de AutoSupport

System Manager crea automáticamente una programación predeterminada para los mensajes de AutoSupport. Si lo prefiere, puede especificar su propia programación.

Antes de empezar

Se debe habilitar la función AutoSupport. Puede comprobar si está habilitada en la página AutoSupport.

Acerca de esta tarea

- **Hora diaria** — los envíos diarios se recopilan y se envían cada día durante el intervalo de tiempo especificado. System Manager selecciona un tiempo aleatorio durante el rango. Todas las opciones son en hora universal coordinada (UTC), que puede ser diferente a la hora local de la cabina de almacenamiento. Es necesario convertir la hora local de la cabina de almacenamiento a UTC.
- **Día semanal** — los envíos semanales se recopilan y se envían una vez por semana. System Manager selecciona un día al azar dentro de los días especificados. Anule la selección de los días en los que no desea permitir un mensaje semanal. System Manager selecciona un día al azar dentro de los días permitidos.
- **Tiempo semanal** — los envíos semanales se recopilan y se envían una vez por semana durante el intervalo de tiempo especificado. System Manager selecciona un tiempo aleatorio durante el rango. Todas las opciones son en hora universal coordinada (UTC), que puede ser diferente a la hora local de la cabina de almacenamiento. Es necesario convertir la hora local de la cabina de almacenamiento a UTC.

Pasos

1. Seleccione menú:ficha Soporte[Centro de soporte > AutoSupport].
2. Seleccione **programar mensajes de AutoSupport**.

   Se mostrará el asistente programar mensajes de AutoSupport.

3. Siga los pasos del asistente.

Envíe mensajes de AutoSupport

System Manager permite enviar mensajes de AutoSupport al soporte técnico sin esperar a un mensaje programado.

Antes de empezar

Se debe habilitar la función AutoSupport. Puede comprobar si está habilitada en la página AutoSupport.

Acerca de esta tarea

Esta operación recoge datos de soporte y los envía automáticamente al soporte técnico para que puedan solucionar problemas.

Pasos

1. Seleccione menú:ficha Soporte[Centro de soporte > AutoSupport].

2. Seleccione **Enviar envío AutoSupport**.

   Aparece el cuadro de diálogo Enviar envío AutoSupport.

3. Confirme la operación seleccionando **Enviar**.

Ver el estado de AutoSupport

La página AutoSupport muestra si la función AutoSupport y las funciones individuales de AutoSupport se encuentran habilitadas.

Pasos

1. Seleccione menú:ficha Soporte[Centro de soporte > AutoSupport].
2. Mire a la derecha de la página, justo debajo de las pestañas, para ver si la función AutoSupport está habilitada.
3. Pase el cursor sobre el signo de pregunta para ver si las funciones individuales de AutoSupport están habilitadas.

Ver el registro de AutoSupport

El registro de AutoSupport proporciona información sobre estado, historial de mensajes y errores detectados durante la entrega de envíos de AutoSupport.

Acerca de esta tarea

Pueden existir varios archivos de registro. Cuando el archivo de registro actual alcanza los 200 KB, se archiva y se crea un nuevo archivo de registro. El nombre del archivo de registro archivado es `ASUPMessages.n`, donde *n* es un entero de 1 a 9. Si existen varios archivos de registro, es posible ver el registro más reciente o uno anterior.

- **Registro actual** — muestra una lista de los últimos eventos capturados.
- **Archived log** — muestra una lista de eventos anteriores.

Pasos

1. Seleccione menú:ficha Soporte[Centro de soporte > AutoSupport].
2. Seleccione **Ver registro de AutoSupport**.

   Se muestra el cuadro de diálogo donde se enumera el registro de AutoSupport actual.

3. Si desea ver registros de AutoSupport anteriores, seleccione el botón de opción **Archived** y, a continuación, seleccione un registro de la lista desplegable **Select AutoSupport log**.

   Se muestra la opción archivada únicamente si existen registros archivados en la cabina de almacenamiento.

   En el cuadro de diálogo, se muestra el registro de AutoSupport seleccionado.

4. **Opcional:** para buscar el registro AutoSupport, escriba un término en el cuadro **Buscar** y haga clic en **Buscar**.

   Vuelva a hacer clic en **Buscar** para buscar más apariciones del término.

Habilite la ventana de mantenimiento de AutoSupport

Habilite la ventana de mantenimiento de AutoSupport para evitar la creación automática de incidencias durante eventos de error. En el modo de operación normal, la cabina de almacenamiento utiliza AutoSupport para abrir un caso en soporte si existe un problema.

Pasos

1. Seleccione menú:ficha Soporte[Centro de soporte > AutoSupport].
2. Seleccione **Activar la ventana Mantenimiento de AutoSupport**.
3. Introduzca la dirección de correo electrónico para recibir una confirmación de que se procesó la solicitud de la ventana de mantenimiento.

   Según la configuración existente, se podrán introducir hasta cinco direcciones de correo electrónico. Si desea agregar más de una dirección, seleccione **Agregar otro correo electrónico** para abrir otro campo.

4. Especifique la duración (en horas) para habilitar la ventana de mantenimiento.

   La duración máxima admitida es de 72 horas.

5. Haga clic en **Sí**.

   La creación automática de incidencias de AutoSupport durante eventos de error se evita temporalmente según la ventana de duración especificada.

Después de terminar

La ventana de mantenimiento no se inicia hasta que los servidores de AutoSupport procesan la solicitud de la cabina de almacenamiento. Espere hasta recibir un correo electrónico de confirmación antes de realizar actividades de mantenimiento en la cabina de almacenamiento.

Deshabilite la ventana de mantenimiento AutoSupport

Deshabilite la ventana de mantenimiento AutoSupport para permitir la creación automática de incidencias ante eventos de error. Cuando se deshabilita la ventana de mantenimiento AutoSupport, la cabina de almacenamiento utilizará AutoSupport para abrir un caso en soporte si existe un problema.

Pasos

1. Seleccione menú:ficha Soporte[Centro de soporte > AutoSupport].
2. Seleccione **Deshabilitar la ventana de mantenimiento de AutoSupport**.
3. Introduzca la dirección de correo electrónico para recibir una confirmación de que se procesó la solicitud de deshabilitar la ventana de mantenimiento.

   Según la configuración existente, se podrán introducir hasta cinco direcciones de correo electrónico. Si desea agregar más de una dirección, seleccione **Agregar otro correo electrónico** para abrir otro campo.

4. Haga clic en **Sí**.

   Se habilita la creación automática de incidencias de AutoSupport ante eventos de error.

Después de terminar

La ventana de mantenimiento no se finalizará hasta que los servidores de AutoSupport procesen la solicitud de la cabina de almacenamiento. Espere hasta recibir un correo electrónico de confirmación antes de continuar.

Ver eventos

Información general sobre el registro de eventos

El registro de eventos es un registro histórico de los eventos producidos en la cabina de almacenamiento, lo que ayuda al soporte técnico a solucionar problemas de eventos que pueden producir errores.

Es posible utilizar el registro de eventos como herramienta de diagnóstico complementaria a Recovery Guru para buscar el origen de eventos de cabina de almacenamiento. Consulte siempre Recovery Guru en primer lugar si intenta recuperarse de errores de componentes en la cabina de almacenamiento.

Categorías de eventos

Los eventos del registro de eventos se categorizan con diferentes Estados. Los eventos para los que debe realizar acciones tienen los siguientes Estados:

- Crítico
- Advertencia

Los eventos que son informativos y no requieren acción inmediata son los siguientes:

- Informativo

Eventos críticos

Los eventos críticos indican un problema con la cabina de almacenamiento. Si se resuelve el evento crítico de inmediato, es posible que se evite la pérdida de acceso a los datos.

Cuando se produce un evento crítico, este se añade al registro de eventos. Todos los eventos críticos se envían a la consola de gestión SNMP o al destinatario de correo electrónico que se configuró para recibir notificaciones de alerta. Si no se conoce el ID de bandeja en el momento del evento, el ID de bandeja se muestra como "Shelf unknown".

Cuando reciba un evento crítico, consulte el procedimiento de Recovery Guru para acceder a una descripción detallada de ese evento. Complete el procedimiento de Recovery Guru para corregir el evento crítico. Para corregir ciertos eventos críticos, es posible que deba comunicarse con el soporte técnico.

Ver eventos mediante el registro de eventos

Es posible ver el registro de eventos, que proporciona un registro histórico de los eventos que ocurrieron en la cabina de almacenamiento.

Pasos

1. Seleccione MENU:Soporte[Registro de eventos].

   Aparece la página Registro de eventos.

Detalles de la página

Elemento	Descripción
Campo Ver todos	Permite alternar la vista de todos los eventos o únicamente los eventos críticos y de advertencia.
Campo Filtrar	Filtra los eventos. Útil para mostrar únicamente eventos relacionados con un componente específico, un evento específico, etc.
Icono para seleccionar columnas.	Permite seleccionar otras columnas para ver. Otras columnas proporcionan información adicional sobre el evento.
Casillas de selección	Permite seleccionar los eventos para guardar. La casilla de comprobación del encabezado de la tabla permite seleccionar todos los eventos.
Columna Fecha/hora	La fecha y la hora del evento, según el reloj de la controladora. El registro de eventos inicialmente ordena los eventos de acuerdo con el número de secuencia. Normalmente, esta secuencia corresponde a la fecha y la hora. Sin embargo, los relojes de las dos controladoras de la cabina de almacenamiento podrían estar desincronizados. En este caso, podrían percibirse algunas incoherencias en el registro de eventos entre los eventos y la fecha y hora que se muestran.
Columna prioridad	A continuación se presentan los valores de prioridad: • **Crítico** — existe un problema con la matriz de almacenamiento. Sin embargo, si se actúa inmediatamente, se podría evitar la pérdida del acceso a los datos. Los eventos críticos se usan para notificaciones de alerta. Todos los eventos críticos se envían a cualquier cliente de gestión de red (a través de capturas SNMP) o al destinatario de correo electrónico que se configuró. • **Advertencia** — se ha producido un error que ha degradado el rendimiento y la capacidad de la matriz de almacenamiento para recuperarse de otro error. • **Informativo** — Información no crítica relacionada con la matriz de almacenamiento.
Columna Tipo de componente	El componente que se ve afectado por el evento. El componente podría ser hardware, como una unidad o una controladora, o bien software, como el firmware de la controladora.
Columna ubicación del componente	La ubicación física del componente en la cabina de almacenamiento.

Elemento	Descripción
Columna Descripción	Una descripción del evento. **Ejemplo** — `Drive write failure - retries exhausted`
Columna número de secuencia	Número de 64 bits que identifica exclusivamente una entrada específica del registro para una cabina de almacenamiento. Este número se incrementa de a uno con cada entrada nueva del registro de eventos. Para ver esta información, haga clic en el icono **Seleccionar columnas**.
Columna Tipo de evento	Número de 4 dígitos que identifica cada tipo de evento registrado. Para ver esta información, haga clic en el icono **Seleccionar columnas**.
Columna códigos específicos de evento	Información que utiliza el soporte técnico. Para ver esta información, haga clic en el icono **Seleccionar columnas**.
Columna Categoría de evento	• **Fallo**: Un componente de la cabina de almacenamiento falló; por ejemplo, fallo de la unidad o fallo de la batería. • **Cambio de estado**: Elemento de la cabina de almacenamiento que cambió el estado; por ejemplo, un volumen pasó a ser óptimo o una controladora pasó al estado sin conexión. • **Internal** – Operaciones internas del controlador que no requieren la acción del usuario; por ejemplo, el controlador ha completado la puesta en marcha del día. • **Command**: Comando que se ha emitido a la cabina de almacenamiento; por ejemplo, se ha asignado una pieza de repuesto. • **Error**: Una condición de error detectada en la cabina de almacenamiento; por ejemplo, una controladora no puede sincronizar ni purgar la caché, o un error de redundancia detectado en la cabina de almacenamiento. • **General** – cualquier evento que no se ajuste bien a ninguna otra categoría. Para mostrar esta información, haga clic en el icono **Seleccionar columnas**.
Columna registrado por	Nombre de la controladora que registró el evento. Para mostrar esta información, haga clic en el icono **Seleccionar columnas**.

2. Para recuperar eventos nuevos de la cabina de almacenamiento, haga clic en **Refresh**.

   Para que un evento se registre y se pueda ver en la página Registro de eventos, es posible que se deban esperar varios minutos.

3. Para guardar el registro de eventos en un archivo:
   a. Seleccione la casilla de comprobación junto al evento que desea guardar.
   b. Haga clic en **Guardar**.

El archivo se guarda en la carpeta de descargas del explorador con el nombre `major-event-log-timestamp.log`.

4. Para borrar eventos del registro de eventos:

   El registro de eventos almacena aproximadamente 8,000 eventos antes de reemplazar un evento por otro nuevo. Si desea conservar los eventos, puede guardarlos y borrarlos del registro de eventos.

   a. En primer lugar, guarde el registro de eventos.
   b. Haga clic en **Borrar todo** y confirme que desea realizar la operación.

Gestionar las actualizaciones

Información general del centro de actualización

Use el centro de actualización para descargar las versiones más recientes de software y firmware, y para actualizar las controladoras y las unidades.

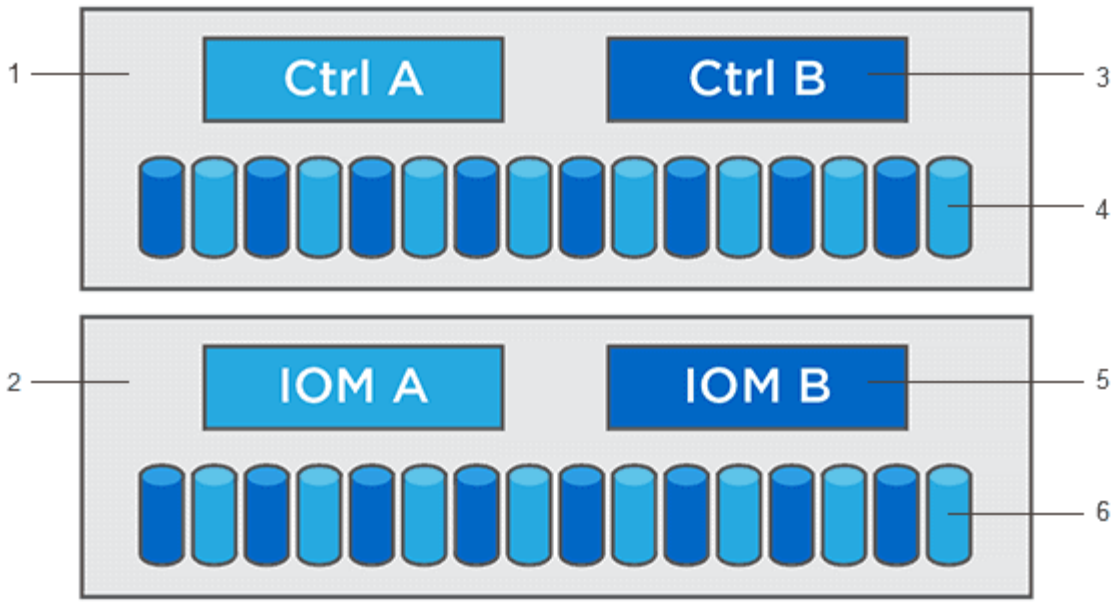
Información general de la actualización de la controladora

Es posible actualizar el software y el firmware de la cabina de almacenamiento para obtener todas las funciones y las correcciones de errores más recientes.

Componentes que se incluyen en la actualización de la controladora de un sistema operativo

Varios componentes de la cabina de almacenamiento contienen software o hardware que puede ser conveniente actualizar de vez en cuando.

- **Software de gestión** — System Manager es el software que administra la matriz de almacenamiento.
- **Firmware de la controladora** — el firmware de la controladora administra las E/S entre hosts y volúmenes.
- **NVSRAM de controladora** — NVSRAM de controladora es un archivo de controladora que especifica las configuraciones predeterminadas para las controladoras.
- **Firmware del IOM** — el firmware del módulo de I/o (IOM) administra la conexión entre una controladora y una bandeja de unidades. Además, supervisa el estado de los componentes.
- **Software de supervisor** — Software de supervisor es la máquina virtual en un controlador en el que se ejecuta el software.



Bandeja de controladoras esta 1; bandeja de unidades esta 2; software de esta versión 3, firmware de la controladora, NVSRAM de la controladora, Software de supervisor; firmware de la unidad de esta 4; firmware de esta 5 IOM; firmware de la unidad de esta versión 6

Se pueden ver las versiones de software y firmware actuales en el cuadro de diálogo Inventario de software y firmware. Vaya al menú:Soporte[Centro de actualización] y, a continuación, haga clic en el vínculo **Inventario de software y firmware**.

Como parte del proceso de actualización, es posible que el controlador de conmutación al nodo de respaldo/multivía del host o el controlador de HBA también deban actualizarse para que el host pueda interactuar con las controladoras correctamente. Para determinar si este es el caso, consulte "Herramienta de matriz de interoperabilidad de NetApp".

Cuándo detener las operaciones de I/O.

Si la cabina de almacenamiento contiene dos controladoras y existe un controlador multivía instalado, la cabina de almacenamiento puede seguir procesando las operaciones de I/o mientras se realiza la actualización. Durante la actualización, la controladora A conmuta todos los volúmenes a la controladora B, se actualiza, retira todos sus volúmenes y los de la controladora B, y después actualiza la controladora B.

Comprobación del estado previa a la actualización

Como parte del proceso de actualización, se ejecuta una comprobación del estado previa a la actualización. La comprobación del estado antes de la actualización evalúa todos los componentes de la cabina de almacenamiento para garantizar que se pueda proceder con la actualización. Las siguientes condiciones podrían evitar la actualización:

- Unidades asignadas con errores
- Piezas de repuesto en uso
- Grupos de volúmenes incompletos
- Operaciones exclusivas en ejecución
- Volúmenes faltantes
- Estado no óptimo de la controladora

- Cantidad excesiva de eventos en el registro de eventos
- Fallo de validación de la base de datos de configuración
- Unidades con versiones de DACstore anteriores

También se puede ejecutar la comprobación del estado antes de la actualización en forma independiente, sin realizar una actualización.

Información general de la actualización de la unidad

El firmware de la unidad controla las características de operación de bajo nivel. Periódicamente, los fabricantes de unidades publican actualizaciones del firmware de la unidad para añadir nuevas funciones, mejorar el rendimiento y corregir defectos.

Actualización del firmware de la unidad en línea y sin conexión

Existen dos tipos de métodos de actualización del firmware de la unidad: En línea y sin conexión.

En línea

Durante una actualización en línea, las unidades se actualizan secuencialmente, una a la vez. La cabina de almacenamiento sigue procesando las operaciones de I/o mientras se produce la actualización. No es necesario detener la actividad de I/O. Si una unidad puede realizar una actualización en línea, se utiliza automáticamente este método.

Las unidades que pueden realizar una actualización en línea son las siguientes:

- Unidades en un pool óptimo
- Unidades en un grupo de volúmenes redundante óptimo (RAID 1, RAID 5 y RAID 6)
- Unidades sin asignar
- Unidades de repuesto en espera

Realizar una actualización del firmware de la unidad en línea puede llevar varias horas, y la cabina de almacenamiento se expone a potenciales fallos de volumen. Los fallos de volumen pueden producirse en los siguientes casos:

- En un grupo de volúmenes RAID 1 o RAID 5, una unidad tiene errores cuando se está actualizando otra unidad en el grupo de volúmenes.
- En un pool o un grupo de volúmenes RAID 6, dos unidades tienen errores cuando se está actualizando otra unidad en el pool o grupo de volúmenes.

Sin conexión (paralelo)

Durante una actualización sin conexión, se actualizan al mismo tiempo todas las unidades del mismo tipo de unidad. Para utilizar este método, hace falta detener la actividad de I/o de los volúmenes asociados con las unidades seleccionadas. Debido a que pueden actualizarse varias unidades de forma simultánea (en paralelo), el tiempo de inactividad total se reduce significativamente. Si una unidad puede realizar únicamente una actualización sin conexión, se utiliza automáticamente este método.

Las siguientes unidades DEBEN utilizar el método sin conexión:

- Unidades en un grupo de volúmenes no redundante (RAID 0)

- Unidades en un pool o grupo de volúmenes que no es óptimo
- Unidades en caché SSD

Compatibilidad

Cada archivo de firmware de la unidad contiene información sobre el tipo de unidad en el que se ejecuta el firmware. Es posible descargar el archivo de firmware específico solo en una unidad compatible. System Manager comprueba automáticamente la compatibilidad durante el proceso de actualización.

Actualice el software y el firmware de las controladoras

Es posible actualizar el software de la cabina de almacenamiento y, de manera opcional, el firmware IOM y la memoria estática de acceso aleatorio no volátil (NVSRAM) para asegurarse de tener las funciones y las correcciones de errores más recientes.

Antes de empezar

- Sabe si desea actualizar el firmware IOM.

  Normalmente, es conveniente actualizar todos los componentes al mismo tiempo. Sin embargo, se puede decidir no actualizar el firmware IOM si no se desea actualizarlo como parte de la actualización de software del sistema operativo SANtricity o si el soporte técnico indica que se degrade el firmware IOM (solo es posible degradar el firmware mediante la interfaz de línea de comandos).

- Sabe si desea actualizar el archivo NVSRAM de controladora.

  Normalmente, es conveniente actualizar todos los componentes al mismo tiempo. Sin embargo, puede decidir no actualizar el archivo NVSRAM de la controladora si el archivo ya se revisó o es una versión personalizada y no desea sobrescribirla.

- Sabe si desea activar la actualización del sistema operativo ahora o más adelante.

  Algunos motivos para activar la actualización más adelante pueden ser:

  - **Hora del día** — la activación del software y del firmware puede llevar mucho tiempo, por lo que es posible que desee esperar hasta que las cargas de E/S sean más livianas. Las controladoras conmutan al nodo de respaldo durante la activación, de manera que el rendimiento podría ser inferior al habitual hasta que finalice la actualización.
  - **Tipo de paquete**: Es posible que desee probar el nuevo software y firmware en una matriz de almacenamiento antes de actualizar los archivos en otras matrices de almacenamiento.
- Sabe si desea cambiar las unidades no seguras o unidades internamente seguras para usar un servidor de gestión de claves (KMS) externo para la seguridad de las unidades.
- Sabe si desea utilizar el control de acceso basado en roles en la cabina de almacenamiento.

Acerca de esta tarea

Es posible optar por actualizar únicamente el archivo de software del sistema operativo o únicamente el archivo NVSRAM de la controladora, o bien actualizar ambos archivos.

Realice esta operación solo cuando el soporte técnico se lo indique.

Riesgo de pérdida de datos o riesgo de daños a la matriz de almacenamiento — no haga cambios en la matriz de almacenamiento mientras se realiza la actualización. Mantenga encendida la cabina de almacenamiento.

Pasos

1. Si la cabina de almacenamiento contiene una sola controladora o no existe un controlador multivía instalado, detenga la actividad de I/o de la cabina de almacenamiento para evitar errores en la aplicación. Si la cabina de almacenamiento tiene dos controladoras y existe un controlador multivía instalado, no necesita detener la actividad de I/O.
2. Seleccione MENU:Support[Upgrade Center].
3. Descargue el archivo nuevo del sitio de soporte en el cliente de gestión.
   a. Haga clic en **Soporte de NetApp** para iniciar la página web de soporte.
   b. En el sitio web de asistencia técnica, haga clic en la ficha **Descargas** y, a continuación, seleccione **Descargas**.
   c. Seleccione **E-Series Software de controladora de sistema operativo SANtricity**.
   d. Siga el resto de las instrucciones.

   Se requiere firmware con firma digital en la versión 8.42 y posteriores. Si intenta descargar firmware sin firmar, se muestra un error y se anula la descarga.

4. Si NO desea actualizar el firmware IOM en este momento, haga clic en **Suspender sincronización automática de IOM**.

   Si se tiene una cabina de almacenamiento con una sola controladora, el firmware IOM no se actualiza.

5. En actualización de software de SANtricity OS, haga clic en **Iniciar actualización**.

   Se muestra el cuadro de diálogo Upgrade SANtricity OS Software.

6. Seleccione uno o varios archivos para comenzar el proceso de actualización:
   a. Seleccione el archivo SANtricity OS Software haciendo clic en **examinar** y desplácese hasta el archivo de software del sistema operativo que descargó del sitio web de soporte.
   b. Seleccione el archivo NVSRAM de la controladora. Para hacerlo, haga clic en **examinar** y desplácese hasta el archivo NVSRAM que descargó del sitio de soporte. Los archivos NVSRAM de la controladora tienen un nombre de archivo similar a `N2800-830000-000.dlp`.

      Se realizan estas acciones:

      - De forma predeterminada, solo se muestran los archivos compatibles con la configuración de la cabina de almacenamiento actual.
      - Cuando se selecciona un archivo para actualizar, se muestran el nombre y el tamaño del archivo.
7. **Opcional:** Si seleccionó un archivo de software de sistema operativo SANtricity para actualizar, puede transferir los archivos al controlador sin activarlos seleccionando la casilla de verificación **transferir archivos ahora, pero no actualizar (activar actualización más tarde)**.
8. Haga clic en **Inicio** y confirme que desea realizar la operación.

   Es posible cancelar la operación durante la comprobación del estado previa a la actualización, pero no durante la transferencia o la activación.

9. **Opcional:** para ver una lista de lo que se actualizó, haga clic en **Guardar registro**.

   El archivo se guarda en la carpeta de descargas del explorador con el nombre `drive_upgrade_log-timestamp.txt`.

Después de terminar

- Verifique que todos los componentes aparezcan en la página hardware.
- Verifique las nuevas versiones de software y firmware. Para ello, consulte el cuadro de diálogo Inventario de software y firmware (vaya al menú:Soporte[Centro de actualización] y, a continuación, haga clic en el vínculo **Inventario de software y firmware**).
- Si actualizó NVSRAM de controladora, toda la configuración personalizada aplicada a la NVSRAM existente se pierde durante el proceso de activación. Se debe volver a aplicar la configuración personalizada a la NVSRAM una vez que finaliza el proceso de activación.

Activar el software y el firmware de la controladora

Puede optar por activar los archivo de actualización inmediatamente o esperar hasta un momento más conveniente.

Acerca de esta tarea

Puede descargar y transferir los archivos sin activarlos. Puede optar por activarlos más tarde por los siguientes motivos:

- **Hora del día** — la activación del software y del firmware puede llevar mucho tiempo, por lo que es posible que desee esperar hasta que las cargas de E/S sean más livianas. Las controladoras conmutan al nodo de respaldo durante la activación, de manera que el rendimiento podría ser inferior al habitual hasta que finalice la actualización.
- **Tipo de paquete**: Es posible que desee probar el nuevo software y firmware en una matriz de almacenamiento antes de actualizar los archivos en otras matrices de almacenamiento.

Cuando existe software o firmware transferido, pero no activado, se muestra una notificación en el área Notificaciones de la página principal de System Manager y también en la página Centro de actualización.

No se puede detener el proceso de activación una vez iniciado.

Pasos

1. Seleccione MENU:Support[Upgrade Center].
2. En el área etiquetada como actualización de software de controlador de sistema operativo SANtricity, haga clic en **Activar** y confirme que desea realizar la operación.

   Es posible cancelar la operación durante la comprobación del estado previa a la actualización, pero no durante la activación.

   Se inicia la comprobación del estado previa a la actualización. Si la comprobación del estado previa a la actualización se realiza correctamente, el proceso de actualización procede a activar los archivos. Si la comprobación del estado previa a la actualización tiene errores, use Recovery Guru o póngase en contacto con el soporte técnico para resolver el problema. Para algunos tipos de condiciones, el soporte técnico puede aconsejarle continuar con la actualización a pesar de los errores seleccionando la casilla de verificación **permitir actualización**.

   Cuando la comprobación del estado previa a la actualización se realiza correctamente, se produce la

activación. El tiempo que requiere la activación depende de la configuración de la cabina de almacenamiento y los componentes que se van a activar.

3. **Opcional:** para ver una lista de lo que se actualizó, haga clic en **Guardar registro**.

   El archivo se guarda en la carpeta de descargas del explorador con el nombre `drive_upgrade_log-timestamp.txt`.

Después de terminar

- Verifique que todos los componentes aparezcan en la página hardware.
- Verifique las nuevas versiones de software y firmware. Para ello, consulte el cuadro de diálogo Inventario de software y firmware (vaya al menú:Soporte[Centro de actualización] y, a continuación, haga clic en el vínculo **Inventario de software y firmware**).
- Si actualizó NVSRAM de controladora, toda la configuración personalizada aplicada a la NVSRAM existente se pierde durante el proceso de activación. Se debe volver a aplicar la configuración personalizada a la NVSRAM una vez que finaliza el proceso de activación.

Actualice el firmware de la unidad

Es posible actualizar el firmware de las unidades para asegurarse de tener todas las funciones y correcciones de errores más recientes.

Antes de empezar

- Se hizo un backup de los datos mediante un backup de disco a disco, una copia de volumen (a un grupo de volúmenes no afectado por la actualización planificada de firmware) o un reflejo remoto.
- La cabina de almacenamiento tiene el estado Optimal.
- Todas las unidades tienen el estado Optimal.
- No se están ejecutando cambios de configuración en la cabina de almacenamiento.
- Si las unidades solo pueden actualizarse sin conexión, se detiene la actividad de I/o de todos los volúmenes asociados con las unidades.

