Utilice las soluciones SANtricity

E-Series Systems

NetApp
July 26, 2024

Tabla de contenidos

Utilice las soluciones SANtricity . . . 1
Proxy de servicios web . . . 1
Mirroring de volumen remoto . . . 37
Complemento de almacenamiento para vCenter . . . 45
Soluciones heredadas . . . 180

Utilice las soluciones SANtricity

Proxy de servicios web

Información general sobre el proxy de servicios web de SANtricity

El proxy de servicios web de SANtricity es un servidor API RESTful que se instala por separado en un sistema host para gestionar cientos de sistemas de almacenamiento E-Series de NetApp nuevos y heredados. El proxy incluye Unified Manager de SANtricity, que es una interfaz basada en web que ofrece funciones similares.

Información general de la instalación

La instalación y la configuración de Web Services Proxy implica los siguientes pasos:

1. "Revise los requisitos de instalación y actualización".
2. "Descargue e instale el archivo Web Services Proxy".
3. "Inicie sesión en API y Unified Manager".
4. "Configure el proxy de servicios web".

Obtenga más información

- Unified Manager: La instalación del proxy incluye Unified Manager de SANtricity, una interfaz web que proporciona acceso de configuración a los nuevos sistemas de almacenamiento E-Series y EF-Series. Para obtener más información, consulte la ayuda en línea de Unified Manager, que está disponible en su interfaz de usuario o en "Sitio de documentación del software SANtricity".
- Repositorio de GitHub: GitHub contiene un repositorio de la colección y organización de scripts de muestra que ilustra el uso de la API de servicios web de SANtricity de NetApp. Para acceder al repositorio, consulte "Ejemplos de WebServices de NetApp".
- Transferencia de estado representacional (REST): Servicios web es una API RESTful que proporciona acceso a prácticamente todas las funcionalidades de gestión de SANtricity, por lo que debería estar familiarizado con los conceptos DE REST. Para obtener más información, consulte "Estilos arquitectónicos y el diseño de arquitecturas de software basadas en red".
- Notación de objetos JavaScript (JSON) — debido a que los datos dentro de los servicios web están codificados a través de JSON, debe estar familiarizado con los conceptos de programación JSON. Para obtener más información, consulte "Presentamos JSON".

Obtenga más información acerca de los servicios web

Información general sobre los servicios web y Unified Manager

Antes de instalar y configurar el proxy de servicios web, lea la información general de servicios web y Unified Manager de SANtricity.

Servicios Web

Servicios web es una interfaz de programación de aplicaciones (API) que permite configurar, gestionar y supervisar sistemas de almacenamiento E-Series y EF-Series de NetApp. Al emitir solicitudes de API, podrá

completar flujos de trabajo como la configuración, el aprovisionamiento y la supervisión del rendimiento de los sistemas de almacenamiento E-Series.

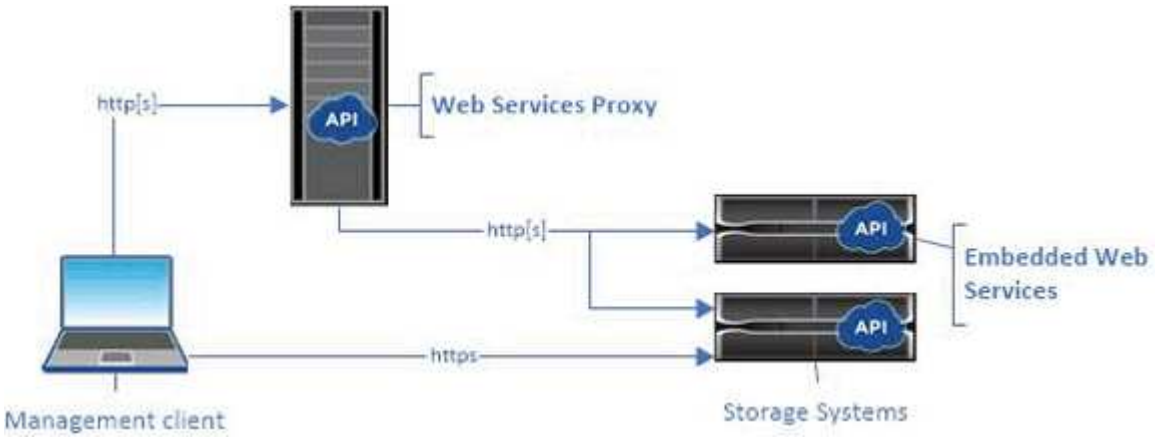
Al usar la API de servicios web para gestionar sistemas de almacenamiento, debe estar familiarizado con lo siguiente:

- Notación de objetos JavaScript (JSON): Debido a que los datos dentro de los servicios web están codificados a través de JSON, debe estar familiarizado con los conceptos de programación de JSON. Para obtener más información, consulte "Presentamos JSON".
- Transferencia de estado representacional (REST): Servicios web es una API RESTful que proporciona acceso a prácticamente todas las funcionalidades de gestión de SANtricity, por lo que debería estar familiarizado con los conceptos DE REST. Para obtener más información, consulte "Estilos arquitectónicos y el diseño de arquitecturas de software basadas en red".
- Conceptos del lenguaje de programación: Java y Python son los lenguajes de programación más comunes que se usan con la API de servicios web, pero cualquier lenguaje de programación que pueda realizar solicitudes HTTP es suficiente para la interacción de API.

Web Services está disponible en dos implementaciones:

- **Integrado**: Se integra Un servidor API RESTful en cada controladora de un sistema de almacenamiento E2800/EF280 que ejecuta SANtricity 11.30 de NetApp o versiones posteriores, un E5700/EF570 que ejecuta SANtricity 11.40 o versiones posteriores, y un EF300 o EF600 que ejecuta SANtricity 11.60 o versiones posteriores. No es necesario realizar ninguna instalación.
- **Proxy** — el proxy de servicios web de SANtricity es un servidor API RESTful instalado por separado en un servidor Windows o Linux. Esta aplicación basada en host puede gestionar cientos de sistemas de almacenamiento E-Series de NetApp nuevos y heredados. En general, debe usar el proxy para redes con más de 10 sistemas de almacenamiento. El proxy puede manejar numerosas solicitudes de forma más eficiente que la API integrada.

El núcleo de la API está disponible en ambas implementaciones.



La tabla siguiente proporciona una comparación entre el proxy y la versión incrustada.

Consideración	Proxy	Integrado
Instalación	Requiere un sistema host (Linux o Windows). El proxy se puede descargar en la "Sitio de soporte de NetApp" o encendido "DockerHub".	No se requiere instalación ni habilitación.
Seguridad	Configuración mínima de seguridad de forma predeterminada. La configuración de seguridad es baja para que los desarrolladores puedan empezar a usar la API de forma rápida y sencilla. Si lo desea, puede configurar el proxy con el mismo perfil de seguridad que la versión incrustada.	Configuración de alta seguridad de forma predeterminada. La configuración de seguridad es alta porque la API se ejecuta directamente en las controladoras. Por ejemplo, no permite el acceso HTTP y deshabilita todos los protocolos de cifrado SSL y TLS anteriores para HTTPS.
Gestión centralizada	Gestiona todos los sistemas de almacenamiento desde un servidor.	Gestiona únicamente el controlador en el que está integrado.

Unified Manager

El paquete de instalación proxy incluye Unified Manager, una interfaz web que proporciona acceso a la configuración de los nuevos sistemas de almacenamiento E-Series y EF-Series, como E2800, E5700, EF300 y EF600.

En Unified Manager, puede realizar las siguientes operaciones en lote:

- Vea el estado de varios sistemas de almacenamiento desde una vista central
- Detectar varios sistemas de almacenamiento en la red
- Importe la configuración de un sistema de almacenamiento a varios sistemas
- Actualizar el firmware para varios sistemas de almacenamiento

Compatibilidad y restricciones

Las siguientes restricciones y compatibilidad se aplican al uso del proxy de servicios web.

Consideración	Compatibilidad o restricción
Soporte HTTP	El proxy de servicios web permite el uso de HTTP o HTTPS. (La versión incrustada de Web Services requiere HTTPS por motivos de seguridad.)

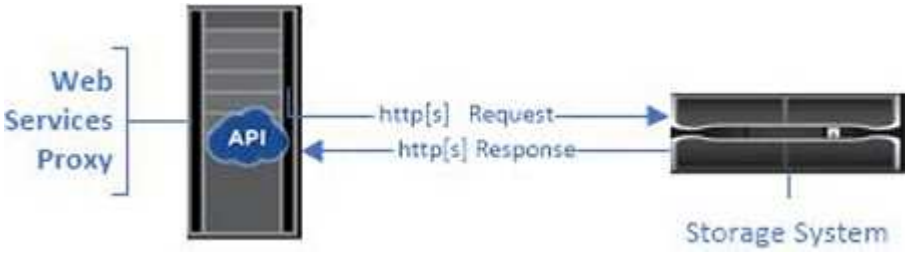
Consideración	Compatibilidad o restricción
Firmware y sistemas de almacenamiento	El proxy de servicios web puede gestionar todos los sistemas de almacenamiento E-Series, incluida una combinación de sistemas anteriores y las últimas versiones de E2800, EF280, E5700, EF570, EF300, Y sistemas de las series EF600.
Compatibilidad con IP	El proxy de servicios web es compatible con el protocolo IPv4 o con el protocolo IPv6. Es posible que se produzca un error en el protocolo IPv6 cuando el proxy de servicios web intenta detectar automáticamente la dirección de gestión de la configuración de la controladora. Entre las posibles causas del fallo se encuentran problemas durante el reenvío de direcciones IP o la activación de IPv6 en los sistemas de almacenamiento, pero no en el servidor.
Restricciones de nombres de archivo de NVSRAM	El proxy de servicios web utiliza nombres de archivo NVSRAM para identificar la información de la versión con precisión. Por lo tanto, no se pueden cambiar los nombres de los archivos NVSRAM cuando se utilizan con el proxy de servicios web. Es posible que el proxy de servicios web no reconozca un archivo NVSRAM cuyo nombre ha cambiado como un archivo de firmware válido.
Web Symbol	Symbol Web es una URL en la API REST. Proporciona acceso a casi todas las llamadas con símbolos. La función Symbol forma parte de la siguiente URL: `http://host:port/devmgr/storage-system/storage array ID/symbol/symbol function` Los sistemas de almacenamiento con deshabilitado Symbol se admiten a través del proxy de servicios web.

Conceptos básicos de API

En la API de servicios web, las comunicaciones HTTP implican un ciclo de solicitud y respuesta.

Elementos de URL en las solicitudes

Independientemente del lenguaje de programación o la herramienta utilizada, cada llamada a la API de servicios web tiene una estructura similar, con una dirección URL, un verbo HTTP y un encabezado Accept.



Todas las solicitudes incluyen una dirección URL, como en el ejemplo siguiente, y contienen los elementos descritos en la tabla.

```
https://webservices.name.com:8443/devmgr/v2/storage-systems
```

Zona	Descripción
Transporte HTTP `https://`	El proxy de servicios web permite el uso de HTTP o HTTPS. Los servicios web integrados requieren HTTPS por motivos de seguridad.
Puerto y URL básicos `webservices.name.com:8443`	Cada solicitud debe enrutarse correctamente a una instancia activa de Web Services. Se requiere el FQDN (nombre de dominio completo) o la dirección IP de la instancia, junto con el puerto de escucha. De forma predeterminada, Web Services se comunica a través del puerto 8080 (para HTTP) y el puerto 8443 (para HTTPS). Para el proxy de servicios web, ambos puertos se pueden cambiar durante la instalación del proxy o en el archivo wsconfig.xml. La contención de puertos es común en los hosts de centro de datos que ejecutan diversas aplicaciones de gestión. En el caso de los servicios web integrados, no se puede cambiar el puerto de la controladora; de forma predeterminada, se establece en el puerto 8443 para conexiones seguras.

Zona	Descripción
Ruta API `devmgr/v2/storage-systems`	Se realiza una solicitud a un recurso DE REST o un extremo específico dentro de la API de servicios web. La mayoría de los extremos tienen el siguiente formato: `devmgr/v2/<resource>/[id]` La ruta API consta de tres partes: • `devmgr` (Administrador de dispositivos) es el espacio de nombres de la API de servicios web. • `v2` Indica la versión de la API a la que tiene acceso. También puede utilizar `utils` para acceder a los extremos de inicio de sesión. • `storage-systems` es una categoría de la documentación.

Verbos HTTP admitidos

Los verbos HTTP admitidos incluyen GET, POST y DELETE:

- Las solicitudes GET se utilizan para solicitudes de sólo lectura.
- LAS solicitudes POST se utilizan para crear y actualizar objetos, así como para solicitudes de lectura que podrían tener implicaciones de seguridad.
- Las solicitudes DE ELIMINACIÓN suelen utilizarse para quitar un objeto de la gestión, quitar un objeto por completo o restablecer el estado del objeto.

> Actualmente, la API de servicios web no admite PUT ni PARCHE. En su lugar, puede usar POST para proporcionar la funcionalidad típica de estos verbos.

Aceptar encabezados

Al devolver un cuerpo de la solicitud, Web Services devuelve los datos en formato JSON (a menos que se especifique lo contrario). Algunos clientes solicitan por defecto "'text/html'" o algo similar. En estos casos, la API responde con un código HTTP 406, indicando que no puede proporcionar datos en este formato. Como práctica recomendada, debe definir el encabezado Accept como "'Application/json'" para los casos en los que espere JSON como tipo de respuesta. En otros casos en los que no se devuelve un cuerpo de respuesta (por ejemplo, ELIMINAR), siempre que el encabezado Accept no provoque ningún efecto no intencional.

Respuestas

Cuando se realiza una solicitud a la API, una respuesta devuelve dos partes fundamentales de información:

- Código de estado HTTP: Indica si la solicitud se ha realizado correctamente.
- Cuerpo de respuesta opcional — normalmente proporciona un cuerpo JSON que representa el estado del recurso o un cuerpo que proporciona más detalles sobre la naturaleza de un fallo.

Debe comprobar el código de estado y la cabecera de tipo de contenido para determinar el aspecto del cuerpo de respuesta resultante. Para los códigos de estado HTTP 200-203 y 422, Web Services devuelve un cuerpo

JSON con la respuesta. Para otros códigos de estado HTTP, Web Services generalmente no devuelve un cuerpo JSON adicional, ya sea porque la especificación no lo permite (204) o porque el estado es autoexplicativo. En la tabla se enumeran los códigos de estado HTTP comunes y las definiciones. También indica si la información asociada con cada código HTTP se devuelve en un cuerpo JSON.

Código de estado HTTP	Descripción	Cuerpo JSON
200 DE ACUERDO	Indica una respuesta correcta.	Sí
201 creado	Indica que se creó un objeto. Este código se utiliza en unos pocos casos excepcionales en lugar de un estado de 200.	Sí
202 aceptado	Indica que la solicitud se acepta para su procesamiento como una solicitud asíncrona, pero debe realizar una solicitud posterior para obtener el resultado real.	Sí
203 Información no autoritativa	Similar a una respuesta de 200, pero Web Services no puede garantizar que los datos estén actualizados (por ejemplo, solo los datos en caché están disponibles en este momento).	Sí
204 sin contenido	Indica una operación correcta, pero no hay cuerpo de respuesta.	No
400 solicitud incorrecta	Indica que el cuerpo JSON proporcionado en la solicitud no es válido.	No
401 no autorizado	Indica que se ha producido un error de autenticación. No se han proporcionado credenciales o el nombre de usuario o la contraseña no son válidos.	No
403 Prohibido	Un error de autorización, que indica que el usuario autenticado no tiene permiso para acceder al extremo solicitado.	No
404 no encontrado	Indica que no se pudo ubicar el recurso solicitado. Este código es válido para API no existentes o recursos no existentes solicitados por el identificador.	No

Código de estado HTTP	Descripción	Cuerpo JSON
422 entidad no procesable	Indica que por lo general, la solicitud está bien formada, pero los parámetros de entrada no son válidos o el estado del sistema de almacenamiento no permite que los servicios web satisfagan la solicitud.	Sí
424 Dependencia con error	Se utiliza en el proxy de servicios web para indicar que no se puede acceder al sistema de almacenamiento solicitado en ese momento. Por lo tanto, Web Services no puede satisfacer la solicitud.	No
429 demasiadas solicitudes	Indica que se ha superado el límite de solicitudes y que se debe volver a intentar más tarde.	No

Scripts de ejemplo

GitHub contiene un repositorio de la colección y la organización de scripts de muestra que ilustra el uso de la API de servicios web de SANtricity de NetApp. Para acceder al repositorio, consulte "Ejemplos de WebServices de NetApp".

Términos y conceptos

Los siguientes términos se utilizan en el proxy de servicios web.

Duración	Definición
API	Una interfaz de programación de aplicaciones (API) es un conjunto de protocolos y métodos que permiten a los desarrolladores comunicarse con los dispositivos. La API de servicios web se utiliza para comunicarse con los sistemas de almacenamiento E-Series.
ASUP	La función AutoSupport (ASUP) recoge datos en un bundle de soporte al cliente y envía automáticamente el archivo de mensaje al soporte técnico para la solución de problemas remota y el análisis de problemas.

Duración	Definición
Extremo	Los extremos son funciones que están disponibles en la API. Un extremo incluye un verbo HTTP, más la ruta de URI. En Web Services, los extremos pueden ejecutar tareas como detectar sistemas de almacenamiento y crear volúmenes.
HTTP Verbo	Un verbo HTTP es una acción correspondiente para un punto final, como la recuperación y la creación de datos. En Servicios Web, los verbos HTTP incluyen POST, GET y DELETE.
JSON	La notación de objetos JavaScript (JSON) es un formato de datos estructurado muy similar a XML, que utiliza un formato mínimo de lectura. Los datos en los servicios web están codificados a través de JSON.
REST/RESTful	La transferencia de estado representacional (REST) es una especificación suelta que define un estilo arquitectónico para una API. Dado que la mayoría de las API DE DESCANSO no cumplen plenamente la especificación, se las describe como «MUY COMPLETAS» o «similar AL TÉRMINO». En general, una API "MUY COMPLETA" es independiente de los lenguajes de programación y tiene las siguientes características: • Basado en HTTP, que sigue la semántica general del protocolo • Productor y consumidor de datos estructurados (JSON, XML, etc.) • Orientado a objetos (a diferencia de orientado a la operación) Servicios web es una API RESTful que proporciona acceso a prácticamente todas las funcionalidades de gestión de SANtricity.
sistema de almacenamiento	Un sistema de almacenamiento es una cabina E-Series que incluye bandejas, controladoras, unidades, software y firmware.
API Symbol	Symbol es una API heredada para gestionar los sistemas de almacenamiento E-Series. La implementación subyacente de la API de servicios web utiliza Symbol.

Duración	Definición
Servicios Web	Web Services es una API que NetApp ha sido diseñada para que los desarrolladores gestionen los sistemas de almacenamiento E-Series. Existen dos implementaciones de Web Services: Integradas en el controlador y un proxy independiente que se puede instalar en Linux o Windows.

Instalar y configurar

Revise los requisitos de instalación y actualización

Antes de instalar Web Services Proxy, revise los requisitos de instalación y actualice sus consideraciones.

Requisitos de instalación

Puede instalar y configurar el proxy de servicios web en un sistema host Windows o Linux.

La instalación de proxy incluye los siguientes requisitos.

Requisito	Descripción
Limitaciones de nombre de host	Asegúrese de que el nombre de host del servidor donde planea instalar el proxy de servicios web contiene sólo letras ASCII, dígitos numéricos y guiones (-). Este requisito se debe a una limitación de Java keytool, que se utiliza para generar un certificado autofirmado para el servidor. Si el nombre de host del servidor contiene otros caracteres, como un guión bajo (_), el servidor web no se iniciará después de la instalación.
Sistemas operativos	Puede instalar el proxy en los sistemas operativos siguientes: • Linux • Windows Para obtener una lista completa de los sistemas operativos y la compatibilidad del firmware, consulte "Herramienta de matriz de interoperabilidad de NetApp".
Linux: Consideraciones adicionales	Las bibliotecas Linux Standard base (init-functions) son necesarias para que el servidor web funcione correctamente. Debe instalar los paquetes lsb/insserv para el sistema operativo. Para obtener más información, consulte la sección "Paquetes adicionales necesarios" del archivo Readme.
Múltiples instancias	Sólo puede instalar una instancia de proxy de servicios web en un servidor; sin embargo, puede instalar el proxy en varios servidores de la red.

Requisito	Descripción
Planificación de la capacidad	El proxy de servicios web requiere un espacio adecuado para el registro. Asegúrese de que su sistema cumpla los siguientes requisitos de espacio en disco disponibles: • Espacio necesario para la instalación — 275 MB • Espacio mínimo de registro — 200 MB • Memoria del sistema — 2 GB; el espacio en el montón es 1 GB de forma predeterminada Puede utilizar una herramienta de supervisión de espacio en disco para verificar el espacio disponible en la unidad de disco para el almacenamiento persistente y el registro.
Licencia	El proxy de servicios web es un producto gratuito e independiente que no requiere una clave de licencia. Sin embargo, se aplican los derechos de autor y las condiciones de servicio aplicables. Si está instalando el proxy en modo gráfico o consola, debe aceptar el Contrato de licencia para el usuario final (EULA).

Consideraciones de renovación

Si está actualizando desde una versión anterior, tenga en cuenta que algunos elementos se conservan o se eliminan.

- Para el proxy de servicios web, se conservan los ajustes de configuración anteriores. Esta configuración incluye contraseñas de usuario, todos los sistemas de almacenamiento detectados, certificados de servidor, certificados de confianza y configuración de tiempo de ejecución del servidor.
- En el caso de Unified Manager, se quitan todos los archivos de sistema operativo SANtricity cargados anteriormente en el repositorio durante la actualización.

Instale o actualice el archivo proxy de servicios web

La instalación implica descargar el archivo y, a continuación, instalar el paquete proxy en un servidor Linux o Windows. También puede actualizar el proxy utilizando estas instrucciones.

Descargue los archivos del proxy de servicios web

Podrás descargar el archivo de instalación y el archivo Léame de la página de descarga de software del sitio de soporte de NetApp.

El paquete de descarga incluye el proxy de servicios web y la interfaz de Unified Manager.

Pasos

1. Vaya a. "Soporte de NetApp: Descargas".
2. Seleccione **E-Series SANtricity Web Services Proxy**.
3. Siga las instrucciones para descargar el archivo. Asegúrese de seleccionar el paquete de descarga correcto para su servidor (por ejemplo, EXE para Windows; BIN o RPM para Linux).

4. Descargue el archivo de instalación en el servidor donde desea instalar el proxy y Unified Manager.

Instale en servidores Windows o Linux

Puede instalar Web Services Proxy y Unified Manager mediante uno de tres modos (gráfica, consola o silenciosa) o utilizando un archivo RPM (sólo Linux).