Pasos

1. Seleccione MENU:Support[Upgrade Center].
2. Descargue los archivos nuevos del sitio de soporte en el cliente de gestión.
   a. En actualización del firmware de la unidad, haga clic en **Soporte de NetApp**.
   b. En el sitio de soporte de NetApp, haga clic en la pestaña **Descargas**.
   c. Seleccione **Unidad de disco y matriz de firmware**.
   d. Siga el resto de las instrucciones.
3. En actualización del firmware de la unidad, haga clic en **comenzar actualización**.

   Se muestra un cuadro de diálogo que enumera los archivos de firmware de la unidad actualmente en uso.

4. Extraiga (descomprima) los archivos que descargó del sitio de soporte.
5. Haga clic en **examinar** y seleccione los nuevos archivos de firmware de la unidad que descargó del sitio de soporte.

   Los archivos de firmware de la unidad tienen un nombre de archivo similar a

`D_HUC101212CSS600_30602291_MS01_2800_0002` con la extensión de `.dlp`.

Es posible seleccionar hasta cuatro archivos de firmware de la unidad, uno por vez. Si más de un archivo de firmware de la unidad es compatible con la misma unidad, se muestra un error de conflicto de archivo. Decida qué archivo de firmware de la unidad desea usar para la actualización y elimine el otro.

6. Haga clic en **Siguiente**.

   Aparece el cuadro de diálogo **Seleccionar unidades**, que enumera las unidades que se pueden actualizar con los archivos seleccionados.

   Solo se muestran las unidades que son compatibles.

   El firmware seleccionado para la unidad aparece en el área de información firmware propuesto. Si debe cambiar el firmware, haga clic en **Atrás** para volver al cuadro de diálogo anterior.

7. Seleccione el tipo de actualización que desea realizar:
   - **En línea (predeterminado)** — muestra las unidades que pueden admitir una descarga de firmware *mientras la matriz de almacenamiento procesa E/S*. No se deben detener las operaciones de I/o de los volúmenes asociados mediante estas unidades cuando se selecciona este método de actualización. Estas unidades se actualizan una por vez mientras la cabina de almacenamiento procesa la actividad de I/o de esas unidades.
   - **Sin conexión (paralelo)** — muestra las unidades que pueden admitir una descarga de firmware *only mientras toda la actividad de I/o se detiene* en cualquier volumen que utilice las unidades. Cuando se selecciona este método de actualización, se debe detener toda la actividad de I/o en cualquier volumen que use las unidades que se están actualizando. Las unidades que no tienen redundancia deben procesarse como una operación sin conexión. Este requisito incluye cualquier unidad asociada con caché SSD, un grupo de volúmenes RAID 0 o cualquier pool o grupo de volúmenes que esté degradado. La actualización sin conexión (paralelo) suele ser más rápida que el método en línea (predeterminado).
8. En la primera columna de la tabla, seleccione la o las unidades que desea actualizar.
9. Haga clic en **Inicio** y confirme que desea realizar la operación.

   Si necesita detener la actualización, haga clic en **Detener**. Se completa cualquier descarga de firmware actualmente en curso. Se cancela cualquier descarga de firmware que no haya comenzado.

   > Si se detiene la actualización del firmware de la unidad, podrían producirse la pérdida de datos o la falta de disponibilidad de las unidades.

10. **Opcional:** para ver una lista de lo que se actualizó, haga clic en **Guardar registro**.

    El archivo se guarda en la carpeta de descargas del explorador con el nombre `drive_upgrade_log-timestamp.txt`.

11. Si se produce alguno de los siguientes errores durante el procedimiento de actualización, realice la acción recomendada.

Errores y acciones recomendadas

Si se encuentra con este error de descarga de firmware…	Realice lo siguiente…
Unidades asignadas con errores	La causa de este error puede ser que la unidad no tenga la firma apropiada. Asegúrese de que la unidad afectada sea una unidad autorizada. Póngase en contacto con el soporte técnico para obtener más información. Al reemplazar una unidad, asegúrese de que la capacidad de la unidad de reemplazo sea igual o mayor que la de la unidad con error que desea reemplazar. Puede reemplazar la unidad con error mientras la cabina de almacenamiento recibe I/O.
Compruebe la cabina de almacenamiento	• Asegúrese de que se haya asignado una dirección IP a cada controladora. • Asegúrese de que ninguno de los cables conectados a la controladora esté dañado. • Asegúrese de que todos los cables estén conectados firmemente.
Unidades de repuesto integradas	Es necesario corregir esta condición de error para poder actualizar el firmware. Ejecute System Manager y use Recovery Guru para resolver el problema.
Grupos de volúmenes incompletos	Si uno o varios grupos de volúmenes o pools de discos se muestran incompletos, es necesario corregir esta condición de error para poder actualizar el firmware. Ejecute System Manager y use Recovery Guru para resolver el problema.
Operaciones exclusivas \(que no sean análisis de medios en segundo plano/paridad\) en ejecución en alguno de los grupos de volúmenes	Si existe una o varias operaciones exclusivas en curso, es necesario completarlas para poder actualizar el firmware. Utilice System Manager para supervisar el progreso de las operaciones.
Volúmenes faltantes	Es necesario corregir la condición de volumen ausente para poder actualizar el firmware. Ejecute System Manager y use Recovery Guru para resolver el problema.
El estado de alguna de las controladoras no es óptimo	Se requiere atención en una de las controladoras de la cabina de almacenamiento. Es necesario corregir esta condición para poder actualizar el firmware. Ejecute System Manager y use Recovery Guru para resolver el problema.
La información de partición de almacenamiento no coincide entre los gráficos de objetos de las controladoras	Se produjo un error durante la validación de los datos en las controladoras. Póngase en contacto con el soporte técnico para resolver este problema.

Si se encuentra con este error de descarga de firmware…	Realice lo siguiente…
Error en la verificación de la controladora de base de datos de SPM	Se produjo un error en la base de datos de asignación de particiones de almacenamiento de una controladora. Póngase en contacto con el soporte técnico para resolver este problema.
Validación de la base de datos de configuración \(si es compatible con la versión del controlador de la cabina de almacenamiento\)	Se produjo un error en la base de datos de configuración de una controladora. Póngase en contacto con el soporte técnico para resolver este problema.
Comprobaciones relacionadas con MEL	Póngase en contacto con el soporte técnico para resolver este problema.
Se notificaron más de 10 eventos críticos MEL o informativos DDE en los últimos 7 días	Póngase en contacto con el soporte técnico para resolver este problema.
Se notificaron más de 2 eventos críticos MEL de página 2C en los últimos 7 días	Póngase en contacto con el soporte técnico para resolver este problema.
Se notificaron más de 2 eventos críticos MEL de canal de unidad degradado en los últimos 7 días	Póngase en contacto con el soporte técnico para resolver este problema.
Se notificaron más de 4 entradas cruciales MEL en los últimos 7 días	Póngase en contacto con el soporte técnico para resolver este problema.

Después de terminar

Se completó la actualización del firmware de la unidad. Es posible reanudar las operaciones normales.

Revisar los posibles errores de actualización de software y firmware

Se pueden producir errores durante la actualización del software de la controladora o la actualización del firmware de la unidad.

Error de descarga de firmware	Descripción	Acción recomendada
Unidades asignadas con errores	No se pudo actualizar una unidad asignada en la cabina de almacenamiento.	La causa de este error puede ser que la unidad no tenga la firma apropiada. Asegúrese de que la unidad afectada sea una unidad autorizada. Póngase en contacto con el soporte técnico para obtener más información. Al reemplazar una unidad, asegúrese de que la capacidad de la unidad de reemplazo sea igual o mayor que la de la unidad con error que desea reemplazar. Puede reemplazar la unidad con error mientras la cabina de almacenamiento recibe I/O.
Unidades de repuesto integradas	Si la unidad se marcó como pieza de repuesto y se usa en un grupo de volúmenes, se produce un error en la actualización del firmware.	Es necesario corregir esta condición de error para poder actualizar el firmware. Ejecute System Manager y use Recovery Guru para resolver el problema.
Grupos de volúmenes incompletos	Si se omite, se quita o no responde una unidad que forma parte de un grupo de volúmenes, se considera un grupo de volúmenes incompleto. Un grupo de volúmenes incompleto impide que se actualice el firmware.	Si uno o varios grupos de volúmenes o pools de discos se muestran incompletos, es necesario corregir esta condición de error para poder actualizar el firmware. Ejecute System Manager y use Recovery Guru para resolver el problema.
Operaciones exclusivas (que no sean análisis de medios en segundo plano/paridad) en ejecución en alguno de los grupos de volúmenes	No se puede actualizar el firmware si existen operaciones exclusivas en curso en un volumen.	Si existe una o varias operaciones exclusivas en curso, es necesario completarlas para poder actualizar el firmware. Utilice System Manager para supervisar el progreso de las operaciones.
Volúmenes faltantes	No se puede actualizar el firmware si no se encuentra algún volumen.	Es necesario corregir la condición de volumen ausente para poder actualizar el firmware. Ejecute System Manager y use Recovery Guru para resolver el problema.

Error de descarga de firmware	Descripción	Acción recomendada
El estado de alguna de las controladoras no es óptimo	No se puede actualizar el firmware si el estado de algunas de las controladoras es diferente a Optimal.	Se requiere atención en una de las controladoras de la cabina de almacenamiento. Es necesario corregir esta condición para poder actualizar el firmware. Ejecute System Manager y use Recovery Guru para resolver el problema.
Error en la verificación de la controladora de base de datos de SPM	No se puede actualizar el firmware debido a que la base de datos de asignación de particiones de almacenamiento se encuentra dañada.	Se produjo un error en la base de datos de asignación de particiones de almacenamiento de una controladora. Póngase en contacto con el soporte técnico para resolver este problema.
Validación de la base de datos de configuración (si es compatible con la versión de la controladora de la cabina de almacenamiento)	No se puede actualizar el firmware debido a que la base de datos de configuración se encuentra dañada.	Se produjo un error en la base de datos de configuración de una controladora. Póngase en contacto con el soporte técnico para resolver este problema.
Comprobaciones relacionadas con MEL	No se puede actualizar el firmware debido a que el registro de eventos contiene errores.	Póngase en contacto con el soporte técnico para resolver este problema.
Se notificaron más de 10 eventos críticos MEL o informativos DDE en los últimos 7 días	No se puede actualizar el firmware debido a que se notificaron más de 10 eventos críticos MEL o informativos DDE en los últimos 7 días.	Póngase en contacto con el soporte técnico para resolver este problema.
Se notificaron más de 2 eventos críticos MEL de página 2C en los últimos 7 días	No se puede actualizar el firmware debido a que se notificaron más de 2 eventos críticos MEL de página 2C en los últimos 7 días.	Póngase en contacto con el soporte técnico para resolver este problema.
Se notificaron más de 2 eventos críticos MEL de canal de unidad degradado en los últimos 7 días	No se puede actualizar el firmware debido a que se notificaron más de 2 eventos críticos MEL de canal de unidad degradado en los últimos 7 días.	Póngase en contacto con el soporte técnico para resolver este problema.
Se notificaron más de 4 entradas cruciales MEL en los últimos 7 días	No se puede actualizar el firmware debido a que se notificaron más de 4 entradas de registro de eventos críticos en los últimos 7 días.	Póngase en contacto con el soporte técnico para resolver este problema.

Error de descarga de firmware	Descripción	Acción recomendada
Se requiere una dirección IP de gestión válida	Se requiere una dirección IP de controladora válida para ejecutar esta operación.	Póngase en contacto con el soporte técnico para resolver este problema.
El comando requiere que se proporcione una dirección IP de gestión activa para cada controladora	Se requiere una dirección IP para cada controladora asociada a la cabina de almacenamiento a fin de realizar esta operación.	Póngase en contacto con el soporte técnico para resolver este problema.
Se devuelve un tipo de archivo de descarga no controlado	No se admite el archivo de descarga especificado.	Póngase en contacto con el soporte técnico para resolver este problema.
Se produjo un error durante el procedimiento de carga y descarga de firmware	No se pudo descargar el firmware debido a que la controladora no pudo procesar la solicitud. Verifique que el estado de la cabina de almacenamiento sea óptimo y vuelva a intentar la operación.	Si este error se vuelve a producir después de verificar que el estado de la cabina de almacenamiento es óptimo, póngase en contacto con el soporte técnico para resolver este problema.
Se produjo un error durante el procedimiento de activación de firmware	No se pudo activar el firmware debido a que la controladora no pudo procesar la solicitud. Verifique que el estado de la cabina de almacenamiento sea óptimo y vuelva a intentar la operación.	Si este error se vuelve a producir después de verificar que el estado de la cabina de almacenamiento es óptimo, póngase en contacto con el soporte técnico para resolver este problema.
Se agotó el tiempo de espera para que se reinicie la controladora {0}	El software de gestión no puede volver a conectarse con la controladora {0} después de un reinicio. Compruebe que exista una ruta de acceso de conexión en funcionamiento a la cabina de almacenamiento y vuelva a intentar la operación si no se completó correctamente.	Si este error se vuelve a producir después de verificar que el estado de la cabina de almacenamiento es óptimo, póngase en contacto con el soporte técnico para resolver este problema.

Puede corregir algunas de estas condiciones mediante Recovery Guru en System Manager. No obstante, es posible que deba ponerse en contacto con el soporte técnico por alguna de las condiciones. La información acerca de la descarga más reciente del firmware de la controladora se encuentra disponible en la cabina de almacenamiento. Con esta información el soporte técnico podrá comprender las condiciones de error por las que no se pudo descargar y actualizar el firmware.

Preguntas frecuentes

¿Qué datos recojo?

La función AutoSupport y la función manual Support Data Collection proporcionan medios para recoger datos en un bundle de soporte al cliente a fin de que el soporte

técnico solucione y analice problemas de forma remota.

El bundle de soporte al cliente reúne todos los tipos de información acerca de la cabina de almacenamiento en un archivo comprimido único. La información recogida incluye la configuración física, la configuración lógica, la información de versión, los eventos, los archivos de registro, datos de rendimiento y rendimiento. Solo el soporte técnico utiliza la información para resolver problemas con la cabina de almacenamiento.

¿Qué indican los datos de sectores ilegibles?

Es posible visualizar datos detallados sobre sectores ilegibles detectados en las unidades de la cabina de almacenamiento.

El registro de sectores ilegibles muestra el sector ilegible más reciente primero. El registro contiene la siguiente información sobre los volúmenes que contienen los sectores ilegibles. Es posible ordenar los campos.

Campo	Descripción
Volumen afectado	Muestra la etiqueta del volumen. Si un volumen faltante contiene sectores ilegibles, aparece el identificador a nivel mundial del volumen faltante.
Número de unidad lógica (LUN)	Muestra el LUN del volumen. Si el volumen no tiene LUN, el cuadro de diálogo muestra NA.
Asignado a.	Muestra los hosts o clústeres de hosts con acceso al volumen. Si el volumen no permite el acceso de un host, un clúster de hosts o incluso un clúster predeterminado, el cuadro de diálogo muestra NA.

Para ver información adicional sobre los sectores ilegibles, haga clic en el símbolo más (+) junto a un volumen.

Campo	Descripción
Fecha/hora	Muestra la fecha y la hora en que se detectó el sector ilegible.
Dirección de bloque del volumen lógico	Muestra la dirección de bloque lógico (LBA) del volumen.
Ubicación de la unidad	Muestra la ubicación de la bandeja de unidades, el cajón (si la bandeja de unidades posee cajones) y la bahía.
Dirección de bloque de la unidad lógica	Muestra el LBA de la unidad.

Campo	Descripción
Tipo de fallo	Muestra uno de los siguientes tipos de fallos: • **Físico** — un error de medios físicos. • **Lógico** — un error de lectura en otra parte de la franja que causa datos ilegibles. Por ejemplo, un sector ilegible debido a errores de medios en otra parte del volumen. • **Incoherente** — datos de redundancia incoherentes. • **Garantía de datos** — un error de Garantía de datos.

¿Qué es una imagen de estado?

Una imagen de estado es un volcado de datos sin formato de la memoria del procesador de la controladora que el soporte técnico puede utilizar para diagnosticar un problema con una controladora.

El firmware genera automáticamente una imagen de estado cuando detecta ciertos errores. En determinadas situaciones de solución de problemas, el soporte técnico puede solicitar la recuperación del archivo de imagen de estado y su envío.

¿Qué hacen las funciones de AutoSupport?

La función AutoSupport cuenta con tres funciones individuales que se habilitan por separado.

- **Basic AutoSupport** — permite que la cabina de almacenamiento recopile y envíe datos al soporte técnico automáticamente.
- **AutoSupport OnDemand** — permite al soporte técnico solicitar la retransmisión de un envío anterior de AutoSupport cuando se necesita solucionar un problema. Todas las transmisiones se inician en la cabina de almacenamiento, no en el servidor de AutoSupport. La cabina de almacenamiento realiza comprobaciones periódicas con el servidor de AutoSupport para determinar si existen solicitudes de retransmisión pendientes y responde de manera acorde.
- **Diagnóstico remoto** — permite al soporte técnico solicitar un nuevo mensaje de AutoSupport actualizado cuando se necesita para solucionar un problema. Todas las transmisiones se inician en la cabina de almacenamiento, no en el servidor de AutoSupport. La cabina de almacenamiento realiza comprobaciones periódicas con el servidor de AutoSupport para determinar si existen solicitudes nuevas pendientes y responde de manera acorde.

¿Qué tipo de datos se recopilan mediante la función AutoSupport?

La función AutoSupport contiene tres tipos de mensajes estándares: Mensajes de evento, mensajes programados y mensajes de diagnóstico bajo demanda y remotos.

Los datos de AutoSupport no incluyen datos de usuario.

- **Mensajes de evento**

  Cuando suceden eventos en el sistema que justifican la notificación proactiva al soporte técnico, la función AutoSupport envía automáticamente un mensaje activado por el evento.

- Se envían cuando ocurre un evento de soporte en la cabina de almacenamiento gestionada.
- Incluyen una Snapshot general de lo que sucedía en la cabina de almacenamiento en el momento en el que ocurrió el evento.

- **Mensajes programados**

  La función AutoSupport envía automáticamente varios mensajes con una programación regular.

  - **Mensajes diarios** — enviados una vez cada día durante un intervalo de tiempo configurable por el usuario. Incluyen los registros de eventos del sistema y los datos de rendimiento actuales.
  - **Mensajes semanales** — enviados una vez cada semana durante un intervalo de tiempo y un día configurables por el usuario. Incluyen información de estado del sistema y la configuración.

- **Mensajes de diagnóstico bajo demanda y remoto de AutoSupport**
  - **AutoSupport OnDemand** — permite al soporte técnico solicitar la retransmisión de un envío anterior de AutoSupport cuando se necesita solucionar un problema. Todas las transmisiones se inician en la cabina de almacenamiento, no en el servidor de AutoSupport. La cabina de almacenamiento realiza comprobaciones periódicas con el servidor de AutoSupport para determinar si existen solicitudes de retransmisión pendientes y responde de manera acorde.
  - **Diagnóstico remoto** — permite al soporte técnico solicitar un nuevo mensaje de AutoSupport actualizado cuando se necesita para solucionar un problema. Todas las transmisiones se inician en la cabina de almacenamiento, no en el servidor de AutoSupport. La cabina de almacenamiento realiza comprobaciones periódicas con el servidor de AutoSupport para determinar si existen solicitudes nuevas pendientes y responde de manera acorde.

¿Cómo se configura el método de entrega para la función AutoSupport?

La función AutoSupport admite los protocolos HTTPS, HTTP y SMTP para entregar mensajes de AutoSupport al soporte técnico.

Antes de empezar

- Se debe habilitar la función AutoSupport. Puede comprobar si está habilitada en la página AutoSupport.
- Debe haber un servidor DNS instalado y configurado en la red. La dirección del servidor DNS debe configurarse en System Manager (esta tarea está disponible en la página hardware).

Acerca de esta tarea

Revise los diferentes protocolos:

- **HTTPS** — le permite conectarse directamente al servidor de soporte técnico de destino mediante HTTPS. Si desea habilitar AutoSupport OnDemand o Remote Diagnostics, el método de entrega de AutoSupport debe configurarse en HTTPS.
- **HTTP** — le permite conectarse directamente al servidor de soporte técnico de destino mediante HTTP.
- **Correo electrónico** — le permite utilizar un servidor de correo electrónico como método de entrega para enviar mensajes AutoSupport.

> **Diferencias entre los métodos HTTPS/HTTP y Email**. El método de entrega por correo electrónico, que utiliza SMTP, tiene algunas diferencias importantes con los métodos de entrega mediante HTTPS y HTTP. Primero, el tamaño de los mensajes para el método de correo electrónico se limita a 5 MB, lo cual significa que algunas recogidas de datos ASUP no se enviarán. Segundo, la función AutoSupport OnDemand solo está disponible en los métodos de entrega mediante HTPP y HTTPS.

Pasos

1. Seleccione menú:ficha Soporte[Centro de soporte > AutoSupport].
2. Seleccione **Configurar método de entrega de AutoSupport**.

   Se muestra un cuadro de diálogo con una lista de los métodos de entrega de mensajes.

3. Seleccione el método de entrega deseado y los parámetros para ese método. Debe realizar una de las siguientes acciones:
   - Si eligió HTTPS o HTTP, seleccione uno de los siguientes parámetros de entrega:
     - **Directamente** — este parámetro de entrega es la selección predeterminada. Esta opción permite la conexión directa con el sistema de soporte técnico de destino mediante el protocolo HTTPS o HTTP.
     - **Via Proxy Server** — elegir esta opción le permite especificar los detalles del servidor proxy HTTP necesarios para establecer la conexión con el sistema de soporte técnico de destino. Es necesario especificar la dirección y el número de puerto del host. No obstante, solo se deben introducir los detalles de autenticación del host (nombre de usuario y contraseña) si así se requiere.
     - **Secuencia de comandos de configuración automática vía Proxy (PAC)**: Especifique la ubicación de un archivo de secuencia de comandos de configuración automática de proxy (PAC). Un archivo de PAC permite al sistema seleccionar automáticamente el servidor proxy adecuado para establecer una conexión con el sistema de soporte técnico de destino.
   - Si seleccionó correo electrónico, introduzca la siguiente información:
     - La dirección del servidor de correo como un nombre de dominio completo, una dirección IPv4 o una dirección IPv6.
     - La dirección de correo electrónico que aparece en el campo de del correo electrónico de envío de AutoSupport.
     - **Opcional; si desea realizar una prueba de configuración.** la dirección de correo electrónico donde se envía una confirmación cuando el sistema AutoSupport recibe el mensaje de prueba.
     - Si desea cifrar mensajes, seleccione **SMTPS** o **STARTTLS** para el tipo de cifrado y, a continuación, seleccione el número de puerto para los mensajes cifrados. De lo contrario, seleccione **Ninguno**.
     - Si es necesario, introduzca un nombre de usuario y una contraseña para la autenticación con el remitente saliente y el servidor de correo.
4. Haga clic en **Configuración de prueba** para probar la conexión al servidor de soporte técnico utilizando los parámetros de entrega especificados. Si habilitó la función AutoSupport bajo demanda, el sistema también probará la conexión para la entrega de mensajes de AutoSupport OnDemand.

   Si la prueba de configuración falla, compruebe los ajustes de configuración y vuelva a ejecutar la prueba. Si la prueba sigue fallando, póngase en contacto con el soporte técnico.

5. Haga clic en **Guardar**.

¿Qué son los datos de configuración?

Al seleccionar recopilar datos de configuración, el sistema guarda el estado actual de la base de datos de configuración RAID.

La base de datos de configuración de RAID incluye todos los datos para grupos de volúmenes y pools de discos en la controladora. La función recoger datos de configuración guarda la misma información que el

comando de la CLI para `save storageArray dbmDatabase`.

¿Qué se debe saber para actualizar el software del SO SANtricity?

Antes de actualizar el software y firmware de la controladora, tenga en cuenta estos puntos.

- Ha leído el documento y el `readme.txt` file y ha determinado que desea realizar la actualización.
- Sabe si desea actualizar el firmware IOM.

  Normalmente, es conveniente actualizar todos los componentes al mismo tiempo. Sin embargo, se puede decidir no actualizar el firmware IOM si no se desea actualizarlo como parte de la actualización de software de la controladora del sistema operativo SANtricity o si el soporte técnico indica que se degrade el firmware IOM (solo es posible degradar el firmware mediante la interfaz de línea de comandos).

- Sabe si desea actualizar el archivo NVSRAM de controladora.

  Normalmente, es conveniente actualizar todos los componentes al mismo tiempo. Sin embargo, puede decidir no actualizar el archivo NVSRAM de la controladora si el archivo ya se revisó o es una versión personalizada y no desea sobrescribirla.

- Sabe si desea activarlo ahora o más adelante.

  Algunos motivos para activar la actualización más adelante pueden ser:

  - **Hora del día** — la activación del software y del firmware puede llevar mucho tiempo, por lo que es posible que desee esperar hasta que las cargas de E/S sean más livianas. Las controladoras conmutan al nodo de respaldo durante la activación, de manera que el rendimiento podría ser inferior al habitual hasta que finalice la actualización.
  - **Tipo de paquete**: Es posible que desee probar el nuevo software y firmware en una matriz de almacenamiento antes de actualizar los archivos en otras matrices de almacenamiento.

Los siguientes componentes forman parte de la actualización de software de la controladora del sistema operativo SANtricity:

- **Software de gestión** — System Manager es el software que administra la matriz de almacenamiento.
- **Firmware de la controladora** — el firmware de la controladora administra las E/S entre hosts y volúmenes.
- **NVSRAM de controladora** — NVSRAM de controladora es un archivo de controladora que especifica las configuraciones predeterminadas para las controladoras.
- **Firmware del IOM** — el firmware del módulo de I/o (IOM) administra la conexión entre una controladora y una bandeja de unidades. Además, supervisa el estado de los componentes.
- **Software de supervisor** — Software de supervisor es la máquina virtual en un controlador en el que se ejecuta el software.

Como parte del proceso de actualización, es posible que el controlador de conmutación al nodo de respaldo/multivía del host o el controlador de HBA también deban actualizarse para que el host pueda interactuar con las controladoras correctamente.

> Para determinar si este es el caso, consulte "Herramienta de matriz de interoperabilidad de NetApp".

Si la cabina de almacenamiento contiene una sola controladora o no existe un controlador multivía instalado, detenga la actividad de I/o de la cabina de almacenamiento para evitar errores en la aplicación. Si la cabina de almacenamiento tiene dos controladoras y existe un controlador multivía instalado, no necesita detener la actividad de I/O.

No haga cambios en la cabina de almacenamiento mientras se realiza la actualización.

¿Qué debo saber antes de suspender la sincronización automática de IOM?

La suspensión de la sincronización automática de IOM impide que el firmware de IOM se actualice la próxima vez que se produzca una actualización de software de la controladora del sistema operativo SANtricity.

Por lo general, el software de la controladora y el firmware del IOM se actualizan en bundle. Puede suspender la sincronización automática del IOM si tiene una compilación especial del firmware del IOM que desea preservar en el compartimento. De lo contrario, revertirá el firmware del IOM que se incluye en el bundle con el software de la controladora la próxima vez que realice una actualización del software de la controladora.

¿Por qué se procesa tan lentamente la actualización del firmware?

El progreso de la actualización del firmware depende de la carga general del sistema.

Si, en el marco de una actualización en línea del firmware de la unidad, se lleva a cabo una transferencia de volumen durante el proceso de reconstrucción rápida, el sistema inicia una reconstrucción completa en el volumen que se transfirió. Es posible que esta operación requiera una cantidad de tiempo considerable. El tiempo de reconstrucción completa real depende de varios factores, incluidos la cantidad de actividad de I/o durante la operación de reconstrucción, la cantidad de unidades en el grupo de volúmenes, la configuración de prioridad de recompilación y el rendimiento de la unidad.

¿Qué debo saber antes de actualizar el firmware de la unidad?

Antes de actualizar el firmware de la unidad, tenga en cuenta los siguientes puntos.

- Como medida de precaución, haga un backup de los datos mediante un backup de disco a disco, una copia de volumen (a un grupo de volúmenes que no esté afectado por la actualización de firmware programada) o un reflejo remoto.
- Tal vez resulte conveniente actualizar solo algunas unidades para probar el comportamiento, con el fin de garantizar que el firmware nuevo funcione correctamente. Si el firmware nuevo funciona correctamente, actualice las unidades restantes.
- Si tiene unidades con error, corrija esos errores antes de comenzar la actualización de firmware.
- Si las unidades pueden hacer una actualización sin conexión, detenga la actividad de I/o de todos los volúmenes asociados con las unidades. Cuando se detiene la actividad de I/o, no pueden producirse operaciones de configuración asociadas a tales volúmenes.
- No quite ninguna unidad mientras se actualiza el firmware de la unidad.
- No haga ningún cambio de configuración en la cabina de almacenamiento mientras se actualiza el firmware de la unidad.

¿Cómo selecciono el tipo de actualización que debo realizar?

El tipo de actualización a realizar en la unidad se selecciona según el estado del pool o

el grupo de volúmenes.

- **En línea**

  Si el pool o el grupo de volúmenes es compatible con la redundancia y está en estado óptimo, se puede usar el método en línea para actualizar el firmware de la unidad. El método en línea descarga el firmware *mientras la cabina de almacenamiento procesa operaciones de I/o* en los volúmenes asociados que utilizan estas unidades. No es necesario detener las operaciones de I/o hacia los volúmenes asociados que utilizan estas unidades. Estas unidades se actualizan de a una por vez en los volúmenes asociados con ellas. Si la unidad no está asignada a un pool o un grupo de volúmenes, su firmware puede actualizarse con los métodos en línea o sin conexión. El rendimiento del sistema puede verse afectado cuando se utiliza el método en línea para actualizar el firmware de la unidad.