Antes de empezar

- "Revise los requisitos de la instalación".
- Asegúrese de haber descargado el archivo de instalación correcto (EXE para Windows; BIN para Linux) en el servidor en el que desea instalar el proxy y Unified Manager.

Instalación en modo gráfico

Puede ejecutar la instalación en modo gráfico para Windows o Linux. En el modo gráfico, las instrucciones aparecen en una interfaz de estilo Windows.

Pasos

1. Acceda a la carpeta en la que descargó el archivo de instalación.
2. Inicie la instalación de Windows o Linux de la siguiente manera:
   - Windows — haga doble clic en el archivo de instalación:

     `santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe`

   - Linux — ejecute el siguiente comando: `santricity_webservices-linux_x64-nn.nn.nn.nnnn.bin`

     En los nombres de archivo anteriores, `nn.nn.nn.nnnn` representa el número de versión.

   Se inicia el proceso de instalación y se muestra la pantalla de bienvenida de NetApp SANtricity Web Services Proxy + Unified Manager.

3. Siga las instrucciones que aparecen en pantalla.

   Durante la instalación, se le pedirá que habilite varias funciones e introduzca algunos parámetros de configuración. Si es necesario, puede cambiar cualquiera de estas selecciones posteriormente en los archivos de configuración.

   > Durante una actualización, no se le solicitan los parámetros de configuración.

4. Cuando aparezca el mensaje servidor web iniciado, haga clic en **Aceptar** para completar la instalación.

   Aparece el cuadro de diálogo instalar completo.

5. Haga clic en las casillas de verificación si desea iniciar Unified Manager o la documentación de API interactiva y, a continuación, haga clic en **hecho**.

Instale en modo de consola

Puede ejecutar la instalación en modo de consola para Windows o Linux. En el modo Consola, las indicaciones aparecen en la ventana de terminal.

Pasos

1. Ejecute el siguiente comando: `<install filename> -i console`

   En el comando anterior, `<install filename>` representa el nombre del archivo de instalación del proxy que ha descargado (por ejemplo: `santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe`).

   > Para cancelar la instalación en cualquier momento durante el proceso de instalación, escriba `QUIT` en el símbolo del sistema.

   Se inicia el proceso de instalación y aparece el mensaje iniciando el instalador — Introducción .

2. Siga las instrucciones que aparecen en pantalla.

   Durante la instalación, se le pedirá que habilite varias funciones e introduzca algunos parámetros de configuración. Si es necesario, puede cambiar cualquiera de estas selecciones posteriormente en los archivos de configuración.

   > Durante una actualización, no se le solicitan los parámetros de configuración.

3. Una vez finalizada la instalación, pulse **Intro** para salir del instalador.

Instalación en modo silencioso

Puede ejecutar la instalación en modo silencioso para Windows o Linux. En el modo silencioso, no aparecen mensajes de retorno ni secuencias de comandos en la ventana de terminal.

Pasos

1. Ejecute el siguiente comando: `<install filename> -i silent`

   En el comando anterior, `<install filename>` representa el nombre del archivo de instalación del proxy que ha descargado (por ejemplo: `santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe`).

2. Pulse **Intro**.

   El proceso de instalación puede tardar varios minutos en completarse. Después de una instalación correcta, aparece un símbolo del sistema en la ventana de terminal.

RPM Command install (instalación DE comando RPM) (sólo Linux)

En el caso de los sistemas Linux que son compatibles con el sistema de gestión de paquetes RPM, puede instalar el proxy de servicios web mediante un archivo RPM opcional.

Pasos

1. Descargue el archivo RPM en el servidor en el que desea instalar el proxy y Unified Manager.
2. Abra una ventana de terminal.
3. Introduzca el siguiente comando:

   ```
   rpm -u santricity_webservices-nn.nn.nn.nnnn-n.x86_64.rpm
   ```

   > En el comando anterior, `nn.nn.nn.nnnn` representa el número de versión.

El proceso de instalación puede tardar varios minutos en completarse. Después de una instalación correcta, aparece un símbolo del sistema en la ventana de terminal.

Inicie sesión en API y Unified Manager

Web Services incluye documentación de API, que permite interactuar directamente con la API DE REST. También incluye Unified Manager, una interfaz basada en navegador para gestionar varios sistemas de almacenamiento E-Series.

Inicie sesión en la API de servicios web

Después de instalar el proxy de servicios web, puede acceder a la documentación de API interactiva en un explorador.

La documentación de API se ejecuta con cada instancia de Web Services, y también está disponible en formato PDF estático del sitio de soporte de NetApp. Para tener acceso a la versión interactiva, abra un explorador e introduzca la URL que indica dónde reside Web Services (una controladora para la versión incrustada o un servidor para el proxy).

> La API de servicios web implementa la especificación OpenAPI (originalmente llamada especificación Swagger).

Para el inicio de sesión inicial, se utilizan las credenciales "admin". "Admin" es considerado un súper administrador con acceso a todas las funciones y funciones.

Pasos

1. Abra un explorador.
2. Introduzca la dirección URL para la implementación de proxy o incrustado:
   - Integrado: `https://<controller>:<port>/devmgr/docs/`

     En esta URL, `<controller>` Es la dirección IP o el FQDN de la controladora y. `<port>` es el número de puerto de gestión de la controladora (el valor predeterminado es 8443).
   - Proxy: `http[s]://<server>:<port>/devmgr/docs/`

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

     > Si el puerto de escucha ya está en uso, el proxy detecta el conflicto y le solicita que elija un puerto de escucha diferente.

   La documentación de API se abre en el explorador.
3. Cuando se abra la documentación interactiva de la API, vaya al menú desplegable situado en la parte superior derecha de la página y seleccione **utils**.
4. Haga clic en la categoría **Login** para ver los puntos finales disponibles.
5. Haga clic en el punto final **POST: /Login** y, a continuación, haga clic en **probar con ello**.
6. Si inicia sesión por primera vez, introduzca admin como nombre de usuario y contraseña.

7. Haga clic en **Ejecutar**.
8. Para acceder a los extremos para la administración de almacenamiento, vaya al menú desplegable de la parte superior derecha y seleccione **v2**.

   Se muestran las categorías de alto nivel de los puntos finales. Puede desplazarse por la documentación de API tal y como se describe en la tabla.

Zona	Descripción
Menú desplegable	En la parte superior derecha de la página, un menú desplegable proporciona opciones para cambiar entre la versión 2 de la documentación de API (V2), la interfaz de símbolos (Symbol V2) y las utilidades API (utils) para iniciar sesión. Dado que la versión 1 de la documentación de API era una versión preliminar y no estaba disponible de forma general, V1 no se incluye en el menú desplegable.
Categorías	La documentación de API está organizada por categorías de alto nivel (por ejemplo, Administración, Configuración). Haga clic en una categoría para ver los puntos finales relacionados.
Puntos finales	Seleccione un punto final para ver sus rutas de URL, los parámetros necesarios, los cuerpos de respuesta y los códigos de estado que es probable que las direcciones URL devuelvan.
Pruébelo	Interactúe directamente con el punto final haciendo clic en **Inténtelo**. Este botón se proporciona en cada una de las vistas ampliadas de los puntos finales. Al hacer clic en el botón, aparecen campos para introducir parámetros (si corresponde). A continuación, puede introducir valores y hacer clic en **Ejecutar**. La documentación interactiva utiliza JavaScript para realizar la solicitud directamente a la API; no es una solicitud de prueba.

Inicie sesión en 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 acceder a Unified Manager, abra un explorador e introduzca la URL donde está instalado el proxy. Se

admiten los siguientes exploradores en las versiones mencionadas.

Navegador	Versión mínima
Google Chrome	79
Internet Explorer de Microsoft	11
Microsoft Edge	79
Mozilla Firefox	70
Safari	12

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 sobre usuarios y contraseñas, consulte la sección Access Management de la ayuda en línea de Unified Manager.

Configure el proxy de servicios web

Es posible modificar la configuración del proxy de servicios web para cumplir con los requisitos operativos y de rendimiento únicos del entorno.

Detenga o reinicie el servidor web

El servicio de WebServer se inicia durante la instalación y se ejecuta en segundo plano. Durante algunas tareas de configuración, es posible que necesite detener o reiniciar el servicio de WebServer.

Pasos

1. Debe realizar una de las siguientes acciones:

   - Para Windows, vaya al menú **Inicio**, seleccione menú:Herramientas administrativas[Servicios], busque **Servicios Web de SANtricity de NetApp** y, a continuación, seleccione **Detener** o **Reiniciar**.
   - Para Linux, elija el método para detener y reiniciar el servidor web para la versión del sistema operativo. Durante la instalación, un cuadro de diálogo emergente indicó lo que se inició el daemon. Por ejemplo:

```
web_services_proxy webserver installed and started. You can interact with it
using systemctl start|stop|restart|status web_services_proxy.service
```

El método más común para interactuar con el servicio es mediante el uso `systemctl` comandos.

Resolver conflictos de puerto

Si el proxy de servicios web está en ejecución mientras otra aplicación está disponible en el puerto o la dirección definidos, puede resolver el conflicto de puerto en el archivo wsconfig.xml.1.

Pasos

1. Abra el archivo wsconfig.xml, ubicado en:
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_Services_proxy
2. Agregue la siguiente línea al archivo wsconfig.xml, en el que *n* es el número de puerto:

   ```
   <sslport clientauth="request">*n*</sslport>
   <port>n</port>
   ```

   En la siguiente tabla, se muestran los atributos que controlan los puertos HTTP y HTTPS.

Nombre	Descripción	Nodo principal	Atributos	Obligatorio
gestión de	El nodo raíz para la configuración	Nulo	Versión: La versión del esquema de configuración es actualmente 1.0.	Sí
puerto de sslport	El puerto TCP para escuchar las solicitudes SSL. El valor predeterminado es 8443.	gestión de	Clientauth	No
puerto	El puerto TCP para escuchar la solicitud HTTP, por defecto es 8080.	gestión de	-	No

3. Guarde y cierre el archivo.
4. Reinicie el servicio Webserver para que el cambio surta efecto.

Configuración de balanceo de carga y/o alta disponibilidad

Para usar el proxy de servicios web en una configuración altamente disponible (ha), se puede configurar el balanceo de carga. En una configuración de alta disponibilidad, normalmente un solo nodo recibe todas las solicitudes mientras los demás están en espera o las solicitudes se equilibran de carga en todos los nodos.

El proxy de servicios web puede existir en un entorno altamente disponible (ha), con la mayoría de las API funcionando correctamente independientemente del destinatario de la solicitud. Las etiquetas y carpetas de metadatos son dos excepciones, ya que las etiquetas y las carpetas se almacenan en una base de datos local y no se comparten entre instancias del proxy de servicios web.

Sin embargo, existen algunos problemas de sincronización conocidos que se producen en un pequeño porcentaje de solicitudes. Específicamente, una instancia del proxy puede tener datos más nuevos más rápidamente que una segunda instancia para una ventana pequeña. El proxy de servicios web incluye una configuración especial que elimina este problema de sincronización. Esta opción no está habilitada de forma predeterminada, ya que aumenta la cantidad de tiempo que se tarda en atender las solicitudes de servicio (para la consistencia de datos). Para habilitar esta opción, debe agregar una propiedad a un archivo .INI (para Windows) o a un archivo .SH (para Linux).

Pasos

1. Debe realizar una de las siguientes acciones:
   - Windows: Abra el archivo appserver64.ini y, a continuación, agregue `Dload-balance.enabled=true` propiedad.

     Por ejemplo: `vmarg.7=-Dload-balance.enabled=true`

   - Linux: Abra el archivo webserver.sh y, a continuación, agregue el `Dload-balance.enabled=true` propiedad.

     Por ejemplo: `DEBUG_START_OPTIONS="-Dload-balance.enabled=true"`

2. Guarde los cambios.
3. Reinicie el servicio Webserver para que el cambio surta efecto.

Desactivar el símbolo HTTPS

Puede deshabilitar los comandos Symbol (ajuste predeterminado) y enviar comandos a través de una llamada a procedimiento remoto (RPC). Esta configuración se puede cambiar en el archivo wsconfig.xml.

De forma predeterminada, el proxy de servicios web envía comandos Symbol a través de HTTPS para todos los sistemas de almacenamiento serie E2800 y E5700 que ejecutan las versiones 08.40 o posteriores de SANtricity OS. Los comandos Symbol enviados a través de HTTPS se autentican en el sistema de almacenamiento. Si es necesario, puede deshabilitar la compatibilidad con símbolos HTTPS y enviar comandos a través de RPC. Siempre que se configura un símbolo a través de RPC, todos los comandos pasivos al sistema de almacenamiento están habilitados sin autenticación.

> Cuando se utiliza Symbol mediante RPC, el proxy de servicios web no se puede conectar a sistemas con el puerto de gestión de Symbol deshabilitado.

Pasos

1. Abra el archivo wsconfig.xml, ubicado en:
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_Services_proxy
2. En la `devicemgt.symbolclientstrategy` entrada, sustituya la `httpsPreferred` valor con `rpcOnly`.

   Por ejemplo:

```
<env key="devicemgt.symbolclientstrategy">rpcOnly</env>
```

3. Guarde el archivo.

Configurar el uso compartido de recursos de origen cruzado

Puede configurar el uso compartido de recursos de origen cruzado (CORS), que es un mecanismo que utiliza encabezados HTTP adicionales para proporcionar una aplicación web que se ejecuta en un origen para tener permiso para acceder a recursos seleccionados desde un servidor de un origen diferente.

CORS es manejado por el archivo cors.cfg ubicado en el directorio de trabajo. La configuración de CORS está abierta de forma predeterminada, por lo que el acceso entre dominios no está restringido.

Si no hay ningún archivo de configuración, CORS está abierto. Pero si el archivo cors.cfg está presente, entonces se utiliza. Si el archivo cors.cfg está vacío, no puede realizar una solicitud CORS.

Pasos

1. Abra el archivo cors.cfg, que se encuentra en el directorio de trabajo.
2. Agregue las líneas deseadas al archivo.

   Cada línea del archivo de configuración CORS es un patrón de expresión regular que debe coincidir. El encabezado de origen debe coincidir con una línea del archivo cors.cfgl. Si cualquier patrón de línea coincide con el encabezado de origen, se permite la solicitud. Se compara el origen completo, no sólo el elemento host.

3. Guarde el archivo.

Las solicitudes se coinciden en el host y según el protocolo, como el siguiente:

- Coincidir localhost con cualquier protocolo — `*localhost*`
- Match localhost sólo para HTTPS — `https://localhost*`

Desinstale el proxy de servicios web

Para quitar Web Services Proxy y Unified Manager, puede utilizar cualquier modo (archivo gráfico, consola, silencioso o RPM), independientemente del método que haya utilizado para instalar el proxy.

Desinstalación en modo gráfico

Puede ejecutar la desinstalación en modo gráfico para Windows o Linux. En el modo gráfico, las instrucciones aparecen en una interfaz de estilo Windows.

Pasos

1. Inicie la desinstalación para Windows o Linux de la siguiente manera:
   - Windows — vaya al directorio que contiene el archivo de desinstalación_web_Services_proxy. El directorio predeterminado se encuentra en la siguiente ubicación: C:/Program Files/NetApp/SANtricity Web Services Proxy/. Haga doble clic `uninstall_web_services_proxy.exe`.

> Como alternativa, puede ir al menú:Panel de control[programas > Desinstalar un programa] y, a continuación, seleccionar "proxy de servicios web de SANtricity de NetApp".

- Linux — vaya al directorio que contiene el archivo de desinstalación del proxy de servicios web. El directorio predeterminado se encuentra en la siguiente ubicación: `/opt/netapp/santricity_web_services_proxy/uninstall_web_services_proxy`

2. Ejecute el siguiente comando:

   ```
   uninstall_web_services_proxy -i gui
   ```

   Aparece la pantalla de bienvenida del proxy de servicios web de SANtricity.

3. En el cuadro de diálogo Desinstalar, haga clic en **Desinstalar**.

   Aparece la barra de progreso Desinstalador y muestra el progreso.

4. Cuando aparezca el mensaje Uninstall Complete (desinstalación completa), haga clic en **Done** (Listo).

Desinstalación en modo de consola

Puede ejecutar la desinstalación en modo de consola para Windows o Linux. En el modo Consola, las indicaciones aparecen en la ventana de terminal.

Pasos

1. Vaya al directorio uninstall_web_Services_proxy.
2. Ejecute el siguiente comando:

   ```
   uninstall_web_services_proxy -i console
   ```

   Se inicia el proceso de desinstalación.

3. Cuando la desinstalación haya finalizado, pulse **Intro** para salir del instalador.

Desinstalación en modo silencioso

Puede ejecutar la desinstalación en modo silencioso para Windows o Linux. En el modo silencioso, no aparecen mensajes de retorno ni secuencias de comandos en la ventana de terminal.

Pasos

1. Vaya al directorio uninstall_web_Services_proxy.
2. Ejecute el siguiente comando:

   ```
   uninstall_web_services_proxy -i silent
   ```

   El proceso de desinstalación se ejecuta, pero no aparecen mensajes de retorno ni secuencias de comandos en la ventana del terminal. Una vez que el proxy de servicios web se ha desinstalado correctamente, aparece un símbolo del sistema en la ventana de terminal.

COMANDO RPM desinstal (sólo Linux)

Puede utilizar un comando RPM para desinstalar el proxy de servicios web de un sistema Linux.

Pasos

1. Abra una ventana de terminal.
2. Introduzca la siguiente línea de comandos:

```
rpm -e santricity_webservices
```

> El proceso de desinstalación podría dejar archivos que no formaban parte de la instalación original. Elimine manualmente estos archivos para quitar Web Services Proxy completamente.

Gestione el acceso de usuarios en el proxy de servicios web

Es posible gestionar el acceso de los usuarios a la API de servicios web y Unified Manager con fines de seguridad.

Información general sobre la gestión de acceso

La gestión de acceso incluye inicios de sesión basados en roles, cifrado de contraseña, autenticación básica e integración LDAP.

Acceso basado en funciones

El control de acceso basado en roles (RBAC) asocia usuarios predefinidos con roles. Cada función otorga permisos a un nivel específico de funcionalidad.

En la siguiente tabla se describe cada rol.

Función	Descripción
security.admin	SSL y gestión de certificados.
storage.admin	Acceso completo de lectura/escritura a la configuración del sistema de almacenamiento.
storage.monitor	Acceso de solo lectura para ver los datos del sistema de almacenamiento.
support.admin	Acceso a todos los recursos de hardware en los sistemas de almacenamiento y operaciones de soporte como la recuperación de AutoSupport (ASUP).

Las cuentas de usuario predeterminadas se definen en el archivo users.propertiesl. Se pueden cambiar cuentas de usuario modificando directamente el archivo users.properties o mediante las funciones Access Management en Unified Manager.

En la siguiente tabla, se enumeran los inicios de sesión de usuario disponibles para el proxy de servicios web.

Inicio de sesión de usuario predefinido	Descripción
admin	Un súper administrador que tiene acceso a todas las funciones e incluye todas las funciones. Para Unified Manager, debe establecer la contraseña en el inicio de sesión por primera vez.
Reducida	El administrador responsable de todo el aprovisionamiento de almacenamiento. Este usuario incluye los siguientes roles: Storage.admin, support.admin y Storage.monitor. Esta cuenta está deshabilitada hasta que se defina una contraseña.
seguridad	El usuario responsable de la configuración de seguridad. Este usuario incluye los siguientes roles: Security.admin y Storage.monitor. Esta cuenta está deshabilitada hasta que se defina una contraseña.
soporte técnico	El usuario responsable de los recursos de hardware, los datos de fallos y las actualizaciones de firmware. Este usuario incluye los siguientes roles: Support.admin y Storage.monitor. Esta cuenta está deshabilitada hasta que se defina una contraseña.
supervisar	Un usuario con acceso de solo lectura al sistema. Este usuario incluye únicamente el rol Storage.monitor. Esta cuenta está deshabilitada hasta que se defina una contraseña.
rw (heredado para matrices antiguas)	el usuario rw (lectura/escritura) incluye los siguientes roles: Storage.admin, support.admin y Storage.monitor. Esta cuenta está deshabilitada hasta que se defina una contraseña.
ro (heredado para cabinas antiguas)	El usuario ro (solo lectura) incluye únicamente el rol Storage.monitor. Esta cuenta está deshabilitada hasta que se defina una contraseña.

Cifrado de contraseñas

Para cada contraseña, puede aplicar un proceso de cifrado adicional mediante la codificación de contraseña SHA256 existente. Este proceso de cifrado adicional aplica un conjunto aleatorio de bytes a cada contraseña (Salt) para cada cifrado hash SHA256. El cifrado SHA256 salado se aplica a todas las contraseñas recién creadas.

> Antes de la versión 3.0 de Web Services Proxy, las contraseñas se cifraban sólo mediante hash SHA256. Todas las contraseñas cifradas SHA256 sólo hash conservan esta codificación y siguen siendo válidas en el archivo users.properties. Sin embargo, las contraseñas cifradas SHA256 sólo hash no son tan seguras como las contraseñas con cifrado SHA256 con salado.

Autenticación básica

De forma predeterminada, la autenticación básica está habilitada, lo que significa que el servidor devuelve un desafío de autenticación básico. Esta configuración se puede cambiar en el archivo wsconfig.xml.

LDAP

El proxy de servicios web habilita un protocolo ligero de acceso a directorios (LDAP), un protocolo de aplicación para acceder a servicios distribuidos de información de directorio y mantenerlos. La integración LDAP permite la autenticación de usuarios y la asignación de roles a grupos.

Para obtener información sobre la configuración de la funcionalidad LDAP, consulte las opciones de configuración en la interfaz de Unified Manager o en la sección LDAP de la documentación de API interactiva.

Configurar el acceso del usuario

Para gestionar el acceso de los usuarios, se puede aplicar cifrado adicional a las contraseñas, configurar la autenticación básica y definir el acceso basado en roles.

Aplicar cifrado adicional a las contraseñas

Para obtener el nivel más alto de seguridad, puede aplicar cifrado adicional a las contraseñas mediante la codificación de contraseña SHA256 existente.

Este proceso de cifrado adicional aplica un conjunto aleatorio de bytes a cada contraseña (Salt) para cada cifrado hash SHA256. El cifrado SHA256 salado se aplica a todas las contraseñas recién creadas.

Pasos

1. Abra el archivo users.properties, ubicado en:
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy\data\config
   - (Linux) — /opt/netapp/santricity_web_Services_proxy/data/config
2. Vuelva a introducir la contraseña cifrada como texto sin formato.
3. Ejecute el `securepasswds` Utilidad de línea de comandos para volver a cifrar la contraseña o simplemente reiniciar el proxy de servicios web. Esta utilidad se instala en el directorio raíz de instalación del proxy de servicios web.