- **Fuera de línea**

  Si el pool o el grupo de volúmenes no es compatible con la redundancia (RAID 0) o se degrada, debe utilizar el método sin conexión para actualizar el firmware de la unidad. El método sin conexión actualizará el firmware _solo cuando se detenga toda la actividad de I/o hacia los volúmenes asociados que utilizan estas unidades. Debe detener las operaciones de I/o hacia todos los volúmenes asociados que utilizan estas unidades. Si la unidad no está asignada a un pool o un grupo de volúmenes, su firmware puede actualizarse con los métodos en línea o sin conexión.

Gestión de varias cabinas con Unified Manager 6

Interfaz principal

Información general de la interfaz de Unified Manager

Unified Manager es una interfaz basada en Web que permite gestionar varias cabinas de almacenamiento en una sola vista.

Página principal

Al iniciar sesión en Unified Manager, la página principal se abre en **gestionar - todo**. En esta página, puede desplazarse por una lista de cabinas de almacenamiento detectadas en la red, ver su estado y realizar operaciones en una sola cabina o en un grupo de cabinas.

Barra lateral Navegación

Puede acceder a las funciones y funciones de Unified Manager desde la barra lateral de navegación.

Zona	Descripción
Gestione	Detecte las cabinas de almacenamiento en la red, inicie la instancia de SANtricity System Manager de una cabina, importe la configuración de una cabina a varias, y gestione grupos de cabinas. Marque las casillas de comprobación junto a los nombres de las cabinas para realizar distintas operaciones, como importar configuraciones y crear grupos de cabinas. Los tres puntos al final de cada fila permiten acceder al menú en línea con las operaciones para cada cabina, por ejemplo, las operaciones de cambio de nombre.
Operaciones	Vea el progreso de las operaciones en lote, como la importación de la configuración de una cabina a otra. Algunas operaciones no están disponibles si una cabina de almacenamiento no tiene un estado óptimo.
Gestión de certificados	Administrar certificados para autenticar entre exploradores y clientes.
Access Management	Establezca la autenticación de usuario para la interfaz de Unified Manager.
Soporte técnico	Vea opciones de soporte técnico, recursos y contactos.

La configuración de la interfaz y la ayuda

En la parte superior derecha de la interfaz, puede acceder a la Ayuda y a otra documentación. También puede acceder a las opciones de administración que están disponibles en el menú desplegable junto a su nombre de inicio de sesión.

Inicios de sesión y contraseñas de usuario

El usuario actual que ha iniciado sesión en el sistema se muestra en la esquina superior derecha de la interfaz.

Para obtener más información sobre usuarios y contraseñas, consulte:

- "Configure la protección con contraseña de administrador"
- "Cambie la contraseña de administrador"
- "Cambiar contraseñas de perfiles de usuario local"

Exploradores compatibles

Para acceder a Unified Manager pueden usarse varios tipos de exploradores.

Se admiten los siguientes exploradores en las versiones mencionadas.

Navegador	Versión mínima
Google Chrome	89
Mozilla Firefox	80
Safari	14
Microsoft Edge	90

El proxy de servicios web debe estar instalado y disponible para el explorador.

Configure la protección con contraseña de administrador

Debe configurar Unified Manager con una contraseña de administrador para proteger la instancia del acceso no autorizado.

Contraseña de administrador y perfiles de usuario

Cuando se inicia Unified Manager por primera vez, se le solicita que establezca una contraseña de administrador. Cualquier usuario que tenga la contraseña de administrador puede realizar cambios de configuración en las cabinas de almacenamiento.

Además de la contraseña de administrador, la interfaz de Unified Manager incluye perfiles de usuario preconfigurados con uno o varios roles asignados. Para obtener más información, consulte "Cómo funciona Access Management".

Los usuarios y las asignaciones no pueden cambiarse. Solo las contraseñas pueden modificarse. Para cambiar las contraseñas, consulte:

- "Cambie la contraseña de administrador"
- "Cambiar contraseñas de perfiles de usuario local"

Tiempos de espera de sesión

El software solicita la contraseña una sola vez durante una misma sesión de gestión. De forma predeterminada, una sesión finaliza a los 30 minutos de inactividad; después de ese plazo, deberá introducir la contraseña otra vez. Si otro usuario accede al software desde otro cliente de gestión y cambia la contraseña mientras su sesión está en progreso, se le solicitará a usted una contraseña la próxima vez que intente realizar una operación de configuración o de vista.

Por razones de seguridad, puede intentar introducir una contraseña solo cinco veces antes de que el software quede bloqueado. En este estado, el software rechaza cualquier nuevo intento de introducir una contraseña. Se deben esperar 10 minutos para que el software se restablezca a un estado normal y usted pueda volver a introducir una contraseña.

Es posible ajustar los tiempos de espera de la sesión, o bien directamente pueden deshabilitarse los tiempos de espera de sesión. Para obtener más información, consulte "Gestionar los tiempos de espera de sesión".

Cambie la contraseña de administrador

Es posible cambiar la contraseña de administrador que se utiliza para acceder a Unified Manager.

Antes de empezar

- Inició sesión como administrador local, lo que incluye permisos de administrador raíz.
- Debe conocer la contraseña de administrador actual.

Acerca de esta tarea

Tenga en cuenta estas directrices al elegir una contraseña:

- Las contraseñas distinguen mayúsculas de minúsculas.
- Los espacios al final de la contraseña no se eliminan si se los utiliza. Procure incluir espacios si se incluyeron en la contraseña.
- Para mayor seguridad, use al menos 15 caracteres alfanuméricos y cambie la contraseña con frecuencia.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la ficha **roles de usuario local**.
3. Seleccione el usuario **admin** de la tabla.

   Se habilita el botón Cambiar contraseña.

4. Seleccione **Cambiar contraseña**.

   Se abre el cuadro de diálogo Cambiar contraseña.

5. Si no se estableció una longitud mínima para las contraseñas de usuario local, marque la casilla de aprobación para solicitarle al usuario que introduzca una contraseña a fin de acceder al sistema.
6. Introduzca la nueva contraseña en los dos campos.
7. Introduzca su contraseña de administrador local para confirmar esta operación y, a continuación, haga clic en **Cambiar**.

Gestionar los tiempos de espera de sesión

Es posible configurar tiempos de espera en System Manager para que las sesiones inactivas de los usuarios se desconecten después de un periodo especificado.

Acerca de esta tarea

De manera predeterminada, el tiempo de espera de sesión para Unified Manager es de 30 minutos. Es posible ajustar el tiempo, o bien directamente pueden deshabilitarse los tiempos de espera de sesión.

> Si se configura Access Management con las funcionalidades del lenguaje de marcado de aserción de seguridad (SAML) integradas en la cabina, es posible que se agote el tiempo de espera de sesión cuando la sesión SSO del usuario alcance su límite máximo. Esto puede ocurrir antes del tiempo de espera de sesión de System Manager.

Pasos

1. En la barra de menú, seleccione la flecha desplegable junto a su nombre de inicio de sesión.
2. Seleccione **Activar/Desactivar tiempo de espera de sesión**.

   Se abre el cuadro de diálogo Habilitar/deshabilitar tiempo de espera de la sesión.

3. Utilice los controles de desplazamiento para aumentar o disminuir el tiempo en minutos.

   El tiempo de espera mínimo que puede configurarse es de 15 minutos.

   > Para desactivar los tiempos de espera de sesiones, desactive la casilla de verificación **establecer el lapso…**.

4. Haga clic en **Guardar**.

Cabinas de almacenamiento

Información general de detección

Para gestionar los recursos de almacenamiento, primero se deben detectar las cabinas de almacenamiento en la red.

¿Cómo se detectan cabinas?

Utilice la página Añadir/detectar para encontrar y añadir las cabinas de almacenamiento que desea gestionar en la red de la organización. Es posible detectar varias cabinas de almacenamiento o una sola. Para hacerlo, debe introducir direcciones IP de red y, a continuación, Unified Manager intentar establecer conexiones individuales con cada dirección IP de ese rango.

Obtenga más información:

- "Consideraciones sobre la detección de cabinas"
- "Detectar varias cabinas de almacenamiento"
- "Detectar una sola cabina"

¿Cómo se gestionan las cabinas?

Después de descubrir las matrices, vaya a la página **gestionar - todo**. En esta página, puede desplazarse por una lista de cabinas de almacenamiento detectadas en la red, ver su estado y realizar operaciones en una sola cabina o en un grupo de cabinas.

Si desea gestionar una sola cabina, puede seleccionarla y abrir System Manager.

Obtenga más información:

- "Consideraciones para acceder a System Manager"
- "Gestione una cabina de almacenamiento individual"
- "Ver el estado de la cabina de almacenamiento"

Conceptos

Consideraciones sobre la detección de cabinas

Para poder mostrar y gestionar los recursos de almacenamiento, Unified Manager debe detectar las cabinas de almacenamiento que se desean gestionar en la red de la organización. Es posible detectar varias cabinas de almacenamiento o una sola.

Detección de varias cabinas de almacenamiento

Si decide detectar varias cabinas de almacenamiento, debe introducir un rango de direcciones IP de red. A continuación, Unified Manager intentar establecer conexiones individuales con cada dirección IP de ese rango. Cada cabina de almacenamiento a la que se accedió correctamente se muestra en la página detectar y se puede añadir al dominio de gestión.

Detección de una sola cabina de almacenamiento

Si decide detectar una sola cabina de almacenamiento, debe introducir la dirección IP única para una de las controladoras de la cabina de almacenamiento. A continuación, se añade la cabina de almacenamiento individual.

> Unified Manager detecta y muestra solamente la dirección IP única o la dirección IP dentro del rango asignado a una controladora. Si existen controladoras alternativas o direcciones IP asignadas a estas controladoras que no se incluyen en esta dirección IP única o este rango de direcciones IP, Unified Manager no las detectará ni las mostrará. Sin embargo, una vez añadida la cabina de almacenamiento, se detectarán todas las direcciones IP asociadas y se mostrarán en la vista gestionar.

Credenciales de usuario

Como parte del proceso de detección, debe suministrar la contraseña de administrador para cada cabina de almacenamiento que desee añadir.

Certificados de servicios web

Como parte del proceso de detección, Unified Manager verifica que las cabinas de almacenamiento detectadas utilicen certificados de un origen de confianza. Unified Manager utiliza dos tipos de autenticación basada en certificados para todas las conexiones que establece con el explorador:

- **Certificados de confianza**

  Para las cabinas de almacenamiento detectadas mediante Unified Manager, es posible que deba instalar certificados de confianza adicionales suministrados por la entidad de certificación.

  Utilice el botón **Importar** para importar estos certificados. Si ya se conectó a esta cabina anteriormente, los certificados de una o ambas controladoras caducaron o se revocaron, o no se encuentra un certificado intermedio o de raíz en la cadena de certificados, Debe sustituir el certificado caducado o revocado, o añadir el certificado intermedio o de raíz ausente para gestionar la cabina de almacenamiento.

- **Certificados autofirmados**

  Además, se pueden utilizar certificados autofirmados. Si el administrador intenta detectar las cabinas sin importar los certificados firmados, Unified Manager muestra un cuadro de diálogo de error en el que el administrador puede aceptar el certificado autofirmado. El certificado autofirmado de la cabina de almacenamiento se marcará como de confianza y la cabina de almacenamiento se añadirá a Unified Manager.

  Si no confía en las conexiones a la cabina de almacenamiento, seleccione **Cancelar** y valide la estrategia de certificación de seguridad de la cabina de almacenamiento antes de añadir la cabina de almacenamiento a Unified Manager.

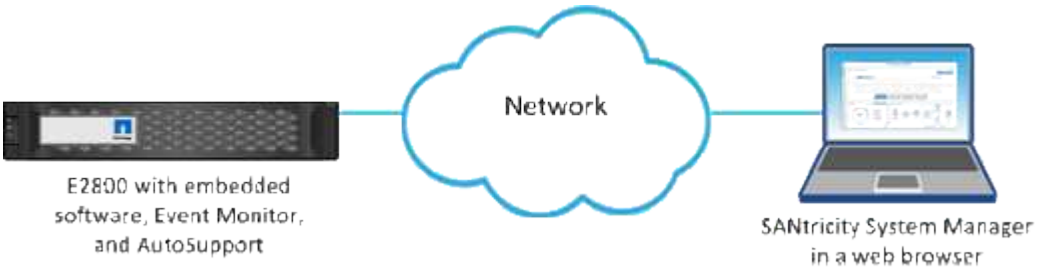
Consideraciones para acceder a System Manager

Es posible seleccionar una o varias cabinas de almacenamiento y usar la opción Iniciar para abrir System Manager cuando se desean configurar y gestionar las cabinas de almacenamiento.

System Manager es una aplicación integrada en las controladoras, que está conectada a la red a través de un puerto de gestión Ethernet. Incluye todas las funciones basadas en cabina.

Para acceder a System Manager, debe tener:

- Uno de los modelos de matriz aquí enumerados: "Información general del hardware de E-Series"
- Una conexión fuera de banda con un cliente de administración de red en un explorador web.



Detectar cabinas de almacenamiento

Detectar varias cabinas de almacenamiento

Detecte varias cabinas para descubrir todas las cabinas de almacenamiento de la subred donde reside el servidor de gestión y añadir automáticamente las cabinas detectadas al dominio de gestión.

Antes de empezar

- Inició sesión con un perfil de usuario que cuenta con permisos de administración de seguridad.
- La cabina de almacenamiento debe estar instalada y configurada correctamente.
- Las contraseñas de las cabinas de almacenamiento deben configurarse mediante el icono Access Management de System Manager.
- Para resolver certificados que no son de confianza, debe tener archivos de certificado de confianza de una entidad de certificación (CA) y los archivos de certificado están disponibles en el sistema local.

La detección de cabinas es un procedimiento de varios pasos.

Paso 1: Introduzca la dirección de red

Se debe introducir un rango de direcciones de red para buscar dentro de la subred local. Todas las cabinas a las que se puede acceder correctamente se muestran en la página detectar, y se pueden añadir al dominio de gestión.

Si necesita detener la operación de detección por cualquier motivo, haga clic en **Detener detección**.

Pasos

1. En la página gestionar, seleccione **Agregar/detectar**.

   Se muestra el cuadro de diálogo Añadir/detectar.

2. Seleccione el botón de opción **detectar todas las cabinas de almacenamiento en un rango de red**.
3. Introduzca la dirección de red inicial y la dirección de red final para buscar en la subred local y, a continuación, haga clic en **Iniciar detección**.

   Se inicia el proceso de detección. El proceso puede tardar varios minutos en completarse. La tabla de la página detectar se carga a medida que se van detectando las cabinas de almacenamiento.

   > Si no se detectan cabinas gestionables, compruebe que las cabinas de almacenamiento estén bien conectadas a la red y que las direcciones asignadas se encuentren dentro del rango correspondiente. Haga clic en **nuevos parámetros de descubrimiento** para volver a la página Agregar/detectar.

4. Revise la lista de cabinas de almacenamiento detectadas.
5. Marque la casilla de comprobación junto a la cabina de almacenamiento que desea añadir al dominio de gestión y haga clic en **Siguiente**.

   Unified Manager comprueba las credenciales de cada cabina que se añade al dominio de gestión. Es posible que deba resolver los certificados autofirmados y los certificados no confiables que estén asociados con esa cabina.

6. Haga clic en **Siguiente** para continuar con el siguiente paso del asistente.

Paso 2: Resuelva los certificados autofirmados durante la detección

Como parte del proceso de detección, el sistema comprueba que las cabinas de almacenamiento estén usando certificados de un origen de confianza.

Pasos

1. Debe realizar una de las siguientes acciones:

- Si confía en las conexiones con las cabinas de almacenamiento detectadas, continúe a la siguiente tarjeta del asistente. Los certificados autofirmados se marcarán como certificados de confianza y las cabinas de almacenamiento se añadirán a Unified Manager.
- Si no confía en dichas conexiones, seleccione **Cancelar** y valide la estrategia de certificado de seguridad de cada cabina de almacenamiento antes de añadir cualquiera de ellas a Unified Manager.

2. Haga clic en **Siguiente** para continuar con el siguiente paso del asistente.

Paso 3: Resolver certificados que no son de confianza durante la detección

Los certificados dejan de ser de confianza cuando una cabina de almacenamiento intenta establecer una conexión con Unified Manager, pero no se confirma que la conexión sea segura. Durante el proceso de detección de cabinas, puede resolver certificados que no son de confianza al importar un certificado de una entidad de certificación (CA) (o certificado firmado por CA) que emitió un tercero de confianza.

Es posible que necesite instalar otros certificados de CA de confianza si se da alguna de las siguientes condiciones:

- Añadió recientemente una cabina de almacenamiento.
- Uno o ambos certificados caducaron.
- Uno o ambos certificados fueron revocados.
- Falta un certificado raíz o intermedio en uno o ambos certificados.

Pasos

1. Marque la casilla de comprobación junto a una cabina de almacenamiento para la cual desee resolver certificados que no son de confianza; a continuación, seleccione el botón **Importar**.

   Se abre un cuadro de diálogo para importar los archivos de certificado de confianza.

2. Haga clic en **examinar** para seleccionar los archivos de certificado para las matrices de almacenamiento.

   Se muestran los nombres de los archivos en el cuadro de diálogo.

3. Haga clic en **Importar**.

   Los archivos se cargan y validan.

   > Si una cabina de almacenamiento tiene problemas de certificados que no son de confianza y aún no se han resuelto, no se podrá añadir a Unified Manager.

4. Haga clic en **Siguiente** para continuar con el siguiente paso del asistente.

Paso 4: Proporcionar contraseñas

Debe introducir las contraseñas de las cabinas de almacenamiento que desea añadir al dominio de gestión.

Pasos

1. Introduzca la contraseña para cada cabina de almacenamiento que desea añadir a Unified Manager.
2. **Opcional:** asocie las matrices de almacenamiento a un grupo: En la lista desplegable, seleccione el grupo que desee asociar a las matrices de almacenamiento seleccionadas.
3. Haga clic en **Finalizar**.

Después de terminar

Las cabinas de almacenamiento se añaden al dominio de gestión y se asocian con el grupo seleccionado (si se especificó alguno).

> Unified Manager puede tardar varios minutos en conectarse a las cabinas de almacenamiento especificadas.

Detectar una sola cabina

Utilice la opción Añadir/detectar una cabina de almacenamiento única para detectar y añadir manualmente una sola cabina de almacenamiento a la red de la organización.

Antes de empezar

- La cabina de almacenamiento debe estar instalada y configurada correctamente.
- Las contraseñas de las cabinas de almacenamiento deben configurarse mediante el icono Access Management de System Manager.

Pasos

1. En la página gestionar, seleccione **Agregar/detectar**.

   Se muestra el cuadro de diálogo Añadir/detectar.

2. Seleccione el botón de opción **detectar una única cabina de almacenamiento**.
3. Introduzca la dirección IP de una de las controladoras de la cabina de almacenamiento y haga clic en **Iniciar la detección**.

   Es posible que Unified Manager demore varios minutos en conectarse a la cabina de almacenamiento especificada.

   > Se mostrará el mensaje cabina de almacenamiento no accesible cuando no se pueda establecer la conexión con la dirección IP de la controladora especificada.

4. Si se le solicita, resuelva los certificados autofirmados.

   Como parte del proceso de detección, el sistema verifica que las cabinas de almacenamiento detectadas utilicen certificados de un origen de confianza. Si no puede localizar un certificado digital para una cabina de almacenamiento, el sistema le solicita que añada una excepción de seguridad para resolver el certificado que no está firmado por una entidad de certificación (CA) reconocida.

5. Si se le solicita, resuelva los certificados que no son de confianza.

   Los certificados dejan de ser de confianza cuando una cabina de almacenamiento intenta establecer una conexión con Unified Manager, pero no se confirma que la conexión sea segura. Importe un certificado de entidad de certificación (CA) emitido por un tercero de confianza para resolver los certificados no confiables.

6. Haga clic en **Siguiente**.
7. **Opcional:** asocie la cabina de almacenamiento detectada a un grupo: En la lista desplegable, seleccione el grupo que desea asociar a la cabina de almacenamiento.

   El grupo "todo" está seleccionado de forma predeterminada.

8. Introduzca la contraseña de administrador para la cabina de almacenamiento que desea añadir al dominio de gestión y haga clic en **Aceptar**.

Después de terminar

La cabina de almacenamiento se añade a Unified Manager y, si se especificó, también se añade al grupo seleccionado.

Si se habilitó la recogida automática de datos de soporte, se recogen automáticamente datos de soporte para la cabina de almacenamiento que se añade.

Gestione las cabinas

Ver el estado de la cabina de almacenamiento

Unified Manager muestra el estado de cada cabina de almacenamiento detectada.

Vaya a la página **Administrar - todo**. En esta página, es posible ver el estado de la conexión entre el proxy de servicios web y la cabina de almacenamiento.

Los indicadores de estado se describen en la siguiente tabla.

Estado	Lo que indica
Óptimo	La cabina de almacenamiento tiene el estado óptimo. No hay problemas de certificados y la contraseña es válida.
Contraseña no válida	Se proporcionó una contraseña no válida para la cabina de almacenamiento.
Certificado no confiable	Una o varias conexiones con la cabina de almacenamiento no son de confianza porque el certificado HTTPS está autofirmado o no se ha importado; o bien, se trata de un certificado firmado por una CA y los certificados de CA raíz e intermedios no se importaron.
Necesita atención	Hay un problema con la cabina de almacenamiento que requiere de su intervención para corregirlo.
Bloqueo	La cabina de almacenamiento está en estado bloqueado.
Desconocido	No se contactó a la cabina de almacenamiento. Esto puede ocurrir cuando el proxy de servicios web se está iniciando y aún no estableció contacto con la cabina de almacenamiento, o bien cuando la cabina se encuentra sin conexión y nunca se la contactó desde que se inició el proxy de servicios web.
Sin conexión	El proxy de servicios web se había contactado previamente con la cabina de almacenamiento, pero ahora perdió toda conexión con ella.

Gestione una cabina de almacenamiento individual

Si desea realizar operaciones de gestión, puede usar la opción Iniciar para abrir la instancia de System Manager basada en el explorador que corresponde a una o más

cabinas de almacenamiento.

Pasos

1. En la página gestionar, seleccione una o más cabinas de almacenamiento que desee gestionar.
2. Haga clic en **Iniciar**.

   El sistema abre una nueva ventana y muestra la página de inicio de sesión de System Manager.

3. Introduzca su nombre de usuario y contraseña y, a continuación, haga clic en **Iniciar sesión**.

Cambiar contraseñas de las cabinas de almacenamiento

Puede actualizar las contraseñas que se utilizan para ver y acceder a las cabinas de almacenamiento en Unified Manager.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de almacenamiento.
- Debe conocer la contraseña actual de la cabina de almacenamiento que se estableció en System Manager.

Acerca de esta tarea

En esta tarea, debe introducir la contraseña actual de una cabina de almacenamiento para poder acceder a esta en Unified Manager. Esto puede ser necesario si se modificó la contraseña de la cabina en System Manager y ahora se debe modificar también Unified Manager.

Pasos

1. En la página gestionar, seleccione una o varias cabinas de almacenamiento.
2. Seleccione menú:tareas no comunes[proporcionar contraseñas de cabina de almacenamiento].
3. Introduzca la contraseña o las contraseñas de cada cabina de almacenamiento y haga clic en **Guardar**.

Quite las cabinas de almacenamiento de SANtricity Unified Manager

Es posible quitar una o varias cabinas de almacenamiento si ya no se van a gestionar desde Unified Manager.

Acerca de esta tarea

No es posible acceder a ninguna de las cabinas de almacenamiento que se quiten. Sin embargo, puede establecerse una conexión con cualquiera de las cabinas de almacenamiento eliminadas si se apunta un explorador directamente a su dirección IP o nombre de host.

Al quitar una cabina de almacenamiento, ni ella ni sus datos se ven afectados de forma alguna. Si una cabina de almacenamiento se quita por error, es posible volver a añadirla.

Pasos

1. Seleccione la página **Administrar**.
2. Seleccione una o varias cabinas de almacenamiento que desee quitar.
3. Seleccione menú:tareas no comunes[Quitar cabina de almacenamiento].

   La cabina de almacenamiento se elimina de todas las vistas de SANtricity Unified Manager.

Importación de la configuración

Información general de importación de la configuración

La función Importar configuración permite realizar una operación en lote para importar la configuración de una cabina a varias. Esta función permite ahorrar tiempo cuando se necesitan configurar varias matrices en la red.

¿Qué configuración se puede importar?

Es posible importar métodos de alerta, configuraciones de AutoSupport, configuraciones de servicios de directorio, configuraciones de almacenamiento (como grupos de volúmenes y pools) y configuraciones del sistema (como equilibrio de carga automático).

Obtenga más información:

- "Cómo funciona la importación de configuración"
- "Requisitos para replicar configuraciones de almacenamiento"

¿Cómo se realiza una importación por lotes?

En una cabina de almacenamiento que se usará como origen, abra System Manager y configure los ajustes deseados. A continuación, desde Unified Manager, vaya a la página gestionar e importe la configuración a una o varias cabinas.

Obtenga más información:

- "Importar la configuración de alerta"
- "Importe la configuración de AutoSupport"
- "Importe la configuración de servicios de directorio"
- "Importe los ajustes de configuración de almacenamiento"
- "Importe la configuración del sistema"

Conceptos

Cómo funciona la importación de configuración

Es posible usar Unified Manager para importar la configuración de una cabina de almacenamiento a varias cabinas de almacenamiento. La función Importar configuración es una operación en lote que permite ahorrar tiempo cuando se necesitan configurar varias cabinas en la red.

Configuración disponible para la importación

Las siguientes configuraciones pueden importarse en varias cabinas:

- **Alertas** — métodos de alerta para enviar eventos importantes a los administradores, mediante correo electrónico, un servidor syslog o un servidor SNMP.
- **AutoSupport**: Función que supervisa el estado de una matriz de almacenamiento y envía mensajes

automáticos al soporte técnico.

- **Servicios de directorio** — método de autenticación de usuario que se administra a través de un servidor LDAP (protocolo ligero de acceso a directorios) y un servicio de directorio, como Active Directory de Microsoft.
- **Configuración de almacenamiento** — configuraciones relacionadas con lo siguiente:
  - Volúmenes (solo volúmenes gruesos y que no pertenecen al repositorio)
  - Grupos de volúmenes y pools
  - Asignaciones de unidad de repuesto
- **Ajustes del sistema** — configuraciones relacionadas con lo siguiente:
  - Configuración de escaneo de medios para un volumen
  - Configuración de SSD
  - Equilibrio de carga automático (no incluye la generación de informes de conectividad de host)

Flujo de trabajo de configuración

Para importar la configuración, siga este flujo de trabajo:

1. En una cabina de almacenamiento que se usará como origen, configure los ajustes mediante System Manager.
2. En las cabinas de almacenamiento que se usarán como objetivo, realice una copia de seguridad de la configuración mediante System Manager.
3. Desde Unified Manager, vaya a la página **Administrar** e importe la configuración.
4. En la página **Operaciones**, revise los resultados de la operación Importar configuración.

Requisitos para replicar configuraciones de almacenamiento

Antes de importar una configuración de almacenamiento desde una cabina de almacenamiento a otra, revise los requisitos y las directrices.

Bandejas

- Las bandejas donde residen las controladoras deben ser idénticas en las cabinas de origen y objetivo.
- Los ID de bandeja deben ser idénticos en las cabinas de origen y objetivo.
- Las bandejas de expansión deben llenarse en las mismas ranuras con los mismos tipos de unidad (si la unidad se usó en la configuración, la ubicación de las unidades sin usar no importa).

Controladoras

- El tipo de controladora puede ser diferente para las cabinas de origen y objetivo (por ejemplo, se puede importar de E2800 a E5700), pero el tipo de compartimento RBOD debe ser idéntico.
- Las HIC, incluidas las capacidades DE GARANTÍA de DATOS del host, deben ser idénticas para las cabinas de origen y objetivo.
- No se admite la importación de una configuración doble a una simple; sí se admite la configuración simple a doble.
- La configuración de unidades FDE no está incluida en el proceso de importación.

Estado

- Las cabinas objetivo deben tener el estado óptimo.
- La cabina de origen no necesita tener el estado óptimo.

Reducida

- La capacidad de una unidad puede variar entre las cabinas de origen y las objetivo, siempre y cuando la capacidad de volumen en la cabina objetivo sea mayor que en la de origen. (Una cabina objetivo puede tener unidades más nuevas y con mayor capacidad que la operación de replicación quizás no configure por completo en volúmenes).
- Un volumen de pool de discos de 64 TB o mayor en la cabina de origen impide el proceso de importación en las cabinas objetivo.
- Los volúmenes finos no están incluidos en el proceso de importación.

Utilizar importaciones por lotes

Importar la configuración de alerta

Es posible importar la configuración de alerta de una cabina de almacenamiento en otras cabinas de almacenamiento. Esta operación en lote permite ahorrar tiempo cuando se necesitan configurar varias matrices en la red.

Antes de empezar

- Las alertas se configuran en la instancia de System Manager correspondiente a la cabina de almacenamiento que se quiere usar como origen (**Configuración › Alertas**).
- La configuración actual de las cabinas de almacenamiento objetivo cuenta con una copia de seguridad en System Manager (menú:Configuración[sistema > Guardar configuración de la cabina de almacenamiento]).