> Como alternativa, es posible saldar y hash de contraseñas de usuario local siempre que se realice la edición de contraseñas mediante Unified Manager.

Configurar la autenticación básica

La autenticación básica predeterminada está habilitada, lo que significa que el servidor devuelve un desafío de autenticación básico. Si lo desea, puede cambiar esa configuración en el archivo wsconfig.xmlI.

1. Abra el archivo wsconfig.xml, ubicado en:
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_Services_proxy
2. Modifique la siguiente línea del archivo especificando false (no habilitado) o true (activado).

   Por ejemplo: `<env key="enable-basic-auth">true</env>`

3. Guarde el archivo.
4. Reinicie el servicio Webserver para que el cambio surta efecto.

Configure el acceso basado en roles

Para limitar el acceso de los usuarios a funciones específicas, puede modificar qué roles se especifican para cada cuenta de usuario.

El proxy de servicios web incluye el control de acceso basado en roles (RBAC), en el cual los roles están asociados con usuarios predefinidos. Cada función otorga permisos a un nivel específico de funcionalidad. Puede cambiar los roles asignados a las cuentas de usuario modificando directamente el archivo users.properties.

> También es posible cambiar las cuentas de usuario mediante Access Management en Unified Manager. Para obtener más información, consulte la ayuda en línea disponible con Unified Manager.

Pasos

1. Abra el archivo users.properties, ubicado en:
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy\data\config
   - (Linux) — /opt/netapp/santricity_web_Services_proxy/data/config
2. Busque la línea de la cuenta de usuario que desea modificar (almacenamiento, seguridad, supervisión, soporte, rw, o ro).

   > No modifique el usuario administrador. Se trata de un superusuario con acceso a todas las funciones.

3. Añada o quite los roles especificados, según lo desee.

   Entre los roles, se incluyen:

   - Security.admin — SSL y gestión de certificados.
   - Storage.admin — acceso completo de lectura/escritura a la configuración del sistema de almacenamiento.
   - Storage.monitor — acceso de solo lectura para ver los datos del sistema de almacenamiento.
   - Support.admin — brinda acceso a todos los recursos de hardware en los sistemas de almacenamiento y a operaciones de soporte como la recuperación AutoSupport (ASUP).

     > El rol Storage.monitor se requiere para todos los usuarios, incluido el administrador.

4. Guarde el archivo.

Gestione la seguridad y los certificados en el proxy de servicios web

Para obtener seguridad en el proxy de servicios web, es posible especificar una designación de puerto SSL y gestionar certificados. Los certificados identifican propietarios de sitios web para lograr conexiones seguras entre servidores y clientes.

Habilite SSL

El proxy de servicios web utiliza Secure Sockets Layer (SSL) para obtener seguridad, que se habilita durante la instalación. Puede cambiar la designación de puerto SSL en el archivo wsconfig.xml.

Pasos

1. Abra el archivo wsconfig.xml, ubicado en:
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_Services_proxy
2. Añada o cambie el número de puerto SSL, de forma similar al ejemplo siguiente:

```
<sslport clientauth="request">8443</sslport>
```

Resultado

Cuando el servidor se inicia con SSL configurado, el servidor busca los archivos del almacén de claves y del almacén de confianza.

- Si el servidor no encuentra un almacén de claves, el servidor utiliza la dirección IP de la primera dirección IPv4 no loopback detectada para generar un almacén de claves y, a continuación, añadir un certificado autofirmado al almacén de claves.
- Si el servidor no encuentra un almacén de confianza o no se especifica el almacén de confianza, el servidor utiliza el almacén de claves como almacén de confianza.

Omitir la validación del certificado

Para admitir conexiones seguras, el proxy de servicios web valida los certificados de los sistemas de almacenamiento con sus propios certificados de confianza. Si es necesario, puede especificar que el proxy omita esa validación antes de conectarse a los sistemas de almacenamiento.

Antes de empezar

- Todas las conexiones a los sistemas de almacenamiento deben ser seguras.

Pasos

1. Abra el archivo wsconfig.xml, ubicado en:
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_Services_proxy
2. Introduzca `true` en la `trust.all.arrays` entrada, como se muestra en el ejemplo:

```
<env key="trust.all.arrays">true</env>
```

3. Guarde el archivo.

Genere e importe un certificado de gestión de host

Los certificados identifican propietarios de sitios web para lograr conexiones seguras entre servidores y clientes. Para generar e importar certificados de una entidad de certificación (CA) para el sistema host donde está instalado el proxy de servicios web, puede usar extremos de API.

Para gestionar los certificados para el sistema host, debe realizar las siguientes tareas con la API:

- Cree una solicitud de firma de certificación (CSR) para el sistema host.

- Envíe el archivo CSR a una CA y espere que la autoridad envíe los archivos de certificado.
- Importe los certificados firmados al sistema host.

> También puede gestionar los certificados en la interfaz de Unified Manager. Para obtener más información, consulte la ayuda en línea disponible en Unified Manager.

Pasos

1. Inicie sesión en la "Documentación de API interactiva".
2. Vaya al menú desplegable de la parte superior derecha y seleccione **v2**.
3. Expanda el enlace **Administración** y desplácese hacia abajo hasta los puntos finales **/certificados**.
4. Genere el archivo CSR:
   a. Seleccione **POST:/certificates** y, a continuación, seleccione **probar**.

      El servidor web regenera un certificado autofirmado. A continuación, puede introducir información en los campos para definir el nombre común, la organización, la unidad de organización, el código alternativo y otra información utilizada para generar la CSR.

   b. Agregue la información necesaria en el panel **valores de ejemplo** para generar un certificado de CA válido y, a continuación, ejecute los comandos.

      > No llame a **POST:/certificates** o **POST:/certificates/reset** otra vez, o debe regenerar la CSR. Al llamar a **POST:/certificates** o **POST:/certificates/reset**, está generando un nuevo certificado autofirmado con una nueva clave privada. Si envía una CSR generada antes del último restablecimiento de la clave privada en el servidor, el nuevo certificado de seguridad no funciona. Debe generar una nueva CSR y solicitar un certificado de CA nuevo.

   c. Ejecute el extremo **GET:/certificates/Server** para confirmar que el estado actual del certificado es el certificado autofirmado con la información agregada del comando **POST:/certificates**.

      El certificado de servidor (indicado por el alias `jetty`) sigue siendo auto-firmado en este punto.

   d. Expanda el extremo **POST:/certificates/export**, seleccione **Inténtelo**, introduzca un nombre de archivo para el archivo CSR y, a continuación, haga clic en **Ejecutar**.
5. Copie y pegue el `fileUrl` En una nueva pestaña del explorador para descargar el archivo CSR y enviar el archivo CSR a una CA válida para solicitar una nueva cadena de certificados de servidor web.
6. Cuando la CA emita una nueva cadena de certificados, use una herramienta del administrador de certificados para extraer los certificados de servidor web, intermedios y raíz, y, a continuación, los importe al servidor del proxy de servicios web:
   a. Expanda el extremo **POST:/sslconfig/Server** y seleccione **probar fuera**.
   b. Introduzca un nombre para el certificado raíz de CA en el campo **alias**.
   c. Seleccione **false** en el campo **placaceMainServerCertificate**.
   d. Vaya a y seleccione el nuevo certificado raíz de CA.
   e. Haga clic en **Ejecutar**.
   f. Confirme que la carga del certificado se ha realizado correctamente.
   g. Repita el procedimiento de carga del certificado de CA para el certificado intermedio de CA.

h. Repita el procedimiento de carga del certificado para el nuevo archivo de certificado de seguridad del servidor web, excepto en este paso, seleccione **true** en el menú desplegable **placeeMainServerCertificate**.

i. Confirme que la importación del certificado de seguridad del servidor web se ha realizado correctamente.

j. Para confirmar que los nuevos certificados raíz, intermedios y de servidor web están disponibles en el almacén de claves, ejecute **GET:/certificates/Server**.

7. Seleccione y expanda el punto final **POST:/certificates/reload** y, a continuación, seleccione **probar**. Cuando se le solicite, si desea reiniciar ambos controladores o no, seleccione **falso**. ("Verdadero" sólo se aplica en el caso de los controladores de matriz doble.) Haga clic en **Ejecutar**.

   El punto final **/certificates/reload** normalmente devuelve una respuesta http 202 correcta. Sin embargo, la recarga del almacén de confianza del servidor web y los certificados del almacén de claves crean una condición de carrera entre el proceso de API y el proceso de recarga de certificados del servidor web. En raras ocasiones, la recarga de certificados del servidor web puede superar el procesamiento de la API. En este caso, la recarga parece fallar aunque se haya completado correctamente. Si esto ocurre, continúe con el siguiente paso de todos modos. Si la recarga realmente falló, el siguiente paso también falla.

8. Cierre la sesión de explorador actual con el proxy de servicios web, abra una sesión de explorador nueva y confirme que se puede establecer una nueva conexión con el proxy de servicios web.

   Mediante el uso de una sesión de exploración incognito o en privado, puede abrir una conexión al servidor sin utilizar los datos guardados de sesiones de exploración anteriores.

Gestione los sistemas de almacenamiento mediante Web Services Proxy

Para gestionar los sistemas de almacenamiento en la red, primero debe detectarlos y después añadirlos a la lista de gestión.

Detectar sistemas de almacenamiento

Es posible establecer la detección automática o detectar manualmente los sistemas de almacenamiento.

Detección automática de sistemas de almacenamiento

Se puede especificar que los sistemas de almacenamiento se detecten automáticamente en la red mediante la modificación de la configuración del archivo wsconfig.xml. De manera predeterminada, la detección automática de IPv6 está deshabilitada y IPv4 está habilitada.

Solo debe proporcionar una dirección IP o DNS de gestión para añadir un sistema de almacenamiento. El servidor detecta automáticamente todas las rutas de administración cuando las rutas no están configuradas o las rutas están configuradas y podridas.

> Si intenta utilizar un protocolo IPv6 para detectar automáticamente sistemas de almacenamiento de la configuración de la controladora después de establecer una conexión inicial, es posible que se produzca un error en el proceso. Entre las posibles causas de este fallo se encuentran problemas durante el reenvío de direcciones IP o la activación de IPv6 en los sistemas de almacenamiento, pero no la activación en el servidor.

Antes de empezar

Antes de habilitar la configuración de detección IPv6, compruebe que la infraestructura admite conectividad

IPv6 con los sistemas de almacenamiento para mitigar cualquier problema de conexión.

Pasos

1. Abra el archivo wsconfig.xml, ubicado en:
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_Services_proxy
2. En las cadenas de detección automática, cambie la configuración desde `true` para `false`, según se desee. Vea el ejemplo siguiente.

```
<env key="autodiscover.ipv6.enable">true</env>
```

> Cuando las rutas están configuradas, pero no configuradas para que el servidor pueda enrutar a las direcciones, se producen errores intermitentes de conexión. Si no puede configurar las direcciones IP para que se puedan enrutar desde el host, desactive la detección automática (cambie la configuración a. `false`).

3. Guarde el archivo.

Detectar y añadir sistemas de almacenamiento con extremos API

Puede usar extremos de API para detectar y añadir sistemas de almacenamiento en la lista gestionada. Este procedimiento crea una conexión de gestión entre el sistema de almacenamiento y la API.

> En esta tarea, se describe cómo detectar y añadir sistemas de almacenamiento mediante la API DE REST, para poder gestionar estos sistemas en la documentación de API interactiva. Sin embargo, es posible que se desee gestionar sistemas de almacenamiento en Unified Manager, que proporciona una interfaz fácil de usar. Para obtener más información, consulte la ayuda en línea disponible con Unified Manager.

Antes de empezar

Para los sistemas de almacenamiento con SANtricity versión 11.30 y posteriores, debe habilitarse la interfaz de gestión heredada para Symbol en la interfaz de SANtricity System Manager. De lo contrario, los extremos de detección se fallarán. Para encontrar este ajuste, abra System Manager y vaya a MENU:Configuración[sistema > Configuración adicional > Cambiar interfaz de gestión].

Pasos

1. Inicie sesión en la "Documentación de API interactiva".
2. Detecte los sistemas de almacenamiento:
   a. En la documentación de la API, asegúrese de que **V2** está seleccionado en la lista desplegable y, a continuación, expanda la categoría **sistemas de almacenamiento**.
   b. Haga clic en el punto final **POST: /Discovery** y, a continuación, haga clic en **Inténtelo**.
   c. Introduzca los parámetros como se describe en la tabla.

IP inicial
IP final

	Reemplace string por el rango de direcciones IP inicial y final para uno o más sistemas de almacenamiento en la red.
	UseAgents
	Establezca este valor en: • True = utilizar agentes en banda para la exploración de red. • False = no utilice agentes en banda para la exploración de red.
	ConnectionTimeout
	Introduzca los segundos permitidos para la exploración antes de que se agote el tiempo de espera de la conexión.
	MaxPortsToUse
	Introduzca un número máximo de puertos utilizados para la exploración de red.

d. Haga clic en **Ejecutar**.

> Las acciones de API se ejecutan sin las peticiones del usuario.

El proceso de detección se ejecuta en segundo plano.

a. Asegúrese de que el código devuelve un 202.
b. En **cuerpo de respuesta**, busque el valor devuelto para el Id. De solicitud. Necesita el ID de solicitud para ver los resultados en el siguiente paso.

3. Vea los resultados de la detección de la siguiente manera:
   a. Haga clic en el punto final **GET: /Discovery** y, a continuación, haga clic en **Inténtelo**.
   b. Introduzca el ID de solicitud del paso anterior. Si deja el **ID de solicitud** en blanco, el extremo tomará por defecto el último ID de solicitud ejecutado.
   c. Haga clic en **Ejecutar**.
   d. Asegúrese de que el código devuelve 200.
   e. En el cuerpo de respuesta, busque su ID de solicitud y las cadenas de sistemas de almacenamiento. Las cadenas tienen un aspecto similar al siguiente ejemplo:

```
"storageSystems": [
    {
      "serialNumber": "123456789",
      "wwn": "000A011000AF0000000000001A0C000E",
      "label": "EF570_Array",
      "firmware": "08.41.10.01",
      "nvsram": "N5700-841834-001",
      "ipAddresses": [
        "10.xxx.xx.213",
        "10.xxx.xx.214"
      ],
```

f. Escriba los valores para wwn, etiqueta e direcciones IP. Se necesitan para el siguiente paso.

4. Añada los sistemas de almacenamiento de la siguiente manera:
   a. Haga clic en el extremo **POST: /Storage-system** y, a continuación, haga clic en **probar fuera**.
   b. Introduzca los parámetros como se describe en la tabla.

id
Introduzca un nombre único para este sistema de almacenamiento. Puede introducir la etiqueta (que se muestra en LA respuesta DE GET: /Discovery), pero el nombre puede ser cualquier cadena que elija. Si no proporciona un valor para este campo, Web Services asigna automáticamente un identificador exclusivo.
ControladorAddresses
Introduzca las direcciones IP que se muestran en la respuesta PARA GET: /Discovery. En el caso de controladoras dobles, las direcciones IP deben separarse con una coma. Por ejemplo: `"IP address 1","IP address 2"`
validar
Introduzca `true`, Para recibir la confirmación de que los servicios Web se pueden conectar al sistema de almacenamiento.
contraseña
Introduzca la contraseña de administración para el sistema de almacenamiento.
wwn
Introduzca el WWN del sistema de almacenamiento (se muestra en la respuesta PARA GET: /Discovery).

c. Quite todas las cadenas después `"enableTrace": true`, de forma que todo el conjunto de cadenas sea similar al ejemplo siguiente:

```
{
  "id": "EF570_Array",
  "controllerAddresses": [
    "Controller-A-Mgmt-IP","Controller-B-Mgmt_IP"
  ],
  "validate":true,
  "password": "array-admin-password",
  "wwn": "000A011000AF0000000000001A0C000E",
  "enableTrace": true
}
```

d. Haga clic en **Ejecutar**.

e. Asegúrese de que la respuesta de código es 201, lo que indica que el punto final se ha ejecutado correctamente.

   El punto final **Post: /Storage-systems** está en cola. Puede ver los resultados utilizando el extremo **GET: /Storage-systems** en el siguiente paso.

5. Confirme la adición de la lista de la siguiente manera:

   a. Haga clic en el extremo **GET: /Storage-system**.

      No es necesario ningún parámetro.

   b. Haga clic en **Ejecutar**.

   c. Asegúrese de que la respuesta de código es 200, lo que indica que el punto final se ha ejecutado correctamente.

   d. En el cuerpo de respuesta, busque la información del sistema de almacenamiento. Los valores devueltos indican que se agregó correctamente a la lista de cabinas gestionadas, de forma similar al siguiente ejemplo:

```
[
  {
    "id": "EF570_Array",
    "name": "EF570_Array",
    "wwn": "000A011000AF0000000000001A0C000E",
    "passwordStatus": "valid",
    "passwordSet": true,
    "status": "optimal",
    "ip1": "10.xxx.xx.213",
    "ip2": "10.xxx.xx.214",
    "managementPaths": [
      "10.xxx.xx.213",
      "10.xxx.xx.214"
  ]
  }
]
```


Escale verticalmente el número de sistemas de almacenamiento gestionados

De forma predeterminada, la API puede gestionar hasta 100 sistemas de almacenamiento. Si necesita administrar más, debe mejorar los requisitos de memoria para el servidor.

El servidor está configurado para utilizar 512 MB de memoria. Por cada 100 sistemas de almacenamiento adicionales de la red, añada 250 MB a ese número. No añada más memoria de la que tiene físicamente. Deje suficiente espacio adicional para su sistema operativo y otras aplicaciones.

> El tamaño predeterminado de la caché es de 8,192 eventos. El uso aproximado de datos de la caché de eventos MEL es de 1 MB por cada 8,192 eventos. Por tanto, si se conservan los valores predeterminados, el uso de caché debe ser de 1 MB aproximadamente para un sistema de almacenamiento.

> Además de la memoria, el proxy utiliza puertos de red para cada sistema de almacenamiento. Linux y Windows consideran los puertos de red como identificadores de archivos. Como medida de seguridad, la mayoría de los sistemas operativos limitan el número de identificadores de archivos abiertos que un proceso o un usuario pueden tener abiertos al mismo tiempo. Especialmente en entornos Linux, donde se considera que las conexiones TCP abiertas son identificadores de archivos, el proxy de servicios web puede superar fácilmente este límite. Dado que la corrección depende del sistema, debe consultar la documentación del sistema operativo para obtener información sobre cómo elevar este valor.

Pasos

1. Debe realizar una de las siguientes acciones:
   - En Windows, vaya al archivo appserver64.init. Localizar la línea, `vmarg.3=-Xmx512M`
   - En Linux, vaya al archivo webserver.shl. Localizar la línea, `JAVA_OPTIONS="-Xmx512M"`
2. Para aumentar la memoria, reemplace `512` Con la memoria deseada en MB.

3. Guarde el archivo.

Administrar el sondeo automático para las estadísticas del proxy de servicios web

Es posible configurar el sondeo automático para todas las estadísticas de disco y volumen en sistemas de almacenamiento detectados.

Descripción general de las estadísticas

Las estadísticas proporcionan información acerca de las tasas de recogida de datos y el rendimiento de los sistemas de almacenamiento.

El proxy de servicios web proporciona acceso a los siguientes tipos de estadísticas:

- Estadísticas sin procesar — total de contadores para puntos de datos en el momento de la recopilación de datos. Las estadísticas sin configurar se pueden utilizar para operaciones de lectura totales o operaciones de escritura totales.
- Estadísticas analizadas: Información calculada para un intervalo. Los ejemplos de estadísticas analizadas son operaciones de entrada/salida (IOPS) de lectura por segundo o rendimiento de escritura.

Las estadísticas sin procesar son lineales y normalmente requieren al menos dos puntos de datos recopilados para derivar datos utilizables de ellos. Las estadísticas analizadas son una derivación de las estadísticas sin procesar, que proporcionan mediciones importantes. Muchos valores que pueden derivarse de las estadísticas sin configurar se muestran en un formato utilizable y momento específico en las estadísticas analizadas para su comodidad.

Es posible recuperar las estadísticas sin procesar independientemente de si el sondeo automático está habilitado o no. Puede agregar el `usecache=true` Cadena de consulta al final de la URL para recuperar las estadísticas en caché del último sondeo. El uso de resultados almacenados en la caché aumenta significativamente el rendimiento de la recuperación de estadísticas. Sin embargo, varias llamadas a una velocidad igual o inferior a la caché de intervalos de sondeo configurada recuperan los mismos datos.

Funcionalidad de estadísticas

El proxy de servicios web proporciona extremos API que permiten recuperar estadísticas sin configurar y analizadas de la controladora y la interfaz desde los modelos de hardware y las versiones de software compatibles.

API de estadísticas sin procesar

- `/storage-systems/{system-id}/controller-statistics`
- `/storage-systems/{system-id}/drive-statistics/{optional list of disk ids}`
- `/storage-systems/{system-id}/interface-statistics/{optional list of interface ids}`
- `/storage-systems/{system-id}/volume-statistics/{optional list of volume ids}`

API de estadísticas analizadas

- `/storage-systems/{id}/analysed-controller-statistics/`
- `/storage-systems/{id}/analysed-drive-statistics/{optional list of disk ids}`

- `/storage-systems/{id}/analysed-interface-statistics/{optional list of interface ids}`
- `/storage-systems/{id}/analysed-volume-statistics/{optional list of volume ids}`

Estas URL recuperan las estadísticas analizadas de la última encuesta y sólo están disponibles cuando se activa el sondeo. Estas direcciones URL incluyen los siguientes datos de entrada y salida:

- Operaciones por segundo
- Rendimiento en megabytes por segundo
- Tiempos de respuesta en milisegundos

Los cálculos se basan en las diferencias entre las iteraciones estadísticas de sondeo, que son las medidas más comunes de rendimiento de almacenamiento. Estas estadísticas son preferibles a las estadísticas no analizadas.

> Cuando se inicia el sistema, no hay ninguna recopilación de estadísticas anterior que utilizar para calcular las diversas métricas, por lo que las estadísticas analizadas requieren al menos un ciclo de sondeo tras el inicio para devolver los datos. Además, si se restablecen los contadores acumulativos, el siguiente ciclo de sondeo tendrá números impredecibles para los datos.

Configurar intervalos de sondeo

Para configurar los intervalos de sondeo, modifique el archivo wsconfig.xml para especificar un intervalo de sondeo en segundos.

> Debido a que las estadísticas se almacenan en la memoria caché, es posible que observe un aumento de aproximadamente 1.5 MB de uso de memoria para cada sistema de almacenamiento.

Antes de empezar

- El proxy debe detectar los sistemas de almacenamiento.

Pasos

1. Abra el archivo wsconfig.xml, ubicado en:
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_Services_proxy
2. Añada la siguiente línea dentro del `<env-entries>` etiquetar, en el que `n` es el número de segundos para el intervalo entre las solicitudes de sondeo:

   ```
   <env key="stats.poll.interval">n</env>
   ```

   Por ejemplo, si se introduce 60, el sondeo comienza a intervalos de 60 segundos. Es decir, el sistema solicita que el sondeo comience 60 segundos después de haber finalizado el periodo de sondeo anterior (independientemente de la duración del periodo de sondeo anterior). Todas las estadísticas están impresas con el tiempo exacto en que fueron recuperadas. El sistema utiliza la Marca de tiempo o la diferencia de tiempo en la que se basa el cálculo de 60 segundos.

3. Guarde el archivo.

Gestione AutoSupport mediante Web Services Proxy

Es posible configurar AutoSupport (ASUP), que recoge datos y luego envía automáticamente esos datos al soporte técnico para la solución de problemas y el análisis de problemas remotos.

Información general de AutoSupport (ASUP)

La función AutoSupport (ASUP) transmite automáticamente los mensajes a NetApp en función de criterios manuales o basados en programaciones.

Cada mensaje de AutoSupport es una colección de archivos de registro, datos de configuración, datos de estado y métricas de rendimiento. De forma predeterminada, AutoSupport transmite los archivos de la siguiente tabla al equipo de soporte de NetApp una vez por semana.

Nombre de archivo	Descripción
x-headers-data.txt	Archivo .txt que contiene la información del encabezado X.
manifest.xml	Archivo .xml en el que se detalla el contenido del mensaje.
arraydata.xml	Un archivo .xml que contiene la lista de datos persistentes del cliente.
appserver-config.txt	Archivo .txt que contiene datos de configuración del servidor de aplicaciones.
wsconfig.txt	Archivo .txt que contiene los datos de configuración del servicio web.
host-info.txt	Un archivo .txt que contiene información sobre el entorno del host.
server-logs.7z	Archivo .7z que contiene cada archivo de registro de servidor web disponible.
client-info.txt	Archivo .txt con pares de clave/valor arbitrarios para contadores específicos de aplicaciones como búsquedas de método y de página web.
webservices-profile.json	Estos archivos contienen datos de perfil de WebServices y datos estadísticos de control de Jersey. De forma predeterminada, las estadísticas de supervisión de Jersey están habilitadas. Puede habilitarlos y deshabilitarlos en el archivo wsconfig.xml de la siguiente manera: • Habilitar: `<env key="enable.jersey.statistics">true</env>` • Desactivar: `<env key="enable.jersey.statistics">false</env>`

Configure AutoSupport

AutoSupport está habilitado de forma predeterminada en la instalación; sin embargo, puede cambiar esa configuración o modificar los tipos de entrega.

Habilite o deshabilite AutoSupport

La función AutoSupport está habilitada o deshabilitada durante la instalación inicial del proxy de servicios web, pero puede cambiar esa configuración en el archivo ASUPConfig.

Puede habilitar o deshabilitar AutoSupport a través del archivo ASUPConfig.xml, como se describe en los pasos siguientes. Como alternativa, puede activar o desactivar esta función a través de la API mediante **Configuración** y **POST/asup** y, a continuación, introduciendo "verdadero" o "falso".

1. Abra el archivo ASUPConfig.xml en el directorio de trabajo.
2. Busque las líneas de <asupdata enable="Boolean_value" timestamp="timestamp">
3. Introduzca `true` (activar) o. `false` (desactivar). Por ejemplo:

```
<asupdata enabled="false" timestamp="0">
```

> La entrada de Marca de hora es superflua.

4. Guarde el archivo.

Configurar el método de entrega de AutoSupport

Es posible configurar la función AutoSupport para que use los métodos de entrega HTTPS, HTTP o SMTP. HTTPS es el método de entrega predeterminado.

1. Acceda al archivo ASUPConfig.xml del directorio de trabajo.
2. En la cadena, `<delivery type="n">`, escriba 1, 2 o 3 como se describe en la tabla:

Valor	Descripción
1	**HTTPS** (predeterminado) <delivery type="1">
2	**HTTP** <delivery type="2">

Valor	Descripción

3	**SMTP** — para configurar correctamente el tipo de entrega de AutoSupport a SMTP, debe incluir la dirección del servidor de correo SMTP, junto con los correos electrónicos del remitente y del usuario destinatario, de forma similar al ejemplo siguiente:
	
	`<delivery type="3">`
	`<smtp>`
	`<mailserver>smtp.example.com</mailserver>`
	`<sender>user@example.com</sender>`
	`<replyto>user@example.com</replyto>`
	`</smtp>`
	`</delivery>`

Mirroring de volumen remoto

Información general sobre volúmenes de almacenamiento remoto

Utilice la función volúmenes de almacenamiento remoto de SANtricity® para importar datos desde un dispositivo de almacenamiento remoto directamente a un volumen de E-Series local. Esta función permite agilizar el proceso de actualizaciones de equipos y proporciona funcionalidades de migración de datos para mover datos desde dispositivos que no son E-Series a sistemas E-Series.

Información general de configuración

La función almacenamiento remoto volúmenes está disponible con SANtricity System Manager en los identificadores de submodelo seleccionados. Para utilizar esta función, debe configurar un sistema de almacenamiento remoto y un sistema de almacenamiento E-Series para que se comuniquen entre sí.

Use el siguiente flujo de trabajo:

1. "Revise los requisitos y las restricciones".
2. "Configure el hardware".
3. "Importe el almacenamiento remoto".

Obtenga más información

- Ayuda en línea, disponible en la interfaz de usuario de System Manager o en la "Sitio de documentación del software SANtricity".
- Para obtener información técnica adicional sobre la función almacenamiento remoto volúmenes, consulte "Informe técnico sobre volúmenes de almacenamiento remotos".

Requisitos y restricciones para el almacenamiento remoto

Antes de configurar la función volúmenes de almacenamiento remoto, revise los siguientes requisitos y restricciones.

Requisitos de hardware

Protocolos compatibles

En el lanzamiento inicial de la función volúmenes de almacenamiento remoto, la compatibilidad solo está disponible para los protocolos iSCSI y IPv4.

Consulte la "Herramienta de matriz de interoperabilidad de NetApp" Para obtener información actualizada sobre soporte y configuración entre el host y la cabina E-Series (destino) utilizada para la función volúmenes de almacenamiento remoto.

Requisitos del sistema de almacenamiento

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.

Requisitos del volumen

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 se inicia 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.

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.

Preparación para las importaciones de producción

Debe realizar una prueba o una importación de "ejecución en seco" antes de importar la producción para verificar la configuración correcta del almacenamiento y del tejido.

Muchas variables pueden afectar a la operación de importación y al tiempo de finalización. Para garantizar que una importación de producción tenga éxito y obtener una estimación de la duración, puede utilizar estas importaciones de prueba para asegurarse de que todas las conexiones están funcionando como se espera y la operación de importación se está completando en un período de tiempo adecuado. A continuación, puede realizar ajustes para lograr los resultados deseados antes de iniciar la importación de producción.

Configurar hardware para volúmenes de almacenamiento remoto

El sistema de almacenamiento E-Series debe configurarse para comunicarse con el sistema de almacenamiento remoto a través del protocolo iSCSI compatible.

Configuración del dispositivo de almacenamiento remoto y de la cabina E-Series

Antes de continuar con SANtricity System Manager para configurar la función almacenamiento remoto volúmenes, haga lo siguiente:

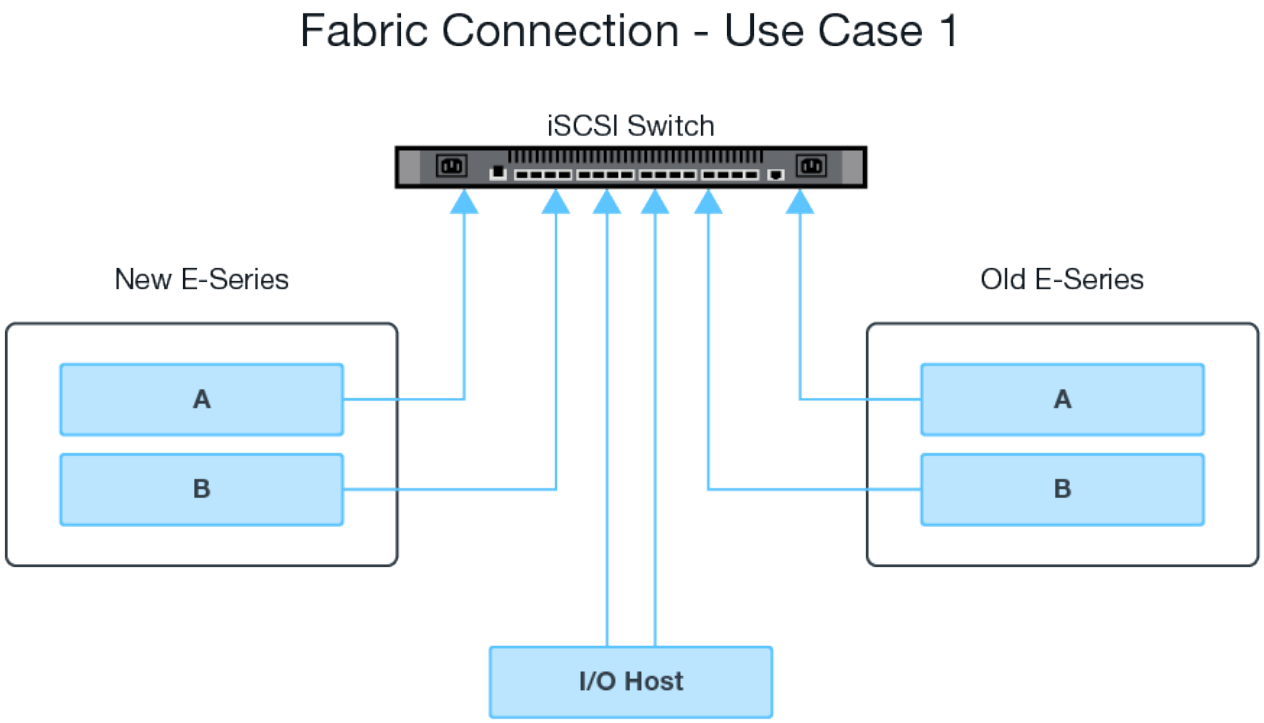
1. Establecer manualmente una conexión por cable entre el sistema E-Series y el sistema de almacenamiento remoto, de modo que los dos sistemas se puedan configurar para comunicarse a través de iSCSI.
2. Configure los puertos iSCSI de modo que el sistema E-Series y el sistema de almacenamiento remoto se puedan comunicar de forma correcta entre sí.
3. Obtenga el IQN del sistema E-Series.
4. Hacer que el sistema E-Series sea visible para el sistema de almacenamiento remoto. Si el sistema de almacenamiento remoto es un sistema E-Series, cree un host mediante el IQN del sistema E-Series de destino como información de conexión del puerto de host.
5. Si un host/aplicación está utilizando el dispositivo de almacenamiento remoto:
   - Detenga las operaciones de I/o en el dispositivo de almacenamiento remoto.
   - Desasigne/desmonte el dispositivo de almacenamiento remoto.
6. Asigne el dispositivo de almacenamiento remoto al host definido para el sistema de almacenamiento E-Series.
7. Obtenga el número de LUN del dispositivo utilizado para la asignación.

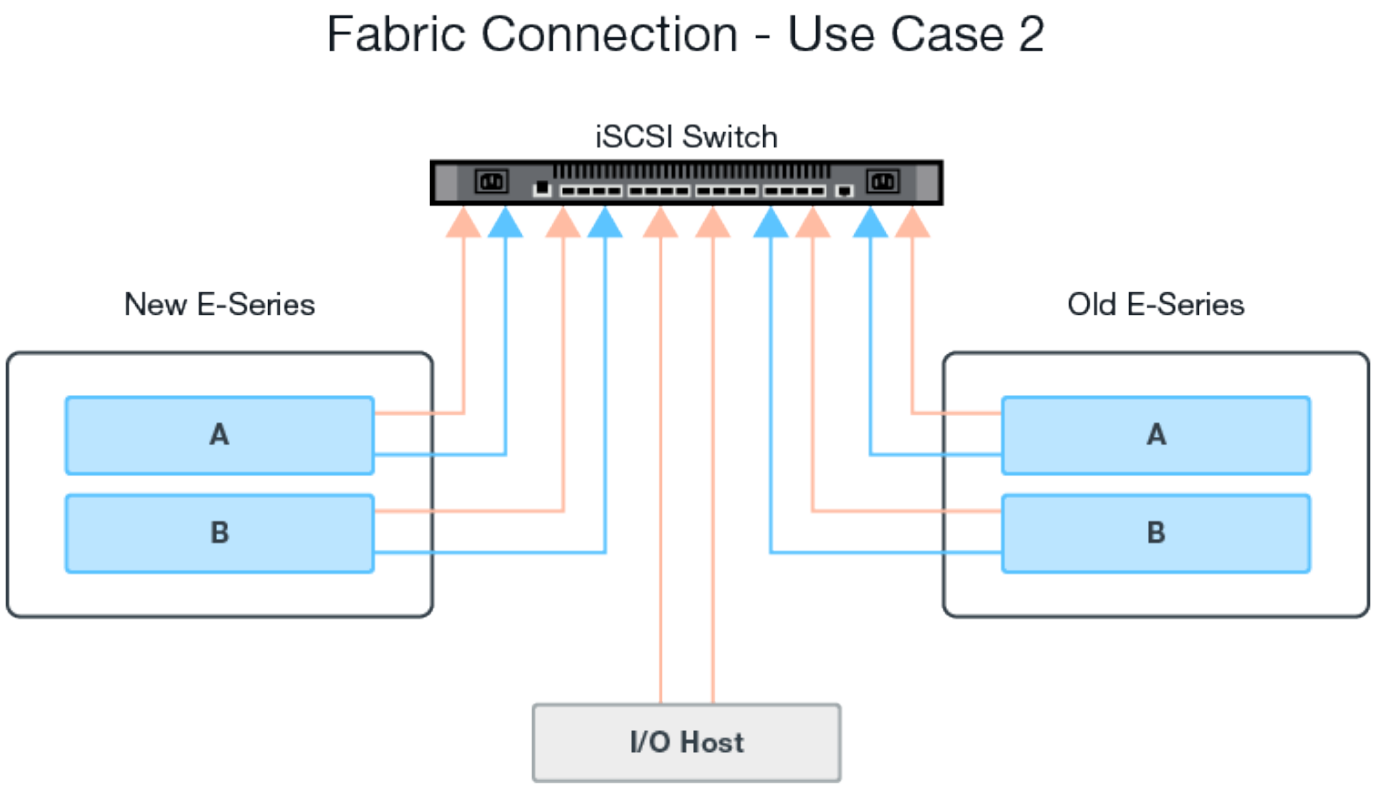
> Recomendación: Realice un backup del volumen de origen remoto antes de iniciar el proceso de importación.

Conecte los cables de las cabinas de almacenamiento

Como parte del proceso de configuración, las cabinas de almacenamiento y el host de I/o deben cablearse a la interfaz compatible con iSCSI.

Los diagramas siguientes proporcionan ejemplos de cómo conectar los sistemas de manera que realicen operaciones de volumen de almacenamiento remoto a través de una conexión iSCSI.





Configure los puertos iSCSI

Debe configurar los puertos iSCSI para garantizar la comunicación entre el destino (cabina de

almacenamiento E-Series local) y el origen (cabina de almacenamiento remota).

Los puertos iSCSI pueden configurarse de varias maneras según la subred. A continuación, se muestran algunos ejemplos de cómo configurar los puertos iSCSI para su uso con la función volúmenes de almacenamiento remoto.

Origen A	Fuente B	Destino a	Objetivo B
10.10.1.100/22	10.10.2.100/22	10.10.1.101/22	10.10.2.101/22

Origen A	Fuente B	Destino a	Objetivo B
10.10.0.100/16	10.10.0.100/16	10.10.0.101/16	10.10.0.101/16

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 en la interfaz de usuario de SANtricity System Manager.

Lo que necesitarás

- El sistema de almacenamiento E-Series debe estar configurado para comunicarse con el sistema de almacenamiento remoto. Consulte "Configure el hardware".
- 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. 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 y restricciones".
- Recomendación: Realice un backup 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.

> Debido a que muchas variables pueden afectar a la operación de importación y a su tiempo de finalización, primero debe realizar 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. En el Administrador del sistema de SANtricity, haga clic en **almacenamiento > almacenamiento remoto**.
2. Haga clic en **Importar almacenamiento remoto**.

   Se muestra el asistente para importar el almacenamiento remoto.

3. En el paso 1a del panel Configurar origen, introduzca la información de conexión.

   a. En el campo **Nombre**, introduzca el nombre del dispositivo de almacenamiento remoto.
   b. En **Propiedades de conexión iSCSI**, introduzca lo siguiente para el dispositivo de almacenamiento remoto: IQN, dirección IP y número de puerto (el valor predeterminado es 3260).

      Si desea agregar otra conexión iSCSI, haga clic en **+Agregar otra dirección IP** para incluir una dirección IP adicional para el almacenamiento remoto. Cuando haya terminado, haga clic en **Siguiente**.

   Después de hacer clic en Siguiente, se muestra el paso 1b del panel Configurar origen.

4. En el campo **LUN**, seleccione el LUN de origen deseado para el dispositivo de almacenamiento remoto 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 la pantalla Revisión, compruebe que los ajustes de dispositivo de almacenamiento remoto, destino e importación especificados son precisos. Haga clic en **Finalizar** para completar la creación del almacenamiento remoto.

   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, vuelve al 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.

   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.

9. 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.

Gestionar el progreso de importación

Una vez que comienza el proceso de importación, puede ver y actuar sobre su progreso.

Para cada operación de importación, la página 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 puede ver Operaciones en curso desde la página de inicio (**Inicio > Mostrar operaciones en curso**).

Pasos

1. En el Administrador del sistema de SANtricity, vaya a la página almacenamiento remoto y seleccione **Ver operaciones**.

   Se muestra el cuadro de diálogo Operaciones en curso.

2. Si lo desea, use los enlaces 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 se dejó. A continuación, aplique una prioridad a la operación Reanudar y, a continuación, haga clic en **Aceptar**.

     La operación Reanudar **no** 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 de almacenamiento remoto

Es posible editar, añadir o eliminar la configuración de conexión para cualquier configuración de almacenamiento remoto mediante la opción Ver/editar configuración.

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. En la pantalla almacenamiento remoto de SANtricity System Manager, seleccione el objeto de almacenamiento remoto que desee en la sección de lista de resultados.
2. Haga clic en **Ver/editar configuración**.

   Se mostrará la pantalla Remote Storage Settings.

3. 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.

4. 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 y la 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.
5. 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.

Pasos

1. Asegúrese de que no haya importaciones asociadas con el objeto de almacenamiento remoto que desee quitar.
2. En la pantalla almacenamiento remoto de SANtricity System Manager, seleccione el objeto de almacenamiento remoto que desee en la sección de lista de resultados.
3. Haga clic en **Quitar**.

   Aparecerá el cuadro de diálogo Confirmar eliminación de conexión de almacenamiento remota.

4. Confirme la operación escribiendo `remove` Y, a continuación, haga clic en **Quitar**.

   Se elimina el objeto de almacenamiento remoto seleccionado.

Complemento de almacenamiento para vCenter

Información general del complemento de almacenamiento para vCenter

El complemento de almacenamiento de SANtricity para vCenter proporciona gestión integrada de las cabinas de almacenamiento E-Series desde una sesión de VMware vSphere Client.

Tareas disponibles

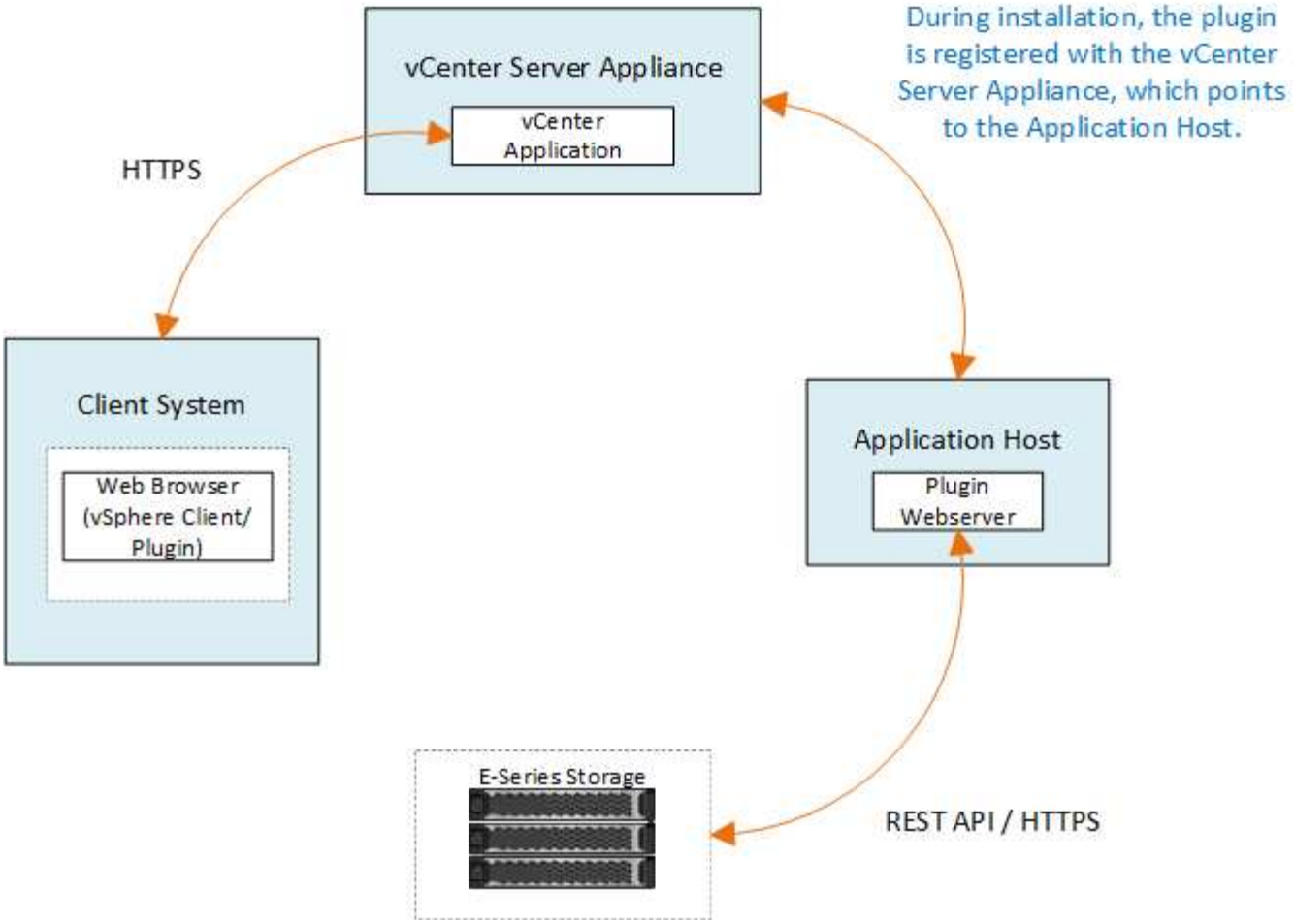
Puede utilizar el plugin para realizar las siguientes tareas:

- Vea y gestione cabinas de almacenamiento detectadas en la red.
- Realizar operaciones de lotes en grupos de varias cabinas de almacenamiento.
- Realizar actualizaciones en el sistema operativo de software.
- Importe la configuración de una cabina de almacenamiento a otra.
- Configurar volúmenes, caché SSD, hosts, clústeres de hosts, pools, y grupos de volúmenes.
- Inicie la interfaz de System Manager para realizar tareas de gestión adicionales en una cabina.