Acerca de esta tarea

Puede seleccionar las opciones de correo electrónico, SNMP o alertas de syslog para la operación de importación. La configuración importada incluye lo siguiente:

- **Alertas por correo electrónico** — una dirección de servidor de correo y las direcciones de correo electrónico de los destinatarios de las alertas.
- **Alertas Syslog** — una dirección de servidor syslog y un puerto UDP.
- **Alertas SNMP** — un nombre de comunidad y una dirección IP para el servidor SNMP.

Pasos

1. En la página gestionar, haga clic en **Importar configuración**.

   Se abre el asistente Importar configuración.

2. En el cuadro de diálogo Seleccionar configuración, seleccione **Alertas por correo electrónico**, **Alertas SNMP** o **Alertas Syslog** y, a continuación, haga clic en **Siguiente**.

   Se abre un cuadro de diálogo para seleccionar la cabina de almacenamiento.

3. En el cuadro de diálogo Seleccionar origen, seleccione la matriz con la configuración que desea importar y, a continuación, haga clic en **Siguiente**.

4. En el cuadro de diálogo Seleccionar objetivos, elija una o más cabinas para que reciban la nueva configuración.

> Las cabinas de almacenamiento con una versión de firmware inferior a 8.50 no están disponibles y no pueden seleccionarse. Asimismo, una cabina no aparecerá en este cuadro de diálogo si Unified Manager no puede comunicarse con esa cabina (por ejemplo, si está desconectada o si tiene problemas de red o con un certificado o una contraseña).

5. Haga clic en **Finalizar**.

   En la página Operaciones, se muestran los resultados de la operación de importación. Si se produce un error en la operación, puede hacer clic en la fila para ver más información.

Resultados

Las cabinas de almacenamiento objetivo ahora están configuradas para enviar alertas a los administradores mediante correo electrónico, SNMP o syslog.

Importe la configuración de AutoSupport

Es posible importar la configuración de AutoSupport desde una cabina de almacenamiento a otras cabinas de almacenamiento. Esta operación en lote permite ahorrar tiempo cuando se necesitan configurar varias matrices en la red.

Antes de empezar

- AutoSupport se configura en la instancia de System Manager correspondiente a la cabina de almacenamiento que se quiere usar como origen (MENU:Support[Support Center]).
- La configuración actual de las cabinas de almacenamiento objetivo cuenta con una copia de seguridad en System Manager (menú:Configuración[sistema > Guardar configuración de la cabina de almacenamiento]).

Acerca de esta tarea

La configuración importada incluye las funciones por separado (Basic AutoSupport, AutoSupport OnDemand y Remote Diagnostics), la ventana de mantenimiento, el método de entrega, y programa de envío.

Pasos

1. En la página gestionar, haga clic en **Importar configuración**.

   Se abre el asistente Importar configuración.

2. En el cuadro de diálogo Seleccionar configuración, seleccione **AutoSupport** y, a continuación, haga clic en **Siguiente**.

   Se abre un cuadro de diálogo para seleccionar la cabina de almacenamiento.

3. En el cuadro de diálogo Seleccionar origen, seleccione la matriz con la configuración que desea importar y, a continuación, haga clic en **Siguiente**.
4. En el cuadro de diálogo Seleccionar objetivos, elija una o más cabinas para que reciban la nueva configuración.

> Las cabinas de almacenamiento con una versión de firmware inferior a 8.50 no están disponibles y no pueden seleccionarse. Asimismo, una cabina no aparecerá en este cuadro de diálogo si Unified Manager no puede comunicarse con esa cabina (por ejemplo, si está desconectada o si tiene problemas de red o con un certificado o una contraseña).

5. Haga clic en **Finalizar**.

   En la página Operaciones, se muestran los resultados de la operación de importación. Si se produce un error en la operación, puede hacer clic en la fila para ver más información.

Resultados

Las cabinas de almacenamiento objetivo ahora están configuradas con los mismos ajustes de AutoSupport que la cabina de origen.

Importe la configuración de servicios de directorio

Es posible importar la configuración de los servicios de directorio desde una cabina de almacenamiento a otras cabinas de almacenamiento. Esta operación en lote permite ahorrar tiempo cuando se necesitan configurar varias matrices en la red.

Antes de empezar

- Los servicios de directorio están configurados en la instancia de System Manager correspondiente a la cabina de almacenamiento que se quiere usar como origen (MENU:Settings[Access Management]).
- La configuración actual de las cabinas de almacenamiento objetivo cuenta con una copia de seguridad en System Manager (menú:Configuración[sistema > Guardar configuración de la cabina de almacenamiento]).

Acerca de esta tarea

La configuración importada incluye el nombre de dominio y la URL de un servidor LDAP (protocolo ligero de acceso a directorios), junto con las asignaciones de los grupos de usuarios del servidor LDAP con los roles predefinidos de la cabina de almacenamiento.

Pasos

1. En la página gestionar, haga clic en **Importar configuración**.

   Se abre el asistente Importar configuración.

2. En el cuadro de diálogo Seleccionar configuración, seleccione **Servicios de directorio** y, a continuación, haga clic en **Siguiente**.

   Se abre un cuadro de diálogo para seleccionar la cabina de almacenamiento.

3. En el cuadro de diálogo Seleccionar origen, seleccione la matriz con la configuración que desea importar y, a continuación, haga clic en **Siguiente**.
4. En el cuadro de diálogo Seleccionar objetivos, elija una o más cabinas para que reciban la nueva configuración.

> Las cabinas de almacenamiento con una versión de firmware inferior a 8.50 no están disponibles y no pueden seleccionarse. Asimismo, una cabina no aparecerá en este cuadro de diálogo si Unified Manager no puede comunicarse con esa cabina (por ejemplo, si está desconectada o si tiene problemas de red o con un certificado o una contraseña).

5. Haga clic en **Finalizar**.

   En la página Operaciones, se muestran los resultados de la operación de importación. Si se produce un error en la operación, puede hacer clic en la fila para ver más información.

Resultados

Las cabinas de almacenamiento objetivo ahora están configuradas con los mismos servicios de directorio que la cabina de origen.

Importe la configuración del sistema

Es posible importar la configuración del sistema desde una cabina de almacenamiento a otras cabinas de almacenamiento. Esta operación en lote permite ahorrar tiempo cuando se necesitan configurar varias matrices en la red.

Antes de empezar

- La configuración del sistema se define en la instancia de System Manager correspondiente a la cabina de almacenamiento que se quiere usar como origen.
- La configuración actual de las cabinas de almacenamiento objetivo cuenta con una copia de seguridad en System Manager (menú:Configuración[sistema > Guardar configuración de la cabina de almacenamiento]).

Acerca de esta tarea

La configuración importada incluye los ajustes de escaneo de medios de un volumen, los ajustes de SSD de las controladoras y el equilibrio de carga automático (no incluye la generación de informes de conectividad de host).

Pasos

1. En la página gestionar, haga clic en **Importar configuración**.

   Se abre el asistente Importar configuración.

2. En el cuadro de diálogo Seleccionar configuración, seleccione **sistema** y, a continuación, haga clic en **Siguiente**.

   Se abre un cuadro de diálogo para seleccionar la cabina de almacenamiento.

3. En el cuadro de diálogo Seleccionar origen, seleccione la matriz con la configuración que desea importar y, a continuación, haga clic en **Siguiente**.
4. En el cuadro de diálogo Seleccionar objetivos, elija una o más cabinas para que reciban la nueva configuración.

   > Las cabinas de almacenamiento con una versión de firmware inferior a 8.50 no están disponibles y no pueden seleccionarse. Asimismo, una cabina no aparecerá en este cuadro de diálogo si Unified Manager no puede comunicarse con esa cabina (por ejemplo, si está desconectada o si tiene problemas de red o con un certificado o una contraseña).

5. Haga clic en **Finalizar**.

   En la página Operaciones, se muestran los resultados de la operación de importación. Si se produce un error en la operación, puede hacer clic en la fila para ver más información.

Resultados

Las cabinas de almacenamiento objetivo ahora están configuradas con los mismos ajustes del sistema que la cabina de origen.

Importe los ajustes de configuración de almacenamiento

Es posible importar la configuración de almacenamiento de una cabina de almacenamiento en otras cabinas de almacenamiento. Esta operación en lote permite ahorrar tiempo cuando se necesitan configurar varias matrices en la red.

Antes de empezar

- El almacenamiento se configura en la instancia de SANtricity System Manager correspondiente a la cabina de almacenamiento que se quiere usar como origen.
- La configuración actual de las cabinas de almacenamiento objetivo cuenta con una copia de seguridad en System Manager (menú:Configuración[sistema > Guardar configuración de la cabina de almacenamiento]).
- Las cabinas de origen y objetivo deben cumplir con los siguientes requisitos:
  - Las bandejas donde residan las controladoras deben ser idénticas.
  - Los ID de bandeja deben ser idénticos.
  - Las bandejas de expansión deben llenarse en las mismas ranuras con los mismos tipos de unidad.
  - El tipo de compartimento RBOD debe ser idéntico.
  - Las HIC, incluidas las capacidades de garantía de datos del host, deben ser idénticas.
  - Las cabinas objetivo deben tener el estado óptimo.
  - La capacidad de volumen de la cabina objetivo es mayor que la capacidad de la cabina de origen.
- Debe considerar las siguientes restricciones:
  - No se admite la importación de una configuración doble a una simple; sí se admite la configuración simple a doble.
  - Un volumen de pool de discos de 64 TB o mayor en la cabina de origen impide el proceso de importación en las cabinas objetivo.
  - Los volúmenes finos no están incluidos en el proceso de importación.

Acerca de esta tarea

La configuración importada incluye volúmenes configurados (solo volúmenes gruesos y que no pertenecen al repositorio), grupos de volúmenes, pools y asignaciones de unidades de repuesto.

Pasos

1. En la página gestionar, haga clic en **Importar configuración**.

   Se abre el asistente Importar configuración.

2. En el cuadro de diálogo Seleccionar configuración, seleccione **Configuración de almacenamiento** y, a continuación, haga clic en **Siguiente**.

   Se abre un cuadro de diálogo para seleccionar la cabina de almacenamiento.

3. En el cuadro de diálogo Seleccionar origen, seleccione la matriz con la configuración que desea importar y, a continuación, haga clic en **Siguiente**.

4. En el cuadro de diálogo Seleccionar objetivos, elija una o más cabinas para que reciban la nueva configuración.

> Las cabinas de almacenamiento con una versión de firmware inferior a 8.50 no están disponibles y no pueden seleccionarse. Asimismo, una cabina no aparecerá en este cuadro de diálogo si Unified Manager no puede comunicarse con esa cabina (por ejemplo, si está desconectada o si tiene problemas de red o con un certificado o una contraseña).

5. Haga clic en **Finalizar**.

   En la página Operaciones, se muestran los resultados de la operación de importación. Si se produce un error en la operación, puede hacer clic en la fila para ver más información.

Resultados

Las cabinas de almacenamiento objetivo ahora están configuradas con los mismos ajustes de almacenamiento que la cabina de origen.

Preguntas frecuentes

¿Qué configuración se importará?

La función Importar configuración es una operación en lote que carga las configuraciones desde una cabina de almacenamiento a varias cabinas de almacenamiento. La configuración que se importe durante esta operación dependerá de cómo esté configurada la cabina de almacenamiento de origen en System Manager.

Las siguientes configuraciones pueden importarse a varias cabinas:

- **Alertas por correo electrónico** — la configuración incluye una dirección de servidor de correo y las direcciones de correo electrónico de los destinatarios de las alertas.
- **Alertas Syslog** — las configuraciones incluyen una dirección de servidor syslog y un puerto UDP.
- **Alertas SNMP** — las configuraciones incluyen un nombre de comunidad y una dirección IP para el servidor SNMP.
- **AutoSupport** — los ajustes incluyen las características independientes (Basic AutoSupport, AutoSupport OnDemand y Remote Diagnostics), la ventana de mantenimiento, el método de entrega, y programa de envío.
- **Servicios de directorio** — la configuración incluye el nombre de dominio y la URL de un servidor LDAP (protocolo ligero de acceso a directorios), junto con las asignaciones de los grupos de usuarios del servidor LDAP a los roles predefinidos de la cabina de almacenamiento.
- **Configuración de almacenamiento** — las configuraciones incluyen volúmenes (sólo volúmenes gruesos y que no pertenecen al repositorio), grupos de volúmenes, pools y asignaciones de unidades de repuesto activo.
- **Ajustes del sistema** — las configuraciones incluyen la configuración de escaneo de medios para un volumen, caché SSD para controladores y equilibrio de carga automático (no incluye la generación de informes de conectividad de host).

¿Por qué no se muestran todas las cabinas de almacenamiento?

Durante la operación Importar configuración, es posible que algunas cabinas de

almacenamiento no estén disponibles en el cuadro de diálogo de selección de objetivos.

Que las cabinas de almacenamiento no aparezcan puede deberse a los siguientes motivos:

- La versión de firmware es inferior a 8.50.
- La cabina de almacenamiento se encuentra sin conexión.
- El sistema no puede comunicarse con esa cabina (por ejemplo, la cabina tiene problemas de red o con un certificado o una contraseña).

Grupos de cabinas

Información general sobre grupos

En la página gestionar grupos, puede crear un conjunto de grupos de cabinas de almacenamiento para simplificar la gestión.

¿Qué son los grupos de cabinas?

Es posible gestionar la infraestructura física y virtualizada si se agrupa un conjunto de cabinas de almacenamiento. Las cabinas de almacenamiento pueden agruparse de modo que sea más sencillo ejecutar las tareas de supervisión o generación de informes.

Existen dos tipos de grupos:

- **Todo el grupo** — el grupo todo es el grupo predeterminado e incluye todas las matrices de almacenamiento detectadas en su organización. Es posible acceder al grupo desde la vista principal.
- **Grupo creado por el usuario** — Un grupo creado por el usuario incluye las matrices de almacenamiento que selecciona manualmente para agregar a ese grupo. Es posible acceder a este tipo de grupo desde la vista principal.

¿Cómo se configuran los grupos?

En la página gestionar grupos, puede crear un grupo y, a continuación, añadir cabinas a dicho grupo.

Obtenga más información:

- "Configure el grupo de cabinas de almacenamiento"

Configure el grupo de cabinas de almacenamiento

Cree grupos de almacenamiento y, a continuación, añada cabinas de almacenamiento a los grupos.

La configuración de grupos es un procedimiento de dos pasos.

Paso 1: Crear grupo

En primer lugar, cree un grupo. El grupo de almacenamiento define las unidades que proporcionan el almacenamiento con el que se compone el volumen.

Pasos

1. En la página gestionar, seleccione **gestionar grupos › Crear grupo de cabinas de almacenamiento**.
2. En el campo **Nombre**, escriba un nombre para el nuevo grupo.
3. Seleccione las cabinas de almacenamiento que desea añadir al nuevo grupo.
4. Haga clic en **Crear**.

Paso 2: Añadir una cabina de almacenamiento a un grupo

Es posible añadir una o varias cabinas de almacenamiento a un grupo creado por un usuario.

Pasos

1. En la vista principal, seleccione **gestionar** y, a continuación, seleccione el grupo al que desea agregar matrices de almacenamiento.
2. Seleccione menú:gestionar grupos[Añadir cabinas de almacenamiento a grupo].
3. Seleccione las cabinas de almacenamiento que desea añadir al grupo.
4. Haga clic en **Agregar.**

Quite las cabinas de almacenamiento del grupo

Es posible quitar una o varias cabinas de almacenamiento gestionadas de un grupo si ya no se van a gestionar desde un grupo de almacenamiento específico.

Acerca de esta tarea

Al quitar cabinas de almacenamiento de un grupo, ni ellas ni sus datos se ven afectados de forma alguna. Si System Manager gestiona su cabina de almacenamiento, es posible gestionarla desde un explorador. Si una cabina de almacenamiento se quita por error de un grupo, es posible volver a añadirla.

Pasos

1. En la página gestionar, seleccione menú:gestionar grupos[Quitar cabinas de almacenamiento del grupo].
2. En el menú desplegable, seleccione el grupo que contiene las cabinas de almacenamiento que desea quitar y luego haga clic en la casilla de comprobación junto a cada cabina de almacenamiento que desea quitar del grupo.
3. Haga clic en **Quitar**.

Elimine grupo de cabinas de almacenamiento

Puede eliminar uno o varios grupos de cabinas de almacenamiento que ya no sean necesarios.

Acerca de esta tarea

Esta operación solo elimina el grupo de cabinas de almacenamiento. Todavía es posible acceder a las cabinas de almacenamiento asociadas con el grupo eliminado a través de la vista gestionar todo o de otro grupo con el que todavía se encuentren asociadas.

Pasos

1. En la página gestionar, seleccione **gestionar grupos › Eliminar grupo de cabinas de almacenamiento**.
2. Seleccione el o los grupos de cabinas de almacenamiento que desee eliminar.
3. Haga clic en **Eliminar**.

Cambiar el nombre de un grupo de cabinas de almacenamiento

Es posible cambiar el nombre de un grupo de cabinas de almacenamiento si el nombre actual ya no es significativo o no corresponde.

Acerca de esta tarea

Tenga en cuenta estas directrices.

- Un nombre puede consistir de letras, números y los caracteres especiales de subrayado (_), guión (-) y almohadilla (#). Si elige otros caracteres, aparece un mensaje de error. Se le solicitará que elija otro nombre.
- El nombre puede tener 30 caracteres como máximo. Los espacios iniciales o finales del nombre se eliminan.
- Use un nombre único, significativo, que sea fácil de entender y de recordar.
- Evite nombres arbitrarios o nombres que rápidamente pueden perder sentido en el futuro.

Pasos

1. En la ventana principal, seleccione **gestionar** y seleccione el grupo de cabinas de almacenamiento al que desea cambiarle el nombre.
2. Seleccione **gestionar grupos › Cambiar nombre de grupo de cabinas de almacenamiento**.
3. En el campo **Nombre del grupo**, escriba un nuevo nombre para el grupo.
4. Haga clic en **Cambiar nombre.**

Actualizaciones

Información general del centro de actualización

En el Centro de actualización, puede gestionar las actualizaciones de NVSRAM y de software de sistema operativo SANtricity para varias cabinas de almacenamiento.

¿Cómo funcionan las actualizaciones?

Descargue el software de sistema operativo más reciente y después actualice una o varias cabinas.

Actualizar el flujo de trabajo

Los siguientes pasos constituyen un flujo de trabajo de alto nivel para ejecutar actualizaciones de software.

1. Descargue el archivo de software del sistema operativo SANtricity más reciente en el sitio de soporte (hay un enlace disponible en Unified Manager, en la página Soporte). Guarde el archivo en el sistema host de gestión (el host desde donde se accede a Unified Manager en un explorador) y descomprima el archivo.
2. En Unified Manager, puede cargar el archivo de software del sistema operativo SANtricity y el archivo NVSRAM en el repositorio (un área del servidor proxy de servicios web donde se almacenan los archivos). Puede añadir archivos desde MENU:Centro de actualización[Actualizar software de sistema operativo SANtricity o desde Centro de actualización > gestionar el repositorio de software].
3. Una vez que se hayan cargado los archivos en el repositorio, seleccione el archivo que usará en la actualización. En la página Actualizar software de sistema operativo SANtricity (menú:Centro de actualización[Actualizar software de sistema operativo SANtricity]), puede seleccionar el archivo de software de sistema operativo SANtricity y el archivo de NVSRAM. Después de seleccionar un archivo de

software, se muestra en la página una lista con las cabinas de almacenamiento compatibles. A continuación, seleccione las cabinas de almacenamiento que desea actualizar con el nuevo software. (No puede seleccionar cabinas incompatibles).

4. Luego, puede iniciar una transferencia y activación inmediatas del software, o puede optar por preconfigurar los archivos para su activación más adelante. Durante el proceso de actualización, Unified Manager realiza las siguientes tareas:
   a. Realiza una comprobación del estado de las cabinas de almacenamiento para determinar si existe alguna condición que pudiera impedir que se complete la actualización. Si ocurre un error en la comprobación del estado de alguna cabina, puede omitir esa cabina en particular y continuar la actualización de las otras cabinas. Otra opción es detener el proceso por completo y solucionar los problemas de las cabinas que presentaron errores.
   b. Transfiere los archivos de actualización a cada controladora.
   c. Reinicia las controladoras y activa el nuevo software del sistema operativo SANtricity de a una controladora por vez. Durante la activación, el archivo del sistema operativo SANtricity existente se reemplaza por el nuevo archivo.

      También es posible especificar que el software se active en otro momento.

Actualización inmediata o almacenamiento temporal

Puede activar la actualización de inmediato o almacenarla temporalmente para otro momento. Puede optar por activarlos más tarde por los siguientes motivos:

- **Hora del día** — la activación del software puede llevar mucho tiempo, por lo que es posible que desee esperar hasta que las cargas de E/S sean más livianas. Según la carga de I/o y el tamaño de caché, la actualización de una controladora generalmente puede demorar entre 15 y 25 minutos en completarse. Las controladoras se reinician y conmutan al nodo de respaldo durante la activación, de manera que el rendimiento podría ser inferior al habitual hasta que finalice la actualización.
- **Tipo de paquete**: Es posible que desee probar el nuevo software y firmware en una matriz de almacenamiento antes de actualizar los archivos en otras matrices de almacenamiento.

Para activar el software almacenado temporalmente, vaya al menú:Soporte[Centro de actualización] y haga clic en **Activar** en el área etiquetada como actualización de software del controlador de sistema operativo SANtricity.

Comprobación del estado

Una comprobación del estado se ejecuta como parte del proceso de actualización, pero es posible ejecutarla por separado, antes de comenzar (vaya a menú:Centro de actualización[Comprobación del estado previa a la actualización]).

La comprobación del estado evalúa todos los componentes de la cabina de almacenamiento para garantizar que se pueda proceder con la actualización. Las siguientes condiciones podrían evitar la actualización:

- Unidades asignadas con errores
- Piezas de repuesto en uso
- Grupos de volúmenes incompletos
- Operaciones exclusivas en ejecución
- Volúmenes faltantes

- Estado no óptimo de la controladora
- Cantidad excesiva de eventos en el registro de eventos
- Fallo de validación de la base de datos de configuración
- Unidades con versiones de DACstore anteriores

¿Qué debo saber antes de actualizar?

Antes de actualizar varias cabinas de almacenamiento, revise las consideraciones fundamentales como parte de la planificación.

Versiones actuales

Puede ver las versiones actuales del software de sistema operativo SANtricity desde la página gestionar de Unified Manager en cada cabina de almacenamiento detectada. La versión se muestra en la columna Software de sistema operativo SANtricity. Si hace clic en la versión de sistema operativo SANtricity en cada fila, puede encontrar información de NVSRAM y del firmware de la controladora en un cuadro de diálogo emergente.

Otros componentes que requieren actualización

Como parte del proceso de actualización, es posible que también necesite actualizar el controlador de conmutación al nodo de respaldo/multivía del host o el controlador de HBA de modo que el host pueda interactuar con las controladoras correctamente.

Para obtener información sobre compatibilidad, consulte "Matriz de interoperabilidad de NetApp". Asimismo, consulte los procedimientos en las guías exprés del sistema operativo. Las guías exprés están disponibles en "Documentación de E-Series y SANtricity".

Controladoras dobles

Si una cabina de almacenamiento contiene dos controladoras y existe un controlador multivía instalado, la cabina de almacenamiento puede seguir procesando las operaciones de I/o mientras se realiza la actualización. Durante la actualización, ocurre el siguiente proceso:

1. La controladora A conmuta todos sus LUN a la controladora B.
2. La actualización se produce en la controladora A.
3. La controladora A recupera sus LUN y todos los LUN de la controladora B.
4. La actualización se produce en la controladora B.

Una vez que finaliza la actualización, es posible que sea necesario redistribuir los volúmenes manualmente entre las controladoras para garantizar que los volúmenes regresen a la controladora correspondiente.

Actualice software y firmware

Realice la comprobación del estado previa a la actualización

Una comprobación del estado se ejecuta como parte del proceso de actualización, pero también es posible ejecutarla por separado, antes de comenzar. La comprobación del estado evalúa los componentes de la cabina de almacenamiento para garantizar que se pueda proceder con la actualización.

Pasos

1. En la vista principal, seleccione **gestionar** y, a continuación, elija Menú:Centro de actualización[Comprobación del estado previa a la actualización].

   Se abre el cuadro de diálogo Comprobación del estado previa a la actualización, donde se enumeran todos los sistemas de almacenamiento detectados.

2. Si es necesario, puede filtrar u ordenar los sistemas de almacenamiento de la lista, de modo que pueda ver todos los sistemas que están actualmente en estado óptimo.
3. Marque las casillas de comprobación de los sistemas de almacenamiento que quiere incluir en la comprobación del estado.
4. Haga clic en **Inicio**.

   Mientras se lleva a cabo la comprobación del estado, se muestra el progreso en el cuadro de diálogo.

5. Una vez finalizada la comprobación del estado, puede hacer clic en los tres puntos (…) a la derecha de cada fila para ver más información y realizar otras tareas.

   Si ocurre un error en la comprobación del estado de alguna cabina, puede omitir esa cabina en particular y continuar la actualización de las otras cabinas. Otra opción es detener el proceso por completo y solucionar los problemas de las cabinas que presentaron errores.

Actualice el sistema operativo SANtricity

Puede actualizar una o varias cabinas de almacenamiento con el software más reciente y NVSRAM para asegurarse de contar con las funciones y correcciones de errores más recientes. NVSRAM de controladora es un archivo de la controladora que especifica las configuraciones predeterminadas para las controladoras.

Antes de empezar

- Los archivos del sistema operativo SANtricity más reciente están disponibles en el sistema host donde se ejecutan Unified Manager y el proxy de servicios web SANtricity.
- Sabe si desea activar la actualización del software ahora o más adelante.

  Puede optar por activarlos más tarde por los siguientes motivos:

  - **Hora del día** — la activación del software puede llevar mucho tiempo, por lo que es posible que desee esperar hasta que las cargas de E/S sean más livianas. Las controladoras conmutan al nodo de respaldo durante la activación, de manera que el rendimiento podría ser inferior al habitual hasta que finalice la actualización.
  - **Tipo de paquete**: Es posible que desee probar el nuevo software de sistema operativo en una matriz de almacenamiento antes de actualizar los archivos en otras matrices de almacenamiento.

Los sistemas deben ejecutar SANtricity OS 11.70.5 para actualizar a la versión 11,80.x o posterior.

Acerca de esta tarea

> Riesgo de pérdida de datos o riesgo de daños a la cabina de almacenamiento: No introduzca cambios en la cabina de almacenamiento mientras se realiza la actualización. Mantenga encendida la cabina de almacenamiento.

Pasos

1. Si la cabina de almacenamiento contiene una sola controladora o un controlador multivía no está en uso, detenga la actividad de I/o de la cabina de almacenamiento para evitar errores en la aplicación. Si la cabina de almacenamiento tiene dos controladoras y existe un controlador multivía instalado, no necesita detener la actividad de I/O.
2. En la vista principal, seleccione **gestionar** y, a continuación, seleccione una o varias cabinas de almacenamiento que desee actualizar.
3. Seleccione MENU:Centro de actualización[Actualizar software de sistema operativo SANtricity].

   Se muestra la página Actualizar software de sistema operativo SANtricity.

4. Descargue el paquete de software de sistema operativo de SANtricity del sitio de soporte de NetApp en el equipo local.

   a. Haga clic en **Agregar nuevo archivo al repositorio de software**.
   b. Haga clic en el enlace para buscar las últimas **Descargas de SANtricity OS**.
   c. Haga clic en el enlace **Descargar la versión más reciente**.
   d. Siga las restantes instrucciones para descargar el archivo de sistema operativo de SANtricity y el archivo de NVSRAM en el equipo local.

   > Se requiere firmware con firma digital en la versión 8.42 y posteriores. Si intenta descargar firmware sin firmar, se muestra un error y se anula la descarga.

5. Seleccione el archivo de software de sistema operativo y el archivo de NVSRAM que desea usar para actualizar las controladoras:

   a. En el menú desplegable **Seleccione un archivo de software del sistema operativo SANtricity**, seleccione el archivo del sistema operativo que descargó en el equipo local.

      Si hay varios archivos disponibles, se ordenarán del más reciente al más antiguo.

      > En el repositorio de software, figuran todos los archivos de software relacionados con el proxy de servicios web. Si no ve el archivo que desea utilizar, haga clic en el vínculo **Agregar nuevo archivo al repositorio de software**, para buscar la ubicación donde reside el archivo de sistema operativo que desea agregar.

   a. En el menú desplegable **Seleccione un archivo NVSRAM**, seleccione el archivo de la controladora que desea utilizar.

      Si hay varios archivos, se ordenarán del más reciente al más antiguo.

6. En la tabla cabina de almacenamiento compatible, revise las cabinas de almacenamiento que son compatibles con el archivo de software del sistema operativo seleccionado. A continuación, seleccione las cabinas que desea actualizar.
   - Las cabinas de almacenamiento seleccionadas en la vista gestionar que son compatibles con el archivo de firmware elegido están seleccionadas de forma predeterminada en la tabla cabina de almacenamiento compatible.

- Las matrices de almacenamiento que no se pueden actualizar con el archivo de firmware seleccionado no se pueden seleccionar en la tabla matriz de almacenamiento compatible, como indica el estado **incompatible**.