> El plugin no es un reemplazo directo de la interfaz de System Manager, que se integra en cada controladora de una cabina de almacenamiento. System Manager proporciona funciones de gestión adicionales; si lo desea, puede abrir System Manager seleccionando una matriz de almacenamiento en la vista principal del plugin y haciendo clic en **Iniciar**.

El plugin requiere que se haya implementado un dispositivo VMware vCenter Server en el entorno de VMware y un host de aplicaciones para instalar y ejecutar el servidor web del plugin.

Consulte la siguiente figura para obtener más información sobre la comunicación en el entorno vCenter.



Información general de la interfaz

Al iniciar sesión en el plugin, la página principal se abre en **Administrar - todo**. En esta página, es posible ver y gestionar todas las cabinas de almacenamiento detectadas en la red.

Barra lateral Navegación

La barra lateral de navegación muestra lo siguiente:

- **Gestionar**: Permite detectar las cabinas de almacenamiento en la red, iniciar System Manager para una cabina, importar la configuración de una cabina a varias, gestionar grupos de cabinas, actualizar el sistema operativo SANtricity y aprovisionar almacenamiento.
- **Administración de certificados** — Administrar certificados para autenticar entre exploradores y clientes.
- **Operaciones** — Ver el progreso de las operaciones por lotes, como importar la configuración de una matriz a otra.

> Algunas operaciones no están disponibles si una cabina de almacenamiento no tiene un estado óptimo.

- **Soporte** — Ver opciones de soporte técnico, recursos y contactos.

Exploradores compatibles

A partir de varios tipos de exploradores, se puede acceder al complemento de almacenamiento para vCenter.

Se admiten los siguientes exploradores en las versiones mencionadas.

- Google Chrome 89 o posterior
- Mozilla Firefox 80 o posterior
- Microsoft Edge 90 o posterior

Roles y permisos de usuario

Para acceder a las tareas del complemento de almacenamiento para vCenter, el usuario debe tener permisos de lectura y escritura. De forma predeterminada, todos los ID de usuario de VMware vCenter definidos no tienen permisos para realizar tareas en el plugin.

Información general de configuración

La configuración incluye los pasos siguientes:

1. "Instale y registre el complemento".
2. "Configure los permisos de acceso al complemento".
3. "Inicie sesión en la interfaz del complemento".
4. "Detectar las cabinas de almacenamiento".
5. "Aprovisionar almacenamiento".

Obtenga más información

Para obtener más información sobre la gestión de almacenes de datos en vSphere Client, consulte "Documentación de VMware vSphere".

Manos a la obra

Revise los requisitos de instalación y actualización

Antes de instalar o actualizar el complemento de almacenamiento de SANtricity para vCenter, revise los requisitos de instalación y las consideraciones sobre actualizaciones.

Requisitos de instalación

Puede instalar y configurar el complemento de almacenamiento para vCenter en un sistema host de Windows. La instalación del plugin incluye los siguientes requisitos.

Requisito	Descripción
Versiones compatibles	• Versiones compatibles de VMware vCenter Server Appliance: 6.7U3J, 7.0U1, 7.0U2, 7.0U3 y 8.0. • Versión de sistema operativo SANtricity de NetApp: 11.60.2 o posterior • Versiones de host de aplicaciones compatibles: Windows 2016, Windows 2019, Windows 2022. Para obtener más información acerca de la compatibilidad, consulte "Herramienta de matriz de interoperabilidad de NetApp".
Múltiples instancias	Solo puede instalar una instancia de Storage Plugin para vCenter en un host de Windows y solo puede registrarla en una instancia de vcsa.
Planificación de la capacidad	El complemento de almacenamiento para vCenter requiere un espacio adecuado para la ejecución y el registro. Asegúrese de que su sistema cumpla los siguientes requisitos de espacio en disco disponibles: • Espacio de instalación necesario: 275 MB • Espacio de almacenamiento: 275 MB + 200 MB (registro) • Memoria del sistema: 1,5 GB
Licencia	El complemento de almacenamiento para vCenter es un producto gratuito e independiente que no requiere una clave de licencia. Sin embargo, se aplican los derechos de autor y las condiciones de servicio aplicables.

Consideraciones de renovación

Si va a actualizar desde una versión anterior, tenga en cuenta que el plugin debe quedar sin registrar desde la instancia de vcsa antes de la actualización.

- Durante la actualización, se conservan la mayoría de los ajustes de configuración anteriores del plugin. Esta configuración incluye contraseñas de usuario, todos los sistemas de almacenamiento detectados, certificados de servidor, certificados de confianza y configuración de tiempo de ejecución del servidor.
- El proceso de actualización no conserva los archivos **vcenter.properties**, por lo que debe cancelar el registro del plugin antes de la actualización. Una vez que la actualización se realice correctamente, puede volver a registrar el plugin en vcsa.
- Durante la actualización, se quitan todos los archivos de sistema operativo SANtricity que se cargaron previamente en el repositorio.

Instale o actualice el complemento de almacenamiento para vCenter

Siga estos pasos para instalar el complemento de almacenamiento para vCenter y verificar el registro del plugin. También puede actualizar el plugin utilizando estas instrucciones.

Revise los requisitos previos de la instalación

Asegúrese de que sus sistemas cumplen los requisitos en "Revise los requisitos de instalación y actualización".

> El proceso de actualización no conserva los archivos **vcenter.properties**. Si va a actualizar, debe cancelar el registro del plugin antes de proceder a la actualización. Una vez que la actualización se realice correctamente, puede volver a registrar el plugin en vcsa.

Instale el software del complemento

Para instalar el software del complemento:

1. Copie el archivo del instalador en el host que se utilizará como servidor de aplicaciones y, a continuación, acceda a la carpeta en la que descargó el instalador.
2. Haga doble clic en el archivo de instalación:

   ```
   santricity_storage_vcenterplugin-windows_x64-- nn.nn.nn.nnnn.exe
   ```

   En el nombre de archivo anterior: `nn.nn.nn.nnnn` representa el número de versión.

3. Cuando comience la instalación, siga las instrucciones que aparecen en pantalla para habilitar varias funciones e introduzca algunos parámetros de configuración. Si es necesario, puede cambiar cualquiera de estas selecciones posteriormente en los archivos de configuración.

   > Durante una actualización, no se le solicitan los parámetros de configuración.

   > Durante la instalación, se le solicita la validación de certificados. Mantenga seleccionada la casilla de comprobación si desea aplicar la validación de certificados entre el plugin y las cabinas de almacenamiento. Con este cumplimiento, se comprueba que los certificados de la cabina de almacenamiento sean de confianza en el plugin. Si los certificados no son de confianza, no se les permite agregarlos al plugin. Si desea anular la validación de certificados, anule la selección de la casilla de comprobación para que todas las cabinas de almacenamiento puedan añadirse al plugin mediante certificados autofirmados. Para obtener más información sobre los certificados, consulte la ayuda en línea disponible en la interfaz del plugin.

4. Cuando aparezca el mensaje servidor web iniciado, haga clic en **Aceptar** para completar la instalación y, a continuación, haga clic en **hecho**.
5. Compruebe que el servidor de aplicaciones se instaló correctamente ejecutando el comando **Services.msc**.
6. Compruebe que el servicio del servidor de aplicaciones (VCP), **complemento de almacenamiento SANtricity de NetApp para vCenter**, esté instalado y que el servicio se haya iniciado.

> Si es necesario, puede cambiar la configuración de validación de certificados y puerto de servicio web después de la instalación. En el directorio de instalación, abra el archivo wsconfig.xmll. Para quitar la validación de certificado en las cabinas de almacenamiento, cambie el `env` clave, `trust.all.arrays`, a. `true`. Para cambiar el puerto de servicios web, modifique el `sslport` el valor hasta el valor de puerto deseado oscila entre 0 y 65535. Asegúrese de que el número de puerto utilizado no se vincula a otro proceso. Cuando haya terminado, guarde los cambios y reinicie el servidor web del plugin. Si el valor de puerto del servidor web del plugin cambia después de registrar el plugin en vcsa, debe anular el registro y volver a registrar el plugin para que vcsa se comunique en el puerto cambiado al plugin.

Registre el plugin en un dispositivo de vCenter Server

Después de instalar el software del plugin, registre el plugin en una vcsa.

> El plugin sólo puede registrarse en una instancia de vcsa. Para registrarse en otra instancia de vcsa, debe cancelar el registro del plugin desde la instancia actual de vcsa y desinstalarlo desde el host de la aplicación. A continuación, puede volver a instalar el plugin y registrarlo en el otro vcsa.

1. Abra un símbolo del sistema a través de la línea de comandos y navegue hasta el siguiente directorio:

   ```
   <install directory>\vcenter-register\bin
   ```

2. Ejecute el archivo **vcenter-register.bat**:
   ```
   vcenter-register.bat ^
   -action registerPlugin ^
   -vcenterHostname <vCenter FQDN> ^
   -username <Administrator username> ^
   ```
3. Compruebe que el script se ha realizado correctamente.

Los registros se guardan en `%install_dir%/working/logs/vc-registration.log`.

Verifique el registro del plugin

Una vez instalado el plugin y ejecutado el script de registro, compruebe que el plugin se registró correctamente en el dispositivo de vCenter Server.

1. Abra vSphere Client en vCenter Server Appliance.
2. En la barra de menús, seleccione MENU:Administrator[Client Plugins].
3. Asegúrese de que Storage Plugin para vCenter aparezca en la lista como **habilitado**.

   Si el plugin aparece como Desactivado y aparece un mensaje de error que indica que no puede comunicarse con el servidor de aplicaciones, compruebe que el número de puerto definido para el servidor de aplicaciones está habilitado para pasar a través de los firewalls que podrían estar en uso. El número de puerto TCP (Transmission Control Protocol) del servidor de aplicaciones predeterminado es 8445.

Configure los permisos de acceso al complemento

Puede configurar permisos de acceso para el complemento de almacenamiento para

vCenter, lo que incluye usuarios, roles y privilegios.

Revise los privilegios de vSphere requeridos

Para acceder al plugin dentro de vSphere Client, debe asignarse a una función que tenga los privilegios de vSphere correspondientes. Los usuarios con el privilegio “Configure datastore” vSphere tienen acceso de lectura y escritura al plugin, mientras que los usuarios con el privilegio “Browse datastore” tienen acceso de solo lectura. Si un usuario no tiene ninguno de estos privilegios, el plugin muestra un mensaje de “privilegios insuficientes”.

Tipo de acceso de complemento	Se requiere el privilegio de vSphere
Lectura/escritura (configurar)	Datastore.Configure
Solo lectura (Ver)	Datastore.Browse

Configure las funciones de administrador de almacenamiento

Para proporcionar privilegios de lectura/escritura a los usuarios del plugin, puede crear, clonar o editar un rol. Para obtener más información sobre la configuración de roles en vSphere Client, consulte el siguiente tema en el centro de documentación de VMware:

- "Cree un rol personalizado"

Acceder a acciones de funciones

1. En la página de inicio de vSphere Client, seleccione **Administrator** en el área de control de acceso.
2. Haga clic en **roles** en el área de control de acceso.
3. Ejecute una de las siguientes acciones:
   - **Crear nuevo rol**: Haga clic en el icono de acción **Crear rol**.
   - **Clone Role**: Seleccione una función existente y haga clic en el icono de acción **Clone Role**.
   - **Editar función existente**: Seleccione una función existente y haga clic en el icono de acción **Editar función**.

> La función de administrador no se puede editar.

Aparecerá el asistente apropiado, en función de la selección anterior.

Crear un rol nuevo

1. En la lista privilegios, seleccione los permisos de acceso que desea asignar a este rol.

   Para permitir el acceso de solo lectura al plugin, seleccione **Datastore › Browse datastore**. Para permitir el acceso de lectura/escritura, seleccione MENU:Datastore[Configure datastore].

2. Si es necesario, asigne otros privilegios a la lista y, a continuación, haga clic en **Siguiente**.
3. Asigne un nombre al rol y proporcione una descripción.
4. Haga clic en **Finalizar**.

Clonar un rol

1. Asigne un nombre al rol y proporcione una descripción.
2. Haga clic en **Aceptar** para finalizar el asistente.
3. Seleccione la función clonada de la lista y, a continuación, haga clic en **Editar función**.
4. En la lista privilegios, seleccione los permisos de acceso que desea asignar a este rol.

   Para permitir el acceso de solo lectura al plugin, seleccione **Datastore › Browse datastore**. Para permitir el acceso de lectura/escritura, seleccione MENU:Datastore[Configure datastore].

5. Haga clic en **Siguiente**.
6. Actualice el nombre y la descripción, si lo desea.
7. Haga clic en **Finalizar**.

Editar una función existente

1. En la lista privilegios, seleccione los permisos de acceso que desea asignar a este rol.

   Para permitir el acceso de solo lectura al plugin, seleccione **Datastore › Browse datastore**. Para permitir el acceso de lectura/escritura, seleccione MENU:Datastore[Configure datastore].

2. Haga clic en **Siguiente**.
3. Actualice el nombre o la descripción, si lo desea.
4. Haga clic en **Finalizar**.

Establezca permisos para vCenter Server Appliance

Después de configurar privilegios para un rol, debe añadir un permiso a vCenter Server Appliance. Este permiso permite que un usuario o grupo dado tenga acceso al plugin.

1. En la lista desplegable del menú, seleccione **hosts y clústeres**.
2. Seleccione **vCenter Server Appliance** en el área de control de acceso.
3. Haga clic en la ficha **permisos**.
4. Haga clic en el icono de acción **Agregar permiso**.
5. Seleccione el dominio y usuario/grupo adecuados.
6. Seleccione la función creada que permite el privilegio de plugin de lectura/escritura.
7. Active la opción **propagar a niños**, si es necesario.
8. Haga clic en **Aceptar**.

> Es posible seleccionar un permiso existente y modificarlo para usar el rol creado. **Sin embargo, tenga en cuenta que el rol debe tener los mismos privilegios junto con los privilegios de plugin de lectura/escritura que para evitar una regresión en los permisos.**

Para acceder al plugin, debe iniciar sesión en vSphere Client en la cuenta de usuario que tiene los privilegios de lectura/escritura del plugin.

Para obtener más información sobre la gestión de permisos, consulte los siguientes temas en el centro de documentación de VMware:

- "Gestionar los permisos para vCenter Components"
- "Prácticas recomendadas para roles y permisos"

Inicie sesión y navegue por el complemento de almacenamiento para vCenter

Puede iniciar sesión en el complemento de almacenamiento para vCenter para navegar por la interfaz de usuario.

1. Antes de iniciar sesión en el plugin, asegúrese de que está utilizando uno de los siguientes navegadores:
   - Google Chrome 89 o posterior
   - Mozilla Firefox 80 o posterior
   - Microsoft Edge 90 o posterior
2. Inicie sesión en vSphere Client con la cuenta de usuario que tiene privilegios de lectura/escritura para el plugin.
3. En la página de inicio de vSphere Client, haga clic en **SANtricity Storage Plugin for vCenter**.

   El plugin se abre en una ventana de vSphere Client. La página principal del plugin se abre a **gestionar-todo**.

4. Acceda a las tareas de gestión del almacenamiento desde la barra lateral de navegación, que se encuentra a la izquierda:
   - **Gestionar**: Permite detectar las cabinas de almacenamiento en la red, abrir System Manager para una cabina, importar la configuración de una cabina a varias, gestionar grupos de cabinas, actualizar el software de sistema operativo y aprovisionar almacenamiento.
   - **Administración de certificados**: Permite administrar certificados para autenticar entre exploradores y clientes.
   - **Operaciones**: Permite ver el progreso de las operaciones por lotes, como importar la configuración de una matriz a otra.
   - **Soporte** – Ver opciones de soporte técnico, recursos y contactos.

> Algunas operaciones no están disponibles si una cabina de almacenamiento no tiene un estado óptimo.

Detectar cabinas de almacenamiento en el plugin

Para mostrar y gestionar recursos de almacenamiento, debe utilizar la interfaz del complemento de almacenamiento para vCenter para detectar las direcciones IP de las cabinas en la red.

Antes de empezar

- Debe conocer las direcciones IP de red (o el rango de direcciones) de las controladoras de la cabina.
- Las cabinas de almacenamiento deben estar configuradas y configuradas correctamente, y deben conocer las credenciales de inicio de sesión de la cabina de almacenamiento (nombre de usuario y contraseña).

Paso 1: Introduzca las direcciones de red para la detección

Pasos

1. En la página gestionar, seleccione **Agregar/detectar**.

   Se muestra el cuadro de diálogo introducir rango de direcciones de red.

2. Debe realizar una de las siguientes acciones:
   - Para detectar una cabina de almacenamiento, seleccione el botón de opción **detectar una sola cabina de almacenamiento** y luego introduzca la dirección IP de una de las controladoras de la cabina de almacenamiento.
   - Para detectar varias cabinas de almacenamiento, seleccione el botón de opción **detectar todas las cabinas de almacenamiento dentro de un rango de red** y, a continuación, introduzca la dirección de red inicial y la dirección de red final para buscar en la subred local.
3. Haga clic en **Iniciar descubrimiento**.

   Cuando comienza el proceso de detección, el cuadro de diálogo muestra las cabinas de almacenamiento a medida que se detectan. El proceso puede tardar varios minutos en completarse.

   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. Marque la casilla de comprobación junto a la cabina de almacenamiento que desea añadir al dominio de gestión.

   El sistema comprueba las credenciales de cada cabina que se añade al dominio de gestión. Es posible que deba resolver problemas con certificados que no son de confianza antes de continuar.

5. Haga clic en **Siguiente** para continuar con el siguiente paso del asistente.

   Si las cabinas de almacenamiento tienen certificados válidos, vaya a. Paso 3: Proporcionar contraseñas.

   Si alguna cabina de almacenamiento no tiene certificados válidos, se muestra el cuadro de diálogo resolver certificados autofirmados. Vaya a. Paso 2: Resolver certificados que no son de confianza durante la detección.

   Si desea importar certificados firmados por CA, cancele el asistente de detección y haga clic en **Gestión de certificados** en el panel izquierdo. Consulte la ayuda en línea para obtener más instrucciones.

Paso 2: Resolver certificados que no son de confianza durante la detección

Debe resolver todos los problemas de los certificados antes de continuar con el proceso de detección.

1. Si se abre el cuadro de diálogo resolver certificados autofirmados, revise la información que se muestra para los certificados que no son de confianza. Para obtener más información, también puede hacer clic en los tres puntos del extremo de la tabla y seleccionar **Ver** en el menú emergente.
2. Debe realizar una de las siguientes acciones:
   - Si confía en las conexiones con las matrices de almacenamiento detectadas, haga clic en **Siguiente** y, a continuación, en **Sí** para confirmar y continuar con el siguiente cuadro de diálogo del asistente. Los certificados autofirmados se marcan como de confianza y las cabinas de almacenamiento se añadirán al plugin.
   - 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.

3. Haga clic en **Siguiente** para continuar con el siguiente paso del asistente.

Paso 3: Proporcionar contraseñas

Como último paso para la detección, debe introducir las contraseñas de las cabinas de almacenamiento que desea añadir al dominio de gestión.

1. Para cada cabina detectada, introduzca su contraseña de administrador en los campos.
2. Haga clic en **Finalizar**.

   El sistema puede tardar varios minutos en conectarse a las cabinas de almacenamiento especificadas. Cuando finaliza el proceso, las cabinas de almacenamiento se añaden al dominio de gestión y se asocian con el grupo seleccionado (si se especificó alguno).

Aprovisionar almacenamiento en el complemento

Para aprovisionar almacenamiento, debe crear volúmenes, asignar volúmenes a hosts y, a continuación, asignar volúmenes a almacenes de datos.

Paso 1: Crear 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, lo que ayuda a organizar los recursos del sistema. El concepto de "volúmenes" es similar a usar carpetas o directorios en un equipo para organizar archivos con el fin de 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). Estos 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.

Pasos

1. En la página gestionar, seleccione la cabina de almacenamiento.
2. Seleccione MENU:Provisioning[Manage Volumes].
3. Seleccione MENU:Create[Volumes].

   Se muestra el cuadro de diálogo Seleccionar host.

4. 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.
5. Para continuar con la secuencia de creación de volúmenes para el host o clúster de hosts seleccionados, haga clic en **Siguiente**.

   Se muestra el cuadro de diálogo Seleccionar carga de trabajo. Una carga de trabajo contiene volúmenes con características similares, que se optimizan según el tipo de aplicación que es compatible con la carga de trabajo. Es posible definir una carga de trabajo o seleccionar cargas de trabajo existentes.

6. Debe realizar una de las siguientes acciones:
   - Seleccione la opción **Crear volúmenes para una carga de trabajo existente** y, a continuación, seleccione la carga de trabajo en la lista desplegable.

- Seleccione la opción **Crear una carga de trabajo nueva** para definir una carga de trabajo nueva para una aplicación compatible o para “otras” aplicaciones y, a continuación, siga estos pasos:
  i. 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.
  ii. Introduzca el nombre de la carga de trabajo que desea crear.

7. Haga clic en **Siguiente**. Si la carga de trabajo está asociada con un tipo de aplicación admitida, introduzca la información solicitada, de lo contrario, vaya al siguiente paso.

   Se muestra el cuadro de diálogo Añadir/editar volúmenes. En este cuadro de diálogo, se crean volúmenes a partir de pools o grupos de volúmenes elegibles. 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.