7. **Opcional:** para transferir el archivo de software a las matrices de almacenamiento sin activarlo, active la casilla de verificación **transferir el software del sistema operativo a las matrices de almacenamiento, marcarlo como preconfigurado y activarlo posteriormente**.
8. Haga clic en **Inicio**.
9. Según elija activar ahora o más adelante, realice una de las siguientes acciones:
   - Escriba **TRANSFER** para confirmar que desea transferir las versiones propuestas de software del sistema operativo en las matrices que seleccionó para actualizar y, a continuación, haga clic en **transferir**.

     Para activar el software transferido, seleccione MENU:Centro de actualización[Activar software de sistema operativo almacenado temporalmente].

   - Escriba **UPGRADE** para confirmar que desea transferir y activar las versiones propuestas de software del sistema operativo en las matrices que seleccionó para actualizar y, a continuación, haga clic en **Actualizar**.

     El sistema transfiere el archivo de software a cada cabina de almacenamiento que seleccionó para actualizar y, luego, activa el archivo mediante un reinicio.

     Durante la operación de actualización, ocurren las siguientes acciones:

   - Como parte del proceso de actualización, se ejecuta una comprobación del estado previa a la actualización. La comprobación del estado antes de la actualización evalúa todos los componentes de la cabina de almacenamiento para garantizar que se pueda proceder con la actualización.
   - Si ocurre un error en la comprobación del estado de una cabina de almacenamiento, la actualización se detiene. Puede hacer clic en los tres puntos (…). Y seleccione **Guardar registro** para revisar los errores. También puede optar por anular el error de comprobación del estado y hacer clic en **continuar** para continuar con la actualización.
   - Puede cancelar la operación de actualización después de la comprobación del estado previa a la actualización.
10. **Opcional:** una vez completada la actualización, puede ver una lista de lo que se actualizó en una cabina de almacenamiento específica haciendo clic en los tres puntos (…) Y, a continuación, seleccione **Guardar registro**.

    El archivo se guarda en la carpeta de descargas del explorador con el nombre `upgrade_log-<date>.json`.

Active el software de sistema operativo almacenado temporalmente

Puede optar por activar el archivo de actualización inmediatamente o esperar hasta un momento más conveniente. Este procedimiento entiende que se optó por activar el archivo de software más adelante.

Acerca de esta tarea

Puede transferir los archivos del firmware sin activarlos. Puede optar por activarlos más tarde por los siguientes motivos:

- **Hora del día** — la activación del software puede llevar mucho tiempo, por lo que es posible que desee esperar hasta que las cargas de E/S sean más livianas. Las controladoras se reinician y conmutan al nodo de respaldo durante la activación, de manera que el rendimiento podría ser inferior al habitual hasta que finalice la actualización.
- **Tipo de paquete**: Es posible que desee probar el nuevo software y firmware en una matriz de almacenamiento antes de actualizar los archivos en otras matrices de almacenamiento.

No se puede detener el proceso de activación una vez iniciado.

Pasos

1. En la vista principal, seleccione **gestionar**. Si es necesario, haga clic en la columna Estado para ordenar, en la parte superior de la página, todas las cabinas de almacenamiento con el estado "actualización del sistema operativo (esperando la activación)".
2. Seleccione una o varias cabinas de almacenamiento para las cuales desee activar el software y, a continuación, seleccione MENU:Centro de actualización[Activar software de sistema operativo almacenado temporalmente].

   Durante la operación de actualización, ocurren las siguientes acciones:

   - Como parte del proceso de activación, se ejecuta una comprobación del estado previa a la actualización. La comprobación del estado antes de la actualización evalúa todos los componentes de la cabina de almacenamiento para garantizar que se pueda proceder con la activación.
   - Si ocurre un error en la comprobación del estado de una cabina de almacenamiento, la activación se detiene. Puede hacer clic en los tres puntos (…). Y seleccione **Guardar registro** para revisar los errores. También puede optar por anular el error en la comprobación del estado y hacer clic en **continuar** para continuar con la activación.
   - Puede cancelar la operación de activación después de la comprobación del estado previa a la actualización. Cuando la comprobación del estado previa a la actualización se realiza correctamente, se produce la activación. El tiempo que requiere la activación depende de la configuración de la cabina de almacenamiento y los componentes que se van a activar.
3. **Opcional:** una vez completada la activación, puede ver una lista de lo que se activó para una matriz de almacenamiento específica haciendo clic en los tres puntos (…) Y, a continuación, seleccione **Guardar registro**.

   El archivo se guarda en la carpeta de descargas del explorador con el nombre `activate_log-<date>.json`.

Gestionar el repositorio de software

En el repositorio de software, figuran todos los archivos de software relacionados con el proxy de servicios web.

Si no puede ver el archivo que desea utilizar, puede utilizar la opción gestionar repositorio de software para importar uno o más archivos de sistema operativo SANtricity al sistema host donde se ejecutan el proxy de servicios web y Unified Manager. También puede optar por eliminar uno o varios de los archivos de sistema operativo SANtricity que están disponibles en el repositorio de software.

Antes de empezar

Si añade archivos de sistema operativo SANtricity, asegúrese de que estén disponibles en el sistema local.

Pasos

1. En la vista principal, seleccione **gestionar** y, a continuación, elija MENU:Centro de actualización[gestionar el repositorio de software].

   Se muestra el cuadro de diálogo gestionar el repositorio de software.

2. Realice una de las siguientes acciones:

Opción	Haga esto
Importar	a. Haga clic en **Importar.** b. Haga clic en **examinar** y, a continuación, desplácese hasta la ubicación en la que residen los archivos del sistema operativo que desea agregar. Los archivos de sistema operativo tienen un nombre similar a `N2800-830000-000.dlp`. c. Seleccione uno o más archivos de sistema operativo que desee agregar y, a continuación, haga clic en **Importar**.
Eliminar	a. Seleccione uno o varios archivos de sistema operativo que desee quitar del repositorio de software. b. Haga clic en **Eliminar**.

Resultados

Si seleccionó Importar, los archivos se cargan y se validan. Si seleccionó Eliminar, los archivos se quitan del repositorio de software.

Borre el software de sistema operativo almacenado temporalmente

Puede quitar el software de sistema operativo almacenado temporalmente para garantizar que no se active una versión pendiente de manera accidental más adelante. La eliminación del software de sistema operativo almacenado temporalmente no afecta la versión actual que está en ejecución en las cabinas de almacenamiento.

Pasos

1. En la vista principal, seleccione **gestionar** y, a continuación, elija menú:Centro de actualización[Borrar software de sistema operativo almacenado temporalmente].

   Se abre el cuadro de diálogo Borrar software de sistema operativo almacenado temporalmente, donde se enumeran todos los sistemas de almacenamiento detectados con software o NVSRAM pendiente.

2. Si es necesario, puede filtrar u ordenar los sistemas de almacenamiento de la lista, de modo que pueda ver todos los sistemas que tienen software almacenado temporalmente.
3. Marque las casillas de comprobación de los sistemas de almacenamiento con software pendiente que desea borrar.
4. Haga clic en **Borrar**.

   El estado de la operación se muestra en el cuadro de diálogo.

Mirroring

Información general de mirroring

Utilice las funciones de mirroring para replicar datos entre una cabina de almacenamiento local y una cabina de almacenamiento remota, ya sea de forma asíncrona o síncrona.

> El mirroring síncrono no está disponible en los sistemas de almacenamiento EF600 o EF300.

¿Qué es el mirroring?

Las aplicaciones de SANtricity incluyen dos tipos de mirroring: Asíncrono y síncrono. El mirroring asíncrono copia los volúmenes de datos bajo demanda o por programación, lo que minimiza o evita el tiempo de inactividad que se puede producir por pérdidas o daños en los datos. El mirroring síncrono replica los volúmenes de datos en tiempo real para garantizar la disponibilidad continua.

Obtenga más información:

- "Cómo funciona el mirroring"
- "Terminología de mirroring"

¿Cómo se configura el mirroring?

El mirroring síncrono o asíncrono se debe configurar en Unified Manager y, posteriormente, se debe utilizar System Manager para gestionar las sincronizaciones.

Obtenga más información:

- "Flujo de trabajo de configuración de mirroring"
- "Requisitos para usar el mirroring"
- "Cree una pareja reflejada asíncrona"
- "Cree una pareja reflejada síncrona"

Conceptos

Cómo funciona el mirroring

Unified Manager incluye opciones de configuración para las funciones de mirroring de SANtricity, con las cuales los administradores pueden replicar datos entre dos cabinas de almacenamiento para la protección de los datos.

> El mirroring síncrono no está disponible en los sistemas de almacenamiento EF600 o EF300.

Tipos de mirroring

Las aplicaciones de SANtricity incluyen dos tipos de mirroring: Asíncrono y síncrono.

El mirroring asíncrono copia los volúmenes de datos bajo demanda o por programación, lo que minimiza o

evita el tiempo de inactividad que se puede producir por pérdidas o daños en los datos. El mirroring asíncrono captura el estado de un volumen primario en un momento específico y copia solo los datos que han cambiado desde la última captura de imagen. El sitio primario se puede actualizar de inmediato y el sitio secundario se puede actualizar según lo permita el ancho de banda. La información se guarda en la caché y se envía más tarde, a medida que los recursos de red se vuelven disponibles. Este tipo de mirroring es ideal para los procesos periódicos como el backup y el archivado.

El mirroring síncrono replica los volúmenes de datos en tiempo real para garantizar la disponibilidad continua. El propósito es lograr un objetivo de punto de recuperación (RPO) de cero datos perdidos mediante la copia de datos importantes disponibles en caso de que se produzca un desastre en una de las dos cabinas de almacenamiento. La copia es idéntica a los datos de producción en cada momento, ya que cada vez que se realiza una escritura en el volumen primario, se realiza una escritura en el volumen secundario. El host no recibe la confirmación de que la escritura se realizó correctamente hasta que el volumen secundario se actualiza con los cambios realizados en el volumen primario. Este tipo de mirroring es ideal para fines de continuidad del negocio como la recuperación ante desastres.

Diferencias entre los tipos de mirroring

En la siguiente tabla, se describen las principales diferencias entre los dos tipos de mirroring.

Atributo	Asíncrona	Síncrona
Método de replicación	Momento específico: El mirroring se ejecuta bajo demanda o automáticamente de acuerdo con una programación definida por el usuario.	Continuo: El mirroring se ejecuta automáticamente de forma continua; se copian datos en cada escritura del host.
Distancia	Admite largas distancias entre las cabinas. Generalmente, solo las funcionalidades de la red y la tecnología de extensión de canal limitan la distancia.	Limitado a distancias menores entre las cabinas. Generalmente, la distancia debe ser inferior o igual a 10 km (6.2 millas) con respecto a la cabina de almacenamiento local para satisfacer los requisitos de latencia y rendimiento de la aplicación.
Método de comunicación	Una red Fibre Channel o IP estándar.	Solo red Fibre Channel.
Tipos de volúmenes	Estándares o finos.	Solo estándares.

Flujo de trabajo de configuración de mirroring

El mirroring síncrono o asíncrono se debe configurar en Unified Manager y, posteriormente, se debe utilizar System Manager para gestionar las sincronizaciones.

Flujo de trabajo de mirroring asíncrono

El mirroring asíncrono conlleva el siguiente flujo de trabajo:

1. Realice la configuración inicial en Unified Manager:

a. Seleccione la cabina de almacenamiento local como el origen de la transferencia de datos.
b. Cree un grupo de coherencia de reflejos o seleccione uno existente que funcione como contenedor para el volumen primario de la cabina local y el volumen secundario de la cabina remota. Los volúmenes primario y secundario se conocen como la "pareja reflejada". Si es la primera vez que crea el grupo de coherencia de reflejos, debe especificar si desea ejecutar sincronizaciones manuales o programadas.
c. Seleccione un volumen primario de la cabina de almacenamiento local y determine su capacidad reservada. La capacidad reservada es la capacidad física asignada que se utilizará para la operación de copia.
d. Seleccione una cabina de almacenamiento remota como el destino de la transferencia y un volumen secundario y, a continuación, determine su capacidad reservada.
e. Inicie la transferencia de datos inicial desde el volumen primario hacia el volumen secundario. Según el tamaño de los volúmenes, esta transferencia inicial puede tardar varias horas.

2. Compruebe el progreso de la sincronización inicial:
   a. En Unified Manager, inicie la instancia de System Manager para la cabina local.
   b. En System Manager, consulte el estado de la operación de mirroring. Cuando se complete el mirroring, el estado de la pareja reflejada será "óptimo".
3. De manera opcional, puede reprogramar o realizar manualmente transferencias de datos subsiguientes en System Manager. Solo se transferirán los bloques nuevos y cambiados del volumen primario al volumen secundario.

> Como la replicación asíncrona es periódica, el sistema puede consolidar los bloques cambiados y ahorrar ancho de banda de red. El impacto sobre el rendimiento de escritura y la latencia de escritura es mínimo.

Flujo de trabajo de mirroring síncrono

El mirroring síncrono conlleva el siguiente flujo de trabajo:

1. Realice la configuración inicial en Unified Manager:
   a. Seleccione una cabina de almacenamiento local como el origen de la transferencia de datos.
   b. Seleccione un volumen primario de la cabina de almacenamiento local.
   c. Seleccione una cabina de almacenamiento remota como el destino de la transferencia de datos y, a continuación, seleccione un volumen secundario.
   d. Seleccione las prioridades de sincronización y resincronización.
   e. Inicie la transferencia de datos inicial desde el volumen primario hacia el volumen secundario. Según el tamaño de los volúmenes, esta transferencia inicial puede tardar varias horas.
2. Compruebe el progreso de la sincronización inicial:
   a. En Unified Manager, inicie la instancia de System Manager para la cabina local.
   b. En System Manager, consulte el estado de la operación de mirroring. Cuando se complete el mirroring, el estado de la pareja reflejada será "óptimo". Las dos cabinas intentarán mantener la sincronización a través de las operaciones normales. Solo se transferirán los bloques nuevos y cambiados del volumen primario al volumen secundario.
3. De manera opcional, puede cambiar la configuración de sincronización en System Manager.

Como la replicación síncrona es continua, el enlace de replicación entre los dos sitios debe proporcionar funcionalidades de ancho de banda suficientes.

Terminología de mirroring

Conozca la forma en que los términos de mirroring se aplican a su cabina de almacenamiento.

Duración	Descripción
Cabina de almacenamiento local	La cabina de almacenamiento local es aquella sobre la que se actúa en el momento.
Grupo de coherencia de reflejos	Un grupo de coherencia de reflejos es un contenedor para una o más parejas reflejadas. Para las operaciones de mirroring asíncrono, se debe crear un grupo de coherencia de reflejos. Todas las parejas reflejadas de un grupo se resincronizan de forma simultánea para mantener un punto de recuperación consistente. El mirroring síncrono no utiliza grupo de coherencia de reflejos.
Pareja reflejada	Una pareja reflejada comprende dos volúmenes: Un volumen primario y uno secundario. En el mirroring asíncrono, una pareja reflejada siempre pertenece a un grupo de coherencia de reflejos. Primero, se realizan las operaciones de escritura en el volumen primario y, luego, se replican en el secundario. Cada pareja reflejada de un grupo de coherencia de reflejos comparte la misma configuración de sincronización.
Volumen primario	El volumen primario de una pareja reflejada es el volumen de origen que se reflejará.
Cabina de almacenamiento remota	La cabina de almacenamiento remota se designa normalmente como el sitio secundario, que normalmente contiene una réplica de los datos en una configuración de mirroring.
Capacidad reservada	La capacidad reservada es la capacidad física asignada que se usa para cualquier operación de servicio de copia y objeto de almacenamiento. El host no puede leerla directamente. Se requieren estos volúmenes para que la controladora pueda guardar de forma persistente la información necesaria para mantener el mirroring en un estado operativo. Los volúmenes contienen información como registros delta y datos de copia en escritura.
Volumen secundario	El volumen secundario de una pareja reflejada está normalmente ubicado en un sitio secundario y contiene una réplica de los datos.

Duración	Descripción
Sincronización	La sincronización se produce en la sincronización inicial entre la cabina de almacenamiento local y la cabina de almacenamiento remota. La sincronización también se produce cuando los volúmenes primario y secundario dejan de estar sincronizados después de una interrupción de comunicación. Cuando el enlace de comunicación se restablece, todos los datos sin replicar se sincronizan con la cabina de almacenamiento del volumen secundario.

Requisitos para usar el mirroring

Si planea configurar el mirroring, tenga en cuenta los siguientes requisitos.

Unified Manager

- El proxy de servicios web se encuentra en ejecución.
- Unified Manager se ejecuta en el host local a través de una conexión HTTPS.
- SANtricity Unified Manager debe mostrar los certificados SSL válidos para la cabina de almacenamiento. Es posible aceptar un certificado autofirmado o instalar una certificación de seguridad propia con Unified Manager. Para hacerlo, debe navegar hasta MENU:Certificate[Gestión de certificados].

Cabinas de almacenamiento

El mirroring síncrono no está disponible en las cabinas de almacenamiento EF600 o EF300.

- Debe tener dos cabinas de almacenamiento.
- Cada cabina de almacenamiento debe tener dos controladoras.
- Las dos cabinas de almacenamiento se encuentran detectadas en Unified Manager.
- Cada controladora en la cabina primaria y la cabina secundaria debe tener un puerto Ethernet de gestión configurado y debe estar conectada a la red.
- Las cabinas de almacenamiento deben tener la versión de firmware 7.84 como mínimo. (Cada una puede ejecutar versiones de sistema operativo diferentes).
- Debe conocer la contraseña de las cabinas de almacenamiento remota y local.
- Debe tener suficiente capacidad libre en la cabina de almacenamiento remota para crear un volumen secundario mayor o igual que el volumen primario que desea reflejar.
- El mirroring asíncrono se admite en controladoras con puertos de host Fibre Channel (FC) o iSCSI, mientras que el mirroring síncrono solo se admite en controladoras con puertos de host FC.

Requisitos de conectividad

El mirroring (asíncrono o síncrono) a través de una interfaz de FC requiere lo siguiente:

- Cada controladora de la cabina de almacenamiento dedica su puerto de host FC numerado más alto a las operaciones de mirroring.
- Si la controladora tiene tanto puertos base FC como puertos FC de tarjeta de interfaz del host (HIC), en la HIC se encuentra el puerto numerado más alto. Se cerrará la sesión de cualquier host que haya iniciado sesión en el puerto dedicado y no se aceptará ninguna solicitud de inicio de sesión de host. Solo se aceptan las solicitudes I/o en este puerto de las controladoras que participan en las operaciones de

mirroring.

- Los puertos de mirroring dedicados deben pertenecer al entorno estructural de FC que sea compatible con el servicio de directorio y las interfaces del servicio de nombres. En particular, FC-AL y punto a punto no son opciones de conectividad compatibles entre las controladoras que participan en las relaciones de mirroring.

El mirroring (solo asíncrono) a través de una interfaz iSCSI requiere lo siguiente:

- A diferencia de FC, iSCSI no requiere un puerto dedicado. Cuando se utiliza el mirroring asíncrono en entornos iSCSI, no es necesario dedicar ninguno de los puertos iSCSI front-end de la cabina de almacenamiento para usarlos con mirroring asíncrono; esos puertos se comparten tanto para las conexiones de tráfico de reflejos asíncronos como de I/o de host a cabina.
- La controladora conserva una lista de los sistemas de almacenamiento remoto con los cuales el iniciador de iSCSI intenta establecer una sesión. El primer puerto que logra establecer una conexión iSCSI se utiliza para todas las comunicaciones subsiguientes con esa cabina de almacenamiento remota. Si no se produce la comunicación, se intenta una nueva sesión con todos los puertos disponibles.
- Los puertos iSCSI se configuran en el nivel de la cabina, puerto por puerto. La comunicación entre controladoras para la mensajería de configuración y la transferencia de datos utiliza la configuración global, lo que incluye:
  - VLAN: Tanto los sistemas locales como los remotos deben tener el mismo valor de VLAN para comunicarse
  - Puertos de escucha iSCSI
  - Tramas gigantes
  - Prioridad para Ethernet

> La comunicación entre las controladoras iSCSI debe utilizar un puerto con conexión a un host y no el puerto Ethernet de gestión.

Candidatos de volumen reflejado

- El nivel de RAID, los parámetros de almacenamiento en caché y el tamaño de los segmentos pueden ser diferentes en los volúmenes primario y secundario de una pareja reflejada.

> Para las controladoras EF600 y EF300, los volúmenes primario y secundario de una pareja reflejada asíncrona deben coincidir con el mismo protocolo, nivel de soporte, tamaño de segmento, tipo de seguridad y nivel de RAID. Las parejas reflejadas asíncronas no elegibles no aparecerán en la lista de volúmenes disponibles.

- El volumen secundario deber tener al menos el tamaño del volumen primario.
- Un volumen puede participar solo en una relación de reflejo.
- Para una pareja reflejada síncrona, los volúmenes primario y secundario deben ser volúmenes estándar. No pueden ser volúmenes finos o Snapshot.
- Para el mirroring síncrono, existen límites sobre la cantidad de volúmenes que se admiten en una cabina de almacenamiento determinada. Asegúrese de que la cantidad de volúmenes configurados en la cabina de almacenamiento sea menor que el límite admitido. Cuando se activa el mirroring síncrono, los dos volúmenes de capacidad reservada creados se cuentan para el límite de volúmenes.
- Para el mirroring asíncrono, el volumen primario y el volumen secundario deben tener las mismas capacidades Drive Security.

- Si el volumen primario es compatible con FIPS, el volumen secundario debe ser compatible con FIPS.
- Si el volumen primario es compatible con FDE, el volumen secundario debe ser compatible con FDE.
- Si el volumen primario no utiliza Drive Security, el volumen secundario no debe usar Drive Security.

Capacidad reservada

Mirroring asíncrono:

- Se requiere un volumen de capacidad reservada en el volumen primario y en el volumen secundario de una pareja reflejada para registrar la información de escritura que se utiliza en la recuperación de los restablecimientos de la controladora y otras interrupciones temporales.
- Debido a que tanto el volumen primario como el volumen secundario de una pareja reflejada requieren capacidad reservada adicional, debe asegurarse de contar con capacidad libre disponible en ambas cabinas de almacenamiento de la relación de reflejo.

Mirroring síncrono:

- Se requiere capacidad reservada en el volumen primario y en el volumen secundario para registrar la información de escritura que se utiliza en la recuperación de los restablecimientos de la controladora y otras interrupciones temporales.
- Los volúmenes de capacidad reservada se crean automáticamente cuando se activa el mirroring síncrono. Debido a que tanto el volumen primario como el volumen secundario de una pareja reflejada requieren capacidad reservada, debe asegurarse de contar con capacidad libre suficiente en ambas cabinas de almacenamiento que participan en la relación de reflejo síncrono.

Función Drive Security

- Si utiliza unidades compatibles con la función de seguridad, tanto el volumen primario como el secundario deben tener una configuración de seguridad compatible. Esta restricción no se aplica; por lo tanto, debe verificarlo por su cuenta.
- Si utiliza unidades compatibles con la función de seguridad, tanto el volumen primario como el secundario deberían usar el mismo tipo de unidad. Esta restricción no se aplica; por lo tanto, debe verificarlo por su cuenta.
- Si utiliza Data Assurance (DA), el volumen primario y el secundario deben tener la misma configuración DE DA.

Configurar el mirroring

Cree una pareja reflejada asíncrona

Para configurar el mirroring asíncrono, debe crear una pareja reflejada que incluya un volumen primario en la cabina local y un volumen secundario en la cabina remota.

Antes de empezar

Antes de crear una pareja reflejada, debe cumplir con los requisitos para Unified Manager:

- El proxy de servicios web se encuentra en ejecución.
- Unified Manager se ejecuta en el host local a través de una conexión HTTPS.
- SANtricity Unified Manager debe mostrar los certificados SSL válidos para la cabina de almacenamiento. Es posible aceptar un certificado autofirmado o instalar una certificación de seguridad propia con Unified

Manager. Para hacerlo, debe navegar hasta MENU:Certificate[Gestión de certificados].

También debe cumplir con los siguientes requisitos para las cabinas de almacenamiento y los volúmenes:

- Cada cabina de almacenamiento debe tener dos controladoras.
- Las dos cabinas de almacenamiento se encuentran detectadas en Unified Manager.
- Cada controladora en la cabina primaria y la cabina secundaria debe tener un puerto Ethernet de gestión configurado y debe estar conectada a la red.
- Las cabinas de almacenamiento deben tener la versión de firmware 7.84 como mínimo. (Cada una puede ejecutar versiones de sistema operativo diferentes).
- Debe conocer la contraseña de las cabinas de almacenamiento remota y local.
- Debe tener suficiente capacidad libre en la cabina de almacenamiento remota para crear un volumen secundario mayor o igual que el volumen primario que desea reflejar.
- Las cabinas de almacenamiento local y remota se encuentran conectadas a través de una estructura Fibre Channel o una interfaz iSCSI.
- Creó el volumen primario y el volumen secundario que desea usar en la relación de reflejo asíncrono.
- El volumen secundario deber tener al menos el tamaño del volumen primario.

Acerca de esta tarea

El proceso para crear una pareja reflejada asíncrona es un procedimiento de varios pasos.

Paso 1: Cree o seleccione un grupo de coherencia de reflejos

En este paso, debe crear un grupo de coherencia de reflejos nuevo o seleccionar uno existente. Un grupo de coherencia de reflejos es un contenedor para los volúmenes primario y secundario (la pareja reflejada), y especifica el método de resincronización deseado (manual o automático) para todas las parejas del grupo.

Pasos

1. En la página **gestionar**, seleccione la matriz de almacenamiento local que desea utilizar para el origen.
2. Seleccione **acciones › Crear pareja reflejada asíncrona**.

   Se abrirá el asistente Crear pareja reflejada asíncrona.

3. Seleccione un grupo de coherencia de reflejos existente o cree uno nuevo.

   Para seleccionar un grupo existente, asegúrese de que **un grupo de consistencia de mirroring** existente está seleccionado y, a continuación, seleccione el grupo de la tabla. Un grupo de coherencia puede incluir varias parejas reflejadas.

   Para crear un grupo nuevo, realice lo siguiente:

   a. Seleccione **Un nuevo grupo de coherencia de reflejos** y, a continuación, haga clic en **Siguiente**.
   b. Introduzca un nombre único que describa mejor los datos de los volúmenes que se reflejarán entre las dos cabinas de almacenamiento. Un nombre sólo puede contener letras, números y los caracteres especiales de subrayado (_), guión (-) y el signo de hash (#). Un nombre no puede superar los 30 caracteres y no puede contener espacios.
   c. Seleccione la cabina de almacenamiento remota en la que desea establecer una relación de reflejo con la cabina de almacenamiento local.

> Si la cabina de almacenamiento remota está protegida con contraseña, el sistema solicita la contraseña.

d. Elija si desea sincronizar las parejas reflejadas de forma manual o automática:
   - **Manual** — Seleccione esta opción para iniciar manualmente la sincronización de todas las parejas reflejadas dentro de este grupo. Tenga en cuenta que, cuando desee realizar una resincronización más tarde, deberá iniciar System Manager para la cabina de almacenamiento primaria y, a continuación, deberá ir al menú:almacenamiento[Mirroring asíncrono], seleccionar el grupo en la pestaña **grupos de coherencia de reflejos** y seleccionar MENU:más[Resincronizar manualmente].
   - **Automático** — Seleccione el intervalo deseado en **minutos**, **horas** o **días**, desde el comienzo de la actualización anterior hasta el comienzo de la siguiente. Por ejemplo, si se establece el intervalo de sincronización en 30 minutos y el proceso de sincronización comienza a las 4:00 p. m., el siguiente proceso comenzará a las 4:30 p. m.

e. Seleccione las opciones de alerta deseadas:
   - Para las sincronizaciones manuales, especifique el umbral (que se define según el porcentaje de capacidad restante) cuando desea recibir alertas.
   - Para las sincronizaciones automáticas, puede establecer tres métodos de alerta: cuando la sincronización no se completa en un lapso específico, cuando los datos del punto de recuperación en la cabina remota son más antiguos que un límite de tiempo específico y cuando la capacidad reservada está cerca de un umbral específico (definido por el porcentaje de capacidad restante).

4. Seleccione **Siguiente** y vaya a. Paso 2: Seleccione el volumen primario.

   Si definió un grupo de coherencia de reflejos nuevo, Unified Manager crea el grupo de coherencia de reflejos en la cabina de almacenamiento local primero y, a continuación, crea el grupo de coherencia de reflejos en la cabina de almacenamiento remota. Para ver y gestionar el grupo de coherencia de reflejos, inicie la instancia de System Manager de cada cabina.

> Si Unified Manager crea correctamente el grupo de coherencia de reflejos en la cabina de almacenamiento local, pero no logra crearlo en la cabina de almacenamiento remota, elimina automáticamente el grupo de coherencia de reflejos de la cabina de almacenamiento local. Si se produce un error mientras Unified Manager intenta eliminar el grupo de coherencia de reflejos, es necesario eliminarlo en forma manual.

Paso 2: Seleccione el volumen primario

En este paso, se selecciona el volumen primario que se usará en la relación de reflejo y se asigna la capacidad reservada. Si selecciona un volumen primario en la cabina de almacenamiento local, el sistema muestra una lista de todos los volúmenes elegibles para esa pareja reflejada. Si algún volumen no es apto para el uso, no se muestra en esa lista.

Todos los volúmenes que añada al grupo de coherencia de reflejos de la cabina de almacenamiento local tendrán el rol primario en la relación de reflejo.

Pasos

1. En la lista de volúmenes elegibles, seleccione el volumen que desea usar como el volumen primario y haga clic en **Siguiente** para asignar la capacidad reservada.
2. En la lista de candidatos elegibles, seleccione la capacidad reservada para el volumen primario.

   Tenga en cuenta las siguientes directrices:

- La configuración predeterminada para la capacidad reservada es del 20 % del volumen base y, por lo general, esta capacidad es suficiente. Si cambia el porcentaje, haga clic en **Actualizar candidatos**.
- La capacidad necesaria varía, según la frecuencia y el tamaño de las escrituras de I/o en el volumen primario y el tiempo que se requiere conservar la capacidad.
- En general, elija una capacidad mayor para la capacidad reservada si se presentan una o ambas de estas condiciones:
  - Se pretende conservar la pareja reflejada por un periodo prolongado.
  - Un gran porcentaje de bloques de datos cambiará en el volumen primario debido a una gran actividad de I/O. Utilice datos históricos de rendimiento u otra utilidad del sistema operativo para determinar la actividad de I/o típica del volumen primario.

3. Seleccione **Siguiente** y vaya a. Paso 3: Seleccione el volumen secundario.

Paso 3: Seleccione el volumen secundario

En este paso, se selecciona el volumen secundario que se usará en la relación de reflejo y se asigna la capacidad reservada. Si selecciona un volumen secundario en la cabina de almacenamiento remota, el sistema muestra una lista de todos los volúmenes aptos para esa pareja reflejada. Si algún volumen no es apto para el uso, no se muestra en esa lista.

Todos los volúmenes que añada al grupo de coherencia de reflejos de la cabina de almacenamiento remota tendrán el rol secundario en la relación de reflejo.

Pasos

1. En la lista de volúmenes elegibles, seleccione el volumen que desea usar como el volumen secundario en la pareja reflejada y haga clic en **Siguiente** para asignar la capacidad reservada.
2. En la lista de candidatos elegibles, seleccione la capacidad reservada para el volumen secundario.

   Tenga en cuenta las siguientes directrices:

   - La configuración predeterminada para la capacidad reservada es del 20 % del volumen base y, por lo general, esta capacidad es suficiente. Si cambia el porcentaje, haga clic en **Actualizar candidatos**.
   - La capacidad necesaria varía, según la frecuencia y el tamaño de las escrituras de I/o en el volumen primario y el tiempo que se requiere conservar la capacidad.
   - En general, elija una capacidad mayor para la capacidad reservada si se presentan una o ambas de estas condiciones:
     - Se pretende conservar la pareja reflejada por un periodo prolongado.
     - Un gran porcentaje de bloques de datos cambiará en el volumen primario debido a una gran actividad de I/O. Utilice datos históricos de rendimiento u otra utilidad del sistema operativo para determinar la actividad de I/o típica del volumen primario.
3. Seleccione **Finalizar** para completar la secuencia de duplicación asíncrona.

Resultados

Unified Manager realiza las siguientes acciones:

- Comienza la sincronización inicial entre la cabina de almacenamiento local y la remota.
- Crea la capacidad reservada para la pareja reflejada en la cabina de almacenamiento local y la remota.

Si el volumen que se está reflejando es fino, solo los bloques de aprovisionamiento (capacidad asignada en lugar de capacidad notificada) se transfieren al volumen secundario durante la sincronización inicial. Esto reduce la cantidad de datos que se deben transferir para completar la sincronización inicial.

Cree una pareja reflejada síncrona

Para configurar el mirroring síncrono, debe crear una pareja reflejada que incluya un volumen primario en la cabina local y un volumen secundario en la cabina remota.

Esta función no está disponible en los sistemas de almacenamiento EF600 o EF300.

Antes de empezar

Antes de crear una pareja reflejada, debe cumplir con los requisitos para Unified Manager:

- El proxy de servicios web se encuentra en ejecución.
- Unified Manager se ejecuta en el host local a través de una conexión HTTPS.
- SANtricity Unified Manager debe mostrar los certificados SSL válidos para la cabina de almacenamiento. Es posible aceptar un certificado autofirmado o instalar una certificación de seguridad propia con Unified Manager. Para hacerlo, debe navegar hasta MENU:Certificate[Gestión de certificados].

También debe cumplir con los siguientes requisitos para las cabinas de almacenamiento y los volúmenes:

- Las dos cabinas de almacenamiento que planea usar para el mirroring se detectaron en Unified Manager.
- Cada cabina de almacenamiento debe tener dos controladoras.
- Cada controladora en la cabina primaria y la cabina secundaria debe tener un puerto Ethernet de gestión configurado y debe estar conectada a la red.
- Las cabinas de almacenamiento deben tener la versión de firmware 7.84 como mínimo. (Cada una puede ejecutar versiones de sistema operativo diferentes).
- Debe conocer la contraseña de las cabinas de almacenamiento remota y local.
- Las cabinas de almacenamiento local y remota se encuentran conectadas a través de una estructura Fibre Channel.
- Creó el volumen primario y el volumen secundario que desea usar en la relación de reflejo síncrono.
- El volumen primario deber ser un volumen estándar. No puede ser un volumen fino ni un volumen Snapshot.
- El volumen secundario deber ser un volumen estándar. No puede ser un volumen fino ni un volumen Snapshot.
- El volumen secundario deber tener al menos el mismo tamaño que el volumen primario.

Acerca de esta tarea

El proceso para crear parejas reflejadas síncronas es un procedimiento de varios pasos.

Paso 1: Seleccione el volumen primario

En este paso, se selecciona el volumen primario que se usará en la relación de reflejo síncrono. Si selecciona un volumen primario en la cabina de almacenamiento local, el sistema muestra una lista de todos los volúmenes elegibles para esa pareja reflejada. Si algún volumen no es apto para el uso, no se muestra en esa lista. El volumen que seleccione tendrá el rol primario en la relación de reflejo.

Pasos

1. En la página **gestionar**, seleccione la matriz de almacenamiento local que desea utilizar para el origen.
2. Seleccione **acciones › Crear pareja reflejada síncrona**.

   Se abrirá el asistente Crear pareja reflejada síncrona.

3. En la lista de volúmenes elegibles, seleccione el volumen que desea usar como el volumen primario en el reflejo.
4. Seleccione **Siguiente** y vaya a. Paso 2: Seleccione el volumen secundario.

Paso 2: Seleccione el volumen secundario

En este paso, seleccione el volumen secundario que desea usar en la relación de reflejo. Si selecciona un volumen secundario en la cabina de almacenamiento remota, el sistema muestra una lista de todos los volúmenes aptos para esa pareja reflejada. Si algún volumen no es apto para el uso, no se muestra en esa lista. El volumen que seleccione tendrá el rol secundario en la relación de reflejo.

Pasos

1. Seleccione la cabina de almacenamiento remota en la que desea establecer una relación de reflejo con la cabina de almacenamiento local.

   > Si la cabina de almacenamiento remota está protegida con contraseña, el sistema solicita la contraseña.

   - Las cabinas de almacenamiento se enumeran en una lista por nombre. Si no asignó ningún nombre a una cabina de almacenamiento, esta se muestra en la lista como "unnamed".
   - Si la cabina de almacenamiento que desea utilizar no aparece en la lista, asegúrese de que se haya detectado en Unified Manager.
2. En la lista de volúmenes elegibles, seleccione el volumen que desea usar como el volumen secundario en el reflejo.

   > Si se eligió un volumen secundario con una capacidad mayor a la del volumen primario, la capacidad utilizable se restringe al tamaño del volumen primario.

3. Haga clic en **Siguiente** y vaya a. Paso 3: Seleccione la configuración de sincronización.

Paso 3: Seleccione la configuración de sincronización

En este paso, se seleccionan las opciones de configuración que determinan la forma en que se deben sincronizar los datos después de una interrupción de comunicación. Es posible establecer la prioridad que tendrá en cuenta el propietario de la controladora del volumen primario para resincronizar los datos con el volumen secundario después de una interrupción de comunicación. Además, es necesario seleccionar la política de resincronización: Manual o automática.

Pasos

1. Use la barra de desplazamiento para configurar la prioridad de sincronización.

   La prioridad de sincronización determina cuántos recursos del sistema se usan para completar la sincronización inicial y la operación de resincronización después de una interrupción de la comunicación en comparación con las solicitudes de I/o del servicio.

La prioridad que se configure en este cuadro de diálogo se aplicará tanto al volumen primario, como al secundario. Para modificar la tasa del volumen primario en otro momento, deberá ir a System Manager y seleccionar MENU:almacenamiento[Mirroring síncrono > más > Editar configuración].

Las tasas de prioridad de sincronización son las siguientes cinco:

- El más bajo
- Bajo
- Mediano
- Alto
- Máxima

  Si la prioridad de sincronización se configuró con la tasa mínima, se prioriza la actividad de I/o y la operación de resincronización lleva más tiempo. Si la prioridad de sincronización se configuró con la tasa máxima, la operación de resincronización tiene prioridad, pero podría afectar a la actividad de I/o de la cabina de almacenamiento.

2. Elija si desea volver a sincronizar las parejas reflejadas de la cabina de almacenamiento remota en forma manual o automática.
   - **Manual** (la opción recomendada) — Seleccione esta opción para requerir que la sincronización se reanude manualmente después de restaurar la comunicación a una pareja reflejada. Esta opción proporciona la mejor oportunidad para recuperar datos.
   - **Automático** — Seleccione esta opción para iniciar la resincronización automáticamente después de restaurar la comunicación a un par reflejado.

     Para reanudar la sincronización manualmente, vaya a System Manager y seleccione MENU:Storage[Synchronous Mirroring], resalte la pareja reflejada en la tabla y seleccione **Reanudar** en **más**.

3. Haga clic en **Finalizar** para completar la secuencia de duplicación sincrónica.

Resultados

Una vez que se activa el mirroring, el sistema ejecuta las siguientes acciones:

- Comienza la sincronización inicial entre la cabina de almacenamiento local y la remota.
- Configura la prioridad de sincronización y la política de resincronización.
- Reserva el puerto que tiene el número más alto de la HIC de la controladora para reflejar la transmisión de datos.

  Las solicitudes de I/o que se reciben en este puerto son aceptadas únicamente de la controladora remota preferida, propietaria del volumen secundario en la pareja reflejada. (Se permiten las reservas en el volumen primario.)

- Crea dos volúmenes de capacidad reservada, uno para cada controladora, que se utilizan para registrar información de escritura para recuperarse de reinicios de controladoras y otras interrupciones temporales.

  La capacidad de cada volumen es 128 MIB. Sin embargo, si los volúmenes se colocan en un pool, se reservarán 4 GIB para cada volumen.

Después de terminar

Vaya a System Manager y seleccione MENU:Inicio[Ver operaciones en curso] para ver el progreso de la

operación de mirroring síncrono. Es posible que esta operación demore y que afecte el rendimiento del sistema.

Preguntas frecuentes

¿Qué debo saber antes de crear un grupo de coherencia de reflejos?

Siga estas directrices para poder crear un grupo de coherencia de reflejos.

Cumpla con los siguientes requisitos para Unified Manager:

- El proxy de servicios web se encuentra en ejecución.
- Unified Manager se ejecuta en el host local a través de una conexión HTTPS.
- SANtricity Unified Manager debe mostrar los certificados SSL válidos para la cabina de almacenamiento. Es posible aceptar un certificado autofirmado o instalar una certificación de seguridad propia con Unified Manager. Para hacerlo, debe navegar hasta MENU:Certificate[Gestión de certificados].

También debe cumplir con los siguientes requisitos para las cabinas de almacenamiento:

- Las dos cabinas de almacenamiento se encuentran detectadas en Unified Manager.
- Cada cabina de almacenamiento debe tener dos controladoras.
- Cada controladora en la cabina primaria y la cabina secundaria debe tener un puerto Ethernet de gestión configurado y debe estar conectada a la red.
- Las cabinas de almacenamiento deben tener la versión de firmware 7.84 como mínimo. (Cada una puede ejecutar versiones de sistema operativo diferentes).
- Debe conocer la contraseña de las cabinas de almacenamiento remota y local.
- Las cabinas de almacenamiento local y remota se encuentran conectadas a través de una estructura Fibre Channel o una interfaz iSCSI.

> El mirroring síncrono no está disponible en los sistemas de almacenamiento EF600 o EF300.

¿Qué debo saber antes de crear una pareja reflejada?

Antes de crear una pareja reflejada, siga estas directrices.

- Debe tener dos cabinas de almacenamiento.
- Cada cabina de almacenamiento debe tener dos controladoras.
- Las dos cabinas de almacenamiento se encuentran detectadas en Unified Manager.
- Cada controladora en la cabina primaria y la cabina secundaria debe tener un puerto Ethernet de gestión configurado y debe estar conectada a la red.
- Las cabinas de almacenamiento deben tener la versión de firmware 7.84 como mínimo. (Cada una puede ejecutar versiones de sistema operativo diferentes).
- Debe conocer la contraseña de las cabinas de almacenamiento remota y local.
- Debe tener suficiente capacidad libre en la cabina de almacenamiento remota para crear un volumen secundario mayor o igual que el volumen primario que desea reflejar.
- El mirroring asíncrono se admite en controladoras con puertos de host Fibre Channel (FC) o iSCSI, mientras que el mirroring síncrono solo se admite en controladoras con puertos de host FC.

El mirroring síncrono no está disponible en los sistemas de almacenamiento EF600 o EF300.

¿Por qué debería cambiar este porcentaje?

En general, la capacidad reservada constituye el 20 % del volumen base para operaciones de mirroring asíncrono. Por lo general, esta capacidad es suficiente.

La capacidad necesaria varía, según la frecuencia y el tamaño de las escrituras de I/o en el volumen base y el periodo durante el cual se pretenda utilizar la operación de servicios de copia del objeto de almacenamiento. Por lo general, se debe seleccionar un porcentaje alto de capacidad reservada si existe una de estas condiciones, o ambas:

- Si la vida útil de la operación de servicios de copia de un objeto de almacenamiento en particular será muy prolongada.
- Si un gran porcentaje de bloques de datos cambiará en el volumen base debido a una gran actividad de I/O. Utilice los datos históricos de rendimiento u otras utilidades del sistema operativo como ayuda para determinar la actividad de I/o típica en el volumen base.

¿Por qué se muestra más de un candidato de capacidad reservada?

Si existe más de un volumen en un pool o grupo de volúmenes que cumple con el porcentaje de capacidad seleccionado para el objeto de almacenamiento, se mostrarán varios candidatos.

Para actualizar la lista de candidatos recomendados, es posible modificar el porcentaje de espacio de la unidad física que desea reservar en el volumen base para las operaciones de servicios de copia. Se mostrarán los mejores candidatos en función de su selección.

¿Por qué no se muestran todos los volúmenes?

Cuando se selecciona un volumen primario para una pareja reflejada, se muestra una lista con todos los volúmenes elegibles.

Si algún volumen no es apto para el uso, no se muestra en esa lista. Es posible que los volúmenes no sean admisibles por uno de los siguientes motivos:

- El volumen no está en estado óptimo.
- El volumen ya participa en una relación de mirroring.
- Para el mirroring síncrono, los volúmenes primario y secundario de una pareja reflejada deben ser volúmenes estándar. No pueden ser volúmenes finos o Snapshot.
- Para el mirroring asíncrono, los volúmenes finos deben tener la expansión automática habilitada.

Para las controladoras EF600 y EF300, los volúmenes primario y secundario de una pareja reflejada asíncrona deben coincidir con el mismo protocolo, nivel de soporte, tamaño de segmento, tipo de seguridad y nivel de RAID. Las parejas reflejadas asíncronas no elegibles no aparecerán en la lista de volúmenes disponibles.

¿Por qué no se muestran todos los volúmenes en la cabina de almacenamiento remota?

Cuando se selecciona un volumen secundario en la cabina de almacenamiento remota, se muestra una lista de todos los volúmenes elegibles para esa pareja reflejada.

Todos los volúmenes que no son elegibles no aparecen en esa lista. Es posible que haya volúmenes no elegibles por alguno de los siguientes motivos:

- El volumen no es estándar, por ejemplo, un volumen Snapshot.
- El volumen no está en estado óptimo.
- El volumen ya participa en una relación de mirroring.
- Para el mirroring asíncrono, los atributos de volumen fino entre el volumen primario y el volumen secundario no coinciden.
- Si utiliza Data Assurance (DA), el volumen primario y el secundario deben tener la misma configuración DE DA.
  - Si el volumen primario tiene la función DA habilitada, el volumen secundario también debe tenerla.
  - Si el volumen primario no tiene la función DA habilitada, el volumen secundario tampoco debe tenerla.
- Para el mirroring asíncrono, el volumen primario y el volumen secundario deben tener las mismas capacidades Drive Security.
  - Si el volumen primario es compatible con FIPS, el volumen secundario debe ser compatible con FIPS.
  - Si el volumen primario es compatible con FDE, el volumen secundario debe ser compatible con FDE.
  - Si el volumen primario no utiliza Drive Security, el volumen secundario no debe usar Drive Security.

¿Qué impacto tiene la prioridad de sincronización en las tasas de sincronización?

La prioridad de sincronización define la cantidad de tiempo de procesamiento que se asigna a las actividades de sincronización en relación con el rendimiento del sistema.

El propietario de la controladora del volumen primario realiza esta operación en segundo plano. Al mismo tiempo, el propietario de la controladora procesa las escrituras de I/o en el volumen primario y las escrituras remotas asociadas en el volumen secundario. Dado que la resincronización desvía los recursos de procesamiento de la controladora de la actividad de I/o, es posible que tenga un impacto en el rendimiento de la aplicación host.

Tenga en cuentas estas directrices para determinar cuánto puede demorar una prioridad de sincronización y cómo las prioridades de sincronización pueden afectar al rendimiento del sistema.

Las siguientes tasas de prioridad se encuentran disponibles:

- El más bajo
- Bajo
- Mediano
- Alto
- Máxima

La tasa de prioridad más baja es compatible con el rendimiento del sistema, pero la resincronización demora más tiempo. La tasa de prioridad más alta es compatible con la resincronización, pero el rendimiento del sistema puede verse afectado.

Estas directrices aproximan aproximadamente las diferencias entre las prioridades.

Tasa de prioridad para la sincronización completa	Tiempo transcurrido en comparación con la tasa de sincronización más alta
El más bajo	Tiempo aproximadamente 8 veces superior a la tasa de prioridad más alta
Bajo	Tiempo aproximadamente 6 veces superior a la tasa de prioridad más alta
Mediano	Tiempo aproximadamente 3,5 veces superior a la tasa de prioridad más alta
Alto	Tiempo aproximadamente 2 veces superior a la tasa de prioridad más alta

El tamaño del volumen y las cargas de la tasa de I/o del host afectan a las comparaciones de tiempo de sincronización.

¿Por qué se recomienda usar la política de sincronización manual?

Se recomienda la resincronización manual debido a que esta permite gestionar el proceso de resincronización de un modo que garantiza la mejor oportunidad para recuperar los datos.

Si utiliza una política de resincronización automática y surgen problemas de comunicación ocasionales durante la resincronización, podrían dañarse temporalmente los datos del volumen secundario. Una vez finalizada la resincronización, los datos se corrigen.

Certificados

Información general sobre certificados

La gestión de certificados permite crear solicitudes de firma de certificados (CSR), importar certificados y gestionar certificados existentes.

¿Qué son los certificados?

Certificates son archivos digitales que identifican entidades en línea, como sitios web y servidores, para comunicaciones seguras en Internet. Existen dos tipos de certificados: Un *certificado firmado* es validado por una entidad de certificación (CA) y un *certificado autofirmado* es validado por el propietario de la entidad en lugar de por un tercero.

Obtenga más información:

- "Cómo funcionan los certificados"
- "Terminología de certificados"

¿Cómo se configuran los certificados?

En Certificate Management, es posible configurar certificados para la estación de gestión donde se aloja Unified Manager e importar también certificados para las controladoras en las cabinas.

Obtenga más información:

- "Utilice certificados firmados por CA para el sistema de gestión"
- "Importar certificados para cabinas"

Conceptos

Cómo funcionan los certificados

Los certificados son archivos digitales que identifican entidades en línea, como sitios web y servidores, para poder establecer comunicaciones seguras en Internet.

Certificados firmados

Los certificados garantizan que solo se transmitan comunicaciones web en formato cifrado, de forma privada y sin alternaciones, entre el servidor especificado y el cliente. Con Unified Manager, es posible gestionar los certificados para el explorador en un sistema de gestión host y las controladoras en las cabinas de almacenamiento detectadas.

Un certificado puede estar firmado por una autoridad de confianza o puede ser autofirmado. La firma simplemente implica que alguien validó la identidad del propietario y determinó que sus dispositivos son de confianza. Las cabinas de almacenamiento se entregan con un certificado autofirmado generado automáticamente en cada controladora. Puede continuar usando el certificado autofirmado o puede obtener certificados firmados por CA para establecer conexiones más seguras entre las controladoras y los sistemas host.

> Si bien los certificados firmados por CA aumentan la protección de seguridad (por ejemplo, evitan los ataques de tipo "man in the middle"), también aplican tarifas que pueden ser costosas si la red es extensa. En cambio, los certificados autofirmados son menos seguros, pero son gratuitos. Por lo tanto, los certificados autofirmados se utilizan con mayor frecuencia para entornos de prueba internos, no en entornos de producción.

Un certificado firmado es validado por una entidad de certificación (CA), que es una organización de terceros de confianza. Los certificados firmados incluyen detalles sobre el propietario de la entidad (generalmente, un servidor o sitio web), la fecha de emisión y de vencimiento del certificado, los dominios válidos de la entidad, y una firma digital compuesta por letras y números.

Al abrir un explorador y escribir una dirección web, el sistema ejecuta un proceso de comprobación de certificados en segundo plano para determinar si el usuario se está conectando a un sitio web que incluye un certificado válido firmado por una CA. Generalmente, un sitio que está protegido con un certificado firmado incluye un icono de candado y una designación https en la dirección. Si el usuario intenta conectarse a un sitio web que no contiene un certificado firmado por CA, el explorador mostrará una advertencia para indicar que el sitio no es seguro.

La CA toma las medidas necesarias para verificar las identidades durante el proceso de solicitud. La entidad puede enviar un correo electrónico a la empresa registrada, verificar la dirección empresarial, y realizar una verificación de HTTP o DNS. Una vez completado el proceso de solicitud, la CA envía los archivos digitales para cargar en el sistema de gestión host. Normalmente, estos archivos contienen una cadena de confianza

como la siguiente:

- **Raíz** — en la parte superior de la jerarquía está el certificado raíz, que contiene una clave privada utilizada para firmar otros certificados. El certificado raíz identifica una organización de CA determinada. Si utiliza la misma CA para todos los dispositivos de red, solo necesita un certificado raíz.
- **Intermediate** — ramificándose desde la raíz son los certificados intermedios. La CA emite uno o varios certificados intermedios para actuar como intermediarios entre un certificado raíz y los certificados de servidor protegidos.
- **Servidor** — en la parte inferior de la cadena se encuentra el certificado de servidor, que identifica su entidad específica, como un sitio web u otro dispositivo. Cada controladora de una cabina de almacenamiento requiere un certificado de servidor aparte.

Certificados autofirmados

Cada controladora de la cabina de almacenamiento incluye un certificado autofirmado preinstalado. Un certificado autofirmado es similar a un certificado firmado por CA, excepto que es validado por el propietario de la entidad y no por un tercero. Al igual que un certificado firmado por CA, un certificado autofirmado contiene su propia clave privada, y también garantiza que los datos se cifren y se envíen a través de una conexión HTTPS entre un servidor y un cliente.

Los certificados autofirmados no son «'de confianza'» por parte de los navegadores. Cada vez que intente conectarse a un sitio web que solo contiene un certificado autofirmado, el explorador mostrará un mensaje de advertencia. Deberá hacer clic en un enlace del mensaje de advertencia para continuar al sitio web; al hacer eso, estará aceptando básicamente el certificado autofirmado.

Certificados para Unified Manager

La interfaz de Unified Manager se instala con el proxy de servicios web en un sistema host. Al abrir un explorador y intentar una conexión con Unified Manager, el explorador intenta verificar si el host es un origen de confianza mediante la comprobación de un certificado digital. Si el explorador no encuentra un certificado firmado por CA para el servidor, abrirá un mensaje de advertencia. Desde allí, podrá continuar al sitio web para aceptar el certificado autofirmado en esa sesión. También puede obtener certificados digitales firmados de una CA para que ya no vea el mensaje de advertencia.

Certificados para controladoras

Durante una sesión de Unified Manager, es posible que vea mensajes de seguridad adicionales al intentar acceder a una controladora que no tiene un certificado firmado por CA. En este caso, puede confiar de forma permanente en el certificado autofirmado o puede importar los certificados firmados por CA de las controladoras para que el proxy de servicios web pueda autenticar las solicitudes de cliente entrantes procedentes de estas controladoras.

Terminología de certificados

Los siguientes términos se utilizan en la gestión de certificados.

Duración	Descripción
APROX	Una entidad de certificación (CA) es una entidad de confianza que emite documentos electrónicos, denominados certificados digitales, para la seguridad de Internet. Estos certificados identifican a los propietarios de sitios web y, de esta manera, permiten conexiones seguras entre clientes y servidores.

Duración	Descripción
CSR	Una solicitud de firma de certificación (CSR) es un mensaje que envía un solicitante a una entidad de certificación (CA). La CSR valida la información que requiere la CA para emitir un certificado.
Certificado	Un certificado identifica al propietario de un sitio con el fin de brindar seguridad, para evitar que atacantes se hagan pasar por los propietarios del sitio. El certificado tiene información acerca del propietario del sitio y la identidad de la entidad de confianza que certifica (firma) esta información.
Cadena de certificados	La cadena de certificados es una jerarquía de archivos que suma una capa de seguridad a los certificados. Normalmente, la cadena incluye un certificado raíz en la parte superior de la jerarquía, uno o varios certificados intermedios y los certificados de servidor que identifican a las entidades.
Certificado intermedio	Uno o varios certificados intermedios se extienden como una rama del certificado raíz en la cadena de certificados. La CA emite uno o varios certificados intermedios para actuar como intermediarios entre un certificado raíz y los certificados de servidor protegidos.
Almacén de claves	Un almacén de claves es un repositorio en el sistema de gestión host que contiene claves privadas, junto con sus correspondientes claves públicas y certificados. Estas claves y certificados identifican a las entidades propias como, por ejemplo, las controladoras.
Certificado raíz	El certificado raíz se encuentra en la parte superior de la jerarquía de la cadena de certificados y contiene una clave privada que se utiliza para firmar otros certificados. El certificado raíz identifica una organización de CA determinada. Si utiliza la misma CA para todos los dispositivos de red, solo necesita un certificado raíz.
Certificado firmado	Un certificado que ha validado una entidad de certificación (CA). Este archivo de datos contiene una clave privada, y garantiza que los datos se envíen en formato cifrado entre un servidor y un cliente a través de una conexión HTTPS. Además, un certificado firmado incluye detalles sobre el propietario de la entidad (normalmente, un servidor o sitio web) y una firma digital compuesta por letras y números. Un certificado firmado usa una cadena de certificados y, por consiguiente, se utiliza con mayor frecuencia en los entornos de producción. También se conoce como "certificado firmado por CA" o "certificado de gestión".
Certificado autofirmado	Un certificado autofirmado es validado por el propietario de la entidad. Este archivo de datos contiene una clave privada, y garantiza que los datos se envíen en formato cifrado entre un servidor y un cliente a través de una conexión HTTPS. También incluye una firma digital compuesta por letras y números. Un certificado autofirmado no usa la misma cadena de confianza que un certificado firmado por CA y, por consiguiente, se utiliza con mayor frecuencia en los entornos de prueba. También se conoce como certificado "preinstalado".

Duración	Descripción
Certificado de servidor	El certificado de servidor se encuentra en la parte inferior de la cadena de certificados. Este certificado identifica la entidad específica del usuario, por ejemplo, un sitio web u otro dispositivo. Cada controladora de un sistema de almacenamiento requiere un certificado de servidor aparte.
Almacén de confianza	Un almacén de confianza es un repositorio que contiene certificados de terceros de confianza, por ejemplo, entidades de certificación.

Utilice certificados firmados por CA para el sistema de gestión

Es posible obtener e importar certificados firmados por CA para establecer un acceso seguro al sistema de gestión donde se aloja Unified Manager.

Antes de empezar

Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de certificación.

Acerca de esta tarea

El uso de certificados firmados por CA implica un procedimiento de tres pasos.

Paso 1: Complete un archivo CSR

Primero, se debe generar un archivo de solicitud de firma de certificación (CSR), que identifica a la organización y al sistema host donde están instalados el proxy de servicios web y Unified Manager.

> También puede generar un archivo CSR con una herramienta como OpenSSL y saltar a. Paso 2: Enviar archivo CSR.

Pasos

1. Seleccione **Gestión de certificados**.
2. En la ficha Administración, seleccione **completar CSR**.
3. Introduzca la siguiente información y, a continuación, haga clic en **Siguiente**:
   - **Organización** — el nombre completo y legal de su empresa u organización. Incluya sufijos, como Inc. O Corp
   - **Unidad organizativa (opcional)** — la división de su organización que maneja el certificado.
   - **Ciudad/localidad** — la ciudad donde se encuentra su sistema anfitrión o negocio.
   - **Estado/Región (opcional)** — el estado o región donde está ubicado el sistema o negocio anfitrión.
   - **Código ISO de país**: Código ISO (Organización Internacional de Normalización) de dos dígitos de su país, por ejemplo, US.
4. Introduzca la siguiente información sobre el sistema host donde está instalado el proxy de servicios web:
   - **Nombre común** — la dirección IP o el nombre DNS del sistema host donde está instalado Web Services Proxy. Compruebe que la dirección sea correcta; esta debe coincidir exactamente con lo que se escribe para acceder a Unified Manager en el explorador. No incluya http:// ni https://. El nombre DNS no puede comenzar con un comodín.