8. Antes de empezar a añadir volúmenes, lea las directrices de la siguiente tabla.

Campo	Descripción
Capacidad libre	Debido a que se crean volúmenes a partir de pools o grupos de volúmenes, el pool o el grupo de volúmenes seleccionado deben tener suficiente capacidad libre.
Garantía de datos (DA)	Para crear un volumen con la función DA habilitada, la conexión de host que se planea usar debe admitir DA. • 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. 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.

Campo	Descripción
Impulse la seguridad	Para crear un volumen con la función de seguridad habilitada, se debe crear una clave de seguridad para la cabina de almacenamiento. • 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. 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.
Aprovisionamiento de recursos	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).

9. Elija una de estas acciones según si seleccionó "otra" o una carga de trabajo específica de la aplicación en el paso anterior:

   - **Otros** – haga clic en **Añadir nuevo volumen** en cada pool o grupo de volúmenes que desee utilizar para crear uno o más volúmenes.
   - **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 bien 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.

     Aparecen los siguientes campos.

Campo	Descripción
Nombre del volumen	Se 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.

Campo	Descripción
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. La capacidad de un pool se asigna en incrementos de 4 GIB. Se asigna cualquier capacidad que no sea múltiplo de 4 GIB, pero no se puede usar. Para asegurarse de que toda la capacidad se pueda usar, especifique la capacidad en incrementos de 4 GIB. Si hubiese capacidad que no puede usar, la única manera de recuperarla es aumentar la capacidad del volumen.
Tipo de volumen	Si seleccionó "carga de trabajo específica de la aplicación", se muestra el campo Volume Type. Esto 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**: El sistema 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 la función SSD Cache 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 de segmento** – la cantidad de tiempo para cambiar el tamaño de 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 el cifrado. 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.

10. Para continuar con la secuencia de creación de volúmenes para la aplicación seleccionada, haga clic en **Siguiente**.
11. En el último paso, revise un resumen de los volúmenes que pretende crear y realizar los cambios necesarios. Para realizar cambios, haga clic en **Atrás**. Cuando esté satisfecho con la configuración del volumen, haga clic en **Finalizar**.

Paso 2: Cree acceso a host y asigne volúmenes

Un host se puede crear manualmente:

- **Manual** – durante la creación manual de host, puede asociar los identificadores de puerto de host seleccionándolos de una lista o introduciéndolos manualmente. 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.

Creación manual del host

Antes de empezar

Lea las siguientes directrices:

- Ya debe haber añadido o detectado cabinas de almacenamiento en el entorno.
- 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. En la página gestionar, seleccione la cabina de almacenamiento con la conexión del host.
2. Seleccione MENU:Provisioning[Configure hosts].

   Se abre la página Configurar hosts.

3. Haga clic en MENU:Create[Host].

   Se muestra el cuadro de diálogo Crear host.

4. Seleccione la configuración del host que corresponda.

Campo	Descripción
Nombre	Escriba un nombre para el host nuevo.

Campo	Descripción
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 interfaz de E/S** — generalmente, los puertos de host deberían haber iniciado sesión y estar disponibles en la lista desplegable. Puede seleccionar los identificadores de puerto de host de la lista. • **Manual add** — Si un identificador de puerto de host no aparece en la lista, significa que el puerto de host no ha iniciado 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. Se pueden introducir los identificadores de puerto de host manualmente 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.
Configure secreto CHAP del iniciador	(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 **establecer secreto de 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 utilizado es CHAP.

5. Haga clic en **Crear**.
6. Si necesita actualizar la información del host, seleccione el host en la tabla y haga clic en **Ver/editar configuración**.

   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 la IPT del host es `IPT_1`.

7. A continuación, se debe asignar un volumen a un host o un clúster de hosts para poder usarlo para operaciones de I/O. Seleccione MENU:Provisioning[Configure hosts].

   Se abre la página Configurar hosts.

8. 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. Es posible seleccionar cualquiera de las columnas o escribir un elemento en el cuadro Filtrar para facilitar la búsqueda de volúmenes en particular.

9. 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.
10. Haga clic en **asignar** para completar la operación.

    El sistema ejecuta 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.

Paso 3: Crear un almacén de datos en vSphere Client

Para crear un almacén de datos en vSphere Client, consulte "Cree un almacén de datos VMFS en vSphere Client" Tema del Centro de documentación de VMware.

Aumente la capacidad del almacén de datos existente aumentando la capacidad del 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

Asegúrese de que:

- 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 existen unidades de repuesto en uso en el volumen. (Esto se aplica solo a volúmenes que pertenecen a grupos de volúmenes.)

> Solo ciertos sistemas operativos permiten aumentar la capacidad de un volumen. Si aumenta la capacidad de un volumen en un sistema operativo que no admite la expansión de LUN, la capacidad ampliada será inutilizable y no se podrá restaurar la capacidad del volumen original.

Pasos

1. Desplácese hasta el plugin dentro de vSphere Client.

2. En el plugin, seleccione la cabina de almacenamiento que desee.
3. Haga clic en **aprovisionamiento** y seleccione **gestionar volúmenes**.
4. 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.

5. 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.

6. 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).
7. Haga clic en **aumentar**.
8. Vea el panel Recent Tasks para conocer el progreso de la operación de aumento de capacidad que se está ejecutando actualmente para el volumen seleccionado. Es posible que esta operación demore y que afecte el rendimiento del sistema.
9. Una vez que se complete la capacidad del volumen, debe aumentar manualmente el tamaño de VMFS para que coincida como se describe en la "Aumente la capacidad de los almacenes de datos VMFS en vSphere Client" Tema del Centro de documentación de VMware.

Aumente la capacidad del almacén de datos existente añadiendo volúmenes

1. Es posible aumentar la capacidad de un almacén de datos mediante la adición de volúmenes. Siga los pasos de Paso 1: Crear volúmenes.
2. A continuación, asigne los volúmenes al host deseado para aumentar la capacidad del almacén de datos.

   Consulte "Aumente la capacidad de los almacenes de datos VMFS en vSphere Client" Tema en el centro de documentación de VMware para obtener más información.

Ver estado

Puede ver el estado del sistema desde el complemento de almacenamiento para vCenter o desde vSphere Client.

1. Abra el plugin desde vSphere Client.
2. Vea el estado de los siguientes paneles:
   - **Estado de la matriz de almacenamiento** — vaya al panel **gestionar todo**. Para cada cabina detectada, la fila proporciona una columna Estado.
   - **Operaciones en curso** — haga clic en **Operaciones** en el panel lateral para ver todas las tareas de larga ejecución, como importar configuraciones. También se pueden ver las operaciones de ejecución prolongada en la lista desplegable de aprovisionamiento. Para cada operación enumerada en el cuadro de diálogo 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. 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.

Las operaciones que podrían aparecer para el plugin se enumeran en la siguiente tabla. También es posible que se muestren operaciones adicionales en la interfaz de System Manager.

Funcionamiento	Posible estado de la operación	Acciones que se pueden realizar
Volume create (solo volúmenes de pool estáticos de más de 64 TIB)	En curso	ninguno
Volume delete (solo volúmenes de pool estáticos de más de 64 TIB)	En curso	ninguno
Añadir capacidad a un pool o grupo de volúmenes	En curso	ninguno
Cambiar el nivel de RAID de un volumen	En curso	ninguno
Reducir la capacidad de un pool	En curso	ninguno
Comprobar el tiempo restante en una operación de formato de disponibilidad instantánea (IAF) para los volúmenes del pool	En curso	ninguno
Comprobar la redundancia de datos de un grupo de volúmenes	En curso	ninguno
Inicializar un volumen	En curso	ninguno
Aumente la capacidad de un volumen	En curso	ninguno
Cambiar el tamaño de los segmentos de un volumen	En curso	ninguno

Gestionar certificados

Información general sobre certificados

La gestión de certificados en el complemento de almacenamiento para vCenter permite crear solicitudes de firma de certificados (CSR), importar certificados y gestionar certificados existentes.

¿Qué son los certificados?

Los certificados son archivos digitales que identifican entidades en línea, como sitios web y servidores, para poder establecer comunicaciones seguras en Internet. Garantizan que solo se transmitan comunicaciones web en formato cifrado, de forma privada y sin alternaciones, entre el servidor especificado y el cliente. Mediante el complemento de almacenamiento para vCenter, puede 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.

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.

Los certificados autofirmados no son “de confianza” por parte de los exploradores. 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.

Certificado de gestión

Al abrir el plugin, el explorador intenta verificar si el host de gestión es un origen de confianza mediante la comprobación de un certificado digital. Si el explorador no encuentra un certificado firmado por CA, abre un mensaje de advertencia. Desde allí, podrá continuar al sitio web para aceptar el certificado autofirmado en esa sesión. También es posible obtener certificados digitales firmados de una CA para que ya no se vea el mensaje de advertencia.

Certificados de confianza

Durante una sesión del plugin, 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 plugin pueda autenticar las solicitudes de cliente entrantes procedentes de estas controladoras.

Usar certificados firmados por CA

Es posible obtener e importar certificados firmados por CA para establecer un acceso seguro al sistema de gestión donde se aloja el complemento de almacenamiento para vCenter.

El uso de certificados firmados por CA implica un procedimiento de tres pasos:

- Paso 1: Complete un archivo CSR.
- Paso 2: Enviar archivo CSR.
- Paso 3: Importar certificados de gestión.

Paso 1: Complete un archivo CSR

Primero, debe generar un archivo de solicitud de firma de certificación (CSR), que identifica a la organización y al sistema host donde se ejecuta el plugin. 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 **Gestión**, 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 se ejecuta el plugin:
    - **Nombre común** — la dirección IP o el nombre DNS del sistema host donde se ejecuta el plugin. Asegúrese de que esta dirección es correcta; debe coincidir exactamente con lo que escribe para acceder al plugin 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**.

Paso 2: Enviar archivo CSR

Después de crear un archivo de solicitud de firma de certificación (CSR), se envía el archivo CSR generado a una CA para recibir certificados de gestión firmados para el sistema donde se aloja el plugin.

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 se genera una CSR, el sistema crea una pareja 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.

Paso 3: Importar certificados de gestión

Después de recibir certificados firmados de la entidad de certificación (CA), importe los certificados en el sistema host donde se instaló el plugin.

Antes de empezar

- Debe tener los 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. También puede usar la utilidad certmgr de Windows para desempaquetar los archivos (haga clic con el botón derecho y seleccione MENU:All Tasks[Export]). Se recomienda la codificación base-64. Una vez completadas las exportaciones, se mostrará un archivo CER para cada archivo de certificado de la cadena.
- Se deben copiar los archivos de certificado en el sistema host donde se ejecuta el plugin.

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**.

Resultado

Los archivos se cargan y validan. La información del certificado aparece en la página Gestión de certificados.

Restablezca los certificados de gestión

Para el sistema de gestión que aloja el complemento de almacenamiento para vCenter, puede revertir el certificado de gestión a su estado autofirmado original de fábrica.

Acerca de esta tarea

Esta tarea elimina el certificado de gestión actual del sistema host donde se ejecuta el complemento de almacenamiento para vCenter. Una vez restablecido el certificado, el sistema host se revierte al uso del certificado autofirmado.

Pasos

1. Seleccione **Gestión de certificados**.
2. En la ficha **Gestión**, seleccione **Restablecer**.

   Se abre el cuadro de diálogo Confirmar restablecimiento de certificado de gestión.

3. Escriba reset en el campo y 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.

Resultado

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.

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 el complemento de almacenamiento para vCenter. Los certificados pueden estar firmados por una entidad de certificación (CA) o ser autofirmados.

Antes de empezar

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.
4. 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.
5. En el cuadro de diálogo, seleccione el certificado y, a continuación, haga clic en **Importar**.

   El certificado se carga y se valida.

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).

Pasos

1. Seleccione **Gestión de certificados**.
2. Seleccione una de las siguientes pestañas:
   - **Administración** — muestra el certificado para el sistema que aloja el plugin. Un certificado de gestión puede estar autofirmado o estar aprobado por una CA. Permite un acceso seguro al plugin.
   - **Trusted** — muestra certificados a los que el plugin 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 plugin. Un certificado de gestión puede estar autofirmado o estar aprobado por una CA. Permite un acceso seguro al plugin.

- **Trusted** — muestra certificados a los que el plugin 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.

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

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

Si tiene pensado importar un certificado firmado por una CA, asegúrese de que:

- 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

Los certificados dejan de ser de confianza cuando una cabina de almacenamiento intenta establecer una

conexión con el plugin, pero no se confirma que la conexión sea segura. 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 o 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.
4. 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.
5. En el cuadro de diálogo, seleccione el certificado y, a continuación, haga clic en **Importar**.

   El certificado se carga y se valida.

Gestione las cabinas

Información general de la gestión de cabinas

Use la función Añadir/detectar para encontrar y añadir las cabinas de almacenamiento que desea gestionar en el plugin de almacenamiento para vCenter. En la página gestionar, también puede cambiar el nombre, quitar y proporcionar contraseñas nuevas para estas cabinas detectadas.

Consideraciones sobre la detección de cabinas

Para mostrar y gestionar los recursos de almacenamiento, debe detectar las cabinas de almacenamiento que desea gestionar en la red de la organización. Puede detectar y añadir una sola cabina o varias.

Varias cabinas de almacenamiento

Si decide detectar varias cabinas de almacenamiento, debe introducir un rango de direcciones IP de red. A continuación, el sistema intentar establecer conexiones individuales con cada dirección IP de ese rango. En el plugin se muestra toda cabina de almacenamiento a la que se pudo acceder correctamente y luego se pueden añadir al dominio de gestión.

Cabina de almacenamiento única

Si decide detectar una sola cabina de almacenamiento, debe introducir la dirección IP única para una de las controladoras de la cabina de almacenamiento y, a continuación, añadir esa cabina al dominio de gestión.

El plugin detecta y muestra solamente la dirección IP única o la dirección IP dentro del rango asignado a un controlador. Si hay controladoras alternativas o direcciones IP asignadas a estas controladoras que no se incluyen en esta dirección IP única o este rango de direcciones IP, el plugin 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

Debe suministrar la contraseña de administrador para cada cabina de almacenamiento que desee añadir.

Certificados

Como parte del proceso de detección, el sistema verifica que las cabinas de almacenamiento detectadas utilicen certificados de un origen de confianza. El sistema utiliza dos tipos de autenticación basada en certificados para todas las conexiones que establece con el explorador:

- **Certificados de confianza** — puede que necesite instalar certificados de confianza adicionales proporcionados por la entidad emisora de certificados si uno o ambos certificados del controlador han caducado, revocado o falta un certificado en su cadena.
- **Certificados autofirmados** — los arreglos también pueden utilizar certificados autofirmados. Si se intentan detectar cabinas sin importar los certificados firmados, el plugin proporciona un paso adicional que permite aceptar el certificado autofirmado. El certificado autofirmado de la cabina de almacenamiento se marcará como de confianza y la cabina de almacenamiento se añadirá al plugin. Si no confía en las conexiones a la cabina de almacenamiento, seleccione **Cancelar** y valide la estrategia de certificado de seguridad de la cabina de almacenamiento antes de añadir la cabina de almacenamiento al plugin.

Estado de la cabina de almacenamiento

Al abrir el complemento de almacenamiento para vCenter, se establece la comunicación con cada cabina de almacenamiento y se muestra el estado de cada una.

En la página **gestionar - todo**, es posible ver el estado de la cabina de almacenamiento y el estado de la conexión de la cabina de almacenamiento.

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.

Estado	Lo que indica
Bloqueo	La cabina de almacenamiento está en estado bloqueado.
Desconocido	No se contactó a la cabina de almacenamiento. Esto puede ocurrir cuando el plugin se está iniciando y aún no ha establecido 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 plugin.
Sin conexión	El plugin se había contactado previamente con la cabina de almacenamiento, pero ahora perdió toda conexión con ella.

Comparación de la interfaz de complementos con System Manager

Puede utilizar el complemento de almacenamiento para vCenter para tareas operativas básicas en su cabina de almacenamiento; sin embargo, puede haber horas cuando necesite ejecutar System Manager para realizar tareas que no estén disponibles en el plugin.

System Manager es una aplicación integrada en la controladora de la cabina de almacenamiento, que está conectada a la red a través de un puerto de gestión Ethernet. System Manager incluye todas las funciones basadas en cabina.

La siguiente tabla ayuda a decidir si se puede usar la interfaz del plugin o la interfaz de System Manager para una tarea concreta de la cabina de almacenamiento.

Función	Interfaz de complemento	Interfaz de System Manager
Operaciones de lote en grupos de varias cabinas de almacenamiento	Sí	No Las operaciones se ejecutan en una sola cabina.
Actualizaciones para el firmware del sistema operativo SANtricity	Sí. Una o varias cabinas en una operación en lote.	Sí. Solo cabina única.
Importe la configuración de una cabina a varias cabinas	Sí	No
Gestión de hosts y clústeres de hosts (crear, asignar volúmenes, actualizar y eliminar)	Sí	Sí
Gestión de pools y grupos de volúmenes (crear, actualizar, habilitar la seguridad y eliminar)	Sí	Sí
Gestión de volúmenes (creación, cambio de tamaño, actualización y eliminación)	Sí	Sí
Gestión de la caché SSD (creación, actualización y eliminación)	Sí	Sí
Gestión de mirroring y Snapshot	No	Sí

Función	Interfaz de complemento	Interfaz de System Manager
Gestión del hardware (ver el estado de la controladora, configurar conexiones de puertos, desconectar la controladora, habilitar piezas de repuesto, borrar unidades, etc.)	No	Sí
Gestionar alertas (correo electrónico, SNMP y syslog)	No	Sí
Gestión de claves de seguridad	No	Sí
Gestión de certificados para las controladoras	No	Sí
Gestión de acceso para controladoras (LDAP, SAML, etc.)	No	Sí
Gestión de AutoSupport	No	Sí

Detectar las cabinas de almacenamiento

Para mostrar y gestionar recursos de almacenamiento en el complemento de almacenamiento para vCenter, debe detectar las direcciones IP de las cabinas en su red.

Antes de empezar

- Debe conocer las direcciones IP de red (o el rango de direcciones) de las controladoras de la cabina.
- Las cabinas de almacenamiento deben estar configuradas y configuradas correctamente.
- Las contraseñas de las cabinas de almacenamiento deben configurarse mediante el icono Access Management de System Manager.

Acerca de esta tarea

La detección de cabinas es un procedimiento de varios pasos:

- Paso 1: Introduzca las direcciones de red para la detección
- Paso 2: Resolver certificados que no son de confianza durante la detección
- Paso 3: Proporcionar contraseñas

Paso 1: Introduzca las direcciones de red para la detección

Como primer paso para detectar cabinas de almacenamiento, se debe introducir una dirección IP única o un rango de direcciones IP para buscar en la subred local. La función Añadir/detectar abre un asistente que le guía durante el proceso de detección.

Pasos

1. En la página **gestionar**, seleccione **Agregar/detectar**.

   Se muestra el cuadro de diálogo introducir rango de direcciones de red.

2. Debe realizar una de las siguientes acciones:
   - Para detectar una cabina de almacenamiento, seleccione el botón de opción **detectar una sola**

cabina de almacenamiento y luego introduzca la dirección IP de una de las controladoras de la cabina de almacenamiento.

- Para detectar varias cabinas de almacenamiento, seleccione el botón de opción **detectar todas las cabinas de almacenamiento dentro de un rango de red** y, a continuación, introduzca la dirección de red inicial y la dirección de red final para buscar en la subred local.

3. Haga clic en **Iniciar descubrimiento**.

   Cuando comienza el proceso de detección, el cuadro de diálogo muestra las cabinas de almacenamiento a medida que se detectan. El proceso puede tardar varios minutos en completarse.

   > 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. Marque la casilla de comprobación junto a la cabina de almacenamiento que desea añadir al dominio de gestión.

   El sistema comprueba las credenciales de cada cabina que se añade al dominio de gestión. Es posible que deba resolver problemas con certificados que no son de confianza antes de continuar.

5. Haga clic en **Siguiente** para continuar con el siguiente paso del asistente.
6. Si las cabinas de almacenamiento tienen certificados válidos, vaya a. Paso 3: Proporcionar contraseñas. Si alguna cabina de almacenamiento no tiene certificados válidos, se muestra el cuadro de diálogo resolver certificados autofirmados; vaya a. Paso 2: Resolver certificados que no son de confianza durante la detección. Si desea importar certificados firmados por CA, cancele los cuadros de diálogo de detección y vaya a. "Importar certificados para cabinas".

Paso 2: Resolver certificados que no son de confianza durante la detección

Si es necesario, debe resolver todos los problemas de certificado antes de continuar con el proceso de detección.

Durante la detección, si alguna cabina de almacenamiento muestra el estado "certificados no confiables", se muestra el cuadro de diálogo resolver certificados autofirmados. Puede resolver certificados que no son de confianza en este cuadro de diálogo, o bien puede importar certificados de CA (consulte "Importar certificados para cabinas").

Pasos

1. Si se abre el cuadro de diálogo resolver certificados autofirmados, revise la información que se muestra para los certificados que no son de confianza. Para obtener más información, también puede hacer clic en los tres puntos del extremo de la tabla y seleccionar **Ver** en el menú emergente.
2. Debe realizar una de las siguientes acciones:
   - Si confía en las conexiones con las matrices de almacenamiento detectadas, haga clic en **Siguiente** y, a continuación, en **Sí** para confirmar y continuar con la siguiente tarjeta del asistente. Los certificados autofirmados se marcarán como certificados de confianza y las cabinas de almacenamiento se añadirán al plugin.
   - 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 al plugin.

Paso 3: Proporcionar contraseñas

Como último paso para la detección, debe introducir las contraseñas de las cabinas de almacenamiento que desea añadir al dominio de gestión.

Pasos

1. De manera opcional, si previamente configuró grupos para las cabinas, es posible usar el menú desplegable para seleccionar un grupo para las cabinas detectadas.
2. Para cada cabina detectada, introduzca su contraseña de administrador en los campos.
3. Haga clic en **Finalizar**.

> El sistema puede tardar varios minutos en conectarse a las cabinas de almacenamiento especificadas.

Resultado

Las cabinas de almacenamiento se añaden al dominio de gestión y se asocian con el grupo seleccionado (si se especificó alguno).

> 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.

Cambie el nombre de la cabina de almacenamiento

Es posible cambiar el nombre de la cabina de almacenamiento que se muestra en la página Manage del Storage Plugin para vCenter.

Pasos

1. En la página **gestionar**, seleccione la casilla de comprobación a la izquierda del nombre de la cabina de almacenamiento.
2. Seleccione los tres puntos en el extremo derecho de la fila y, a continuación, seleccione **Cambiar nombre de matriz de almacenamiento** en el menú emergente.
3. Introduzca el nuevo nombre y haga clic en **Guardar**.

Cambiar contraseñas de las cabinas de almacenamiento

Puede actualizar las contraseñas que se utilizan para ver y acceder a las cabinas de almacenamiento en el complemento de almacenamiento para vCenter.