- **Direcciones IP alternativas** — Si el nombre común es una dirección IP, opcionalmente puede escribir cualquier dirección IP adicional o alias para el sistema host. Si va a introducir varios datos, use un formato delimitado por comas.
- **Nombres DNS alternativos** — Si el nombre común es un nombre DNS, introduzca cualquier nombre DNS adicional para el sistema host. Si va a introducir varios datos, use un formato delimitado por comas. Si no hay nombres DNS alternativos, pero especificó un nombre DNS en el primer campo, copie ese nombre aquí. El nombre DNS no puede comenzar con un comodín.

5. Asegúrese de que la información del host sea correcta. Si no lo es, los certificados que se devuelven de la CA fallarán cuando intente importarlos.
6. Haga clic en **Finalizar**.
7. Vaya a. Paso 2: Enviar archivo CSR.

Paso 2: Enviar archivo CSR

Después de crear un archivo de solicitud de firma de certificación (CSR), se lo envía a una entidad de certificación (CA) para recibir certificados de gestión firmados para el sistema donde se aloja Unified Manager y el proxy de servicios web.

> Los sistemas E-Series requieren un formato PEM (codificación ASCII Base64) para certificados firmados, que incluye los siguientes tipos de archivo: .Pem, .crt, .cer o .key.

Pasos

1. Busque el archivo CSR descargado.

   La ubicación de la carpeta de la descarga depende del explorador.

2. Envíe el archivo CSR a una CA (por ejemplo, VeriSign o DigiCert) y solicite certificados firmados en formato PEM.

   > **Después de enviar un archivo CSR a la CA, NO vuelva a generar otro archivo CSR.** cada vez que genere una CSR, el sistema creará un par de claves pública y privada. La clave pública se incluye en la CSR, mientras que la clave privada se conserva en el almacén de claves del sistema. Cuando recibe los certificados firmados e importarlos, el sistema se asegura de que las claves pública y privada sean la pareja original. Si las claves no coinciden, los certificados firmados no funcionarán y debe solicitar certificados nuevos de la CA.

3. Cuando la CA devuelva los certificados firmados, vaya a. Paso 3: Importar certificados de gestión.

Paso 3: Importar certificados de gestión

Después de recibir certificados firmados de la CA, importe los certificados al sistema host donde se instalaron la interfaz de proxy de servicios web y Unified Manager.

Antes de empezar

- Recibió certificados firmados de la CA. Estos archivos incluyen el certificado raíz, uno o varios certificados intermedios y el certificado de servidor.
- Si la CA proporcionó un archivo de certificado encadenado (por ejemplo, un archivo .p7b), debe desempaquetar el archivo encadenado en archivos individuales: El certificado raíz, el o los certificados intermedios y el certificado de servidor. Puede utilizar Windows `certmgr` Utilidad para desempaquetar los archivos (haga clic con el botón derecho y seleccione MENU:todas las tareas[Exportar]). Se recomienda la

codificación base-64. Una vez completadas las exportaciones, se mostrará un archivo CER para cada archivo de certificado de la cadena.

- Copió los archivos de certificado en el sistema host donde se ejecuta el proxy de servicios web.

Pasos

1. Seleccione **Gestión de certificados**.
2. En la ficha Administración, seleccione **Importar**.

   Se abre un cuadro de diálogo para importar los archivos de certificado.

3. Haga clic en **examinar** para seleccionar primero los archivos de certificado raíz e intermedio y, a continuación, seleccionar el certificado de servidor. Si generó la CSR desde una herramienta externa, también debe importar el archivo de claves privadas que se creó junto con la CSR.

   Se muestran los nombres de los archivos en el cuadro de diálogo.

4. Haga clic en **Importar**.

Resultados

Los archivos se cargan y validan. La información del certificado aparece en la página Gestión de certificados.

Restablezca los certificados de gestión

Es posible revertir el certificado de gestión a su estado autofirmado original de fábrica.

Antes de empezar

Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de certificación.

Acerca de esta tarea

Esta tarea elimina el certificado de gestión actual del sistema host donde están instalados el proxy de servicios web y Unified Manager. Una vez restablecido el certificado, el sistema host se revierte al uso del certificado autofirmado.

Pasos

1. Selecciona **Ajustes > Certificados**.
2. Seleccione la pestaña **Array Management** y, a continuación, seleccione **Reset**.

   Se abre el cuadro de diálogo Confirmar restablecimiento de certificado de gestión.

3. Tipo `reset` En el campo y, a continuación, haga clic en **Restablecer**.

   Una vez que se actualiza el explorador, es posible que el explorador bloquee el acceso al sitio de destino e informe de que el sitio utiliza HTTP estricto Transport Security. Esta condición surge cuando se cambia a certificados autofirmados. Para borrar la condición que bloquea el acceso al destino, debe borrar los datos de navegación del explorador.

Resultados

El sistema se revierte al uso del certificado autofirmado del servidor. Como resultado, el sistema solicita a los usuarios que acepten manualmente el certificado autofirmado para sus sesiones.

Usar certificados de cabina

Importar certificados para cabinas

Si es necesario, puede importar certificados para las cabinas de almacenamiento de modo que estas se puedan autenticar con el sistema donde se aloja Unified Manager. Los certificados pueden estar firmados por una entidad de certificación (CA) o ser autofirmados.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de certificación.
- Si desea importar certificados de confianza, es necesario importar los certificados para las controladoras de las cabinas de almacenamiento mediante System Manager.

Pasos

1. Seleccione **Gestión de certificados**.
2. Seleccione la ficha **Trusted**.

   Esta página muestra todos los certificados notificados para las cabinas de almacenamiento.

3. Seleccione menú:Importar[certificados] para importar un certificado de CA o menú:Importar[certificados de la cabina de almacenamiento autofirmados] para importar un certificado autofirmado.

   Para limitar la vista, puede utilizar el campo de filtrado **Mostrar certificados…** o puede ordenar las filas de certificados haciendo clic en uno de los encabezados de columna.

4. En el cuadro de diálogo, seleccione el certificado y, a continuación, haga clic en **Importar**.

   El certificado se carga y se valida.

Elimine certificados de confianza

Puede eliminar uno o varios certificados que ya no sean necesarios, por ejemplo, un certificado caducado.

Antes de empezar

Importe el certificado nuevo antes de eliminar el antiguo.

> Tenga en cuenta que la eliminación de un certificado intermedio o de raíz puede afectar a varias cabinas de almacenamiento, ya que es posible que estas cabinas compartan los mismos archivos de certificado.

Pasos

1. Seleccione **Gestión de certificados**.
2. Seleccione la ficha **Trusted**.
3. Seleccione uno o varios certificados de la tabla y, a continuación, haga clic en **Eliminar**.

   > La función **Eliminar** no está disponible para los certificados preinstalados.

Se abrirá el cuadro de diálogo Confirmar eliminación de certificado de confianza.

4. Confirme la eliminación y haga clic en **Eliminar**.

   El certificado se eliminará de la tabla.

Resuelva los certificados que no son de confianza

Los certificados dejan de ser de confianza cuando una cabina de almacenamiento intenta establecer una conexión con Unified Manager, pero no se confirma que la conexión sea segura.

En la página Certificado, puede resolver certificados que no son de confianza al importar un certificado autofirmado de la cabina de almacenamiento o al importar un certificado de una entidad de certificación (CA) que emitió un tercero de confianza.

Antes de empezar

- Inició sesión con un perfil de usuario que cuenta con permisos de administración de seguridad.
- Si tiene pensado importar un certificado firmado por una CA:
  - Generó una solicitud de firma de certificación (archivo .CSR) para cada controladora en la cabina de almacenamiento y la envió a la CA.
  - La CA devolvió archivos de certificado de confianza.
  - Los archivos de certificado están disponibles en el sistema local.

Acerca de esta tarea

Es posible que necesite instalar otros certificados de CA de confianza si se da alguna de las siguientes condiciones:

- Añadió recientemente una cabina de almacenamiento.
- Uno o ambos certificados caducaron.
- Uno o ambos certificados fueron revocados.
- Falta un certificado raíz o intermedio en uno o ambos certificados.

Pasos

1. Seleccione **Gestión de certificados**.
2. Seleccione la ficha **Trusted**.

   Esta página muestra todos los certificados notificados para las cabinas de almacenamiento.

3. Seleccione menú:Importar[certificados] para importar un certificado de CA o menú:Importar[certificados de la cabina de almacenamiento autofirmados] para importar un certificado autofirmado.

   Para limitar la vista, puede utilizar el campo de filtrado **Mostrar certificados…** o puede ordenar las filas de certificados haciendo clic en uno de los encabezados de columna.

4. En el cuadro de diálogo, seleccione el certificado y, a continuación, haga clic en **Importar**.

   El certificado se carga y se valida.

Gestionar certificados

Ver certificados

Es posible ver información resumida de un certificado, incluida la organización que utiliza el certificado, la entidad que lo emite, el periodo de validez y las huellas digitales (identificadores únicos).

Antes de empezar

Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de certificación.

Pasos

1. Seleccione **Gestión de certificados**.
2. Seleccione una de las siguientes pestañas:
   - **Administración** — muestra el certificado para el sistema que aloja el proxy de servicios web. Un certificado de gestión puede estar autofirmado o estar aprobado por una CA. Permite un acceso seguro a Unified Manager.
   - **Trusted**: Muestra los certificados a los que Unified Manager puede acceder para matrices de almacenamiento y otros servidores remotos, como un servidor LDAP. Los certificados pueden emitirse mediante una CA o estar autofirmados.
3. Para ver más información sobre un certificado, seleccione la fila correspondiente, seleccione las tres puntos al final de la fila y haga clic en **Ver** o **Exportar**.

Exportar certificados

Es posible exportar un certificado para ver todos sus detalles.

Antes de empezar

Para abrir el archivo exportado, debe contar con una aplicación para visualización de certificados.

Pasos

1. Seleccione **Gestión de certificados**.
2. Seleccione una de las siguientes pestañas:
   - **Administración** — muestra el certificado para el sistema que aloja el proxy de servicios web. Un certificado de gestión puede estar autofirmado o estar aprobado por una CA. Permite un acceso seguro a Unified Manager.
   - **Trusted**: Muestra los certificados a los que Unified Manager puede acceder para matrices de almacenamiento y otros servidores remotos, como un servidor LDAP. Los certificados pueden emitirse mediante una CA o estar autofirmados.
3. Seleccione un certificado de la página y, a continuación, haga clic en los tres puntos al final de la fila.
4. Haga clic en **Exportar** y guarde el archivo de certificado.
5. Abra el archivo en la aplicación para visualización de certificados.

Gestión del acceso

Información general de Access Management

Access Management es un método para configurar la autenticación de usuario en Unified Manager.

¿Qué métodos de autenticación están disponibles?

Están disponibles los siguientes métodos de autenticación:

- **Roles de usuario local** — la autenticación se administra mediante funciones RBAC (control de acceso basado en roles). Los roles de usuario local incluyen perfiles de usuario predefinidos con permisos de acceso específicos.
- **Servicios de directorio** — la autenticación se administra a través de un servidor LDAP (protocolo ligero de acceso a directorios) y un servicio de directorio, como Active Directory de Microsoft.
- **SAML** — la autenticación se gestiona a través de un proveedor de identidades (IDP) que utiliza SAML 2.0.

Obtenga más información:

- "Cómo funciona Access Management"
- "Terminología de Access Management"
- "Permisos para roles asignados"
- "SAML"

¿Cómo se configura Access Management?

El software SANtricity está preconfigurado para usar roles de usuario local. Si desea utilizar LDAP, puede configurarlo en la página Access Management.

Obtenga más información:

- "Access Management con roles de usuario local"
- "Access Management con servicios de directorio"
- "Configure SAML"

Conceptos

Cómo funciona Access Management

Utilice Access Management para establecer la autenticación de usuario en Unified Manager.

Flujo de trabajo de configuración

La configuración de Access Management funciona de la siguiente manera:

1. Un administrador inicia sesión en Unified Manager con un perfil de usuario que incluye permisos de administrador de seguridad.

> La primera vez que se inicia sesión, el nombre de usuario `admin` se muestra automáticamente y no se puede cambiar. La `admin` el usuario tiene acceso completo a todas las funciones del sistema. La contraseña se debe establecer en el primer inicio de sesión.

2. El administrador se desplaza hasta Access Management en la interfaz de usuario, donde se incluyen roles de usuario local preconfigurados. Estos roles son una implementación de las funcionalidades de control de acceso basado en roles (RBAC).
3. El administrador configura uno o varios de los siguientes métodos de autenticación:
   - **Roles de usuario local** — la autenticación se administra mediante capacidades RBAC. Los roles de usuario local incluyen usuarios predefinidos con permisos de acceso específicos. Los administradores pueden usar estos roles de usuario local como el único método de autenticación o usarlos en combinación con un servicio de directorio. No hace falta configurar nada más allá de las contraseñas de los usuarios.
   - **Servicios de directorio** — la autenticación se administra a través de un servidor LDAP (protocolo ligero de acceso a directorios) y un servicio de directorio, como Active Directory de Microsoft. Un administrador se conecta con el servidor LDAP y, a continuación, asigna los usuarios LDAP a los roles de usuario local.
   - **SAML** — la autenticación se gestiona a través de un proveedor de identidades (IDP) utilizando el lenguaje de marcado de aserción de seguridad (SAML) 2.0. Un administrador establece comunicación entre el sistema IDP y la cabina de almacenamiento, y luego asigna los usuarios IDP a los roles de usuario local integrados en la cabina de almacenamiento.
4. El administrador proporciona credenciales de inicio de sesión en Unified Manager a los usuarios.
5. Los usuarios inician sesión en el sistema con sus credenciales. Durante el inicio de sesión, el sistema realiza las siguientes tareas en segundo plano:
   - Autentica el nombre de usuario y la contraseña en relación con la cuenta de usuario.
   - Determina los permisos del usuario según los roles asignados.
   - Ofrece acceso al usuario a las funciones en la interfaz de usuario.
   - Muestra el nombre de usuario en el banner superior.

Funciones disponibles en Unified Manager

El acceso a las funciones depende de los roles asignados a un usuario, entre los cuales se encuentran los siguientes:

- **Storage admin** — acceso completo de lectura/escritura a los objetos de almacenamiento de las matrices, pero sin acceso a la configuración de seguridad.
- **Security admin** — acceso a la configuración de seguridad en Access Management y Certificate Management.
- **Support admin** — acceso a todos los recursos de hardware en matrices de almacenamiento, datos de fallos y eventos MEL. No brinda acceso a los objetos de almacenamiento ni a la configuración de seguridad.
- **Monitor** — acceso de sólo lectura a todos los objetos de almacenamiento, pero sin acceso a la configuración de seguridad.

Una función no disponible se muestra atenuada o directamente no se muestra en la interfaz de usuario.

Terminología de Access Management

Conozca la forma en que los términos de Access Management se aplican a Unified Manager.

Duración	Descripción
Active Directory	Active Directory (AD) es un servicio de directorio de Microsoft en el que se utiliza LDAP para redes de dominio de Windows.
Vinculación	Las operaciones de vinculación se usan para autenticar clientes en el servidor de directorio. Por lo general, la vinculación requiere credenciales de cuenta y contraseña, pero algunos servidores aceptan operaciones de vinculación anónimas.
APROX	Una entidad de certificación (CA) es una entidad de confianza que emite documentos electrónicos, denominados certificados digitales, para la seguridad de Internet. Estos certificados identifican a los propietarios de sitios web y, de esta manera, permiten conexiones seguras entre clientes y servidores.
Certificado	Un certificado identifica al propietario de un sitio con el fin de brindar seguridad, para evitar que atacantes se hagan pasar por los propietarios del sitio. El certificado tiene información acerca del propietario del sitio y la identidad de la entidad de confianza que certifica (firma) esta información.
LDAP	El protocolo ligero de acceso a directorios (LDAP) es un protocolo de aplicación para acceder a servicios distribuidos de información de directorio y mantenerlos. Este protocolo permite que varias aplicaciones y servicios se conecten con el servidor LDAP para validar usuarios.
RBAC	El control de acceso basado en funciones (RBAC) es un método para regular el acceso a los recursos informáticos o de red en función de las funciones de los usuarios individuales. Unified Manager incluye roles predefinidos.
SAML	El lenguaje de marcado de aserción de seguridad (SAML) es un estándar basado en XML para fines de autenticación y autorización entre dos entidades. SAML permite utilizar la autenticación multifactor, en la cual los usuarios deben introducir dos o más elementos para validar su identidad (por ejemplo, una contraseña y una huella digital). La función de SAML integrada de la cabina de almacenamiento es compatible con SAML2,0 para autenticación, autorización y confirmación de identidades.
SSO	El inicio de sesión único (SSO) es un servicio de autenticación que permite el uso de un conjunto de credenciales de inicio de sesión para acceder a varias aplicaciones.

Duración	Descripción
Proxy de servicios web	El proxy de servicios web, que proporciona acceso mediante mecanismos HTTPS estándar, permite a los administradores configurar servicios de gestión para las cabinas de almacenamiento. El proxy se puede instalar en hosts Windows o Linux. La interfaz de Unified Manager se encuentra disponible con el proxy de servicios web.

Permisos para roles asignados

Las funcionalidades de control de acceso basado en roles (RBAC) incluyen usuarios predefinidos con uno o varios roles asignados. Cada rol incluye permisos para acceder a tareas en Unified Manager.

Los roles permiten que los usuarios accedan a tareas de la siguiente manera:

- **Storage admin** — acceso completo de lectura/escritura a los objetos de almacenamiento de las matrices, pero sin acceso a la configuración de seguridad.
- **Security admin** — acceso a la configuración de seguridad en Access Management y Certificate Management.
- **Support admin** — acceso a todos los recursos de hardware en matrices de almacenamiento, datos de fallos y eventos MEL. No brinda acceso a los objetos de almacenamiento ni a la configuración de seguridad.
- **Monitor** — acceso de sólo lectura a todos los objetos de almacenamiento, pero sin acceso a la configuración de seguridad.

Si un usuario no tiene permisos para una función determinada, esa función no se encuentra disponible para selección o no se muestra en la interfaz de usuario.

Access Management con roles de usuario local

Los administradores pueden utilizar las funcionalidades de control de acceso basado en roles (RBAC) que se aplican en Unified Manager. Estas capacidades se denominan "roles de usuario local".

Flujo de trabajo de configuración

Los roles de usuario local están preconfigurados en el sistema. Para usar roles de usuario local con fines de autenticación, los administradores pueden hacer lo siguiente:

1. Un administrador inicia sesión en Unified Manager con un perfil de usuario que incluye permisos de administrador de seguridad.

   > La `admin` el usuario tiene acceso completo a todas las funciones del sistema.

2. Un administrador revisa los perfiles de usuario, que están predefinidos y no pueden modificarse.
3. De manera opcional, el administrador asigna nuevas contraseñas para cada perfil de usuario.
4. Los usuarios inician sesión en el sistema con las credenciales asignadas.

Gestión

Al utilizar solamente los roles de usuario local para la autenticación, los administradores pueden realizar las siguientes tareas de gestión:

- Cambiar contraseñas.
- Configurar la longitud mínima de las contraseñas.
- Permitir que los usuarios inicien sesión sin contraseñas.

Access Management con servicios de directorio

Los administradores puede usar un servidor de protocolo ligero de acceso a directorios (LDAP) y un servicio de directorio, como Active Directory de Microsoft.

Flujo de trabajo de configuración

Si se utilizan un servidor LDAP y un servicio de directorio en la red, la configuración opera de la siguiente manera:

1. Un administrador inicia sesión en Unified Manager con un perfil de usuario que incluye permisos de administrador de seguridad.

   > La `admin` el usuario tiene acceso completo a todas las funciones del sistema.

2. El administrador introduce los ajustes de configuración del servidor LDAP. Entre ellas se encuentran el nombre de dominio, la URL y la información de la cuenta vinculada.
3. Si el servidor LDAP utiliza un protocolo seguro (LDAPS), el administrador carga una cadena de certificados de una entidad de certificación (CA) para la autenticación entre el servidor LDAP y el sistema host donde se instaló el proxy de servicios web.
4. Después de establecer la conexión del servidor, el administrador asigna los grupos de usuarios a los roles de usuario local. Estos roles están predefinidos y no pueden modificarse.
5. El administrador prueba la conexión entre el servidor LDAP y el proxy de servicios web.
6. Los usuarios inician sesión en el sistema con las credenciales de LDAP/servicios de directorio asignadas.

Gestión

Al utilizar los servicios de directorio para la autenticación, los administradores pueden realizar las siguientes tareas de gestión:

- Añadir servidor de directorio.
- Editar la configuración del servidor de directorio.
- Asignar usuarios LDAP a roles de usuario local.
- Quitar un servidor de directorio.
- Cambiar contraseñas.
- Configurar la longitud mínima de las contraseñas.
- Permitir que los usuarios inicien sesión sin contraseñas.

Access Management con SAML

Para Access Management, los administradores pueden usar las funcionalidades de lenguaje de marcado de aserción de seguridad (SAML) 2.0 que están integradas en la cabina.

Flujo de trabajo de configuración

La configuración de SAML funciona de la siguiente manera:

1. Un administrador inicia sesión en Unified Manager con un perfil de usuario que incluye permisos de administración de seguridad.

   > La `admin` El usuario tiene acceso completo a todas las funciones en System Manager.

2. El administrador se dirige a la ficha **SAML** de Access Management.
3. Un administrador configura las comunicaciones con el proveedor de identidades (IDP). Un IDP es un sistema externo que se usa para solicitar credenciales a un usuario y determinar si el usuario se autentica correctamente. Para configurar las comunicaciones con la cabina de almacenamiento, el administrador descarga el archivo de metadatos de IdP desde el sistema IdP y luego usa Unified Manager para cargarlo a la cabina de almacenamiento.
4. Un administrador establece una relación de confianza entre el proveedor de servicios y el IDP. Un proveedor de servicios controla la autorización de usuarios; en este caso, la controladora en la cabina de almacenamiento actúa como proveedor de servicios. Para configurar las comunicaciones, el administrador usa Unified Manager para exportar el archivo de metadatos del proveedor de servicios de la controladora. Desde el sistema IdP, el administrador importa el archivo de metadatos al IdP.

   > Los administradores también deben asegurarse de que el IDP admite la capacidad para obtener un ID de nombre en el momento de la autenticación.

5. El administrador asigna los roles de la cabina de almacenamiento a los atributos de usuario definidos en el IDP. Para hacerlo, el administrador usa Unified Manager y crea las asignaciones.
6. El administrador prueba el inicio de sesión de SSO en la URL del IDP. Esta prueba garantiza que la cabina de almacenamiento y el IDP puedan comunicarse.

   > Una vez que se habilita SAML, _no se puede deshabilitar desde la interfaz de usuario, tampoco se puede editar desde la configuración de IDP. Si necesita deshabilitar o editar la configuración de SAML, comuníquese con el soporte técnico para obtener ayuda.

7. En Unified Manager, el administrador del sistema habilita SAML para la cabina de almacenamiento.
8. Los usuarios inician sesión en el sistema con sus credenciales de SSO.

Gestión

Cuando se usa SAML con fines de autenticación, los administradores pueden realizar las siguientes tareas de administración:

- Modifique o cree nuevas asignaciones de roles
- Exporte los archivos del proveedor de servicios

Restricciones de acceso

Cuando se habilita SAML, los usuarios no pueden detectar ni gestionar el almacenamiento de esa cabina desde la interfaz de Storage Manager heredada.

Además, los siguientes clientes no pueden obtener acceso a los recursos y los servicios de la cabina de almacenamiento:

- Enterprise Management Window (EMW)
- Interfaz de línea de comandos (CLI)
- Clientes de kits de desarrollo de software (SDK)
- Clientes en banda
- Clientes HTTP de la API de REST de autenticación básica
- Inicio de sesión mediante extremo estándar de la API de REST

Use los roles de usuario local

Ver los roles de usuario local

Desde la pestaña roles de usuario local, es posible ver las asignaciones de los usuarios a los roles predeterminados. Estas asignaciones forman parte de los RBAC aplicados en el proxy de servicios web de Unified Manager.

Antes de empezar

Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.

Acerca de esta tarea

Los usuarios y las asignaciones no pueden cambiarse. Solo las contraseñas pueden modificarse.

Pasos

1. Seleccione **Access Management**.
2. Seleccione la ficha **roles de usuario local**.

   Los usuarios se muestran en la tabla:

   - **Admin** — Super administrador que tiene acceso a todas las funciones del sistema. Este usuario incluye todos los roles.
   - **Almacenamiento** — el administrador responsable de todo el aprovisionamiento de almacenamiento. Este usuario incluye los siguientes roles: Administrador de almacenamiento, administrador de soporte y Supervisión.
   - **Security**: El usuario responsable de la configuración de seguridad, incluidos Access Management y Certificate Management. Este usuario incluye los siguientes roles: Administrador de seguridad y Supervisión.
   - **Soporte**: El usuario responsable de recursos de hardware, datos de fallos y actualizaciones de firmware. Este usuario incluye los siguientes roles: Administrador de soporte y Supervisión.
   - **Monitor** — un usuario con acceso de sólo lectura al sistema. Este usuario incluye únicamente el rol Supervisión.

- **rw** (lectura/escritura): Este usuario incluye los siguientes roles: Administrador de almacenamiento, administrador de soporte y monitor.
- **Ro** (sólo lectura) — este usuario incluye sólo la función Monitor.

Cambiar contraseñas de perfiles de usuario local

Es posible cambiar las contraseñas de usuario de cada usuario desde Access Management.

Antes de empezar

- Inició sesión como administrador local, lo que incluye permisos de administrador raíz.
- Debe conocer la contraseña de administrador local.

Acerca de esta tarea

Tenga en cuenta estas directrices al elegir una contraseña:

- Todas las contraseñas de usuarios locales nuevas deben alcanzar o superar la configuración de longitud mínima actual de la contraseña (en Ver/editar configuración).
- Las contraseñas distinguen mayúsculas de minúsculas.
- Los espacios al final de la contraseña no se eliminan si se los utiliza. Procure incluir espacios si se incluyeron en la contraseña.
- Para mayor seguridad, use al menos 15 caracteres alfanuméricos y cambie la contraseña con frecuencia.

Pasos

1. Seleccione **Access Management**.
2. Seleccione la ficha **roles de usuario local**.
3. Seleccione un usuario de la tabla.

   Se habilita el botón Cambiar contraseña.

4. Seleccione **Cambiar contraseña**.

   Se abre el cuadro de diálogo Cambiar contraseña.

5. Si no existe una longitud mínima de contraseña establecida para las contraseñas de usuario local, puede seleccionar la casilla de comprobación para requerir que el usuario introduzca una contraseña para acceder al sistema.
6. Introduzca la contraseña nueva para el usuario seleccionado en los dos campos.
7. Introduzca su contraseña de administrador local para confirmar esta operación y, a continuación, haga clic en **Cambiar**.

Resultados

Si el usuario está conectado, el cambio de contraseña provocará el cierre de la sesión activa del usuario.

Cambie la configuración de contraseña de usuario local

Es posible configurar la longitud mínima requerida para todas las contraseñas de usuario local nuevas o actualizadas. También es posible permitir a los usuarios locales que accedan al sistema sin introducir una contraseña.

Antes de empezar

Inició sesión como administrador local, lo que incluye permisos de administrador raíz.

Acerca de esta tarea

Recuerde estas directrices cuando configure la longitud mínima para las contraseñas de usuario local:

- Los cambios en la configuración no afectan a las contraseñas existentes de usuarios locales.
- La configuración de la longitud mínima requerida para las contraseñas de usuario local debe tener entre 0 y 30 caracteres.
- Todas las contraseñas de usuario local nuevas deben alcanzar o superar la configuración de longitud mínima actual.
- No configure una longitud mínima para la contraseña si desea que los usuarios locales accedan al sistema sin introducir una contraseña.

Pasos

1. Seleccione **Access Management**.
2. Seleccione la ficha **roles de usuario local**.
3. Seleccione **Ver/editar configuración**.

   Se abre el cuadro de diálogo Configuración de contraseña de usuario local.

4. Debe realizar una de las siguientes acciones:
   - Para permitir a los usuarios locales que accedan al sistema *without* password, desactive la casilla de verificación "requerir que todas las contraseñas de usuario local tengan al menos…".
   - Si desea configurar una longitud mínima de contraseña para todas las contraseñas de usuario local, active la casilla de comprobación "requerir que todas las contraseñas de usuario local tengan al menos…" y luego use el cuadro de desplazamiento para configurar la longitud mínima requerida para todas las contraseñas de usuario local

     Todas las contraseñas de usuario local nuevas deben alcanzar o superar la configuración actual.

5. Haga clic en **Guardar**.

Uso de los servicios de directorio

Añadir servidor de directorio

Para configurar la autenticación de Access Management, se debe establecer la comunicación entre un servidor LDAP y el host donde se ejecuta el proxy de servicios web para Unified Manager. A continuación, se deben asignar los grupos de usuarios LDAP a los roles de usuario local.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- Debe haber grupos de usuarios definidos en el servicio de directorio.
- Deben estar disponibles las credenciales del servidor LDAP, incluidos el nombre de dominio y la URL del servidor y, de manera opcional, el nombre de usuario y la contraseña de la cuenta de enlace.