Antes de empezar

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 el plugin. Esto puede ser necesario si se modificó la contraseña de la cabina en System Manager.

Pasos

1. En la página **gestionar**, seleccione una o más matrices 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

Puede quitar una o varias cabinas de almacenamiento si ya no quiere gestionarlas desde el complemento de almacenamiento de para vCenter.

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. En la página **gestionar**, seleccione una o más matrices de almacenamiento que desee quitar.
2. Seleccione menú:tareas no comunes[Quitar cabinas de almacenamiento].

   La cabina de almacenamiento se elimina de todas las vistas de la interfaz del plugin.

Inicie System Manager

Para gestionar una sola cabina, use la opción Iniciar para abrir SANtricity System Manager en una nueva ventana del explorador.

System Manager es una aplicación integrada en la controladora de la cabina de almacenamiento, que está conectada a la red a través de un puerto de gestión Ethernet. System Manager incluye todas las funciones basadas en cabina. Para acceder a System Manager, debe tener una conexión fuera de banda con un cliente de gestión de red en un explorador web.

Pasos

1. En la página **gestionar**, seleccione una o más matrices de almacenamiento que desee gestionar.
2. Haga clic en **Iniciar**.

   El sistema abre una nueva pestaña en el explorador y, a continuación, 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**.

Importar la configuración

Información general sobre la configuración de importación

La función Importar configuración es una operación en lote que permite replicar la configuración en una sola cabina de almacenamiento (el origen) en varias cabinas (los destinos) del complemento de almacenamiento para vCenter.

Configuración disponible para la importación

Las siguientes configuraciones pueden importarse de una cabina a otra:

- **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.
- **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)
- **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

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 la interfaz del plugin, 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, 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.

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

Asegúrese de que:

- Las alertas se configuran en System Manager (menú:Configuración[Alertas]) para la cabina de almacenamiento que desea 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]).
- Ha revisado los requisitos para replicar configuraciones de almacenamiento en "Información general sobre la configuración de importación".

Acerca de esta tarea

Puede seleccionar las opciones de correo electrónico, SNMP o alertas de syslog para la operación de importación:

- **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 MENU:Actions[Import Settings].

   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. Además, una matriz no aparece en este cuadro de diálogo si el plugin no puede comunicarse con esa matriz (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.

Resultado

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

Asegúrese de que:

- AutoSupport se configura en System Manager (menú:Support[Support Center]) para 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]).
- Ha revisado los requisitos para replicar configuraciones de almacenamiento en "Información general sobre la configuración de importación".

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 MENU:Actions[Import Settings].

   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. Además, una matriz no aparece en este cuadro de diálogo si el plugin no puede comunicarse con esa matriz (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.

Resultado

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

Asegúrese de que:

- Los servicios de directorio están configurados en System Manager (menú:Configuración[Access Management]) para 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]).
- Ha revisado los requisitos para replicar configuraciones de almacenamiento en "Información general sobre la configuración de importación".

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 MENU:Actions[Import Settings].

   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. Además, una matriz no aparece en este cuadro de diálogo si el plugin no puede comunicarse con esa matriz (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.

Resultado

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

Asegúrese de que:

- 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]).
- Ha revisado los requisitos para replicar configuraciones de almacenamiento en "Información general sobre la configuración de importación".

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 MENU:Actions[Import Settings].

   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. Además, una matriz no aparece en este cuadro de diálogo si el plugin no puede comunicarse con esa matriz (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.

Resultado

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

Asegúrese de que:

- El almacenamiento se configura 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]).
- Ha revisado los requisitos para replicar configuraciones de almacenamiento en "Información general sobre la configuración de importación".
- 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.

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 MENU:Actions[Import Settings].

   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. Además, una matriz no aparece en este cuadro de diálogo si el plugin no puede comunicarse con esa matriz (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.

Resultado

Las cabinas de almacenamiento objetivo ahora están configuradas con los mismos ajustes de almacenamiento que la cabina de origen.

Gestione grupos de cabinas

Información general sobre grupos de cabinas

Puede gestionar la infraestructura física y virtualizada en el complemento de almacenamiento para vCenter mediante la agrupación de 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.

Tipos de grupos de cabinas de almacenamiento:

- **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.

Cree un grupo de cabinas de almacenamiento

Cree grupos de almacenamiento y, a continuación, añada cabinas de almacenamiento a los grupos. 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**.

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**.

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**.

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**.

Actualizar el software del sistema operativo

Información general de la actualización

En el complemento de almacenamiento para vCenter, puede gestionar las actualizaciones de NVSRAM y de software SANtricity para varias cabinas de almacenamiento del mismo tipo.

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 del sistema operativo SANtricity más reciente en el sitio de soporte (hay un enlace disponible en la página Soporte). Guarde el archivo en el sistema host de gestión (el host desde donde se accede al plugin en un explorador) y descomprima el archivo.
2. En el complemento, puede cargar el archivo de software del sistema operativo SANtricity y el archivo NVSRAM en el repositorio (un área del servidor donde se almacenan los archivos).
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, puede seleccionar el archivo de software de sistema operativo 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, el plugin realiza las siguientes tareas:
   - 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.
   - Transfiere los archivos de actualización a cada controladora.
   - Reinicia las controladoras y activa el nuevo software del sistema operativo, una controladora por vez. Durante la activación, el archivo del sistema operativo existente se reemplaza por el nuevo archivo.

> También es posible especificar que el software se active en otro momento.

Consideraciones de renovación

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 del complemento de almacenamiento para vCenter para 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 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 "Herramienta de matriz de interoperabilidad".

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.

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

Asegúrese de que:

- Los archivos del sistema operativo SANtricity más reciente están disponibles en el sistema host donde se ejecuta el plugin.
- 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.

> **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 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 > SANtricity OS > Software].

   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 en el equipo local.
   a. Haga clic en Añadir nuevo archivo a 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 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 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 asociados con el plugin. 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 cabinas de almacenamiento sin activarlo, active la casilla de comprobación **transferir el software de sistema operativo a las cabinas 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:
   - Tipo `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 SANtricity preconfigurado].
   - Tipo `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 puntos suspensivos (…). 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 en particular. Para ello, haga 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 matrices 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 SANtricity 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 puntos suspensivos (…). 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 en una cabina de almacenamiento en particular. Para ello, haga 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`.

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 SANtricity almacenado temporalmente].

   Se abre el cuadro de diálogo Borrar software SANtricity 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.

Gestionar el repositorio de software

Puede ver y gestionar un repositorio de software, que enumera todos los archivos de software asociados con el complemento de almacenamiento para vCenter.

Antes de empezar

Si utiliza el repositorio para añadir archivos de sistema operativo SANtricity, asegúrese de que estén disponibles en el sistema local.

Acerca de esta tarea

Puede utilizar la opción gestionar repositorio de software de sistema operativo SANtricity para importar uno o más archivos de sistema operativo al sistema host donde se ejecuta el plugin. También puede optar por eliminar uno o varios de los archivos de sistema operativo que están disponibles en el repositorio de software.

Pasos

1. En la vista principal, seleccione **gestionar** y, a continuación, elija Menú:Centro de actualización[gestionar el repositorio de software de SANtricity].

   Se muestra el cuadro de diálogo gestionar el repositorio de software de sistema operativo SANtricity.

2. Ejecute una de las siguientes acciones:
   - **Importar:**
     i. Haga clic en **Importar**.
     ii. 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`.

iii. Seleccione uno o más archivos de sistema operativo que desee agregar y, a continuación, haga clic en **Importar**.

- **Eliminar:**

  i. Seleccione uno o varios archivos de sistema operativo que desee quitar del repositorio de software.

  ii. Haga clic en **Eliminar**.

Resultado

Si seleccionó Importar, los archivos se cargan y se validan. Si seleccionó Eliminar, los archivos se quitan del repositorio de software.

Aprovisionar almacenamiento

Información general de aprovisionamiento

En el complemento de almacenamiento para vCenter, puede crear contenedores de datos, denominados volúmenes, de modo que el host pueda acceder al almacenamiento de la cabina.

Tipos de volúmenes y características

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, lo que ayuda a organizar los recursos del sistema. El concepto de "volúmenes" es similar a usar carpetas o directorios en un equipo para organizar archivos con el fin de 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). Estos 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.

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 tiene 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.

- **Aprovisionamiento de recursos** — para matrices de almacenamiento EF600 o EF300, puede especificar que los volúmenes se utilicen inmediatamente sin ningún 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).
- **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.

Capacidad para 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.

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.

> La interfaz del complemento no proporciona ninguna opción para crear volúmenes finos.

Capacidad notificada para volúmenes

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 se establece como la capacidad máxima hasta la que se

cree que el volumen se extenderá. Los volúmenes ofrecen 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.

Límites de capacidad

La capacidad mínima de un volumen 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, 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.

Cargas de trabajo específicas de una aplicación

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 del volumen, el sistema solicita que se respondan preguntas acerca del uso de la carga 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 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
  - Servidor de Microsoft Exchange

- 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, inicie System Manager. 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.
- Es posible 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.

Crear almacenamiento

En el complemento de almacenamiento para vCenter, debe crear almacenamiento. Para ello, primero crea una carga de trabajo para un tipo de aplicación específica. Después, debe añadir capacidad de almacenamiento a la carga de trabajo mediante la creación de volúmenes con características subyacentes similares.

Paso 1: Crear cargas 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.

Acerca de esta tarea

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.

El sistema recomienda una configuración de volumen optimizada solo para los siguientes tipos de aplicaciones:

- Microsoft SQL Server
- Servidor de Microsoft Exchange
- Videovigilancia

- VMware ESXi (para volúmenes que se usarán con Virtual Machine File System)

Pasos

1. En la página gestionar, seleccione la cabina de almacenamiento.
2. Seleccione MENU:Provisioning[Manage Volumes].
3. Seleccione MENU:Create[Workload].

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

4. 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.
5. Haga clic en **Crear**.

Paso 2: Crear 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.

Acerca de esta tarea

La mayoría de los tipos de aplicaciones adoptan la configuración de volúmenes definida por el usuario en forma predeterminada, mientras que otros tipos tienen una configuración inteligente aplicada al crear volúmenes. Por ejemplo, si se crean volúmenes para una 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. El sistema utiliza esta información para crear una configuración de volumen óptima para el usuario, que se puede editar en caso de ser necesario.

Puede crear volúmenes desde el menú:aprovisionamiento[gestionar volúmenes > Crear > volúmenes] o desde el menú:aprovisionamiento[Configurar agrupaciones y grupos de volúmenes > Crear > volúmenes]. El procedimiento es el mismo para cualquiera de las dos selecciones.

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

Paso 2a: Seleccione un host para un volumen

En el primer paso, puede seleccionar un host o un clúster de hosts específicos para el volumen, o puede elegir asignar el host más adelante.

Antes de empezar

Asegúrese de que:

- Se definieron hosts o clústeres de hosts válidos (vaya al menú:aprovisionamiento[Configurar hosts]).
- Se definieron identificadores de puertos de host para el host.
- La conexión de host debe admitir Data Assurance (DA) si se planea crear volúmenes con la función DA habilitada. 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. En la página gestionar, seleccione la cabina de almacenamiento.
2. Seleccione MENU:Provisioning[Manage Volumes].
3. Seleccione MENU:Create[Volumes].

   Se muestra el cuadro de diálogo Seleccionar host.

4. 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.
5. Para continuar con la secuencia de creación de volúmenes para el host o clúster de hosts seleccionados, haga clic en **Siguiente.**

   Se muestra el cuadro de diálogo Seleccionar carga de trabajo.

Paso 2b: Seleccionar una carga de trabajo para un volumen

En el segundo paso, debe seleccionar una carga de trabajo para personalizar la configuración de la cabina de almacenamiento para una aplicación específica, por ejemplo, VMware.

Acerca de esta tarea

En esta tarea, se describe cómo crear volúmenes para una carga de trabajo. Por lo general, una carga de trabajo contiene volúmenes con características similares, que se optimizan según el tipo de aplicación que es compatible con la carga de trabajo. Es posible definir una carga de trabajo en este paso o seleccionar cargas de trabajo existentes.

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 (disponible en el siguiente paso).
- Cuando se usa otro tipo de aplicaciones, se especifica manualmente la configuración de volumen con el cuadro de diálogo Añadir/editar volúmenes (disponible en el siguiente paso).

Pasos

1. Debe realizar una de las siguientes acciones:
    - Seleccione la opción **Crear volúmenes para una carga de trabajo existente** y, a continuación, seleccione la carga de trabajo en la lista desplegable.
    - Seleccione la opción **Crear una carga de trabajo nueva** para definir una carga de trabajo nueva para una aplicación compatible o para "otras" aplicaciones y, a continuación, siga estos pasos:
        - 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 al siguiente paso.

Paso 2c: Añadir o editar volúmenes

En el tercer paso, debe definir la configuración de volumen.

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.
    - 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. 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.
    - 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 figure Sí junto a "compatible con la función de seguridad" en la tabla de candidatos de pools o grupos de volúmenes).
    - Las funcionalidades de seguridad de la unidad se presentan a nivel del pool y grupo de volúmenes. 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 a partir de pools o grupos de volúmenes elegibles, que se muestran en el cuadro de diálogo Añadir/editar volúmenes. 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 en el paso anterior:
    - **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	Se 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. Se asigna cualquier capacidad que no sea múltiplo de 4 GIB, pero no se puede usar. Para asegurarse de que toda la capacidad se pueda usar, especifique la capacidad en incrementos de 4 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** — el sistema 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	Se 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. Se asigna cualquier capacidad que no sea múltiplo de 4 GIB, pero no se puede usar. Para asegurarse de que toda la capacidad se pueda usar, especifique la capacidad en incrementos de 4 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** — el sistema 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.

2. Para continuar con la secuencia de creación de volúmenes para la aplicación seleccionada, haga clic en **Siguiente**.

Paso 2d: Revisar la configuración de volumen

En el último paso, debe revisar un resumen de los volúmenes que pretende crear y realizar los cambios necesarios.

Pasos

1. Revise los volúmenes que desea crear. Para realizar cambios, haga clic en **Atrás**.
2. Cuando esté satisfecho con la configuración del volumen, haga clic en **Finalizar**.

Después de terminar

- En vSphere Client, cree almacenes de datos para los volúmenes.
- Realice cualquier modificación necesaria del sistema operativo en el host de la aplicación para que las aplicaciones puedan usar el volumen.
- Ejecute la utilidad específica del sistema operativo (disponible de un proveedor de terceros) y, a continuación, ejecute el comando SMcli `-identifyDevices` para correlacionar los nombres de los volúmenes con los nombres de las cabinas de almacenamiento host.

  La interfaz SMcli se incluye en el sistema operativo SANtricity y se puede descargar a través de SANtricity System Manager. Para obtener más información sobre cómo descargar la interfaz SMcli mediante SANtricity System Manager, consulte la "Descargue el tema de la CLI en la ayuda en línea de comandos de SANtricity System Manager".

Aumente la capacidad de un volumen

Es posible cambiar el tamaño de un volumen para aumentar la capacidad notificada.

Antes de empezar

Asegúrese de que:

- 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 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

En esta tarea, se describe cómo 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. Asegúrese de considerar todos los requisitos de capacidad futuros que puede tener para otros volúmenes en este pool o grupo de volúmenes.

> 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. En la página **gestionar**, seleccione la cabina de almacenamiento que contiene los volúmenes cuyo tamaño desea cambiar.
2. Seleccione MENU:Provisioning[Manage Volumes].
3. 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.

4. 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.

5. 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).
6. Haga clic en **aumentar**.

   La capacidad del volumen se aumenta según lo seleccionado. Sea consciente de que esta operación puede ser muy prolongada y que esto podría afectar al 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.

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

Asegúrese de que el volumen que desea cambiar esté en estado óptimo.

Pasos

1. En la página gestionar, seleccione la cabina de almacenamiento que contiene los volúmenes que desea cambiar.
2. Seleccione MENU:Provisioning[Manage Volumes].
3. 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.

4. 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.
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.
Identificadores	Muestra los identificadores del volumen seleccionado. • Identificador a nivel mundial (WWID). Identificador hexadecimal único del volumen. • Identificador único extendido (EUI). Un identificador EUI-64 del volumen. • Identificador de subsistema (SSID). Identificador del subsistema de la cabina de almacenamiento de un volumen.

5. 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** — el sistema 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.
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.

Ajuste	Descripción
Caché SSD	(Esta función no está disponible en los sistemas de almacenamiento EF600 o EF300). 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 de seguridad de unidad 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.

6. Haga clic en **Guardar**.

Resultado

La configuración del volumen se modificará según sus preferencias.

Añadir volúmenes a la carga de trabajo

Es posible añadir volúmenes sin asignar a una carga de trabajo nueva o existente.

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. En la página gestionar, seleccione la cabina de almacenamiento que contiene los volúmenes que desea añadir.
2. Seleccione MENU:Provisioning[Manage Volumes].
3. Seleccione la ficha **aplicaciones y cargas de trabajo**.

   Se muestra la vista aplicaciones y cargas de trabajo.

4. Seleccione **Agregar a carga de trabajo**.

   Se muestra el cuadro de diálogo Seleccionar carga de trabajo.

5. 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.
6. Seleccione **Siguiente** para continuar con la secuencia de añadir a carga de trabajo.

   Se muestra el cuadro de diálogo Seleccionar volúmenes.

7. Seleccione los volúmenes que desea añadir a la carga de trabajo.
8. Revise los volúmenes que desea añadir a la carga de trabajo seleccionada.
9. Cuando esté satisfecho con la configuración de su carga de trabajo, haga clic en **Finalizar**.

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.

Pasos

1. En la página gestionar, seleccione la cabina de almacenamiento que contiene la carga de trabajo que desea cambiar.
2. Seleccione MENU:Provisioning[Manage Volumes].
3. Seleccione la ficha **aplicaciones y cargas de trabajo**.

   Se muestra la vista aplicaciones y cargas de trabajo.

4. 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.

5. (Opcional) Si lo desea, puede cambiar el nombre de la carga de trabajo provisto por el usuario.
6. Haga clic en **Guardar**.

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 óptimo y no hay operaciones de modificación en curso en el volumen.*atención: *No se puede cancelar la operación después de iniciarse. 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 pueden inicializarse:

- 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 procedimiento se aplica solo a volúmenes estándar creados a partir de pools o grupos de volúmenes.

Pasos

1. En la página gestionar, seleccione la cabina de almacenamiento que contiene los volúmenes que desea inicializar.
2. Seleccione MENU:Provisioning[Manage Volumes].
3. 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.

4. Seleccione uno o varios volúmenes para inicializar y confirme que desea realizar la operación.

Resultados

El sistema ejecuta las siguientes acciones:

- 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).

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 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. En la página gestionar, seleccione la cabina de almacenamiento que contiene los volúmenes que desea redistribuir.
2. Seleccione MENU:Provisioning[Manage Volumes].
3. 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.

4. Seleccione el o los volúmenes que desea redistribuir y confirme que desea ejecutar la operación.

Resultado

El sistema 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. En la página gestionar, seleccione la cabina de almacenamiento que contiene los volúmenes para los que desea cambiar la propiedad de la controladora.
2. Seleccione MENU:Provisioning[Manage Volumes].
3. 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.

4. 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

- El sistema 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.

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 al mismo tiempo.

Pasos

1. En la página gestionar, seleccione la cabina de almacenamiento que contiene los volúmenes para los cuales desea cambiar la configuración de caché.
2. Seleccione MENU:Provisioning[Manage Volumes].
3. 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.

4. 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.

5. 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

Ajuste	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.
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. PRECAUCIÓN: **Posible pérdida de datos** — Si selecciona esta opción y no dispone de una fuente de alimentación universal de protección, puede perder datos. Además, es posible perder datos si la controladora no tiene baterías y se habilita la opción almacenamiento en caché de escritura sin baterías.
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.

6. 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. En la página gestionar, seleccione la cabina de almacenamiento que contiene los volúmenes para los que desea cambiar la configuración de análisis de medios.
2. Seleccione MENU:Provisioning[Manage Volumes].
3. 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.

4. 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.
5. Especifique el número de días durante los cuales desea que se ejecute el análisis de medios.
6. Seleccione la casilla de comprobación **escaneo de medios** para cada volumen donde desea realizar un análisis de medios. El sistema 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**.

7. Haga clic en **Guardar**.

Resultado

El sistema aplica los cambios de los análisis de medios en segundo plano sobre la base de la selección.

Elimine el volumen

Es posible eliminar uno o varios volúmenes para aumentar la capacidad libre de un pool o grupo de volúmenes.

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

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

> Al eliminar un volumen, se produce la pérdida de todos los datos en estos volúmenes.

Tenga en cuenta que **no puede** eliminar un volumen que tenga una de estas 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.

> Cuando un volumen supera un tamaño determinado (actualmente 128 TB), la operación de eliminación se ejecuta en segundo plano y es posible que el espacio liberado no esté disponible inmediatamente.

Pasos

1. En la página **gestionar**, seleccione la cabina de almacenamiento que contiene los volúmenes que desea eliminar.
2. Seleccione MENU:Provisioning[Manage Volumes].
3. Haga clic en **Eliminar**.

Se muestra el cuadro de diálogo Eliminar volúmenes.

4. Seleccione uno o varios volúmenes para eliminar y confirme que desea realizar la operación.
5. Haga clic en **Eliminar**.

Configurar hosts

Información general de creación de hosts

Para gestionar el almacenamiento con el complemento de almacenamiento para vCenter, debe detectar o definir cada host de la red. Un host es un servidor que envía I/o a un volumen de una cabina de almacenamiento.

Creación manual de hosts

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. Un host se puede crear manualmente.

- **Manual** — durante la creación manual de host, usted asocia identificadores de puerto de host seleccionándolos de una lista o introduciéndolos manualmente. 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

Para que un host envíe I/o a un volumen, se debe asignar el volumen. 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.

Cree acceso de hosts

Para gestionar el almacenamiento con el complemento de almacenamiento para vCenter, debe detectar o definir cada host de la red.

Acerca de esta tarea

Al crear un host, se deben definir los parámetros de host para proporcionar conexión a la cabina de

almacenamiento y acceso de I/o a los volúmenes.

Al crear un host, tenga en cuenta las siguientes directrices:

- 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. En la página gestionar, seleccione la cabina de almacenamiento con la conexión del host.
2. Seleccione MENU:Provisioning[Configure hosts].

   Se abre la página Configurar hosts.

3. Haga clic en MENU:Create[Host].

   Se muestra el cuadro de diálogo Crear host.