- En el caso de los servidores LDAPS que utilizan un protocolo seguro, se debe instalar la cadena de certificados del servidor LDAP en la máquina local.

Acerca de esta tarea

La adición de un servidor de directorio es un proceso que consta de dos pasos. Primero, se debe introducir la URL y el nombre de dominio. Si el servidor utiliza un protocolo seguro, se debe cargar también un certificado de CA para autenticación si no se encuentra firmado por una entidad de firma estándar. Si se poseen credenciales de una cuenta de enlace, es posible introducir también el nombre de cuenta de usuario y la contraseña. Luego, se deben asignar los grupos de usuarios del servidor LDAP a los roles de usuario local.

Pasos

1. Seleccione **Access Management**.
2. En la ficha **Servicios de directorio**, seleccione **Agregar servidor de directorio**.

   Se abre el cuadro de diálogo Añadir servidor de directorio.

3. En la ficha **Configuración del servidor**, introduzca las credenciales del servidor LDAP.

Detalles del campo

Ajuste	Descripción
Ajustes de configuración	Dominios
Introduzca el nombre de dominio del servidor LDAP. Si desea introducir varios dominios, escríbalos en una lista separada por comas. El nombre de dominio se utiliza en el inicio de sesión (*username@domain*) para especificar con qué servidor de directorio debe realizarse la autenticación.	URL del servidor
Introduzca la URL para acceder al servidor LDAP con el formato de `ldap[s]://host:*port*`.	Cargar certificado (opcional)

Ajuste	Descripción
Este campo aparece solo si se especific a un protocolo LDAPS en el campo URL del servidor arriba. Haga clic en **examinar** y seleccione un certificado de CA para cargar. Este es el certificado o la cadena de certificados de confianza utilizado para autenticar el servidor LDAP.	Enlazar cuenta (opcional)
Introduzca una cuenta de usuario de solo lectura para realizar consultas de búsqueda en el servidor LDAP y para buscar dentro de los grupos. Introduzca el nombre de cuenta con formato tipo LDAP. Por ejemplo, si el usuario de enlace se denomina "bindacct", es posible introducir un valor como el siguiente `CN=bindacct,CN=Users,DC=cpoc,DC=local`.	Enlazar contraseña (opcional)

Ajuste	Descripción
Este campo se muestra cuando se introduce una cuenta de enlace. Introduzca la contraseña de la cuenta de enlace.	Probar conexión del servidor antes de añadir
Seleccione esta casilla de comprobación si desea asegurarse de que el sistema pueda comunicarse con la configuración de servidor LDAP que introdujo. La prueba se produce después de hacer clic en **Agregar** en la parte inferior del cuadro de diálogo. Si esta casilla de comprobación está seleccionada y la prueba falla, no se añadirá la configuración. Debe resolver el error o anular la selección de la casilla de comprobación para omitir la comprobación y añadir la configuración.	**Configuración de privilegios**
DN base de búsqueda	Introduzca el contexto de LDAP para buscar usuarios, generalmente con el formato de `CN=Users, DC=cpoc, DC=local`.
Atributo de nombre de usuario	Introduzca el atributo vinculado al ID de usuario para los fines de autenticación. Por ejemplo: `sAMAccountName`.

Ajuste	Descripción
Atributos de grupo	Introduzca una lista de atributos de grupo en el usuario, que se utilizará para la asignación de grupos a roles. Por ejemplo: `memberOf, managedObjects`.

4. Haga clic en la ficha **asignación de roles**.
5. Asigne grupos LDAP a los roles predefinidos. Un grupo puede tener varios roles asignados.

Detalles del campo

Ajuste	Descripción
Asignaciones	DN de grupo
Especifique el nombre distintivo (DN) del grupo correspondiente al grupo de usuarios LDAP que se asignará. Se admiten expresiones regulares. Estos caracteres especiales de expresión regular deben escaparse con una barra diagonal inversa (\) si no forman parte de un patrón de expresión regular: \.[]{}()<>*+-=?<$	
Funciones	Haga clic en el campo y seleccione uno de los roles de usuario local que se asignará al DN del grupo. Debe seleccionar individualmente cada rol que desee incluir en este grupo. Se requiere el rol de supervisión junto con los demás roles para iniciar sesión en SANtricity Unified Manager. Los roles asignados incluyen los siguientes permisos: • **Storage admin** — acceso completo de lectura/escritura a los objetos de almacenamiento de las matrices, pero sin acceso a la configuración de seguridad. • **Security admin** — acceso a la configuración de seguridad en Access Management y Certificate Management. • **Support admin** — acceso a todos los recursos de hardware en matrices de almacenamiento, datos de fallos y eventos MEL. No brinda acceso a los objetos de almacenamiento ni a la configuración de seguridad. • **Monitor** — acceso de sólo lectura a todos los objetos de almacenamiento, pero sin acceso a la configuración de seguridad.

El rol de supervisión se requiere para todos los usuarios, incluido el administrador.

6. Si lo desea, haga clic en **Agregar otra asignación** para introducir más asignaciones de grupo a rol.
7. Cuando termine de asignar, haga clic en **Agregar**.

   El sistema realiza una validación y se asegura de que la cabina de almacenamiento y el servidor LDAP pueden comunicarse. Si aparece un mensaje de error, compruebe las credenciales que introdujo en el cuadro de diálogo y vuelva a introducir la información, de ser necesario.

Editar ajustes y asignaciones de roles del servidor de directorios

Si anteriormente configuró un servidor de directorio en Access Management, es posible cambiar sus ajustes en cualquier momento. Entre estos ajustes se encuentran la información de conexión del servidor y las asignaciones de grupos a roles.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- Debe definirse un servidor de directorio.

Pasos

1. Seleccione **Access Management**.
2. Seleccione la ficha **Servicios de directorio**.
3. Si se define más de un servidor, seleccione el servidor que desea editar en la tabla.
4. Seleccione **Ver/editar configuración**.

   Se abre el cuadro de diálogo Configuración del servidor de directorio.

5. En la ficha **Configuración del servidor**, cambie la configuración deseada.

Detalles del campo

Ajuste	Descripción
Ajustes de configuración	Dominios
Los nombres de dominio de los servidores LDAP. Si desea introducir varios dominios, escríbalos en una lista separada por comas. El nombre de dominio se utiliza en el inicio de sesión (*username@domain*) para especificar con qué servidor de directorio debe realizarse la autenticación.	URL del servidor
La URL para acceder al servidor LDAP con el formato de `ldap[s]://host:port`.	Enlazar cuenta (opcional)
La cuenta de usuario de solo lectura para realizar consultas en el servidor LDAP y buscar dentro de grupo.	Enlazar contraseña (opcional)
La contraseña de la cuenta vinculada. (Este campo se muestra cuando se introduce una cuenta vinculada.)	Probar conexión del servidor antes de guardar

Ajuste	Descripción
Comprueba que el sistema pueda comunicarse con la configuración del servidor LDAP. La prueba se produce después de hacer clic en **Guardar**. Si se selecciona esta casilla de comprobación y la prueba falla, no se modifica la configuración. Debe resolver el error o desmarcar la casilla de comprobación para omitir la prueba y volver a editar la configuración.	**Configuración de privilegios**
DN base de búsqueda	El contexto de LDAP para buscar usuarios, normalmente en la forma de `CN=Users, DC=cpoc, DC=local`.
Atributo de nombre de usuario	El atributo que está vinculado al ID de usuario para la autenticación. Por ejemplo: `sAMAccountName`.
Atributos de grupo	Lista de atributos de grupo en el usuario, que se utiliza para la asignación de grupos a roles. Por ejemplo: `memberOf, managedObjects`.

6. En la ficha **asignación de roles**, cambie la asignación deseada.

Detalles del campo

Ajuste	Descripción
Asignaciones	DN de grupo
El nombre de dominio para asignar el grupo de usuarios LDAP. Se admiten expresiones regulares. Estos caracteres especiales de expresión regular deben escaparse con una barra invertida (\) si no forman parte de un patrón de expresión regular: \.[]{}()<>*+-=	Funciones

El rol de supervisión se requiere para todos los usuarios, incluido el administrador.

7. Si lo desea, haga clic en **Agregar otra asignación** para introducir más asignaciones de grupo a rol.
8. Haga clic en **Guardar**.

Resultados

Una vez finalizada esta tarea, se finalizarán todas las sesiones de usuario activas. Solo se mantiene la sesión de usuario actual.

Quitar un servidor de directorio

Para interrumpir la conexión entre un servidor de directorio y el proxy de servicios web, es posible quitar la información del servidor de la página Access Management. Se recomienda ejecutar esta tarea si se configuró un servidor nuevo y se desea eliminar el anterior.

Antes de empezar

Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.

Acerca de esta tarea

Una vez finalizada esta tarea, se finalizarán todas las sesiones de usuario activas. Solo se mantiene la sesión de usuario actual.

Pasos

1. Seleccione **Access Management**.
2. Seleccione la ficha **Servicios de directorio**.

3. Seleccione el servidor de directorio que desea eliminar de la lista.
4. Haga clic en **Quitar**.

   Se abrirá el cuadro de diálogo Quitar servidor de directorio.

5. Tipo `remove` En el campo y, a continuación, haga clic en **Quitar**.

   Se eliminará la configuración del servidor de directorio, la configuración de privilegios y las asignaciones de roles. Los usuarios ya no podrán iniciar sesión con las credenciales de este servidor.

Use SAML

Configure SAML

Para configurar la autenticación de Access Management, puede usar las funcionalidades de lenguaje de marcado de aserción de seguridad (SAML) que están integradas en la cabina de almacenamiento. Esta configuración establece una conexión entre un proveedor de identidades y el proveedor de almacenamiento.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- Debe conocer la dirección IP o el nombre de dominio de la controladora de la cabina de almacenamiento.
- Un administrador de IDP configuró un sistema IDP.
- Un administrador de IDP comprobó que el IDP admite la capacidad para obtener un ID de nombre en el momento de la autenticación.
- Un administrador comprobó que el reloj del servidor de IdP y de la controladora está sincronizado (ya sea mediante un servidor NTP o mediante el ajuste de la configuración del reloj de la controladora).
- Se descargó un archivo de metadatos de IdP del sistema de IdP y ese archivo está disponible en el sistema local que se usa para acceder a Unified Manager.

Acerca de esta tarea

Un proveedor de identidades (IDP) es un sistema externo que se usa para solicitar credenciales a un usuario y para determinar si el usuario se autentica correctamente. El IDP se puede configurar para ofrecer autenticación multifactor y para usar cualquier base de datos de usuario, como Active Directory. El equipo de seguridad es responsable de mantener el IDP. Un proveedor de servicios (SP) es un sistema que controla la autenticación y el acceso de usuario. Cuando se configura Access Management con SAML, la cabina de almacenamiento actúa como proveedor de servicios, ya que solicita la autenticación del proveedor de identidades. Para establecer una conexión entre el IDP y la cabina de almacenamiento, se deben compartir archivos de metadatos entre estas dos entidades. A continuación, se deben asignar las entidades de usuario de IDP con los roles de la cabina de almacenamiento. Y, finalmente, se debe probar la conexión y los inicios de sesión SSO antes de habilitar SAML.

> **SAML y Directory Services**. Si SAML se habilita cuando Directory Services está configurado como método de autenticación, SAML sustituye a Directory Services en Unified Manager. Si se deshabilita SAML posteriormente, la configuración de Directory Services se establece en los valores anteriores.

Edición y desactivación. una vez que SAML está habilitado, *no puede* desactivarlo a través de la interfaz de usuario, ni puede editar la configuración de IDP. Si necesita deshabilitar o editar la configuración de SAML, comuníquese con el soporte técnico para obtener ayuda.

La configuración de la autenticación SAML es un procedimiento de varios pasos.

Paso 1: Cargue el archivo de metadatos de IDP

Para brindar información de conexión de IdP a la cabina de almacenamiento, se deben importar los metadatos de IdP en Unified Manager. El sistema IDP necesita los metadatos para redirigir las solicitudes de autenticación a la URL correcta y validar las respuestas recibidas.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la pestaña **SAML**.

   La página muestra información general de los pasos de configuración.

3. Haga clic en el enlace **Import Identity Provider (IDP) file**.

   Se abre el cuadro de diálogo Importar archivo del proveedor de identidades.

4. Haga clic en **examinar** para seleccionar y cargar el archivo de metadatos IDP que copió en el sistema local.

   Una vez seleccionado el archivo, se muestra el ID de entidad IDP.

5. Haga clic en **Importar**.

Paso 2: Exporte los archivos del proveedor de servicios

Para establecer una relación de confianza entre IDP y la cabina de almacenamiento, se deben importar los metadatos del proveedor de servicios en IDP. IDP necesita estos metadatos para establecer una relación de confianza con la controladora y procesar las solicitudes de autorización. El archivo incluye información, como el nombre de dominio de la controladora o la dirección IP, por lo que IDP se puede comunicar con los proveedores de servicios.

Pasos

1. Haga clic en el enlace **Exportar archivos del proveedor de servicios**.

   Se abre el cuadro de diálogo Exportar archivos del proveedor de servicios.

2. Introduzca la dirección IP del controlador o el nombre DNS en el campo **controladora A** y, a continuación, haga clic en **Exportar** para guardar el archivo de metadatos en el sistema local.

   Después de hacer clic en **Exportar**, los metadatos del proveedor de servicios se descargan en el sistema local. Anote en qué lugar se almacena el archivo.

3. Desde el sistema local, busque el archivo de metadatos del proveedor de servicios con formato XML que exportó.
4. Desde el servidor IdP, importe el archivo de metadatos del proveedor de servicios para establecer la relación de confianza. Es posible importar el archivo directamente o bien introducir manualmente la información de la controladora desde el archivo.

Paso 3: Asignar roles

Para proporcionar autorización y acceso a Unified Manager a los usuarios, se deben asignar los atributos de usuario IdP y las membresías de grupo a los roles predefinidos de la cabina de almacenamiento.

Antes de empezar

- Un administrador IDP configuró los atributos del usuario y la pertenencia al grupo en el sistema IDP.
- Se importó el archivo de metadatos de IdP a Unified Manager.
- Para la relación de confianza, se importó un archivo de metadatos del proveedor de servicios para la controladora en el sistema IdP.

Pasos

1. Haga clic en el enlace para **mapping Unified Manager** roles.

   Se abre el cuadro de diálogo asignación de roles.

2. Asigne los grupos y atributos de usuario IDP a los roles predefinidos. Un grupo puede tener varios roles asignados.

   Detalles del campo

Ajuste	Descripción
Asignaciones	Atributo de usuario
Especifique un atributo (por ejemplo, "miembro de") para el grupo SAML que será asignado.	Valor de atributo
Especifique el valor de atributo para el grupo que será asignado. Se admiten expresiones regulares. Estos caracteres especiales de expresión regular deben escaparse con una barra invertida (\) si no forman parte de un patrón de expresión regular: \.[]{}()<>*+-=	Funciones

> El rol de supervisión se requiere para todos los usuarios, incluido el administrador. Unified Manager no funcionará correctamente para los usuarios que no tengan el rol de supervisión.

3. Si lo desea, haga clic en **Agregar otra asignación** para introducir más asignaciones de grupo a rol.

Es posible modificar las asignaciones de roles después de haber habilitado SAML.

4. Cuando termine de asignar, haga clic en **Guardar**.

Paso 4: Probar el inicio de sesión SSO

Para garantizar la comunicación entre el sistema IDP y la cabina de almacenamiento, de manera opcional, se puede probar un inicio de sesión SSO. Esa prueba también se puede llevar a cabo durante el paso final para habilitar SAML.

Antes de empezar

- Se importó el archivo de metadatos de IdP a Unified Manager.
- Para la relación de confianza, se importó un archivo de metadatos del proveedor de servicios para la controladora en el sistema IdP.

Pasos

1. Seleccione el enlace **probar inicio de sesión SSO**.

   Se abre un cuadro de diálogo para introducir las credenciales de SSO.

2. Introduzca las credenciales de inicio de sesión para un usuario, tanto con permisos de administración de seguridad como de supervisión.

   Se abre un cuadro de diálogo mientras el sistema prueba el inicio de sesión.

3. Busque el mensaje Test Successful. Si el análisis se realiza correctamente, vaya al siguiente paso para habilitar SAML.

   Si el análisis no se realiza correctamente, se muestra un mensaje de error con más información. Asegúrese de que:

   - El usuario pertenezca a un grupo con permisos de administración de seguridad y supervisión.
   - Los metadatos cargados para el servidor IDP sean correctos.
   - La dirección de la controladora en los archivos de metadatos de SP sea correcta.

Paso 5: Habilite SAML

El paso final es completar la configuración de SAML para la autenticación de usuarios. Durante este proceso, el sistema también le indica que pruebe un inicio de sesión SSO. El proceso de prueba de inicio de sesión con SSO se describe en el paso anterior.

Antes de empezar

- Se importó el archivo de metadatos de IdP a Unified Manager.
- Para la relación de confianza, se importó un archivo de metadatos del proveedor de servicios para la controladora en el sistema IdP.
- Se debe configurar al menos una asignación de rol de administración de seguridad y una de rol de supervisión.

Edición y desactivación. una vez que SAML está habilitado, *no puede* desactivarlo a través de la interfaz de usuario, ni puede editar la configuración de IDP. Si necesita deshabilitar o editar la configuración de SAML, comuníquese con el soporte técnico para obtener ayuda.

Pasos

1. En la ficha **SAML**, seleccione el enlace **Habilitar SAML**.

   Se abre el cuadro de diálogo Confirmar acción de habilitar SAML.

2. Tipo `enable`Y, a continuación, haga clic en **Activar**.
3. Introduzca las credenciales de usuario para llevar a cabo una prueba de inicio de sesión SSO.

Resultados

Una vez que el sistema habilita SAML, se cierran todas las sesiones activas y se inicia la autenticación de usuarios a través de SAML.

Cambiar las asignaciones de roles SAML

Si anteriormente configuró SAML para Access Management, puede cambiar las asignaciones de roles entre los grupos IDP y los roles predefinidos de la cabina de almacenamiento.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- Un administrador IDP configuró los atributos del usuario y la pertenencia al grupo en el sistema IDP.
- SAML debe estar configurado y habilitado.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la pestaña **SAML**.
3. Seleccione **asignación de roles**.

   Se abre el cuadro de diálogo asignación de roles.

4. Asigne los grupos y atributos de usuario IDP a los roles predefinidos. Un grupo puede tener varios roles asignados.

   Tenga cuidado de no quitar los permisos mientras SAML está habilitado; de lo contrario, perderá el acceso a Unified Manager.

Detalles del campo

Ajuste	Descripción
Asignaciones	Atributo de usuario
Especifique un atributo (por ejemplo, "miembro de") para el grupo SAML que será asignado.	Valor de atributo
Especifique el valor de atributo para el grupo que será asignado.	Funciones

> El rol de supervisión se requiere para todos los usuarios, incluido el administrador. Unified Manager no funcionará correctamente para los usuarios que no tengan el rol de supervisión.

5. Opcionalmente, haga clic en **Agregar otra asignación** para introducir más asignaciones de grupo a rol.
6. Haga clic en **Guardar**.

Resultados

Una vez finalizada esta tarea, se finalizarán todas las sesiones de usuario activas. Solo se mantiene la sesión de usuario actual.

Exporte los archivos de proveedor de servicios SAML

Si es necesario, se pueden exportar metadatos de proveedor de servicios para la cabina de almacenamiento y volver a importar el archivo en el sistema del proveedor de identidades (IdP).

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- SAML debe estar configurado y habilitado.

Acerca de esta tarea

En esta tarea, se exportan metadatos de la controladora. IDP necesita estos metadatos para establecer una relación de confianza con la controladora y procesar solicitudes de autenticación. El archivo incluye información, como el nombre de dominio o la dirección IP de la controladora, que IDP puede usar para enviar solicitudes.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la pestaña **SAML**.

3. Seleccione **Exportar**.

   Se abre el cuadro de diálogo Exportar archivos del proveedor de servicios.

4. Haga clic en **Exportar** para guardar el archivo de metadatos en su sistema local.

   El campo de nombre de dominio es de sólo lectura.

   Anote en qué lugar se almacena el archivo.

5. Desde el sistema local, busque el archivo de metadatos del proveedor de servicios con formato XML que exportó.
6. Desde el servidor IdP, importe el archivo de metadatos del proveedor de servicios. Es posible importar el archivo directamente o introducir manualmente la información de la controladora.
7. Haga clic en **Cerrar**.

Preguntas frecuentes

¿Por qué no puedo iniciar sesión?

Si recibe un error al intentar iniciar sesión, revise estas causas posibles.

Los errores de inicio de sesión pueden ocurrir por uno de estos motivos:

- Introdujo un nombre de usuario o contraseña incorrectos.
- No tiene privilegios suficientes.
- Intentó iniciar sesión reiteradamente sin éxito y se activó el modo de bloqueo. Aguarde 10 minutos y vuelva a intentarlo.
- La autenticación SAML está habilitada. Actualice el explorador para iniciar sesión.

¿Qué debo saber antes de añadir un servidor de directorio?

Antes de añadir un servidor de directorio en Access Management, debe cumplir ciertos requisitos.

- Debe haber grupos de usuarios definidos en el servicio de directorio.
- Deben estar disponibles las credenciales del servidor LDAP, incluidos el nombre de dominio y la URL del servidor y, de manera opcional, el nombre de usuario y la contraseña de la cuenta de enlace.
- En el caso de los servidores LDAPS que utilizan un protocolo seguro, se debe instalar la cadena de certificados del servidor LDAP en la máquina local.

¿Qué debo saber acerca de la asignación de roles de la cabina de almacenamiento?

Antes de asignar grupos a roles, revise las directrices.

Las funcionalidades de RBAC incluyen los siguientes roles:

- **Storage admin** — acceso completo de lectura/escritura a los objetos de almacenamiento de las matrices, pero sin acceso a la configuración de seguridad.

- **Security admin** — acceso a la configuración de seguridad en Access Management y Certificate Management.
- **Support admin** — acceso a todos los recursos de hardware en matrices de almacenamiento, datos de fallos y eventos MEL. No brinda acceso a los objetos de almacenamiento ni a la configuración de seguridad.
- **Monitor** — acceso de sólo lectura a todos los objetos de almacenamiento, pero sin acceso a la configuración de seguridad.

> El rol de supervisión se requiere para todos los usuarios, incluido el administrador.

Si usa un servidor de protocolo ligero de acceso a directorios (LDAP) y servicios de directorio, asegúrese de que:

- Un administrador haya definido grupos de usuarios en el servicio de directorio.
- Conoce los nombres de dominio de los grupos de usuarios LDAP.

SAML

Si usa las funcionalidades de lenguaje de marcado de aserción de seguridad (SAML) incorporadas en la cabina de almacenamiento, asegúrese de que:

- Un administrador de proveedor de identidades (IDP) haya configurado atributos de usuario y pertenencia a grupos en el sistema del IDP.
- Conoce los nombres de pertenencia a grupos.
- Conoce el valor de atributo para el grupo que será asignado. Se admiten expresiones regulares. Estos caracteres especiales de expresión regular deben escaparse con una barra invertida (`\`) si no forman parte de un patrón de expresión regular:

  ```
  \.[]{}()<>*+-=!?^$|
  ```

- El rol de supervisión se requiere para todos los usuarios, incluido el administrador. Unified Manager no funcionará correctamente para los usuarios que no tengan el rol de supervisión.

¿Qué debo saber antes de configurar y habilitar SAML?

Antes de configurar y habilitar las funcionalidades de lenguaje de marcado de aserción de seguridad (SAML) para la autenticación, asegúrese de cumplir con los siguientes requisitos y comprender las restricciones de SAML.

Requisitos

Antes de comenzar, compruebe lo siguiente:

- Se configuró un proveedor de identidades (IDP) en la red. Un IDP es un sistema externo que se usa para solicitar credenciales a un usuario y determinar si el usuario se autentica correctamente. El equipo de seguridad es responsable de mantener el IDP.
- Un administrador IDP configuró los atributos y los grupos del usuario en el sistema IDP.
- Un administrador de IDP comprobó que el IDP admite la capacidad para obtener un ID de nombre en el momento de la autenticación.

- Un administrador comprobó que el reloj del servidor de IdP y de la controladora está sincronizado (ya sea mediante un servidor NTP o mediante el ajuste de la configuración del reloj de la controladora).
- Se descargó un archivo de metadatos de IdP del sistema de IdP y ese archivo está disponible en el sistema local que se usa para acceder a Unified Manager.
- Conoce la dirección IP o el nombre de dominio de la controladora de la cabina de almacenamiento.

Restricciones

Además de los requisitos mencionados más arriba, asegúrese de comprender las siguientes restricciones:

- Una vez que se habilita SAML, _no se puede deshabilitar desde la interfaz de usuario, tampoco se puede editar desde la configuración de IDP. Si necesita deshabilitar o editar la configuración de SAML, comuníquese con el soporte técnico para obtener ayuda. Se recomienda que pruebe los inicios de sesión SSO para poder habilitar SAML en el paso final de la configuración. (El sistema también hace una prueba de inicio de sesión SSO antes de habilitar SAML.)
- Si deshabilita SAML en el futuro, el sistema restaura automáticamente la configuración anterior (local User roles o Directory Services).
- Si Directory Services está actualmente configurado para la autenticación de usuario, SAML anula esa configuración.
- Cuando se configura SAML, los siguientes clientes no pueden acceder a los recursos de la cabina de almacenamiento:
  - Enterprise Management Window (EMW)
  - Interfaz de línea de comandos (CLI)
  - Clientes de kits de desarrollo de software (SDK)
  - Clientes en banda
  - Clientes HTTP de la API de REST de autenticación básica
  - Inicio de sesión mediante extremo estándar de la API de REST

¿De qué se tratan los usuarios locales?

Los usuarios locales están predefinidos en el sistema e incluyen permisos específicos.

Entre ellos, se incluyen:

- **Admin** — Super administrador que tiene acceso a todas las funciones del sistema. Este usuario incluye todos los roles. La contraseña se debe establecer en el primer inicio de sesión.
- **Almacenamiento** — el administrador responsable de todo el aprovisionamiento de almacenamiento. Este usuario incluye los siguientes roles: Administrador de almacenamiento, administrador de soporte y Supervisión. Esta cuenta está deshabilitada hasta que se defina una contraseña.
- **Security**: El usuario responsable de la configuración de seguridad, incluidos Access Management y Certificate Management. Este usuario incluye los siguientes roles: Administrador de seguridad y Supervisión. Esta cuenta está deshabilitada hasta que se defina una contraseña.
- **Soporte**: El usuario responsable de recursos de hardware, datos de fallos y actualizaciones de firmware. Este usuario incluye los siguientes roles: Administrador de soporte y Supervisión. Esta cuenta está deshabilitada hasta que se defina una contraseña.
- **Monitor** — un usuario con acceso de sólo lectura al sistema. Este usuario incluye únicamente el rol Supervisión. Esta cuenta está deshabilitada hasta que se defina una contraseña.

- **rw** (lectura/escritura): Este usuario incluye los siguientes roles: Administrador de almacenamiento, administrador de soporte y monitor. Esta cuenta está deshabilitada hasta que se defina una contraseña.
- **Ro** (sólo lectura) — este usuario incluye sólo la función Monitor. Esta cuenta está deshabilitada hasta que se defina una contraseña.

Versiones anteriores

Visite los siguientes enlaces para acceder a la documentación de versiones anteriores del hardware E-Series y del software SANtricity. Los vínculos lo llevan a otro sitio de documentación.

Documentación de hardware para versiones anteriores

- "Instalar los soportes de unidades de controladoras E2712, E2724, E5612 y E5624 y los soportes de unidades de expansión DE1600 y DE5600"
- "Instale los soportes de unidades de controladoras E2760 y E5660 y los soportes de unidades de expansión DE6600"
- "Instale las cabinas flash EF560 y las bandejas de expansión flash DE5600"
- "Instale sistemas más antiguos"
- "Mantenga los sistemas más antiguos"
- "Añada una segunda controladora a E2600 y E2700"
- "Cambie o añada protocolos de host"
- "Convierta de CA a alimentación de CC"

Documentación de software de versiones anteriores

SANtricity versión 11,7

- "Ayuda de System Manager"
- "Ayuda de Unified Manager"

SANtricity versión 11.6

- "Ayuda de System Manager"
- "Ayuda de Unified Manager"

SANtricity versión 11.5

- "Ayuda de System Manager"

SANtricity versión 11.4

- "AMW (E2700, E5600/EF560) AYUDA"
- "AYUDA DE EMW (E2700, E5600/EF560)"

Avisos legales

Los avisos legales proporcionan acceso a las declaraciones de copyright, marcas comerciales, patentes y mucho más.

Derechos de autor

"https://www.netapp.com/company/legal/copyright/"

Marcas comerciales

NETAPP, el logotipo de NETAPP y las marcas enumeradas en la página de marcas comerciales de NetApp son marcas comerciales de NetApp, Inc. Los demás nombres de empresas y productos son marcas comerciales de sus respectivos propietarios.

"https://www.netapp.com/company/legal/trademarks/"

Estadounidenses

Puede encontrar una lista actual de las patentes propiedad de NetApp en:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de privacidad

"https://www.netapp.com/company/legal/privacy-policy/"

Código abierto

Los archivos de notificación proporcionan información sobre los derechos de autor y las licencias de terceros que se utilizan en software de NetApp.

"Aviso sobre el sistema operativo SANtricity E-Series/EF-Series"