4. 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 interfaz de E/S** — generalmente, los puertos de host deberían haber iniciado sesión y estar disponibles en la lista desplegable. Puede seleccionar los identificadores de puerto de host de la lista. • **Manual add** — Si un identificador de puerto de host no aparece en la lista, significa que el puerto de host no ha iniciado 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. Se pueden introducir los identificadores de puerto de host manualmente 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.
Configure secreto CHAP del iniciador	(Opcional) Si seleccionó o introdujo manualmente un puerto de host mediante un IQN de iSCSI y desea solicitar la autenticación de un host que intenta acceder a la cabina de almacenamiento mediante un protocolo de autenticación por desafío mutuo (CHAP), seleccione la casilla de verificación “establecer secreto de 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 utilizado es CHAP.

5. Haga clic en **Crear**.

6. Si necesita actualizar la información del host, seleccione el host en la tabla y haga clic en **Ver/editar configuración**.

Resultado

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 la IPT del host es `IPT_1`.

Después de terminar

Es necesario asignar un volumen a un host para que se pueda usar en operaciones de I/O. Vaya a. "Asignar volúmenes a hosts".

Cree un clúster de hosts

Cuando dos o más hosts requieren acceso de I/o a los mismos volúmenes, es posible crear un clúster de hosts.

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 se pueden combinar 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. En la página gestionar, seleccione la cabina de almacenamiento con la conexión del host.
2. Seleccione MENU:Provisioning[Configure hosts].

   Se abre la página Configurar hosts.

3. Seleccione MENU:Create[Host cluster].

   Se muestra el cuadro de diálogo Crear clúster de hosts.

4. Seleccione la configuración del clúster de hosts que corresponda.

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.

5. 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.

Resultado

El nuevo clúster de hosts se muestra en la tabla con los hosts asignados en las filas de abajo.

Después de terminar

Se debe asignar un volumen a un clúster de hosts para poder usarlo en operaciones de I/O. Vaya a. "Asignar volúmenes a hosts".

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.

Antes de empezar

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, todos los volúmenes revertirán a la inicialización más lenta.

Acerca de esta tarea

Una asignación de volumen otorga acceso a un host o un clúster de hosts al volumen en una cabina de almacenamiento.

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.

  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.

Pasos

1. En la página gestionar, seleccione la cabina de almacenamiento con la conexión del host.
2. Seleccione MENU:Provisioning[Configure hosts].

   Se abre la página Configurar hosts.

3. 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. Es posible seleccionar cualquiera de las columnas o escribir un elemento en el cuadro Filtrar para facilitar la búsqueda de volúmenes en particular.

4. 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.
5. 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.

Anule la asignación de volúmenes

Si ya no necesita acceso de I/o a un volumen, es posible anular la asignación de este recurso desde el 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. En la página gestionar, seleccione la cabina de almacenamiento con la conexión del host.
2. Seleccione MENU:Provisioning[Configure hosts].

Se abre la página Configurar hosts.

3. 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.

4. 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.
5. 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.

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 o clúster de hosts.

Pasos

1. En la página gestionar, seleccione la cabina de almacenamiento con la conexión del host.
2. Seleccione MENU:Provisioning[Configure hosts].

   Se abre la página Configurar hosts.

3. 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.

4. Para cambiar las propiedades del host, asegúrese de que la ficha **Propiedades** está seleccionada y, a continuación, 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. Para cambiar la configuración del puerto, haga clic en la ficha **puertos de host** y cambie la configuración según corresponda.

   Detalles del campo

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). El sistema 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.

6. Haga clic en **Guardar**.

Elimine host o clúster de hosts

Es posible quitar un host o un clúster de hosts para que los volúmenes ya no estén asociados con ese host.

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. En la página gestionar, seleccione la cabina de almacenamiento con la conexión del host.
2. Seleccione MENU:Provisioning[Configure hosts].

   Se abre la página Configurar hosts.

3. 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.

4. 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.

Configure los pools y los grupos de volúmenes

Información general sobre los pools y el grupo de volúmenes

Para aprovisionar almacenamiento en el complemento de almacenamiento para vCenter, debe crear un pool o un grupo de volúmenes que contendrá las unidades de disco duro (HDD) o los discos de estado sólido (SSD) que desea usar en la cabina de almacenamiento.

El provisionamiento

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

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.

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, el sistema 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. El sistema 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, 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.

Decidir si se deben usar pools o grupos de volúmenes

Seleccione un pool

- Si necesita recompilaciones de la unidad más rápidas y gestión de almacenamiento simplificada y/o tiene 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 puede configurar o cambiar el nivel de RAID de los pools o los volúmenes en los pools. Los pools utilizan RAID nivel 6.

Seleccione 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.

Creación de pools automática versus manual

Según la configuración del almacenamiento, puede permitir que el sistema cree pools de forma automática o puede crearlos manualmente. Un pool es un conjunto de unidades agrupadas lógicamente.

Antes de crear y gestionar pools, revise las siguientes secciones sobre cómo se crean automáticamente los pools y cuándo es posible que deba crearlos manualmente.

Creación automática

Cuando el sistema detecta capacidad sin asignar en la cabina de almacenamiento, inicia la creación automática de pools cuando el sistema detecta capacidad sin asignar en una cabina de almacenamiento. 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 de un pool debe ser del mismo tipo (unidad de disco duro o unidad de estado sólido) y tener una capacidad similar. El sistema le solicitará 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 estado de protección contra pérdida de bandeja o protección contra pérdida de cajón.también es posible 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.

Crear un pool automáticamente

Es posible crear pools automáticamente cuando el sistema detecta al menos 11 unidades sin asignar o detecta una unidad sin asignar que es elegible para un pool existente. Un pool es un conjunto de unidades agrupadas lógicamente.

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

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.

Se debe recordar lo siguiente:

- Si se añaden unidades a una cabina de almacenamiento, el sistema 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, el sistema automáticamente ofrece la opción de añadir las unidades compatibles a un pool existente. Si se añaden unidades nuevas a un pool existente, el sistema 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. Para la creación de un pool, se deben usar todas las unidades de la cabina de almacenamiento.

Pasos

1. En la página gestionar, seleccione la cabina de almacenamiento para el pool.
2. Seleccione MENU:Provisioning[Configure Pools and Volume Groups].
3. 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.

   Observe que el sistema hace lo siguiente:

   - 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.

4. Para cambiar el nombre de una nueva agrupación, haga clic en el icono **Editar** (el lápiz).
5. Para ver las características adicionales del pool, ubique 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.

6. Haga clic en **Aceptar**.

Crear un pool manualmente

Puede crear un pool manualmente si su configuración no cumple los requisitos para la configuración automática del pool. Un pool es un conjunto de unidades agrupadas lógicamente.

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. Para la creación de un pool, se deben usar todas las unidades de la cabina de almacenamiento.

Acerca de esta tarea

Durante la creación de un pool, se determinan sus características, como el tipo de unidad, la funcionalidad 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, las configuraciones también incluyen aprovisionamiento de recursos y tamaños de bloques de volúmenes.

Pasos

1. En la página gestionar, seleccione la cabina de almacenamiento para el pool.
2. Seleccione MENU:Provisioning[Configure Pools and Volume Groups].
3. Haga clic en MENU:Create[Pool].

   Se muestra el cuadro de diálogo Crear un pool.

4. Escriba un nombre para el pool.
5. (Opcional) Si tiene más de un tipo de unidad en la cabina de almacenamiento, seleccione el tipo de unidad

que desea usar.

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

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

Detalles del campo

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.
Unidades totales	Indica la cantidad de unidades disponibles en el candidato de pool. El sistema reserva automáticamente tantas unidades como sea posible para la capacidad de conservación (para cada seis unidades de un pool, el sistema 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. Si desea usar DA, seleccione un pool que sea compatible con ESTA función. Esta opción solo está disponible si está habilitada la función DA. Un pool 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.
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 crear un grupo de volúmenes para 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.

Antes de empezar

Revise las siguientes directrices:

- Se necesita al menos una unidad sin asignar.
- Existen límites en cuanto a la cantidad de capacidad de unidad que se puede tener en un único grupo de volúmenes. Estos límites varían según el tipo de host.

- 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.
- 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. El sistema actualmente 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.

Acerca de esta tarea

Durante la creación de un grupo de volúmenes, se determinan las características de grupo, como la cantidad de unidades, la funcionalidad 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, las configuraciones también incluyen aprovisionamiento de recursos, tamaños de bloques de unidades y tamaños de bloques de volúmenes.

> 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.

Pasos

1. En la página gestionar, seleccione la cabina de almacenamiento para el grupo de volúmenes.
2. Seleccione MENU:Provisioning[Configure Pools and Volume Groups].
3. Haga clic en MENU:Create[Grupo de volúmenes].

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

4. Escriba un nombre para el grupo de volúmenes.
5. 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.
6. (Opcional) Si tiene más de un tipo de unidad en la cabina de almacenamiento, seleccione el tipo de unidad que desea usar.

   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.

7. (Opcional) es posible 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.

No use el método manual a menos que sea un experto que comprenda la redundancia de unidades y las configuraciones de unidades óptimas.

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.

8. 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. Para obtener más información, consulte la documentación de SANtricity System Manager: "Cree un grupo de volúmenes".

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.

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.
- 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 esta tarea, es posible añadir capacidad libre para incluirse en el pool o el 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.

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 una cabina 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. En la página gestionar, seleccione la cabina de almacenamiento con el pool o el grupo de volúmenes.
2. Seleccione MENU:Provisioning[Configure Pools and Volume Groups].
3. 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.

4. 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. • Puede proteger el pool o el grupo de volúmenes con la función Drive Security, pero todas las unidades deben ser compatibles con la función de seguridad para poder utilizar esta función. • 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 compatibles con la función de seguridad pueden ser unidades de cifrado de disco completo (FDE) o 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.

5. 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
6. Para continuar, haga clic en **Sí**; de lo contrario, haga clic en **Cancelar**.

Resultado

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.

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.

Caché SSD no está disponible en los sistemas de almacenamiento EF600 o EF300.

Acerca de esta tarea

Para la creación de una caché SSD, 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 las siguientes 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.
- La capacidad máxima de la caché SSD utilizable en una cabina de almacenamiento depende de la capacidad de 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. En la página gestionar, seleccione la cabina de almacenamiento para la caché.
2. Seleccione MENU:Provisioning[Configure Pools and Volume Groups].
3. Haga clic en menú:Crear[caché SSD].

   Se muestra el cuadro de diálogo Crear caché SSD.

4. Escriba un nombre para la caché SSD.
5. Seleccione el candidato de caché SSD que desea usar según las siguientes características.

Detalles del campo

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, asegúrese de que figure "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, active la casilla de verificación **Habilitar seguridad**. NOTA: Una vez habilitada, la seguridad no se puede desactivar. 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.

6. 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.

7. Haga clic en **Crear**.

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 se puede cambiar el nivel de RAID de un pool mediante la interfaz del plugin. El complemento configura automáticamente los pools como RAID 6.

Pasos

1. En la página gestionar, seleccione la cabina de almacenamiento con el pool.
2. Seleccione MENU:Provisioning[Configure Pools and Volume Groups].
3. Seleccione el pool que desea editar y, a continuación, haga clic en **Ver/editar configuración**.

   Se muestra el cuadro de diálogo Configuración del pool.

4. 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, el plugin envía un mensaje, lo que le da tiempo para agregar más espacio de almacenamiento o eliminar objetos innecesarios. 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 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 pool, la capacidad sin asignar consta de la capacidad de conservación de un pool, la capacidad libre (capacidad que no usan los volúmenes) y una parte de la capacidad utilizable 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.

5. 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. En la página gestionar, seleccione la cabina de almacenamiento con el grupo de volúmenes.
2. Seleccione MENU:Provisioning[Configure Pools and Volume Groups].
3. 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.

4. 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 alto rendimiento y la mejor disponibilidad de datos y es adecuado para almacenar 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.
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.

5. 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**.

Resultado

Si cambia el nivel de RAID de un grupo de volúmenes, el plugin 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.

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.

> Esta función no está disponible en los sistemas de almacenamiento EF600 o EF300.

Pasos

1. En la página gestionar, seleccione la cabina de almacenamiento con la caché SSD.
2. Seleccione MENU:Provisioning[Configure Pools and Volume Groups].
3. 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.

4. 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.

5. 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.

Esta función no está disponible en los sistemas de almacenamiento EF600 o EF300.

Acerca de esta tarea

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 archivo .csv.

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

Pasos

1. En la página gestionar, seleccione la cabina de almacenamiento con la caché SSD.
2. Seleccione MENU:Provisioning[Configure Pools and Volume Groups].
3. Seleccione la caché SSD para la cual desea ver estadísticas y haga clic en menú:más[Ver caché SSD] estadísticas.

   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

Ajuste	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).

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

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. (Los pools se configuran solamente como RAID 6.)

> 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. En la página gestionar, seleccione la cabina de almacenamiento con el pool o el grupo de volúmenes.
2. Seleccione MENU:Provisioning[Configure Pools and Volume Groups].
3. Seleccione menú:tareas no comunes[comprobar redundancia de volumen].

   Se muestra el cuadro de diálogo comprobar redundancia.

4. Seleccione los volúmenes que desea verificar y después escriba check para confirmar que desea llevar a cabo esta operación.
5. 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. En la siguiente tabla, se proporciona más información sobre el estado de la comprobación de redundancia:

Detalles del campo

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.

6. 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. En la página gestionar, seleccione la cabina de almacenamiento con el pool o el grupo de volúmenes.
2. Seleccione MENU:Provisioning[Configure Pools and Volume Groups].
3. 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.

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

Resultados

El sistema ejecuta las siguientes acciones:

- 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. En la página gestionar, seleccione la cabina de almacenamiento con el grupo de volúmenes.
2. Seleccione MENU:Provisioning[Configure Pools and Volume Groups].
3. 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.

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

Resultado

El sistema 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

En la barra lateral de navegación, seleccione **Operaciones** para ver el progreso de la operación consolidar capacidad libre. Es posible que esta operación demore y que afecte el rendimiento del sistema.

Encender las luces de localización

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. En la página gestionar, seleccione la cabina de almacenamiento.
2. Seleccione MENU:Provisioning[Configure Pools and Volume Groups].

3. 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.

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

Elimine capacidad

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.

Los siguientes son posibles impactos 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.

Los siguientes son impactos sobre 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. En la página gestionar, seleccione la cabina de almacenamiento.

   Seleccione MENU:Provisioning[Configure Pools and Volume Groups].

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 total de capacidad 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.

Resultado

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

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. En la página gestionar, seleccione la cabina de almacenamiento con el pool o el grupo de volúmenes.
2. Seleccione MENU:Provisioning[Configure Pools and Volume Groups].
3. 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.

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

Quite el complemento de almacenamiento para vCenter

Puede quitar el plugin de vCenter Server Appliance y desinstalar el servidor web del plugin desde el host de la aplicación.

Estos son dos pasos distintos que puede realizar en cualquier orden. Sin embargo, si decide eliminar el servidor web del plugin del host de la aplicación antes de cancelar el registro del plugin, el script de registro se elimina durante ese proceso y no puede utilizar el método 1 para cancelar el registro.

Cancele el registro del plugin desde una instancia de vCenter Server Appliance

Para cancelar el registro del plugin en una instancia de vCenter Server Appliance, seleccione uno de estos métodos:

- Método 1: Ejecute la secuencia de comandos de registro
- Método 2: Utilice las páginas Mob de vCenter Server

Método 1: Ejecute la secuencia de comandos de registro

1. Abra un símbolo del sistema a través de la línea de comandos y navegue hasta el siguiente directorio:

   ```
   <install directory>\vcenter-register\bin
   ```

2. Ejecute el `vcenter-register.bat` archivo:

   ```
   vcenter-register.bat ^

   -action unregisterPlugin ^

   -vcenterHostname <vCenter FQDN> ^

   -username <Administrator Username> ^
   ```

3. Compruebe que el script se ha realizado correctamente.

   Los registros se guardan en `%install_dir%/working/logs/vc-registration.log`.

Método 2: Utilice las páginas Mob de vCenter Server

1. Abra un navegador web e introduzca la siguiente URL:

   https://<FQDN[] De vCenter Server>/MOB

2. Inicie sesión con las credenciales de administrador.
3. Busque el nombre de la propiedad de `extensionManager` y haga clic en el vínculo asociado a esa propiedad.
4. Expanda la lista de propiedades haciendo clic en **más**… en la parte inferior de la lista.
5. Compruebe que la extensión `plugin.netapp.eseries` está en la lista.
6. Si está presente, haga clic en el método `UnregisterExtension`.
7. Introduzca el valor `plugin.netapp.eseries` En el cuadro de diálogo y haga clic en **Invoke Method**.

8. Cierre el cuadro de diálogo y actualice el navegador web.
9. Compruebe que el `plugin.netapp.eseries` la extensión no está en la lista.

> Este procedimiento cancela el registro del plugin desde vCenter Server Appliance; sin embargo, no se quitan los archivos del paquete de plugins del servidor. Para quitar los archivos de paquetes, use SSH para acceder a vCenter Server Appliance y desplácese hasta el siguiente directorio: `etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity/`. A continuación, quite el directorio asociado al plugin.

Quite el complemento de servidor web del host de la aplicación

Para quitar el software del plugin del host de la aplicación, siga estos pasos:

1. Desde el servidor de aplicaciones, desplácese hasta **Panel de control**.
2. Vaya a **aplicaciones y características** y seleccione **complemento de almacenamiento SANtricity para vCenter**.
3. Haga clic en **Desinstalar/Cambiar**.

   Se mostrará un cuadro de diálogo de confirmación.

4. Haga clic en **Desinstalar**.

   Aparece un mensaje de confirmación cuando se completa la desinstalación.

5. Haga clic en **Listo**.

Preguntas frecuentes

¿Qué configuración se importa?

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).

¿Por qué estos volúmenes no están asociados a 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.

¿Cómo afecta la creación de volúmenes la carga de trabajo seleccionada?

Durante la creación del volumen, se le solicita información sobre el uso de una 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
  - Servidor de Microsoft Exchange
  - 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 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.

¿Por qué no se puede 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.

¿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.

¿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. Por lo general, puede alcanzar 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.

¿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. Puede seleccionar el tipo de host recomendado en la lista desplegable.

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.
So Mac	Admite versiones de Mac OS que usan un controlador ATTO Technology, Inc. Y multipathing.

Tipo de sistema operativo de host	Sistema operativo (SO) y controlador multivía
Windows (ATTO)	Admite sistemas operativos Windows que usan un controlador ATTO Technology, Inc. Y multiruta.
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 (Kernal 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).

¿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.

¿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 que 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, no se debe utilizar el clúster predeterminado. En cambio, se deben asociar los identificadores del puerto de host con sus hosts correspondientes. Esta tarea se puede realizar manualmente durante la operación Crear host. A continuación, se deben asignar los volúmenes a un host individual o a un clúster de hosts.

Solo se debe 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 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.

¿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.

¿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.
- 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.

¿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.

¿Por qué no es posible aumentar la 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.

Es posible cambiar la capacidad de conservación de los pools y los 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.

¿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 utilizar la función DA, seleccione un pool o grupo de volúmenes compatible con DA al crear un volumen nuevo (busque **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 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 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).

¿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 archivo .csv. 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 la caché SSD, vaya a la página **Administrar**. Seleccione MENU:Provisioning[Configure Pools & Volume Groups]. 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.

Esta función no está disponible en los sistemas de almacenamiento EF600 o EF300.

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

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 un archivo .csv.

Las estadísticas detalladas se enumeran después de las estadísticas nominales.

¿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 un solo cajón.	3

Nivel	Criterios para la protección contra pérdida de bandeja	Cantidad mínima requerida de bandejas
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 5	Cada unidad del grupo de volúmenes se encuentra en un cajón aparte	3

Nivel	Criterios para la protección contra pérdida de cajón	Cantidad mínima requerida de cajones
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

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

Para mantener la protección contra pérdida de bandeja y 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.

¿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 usan los volúmenes) y una parte de la capacidad utilizable 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 utilizan 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. 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.

> La función de aprovisionamiento de recursos no está disponible en este momento. En algunas vistas, los componentes pueden notificarse como compatibles con el aprovisionamiento de recursos, pero se ha deshabilitado la capacidad para crear volúmenes aprovisionados mediante recursos hasta que se pueda volver a habilitar en una actualización futura.

Volúmenes aprovisionados mediante recursos

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. 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.

Habilitar y deshabilitar la función

El aprovisionamiento de recursos está habilitado de forma predeterminada en sistemas donde las unidades admiten DULBE. Puede deshabilitar esa configuración predeterminada en Pools y grupos de volúmenes. La deshabilitación del aprovisionamiento de recursos es una acción permanente para los volúmenes existentes y no se puede revertir (es decir, no se puede volver a habilitar el aprovisionamiento de recursos para estos grupos de volúmenes y pools).

Sin embargo, si desea volver a habilitar el aprovisionamiento de recursos para los volúmenes nuevos que cree, puede hacerlo en **Settings › System**. Tenga en cuenta que cuando se vuelve a habilitar el aprovisionamiento de recursos, solo se ven afectados los grupos de volúmenes y pools recién creados. Todos los grupos de volúmenes y pools existentes se mantendrán sin cambios. Si lo desea, también puede deshabilitar el aprovisionamiento de recursos de nuevo desde MENU:Settings[System].

¿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).

¿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

Las claves internas se mantienen y se “ocultan” en una ubicación sin acceso en la memoria persistente del controlador. 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.

Soluciones heredadas

Conector de cloud

Descripción general del conector SANtricity® Cloud

El conector cloud SANtricity es una aplicación Linux basada en host que le permite realizar backup y recuperación de datos completos basados en archivos y bloques en cuentas de presentación de datos de E-Series (por ejemplo, Amazon simple Storage Service y StorageGRID de NetApp) y dispositivo AltaVault de NetApp.

Disponible para su instalación en plataformas RedHat y SUSE Linux, el conector SANtricity Cloud es una solución empaquetada (archivo .bin). Después de instalar SANtricity Cloud Connector, puede configurar la aplicación para realizar trabajos de backup y restauración para volúmenes E-Series en un dispositivo AltaVault o en sus cuentas de Amazon S3 o StorageGRID existentes. Todos los trabajos realizados mediante el conector cloud de SANtricity utilizan API basadas en REST.

> La herramienta SANtricity Cloud Connector quedó obsoleta y ya no está disponible para su descarga.

Consideraciones

Cuando utilice estos procedimientos, tenga en cuenta que:

- Las tareas de configuración y backup/restauración descritas en estos procedimientos se aplican a la versión de la interfaz gráfica de usuario del conector cloud de SANtricity.

- Los flujos de trabajo de la API DE REST para la aplicación SANtricity Cloud Connector no se describen en estos procedimientos. Para desarrolladores con experiencia, hay puntos finales disponibles para cada operación de SANtricity Cloud Connector en la documentación de API. Para acceder a la documentación de la API, vaya a. `http://<hostname.domain>:<port>/docs` mediante un navegador.

Tipos de backups

El conector en cloud de SANtricity proporciona dos tipos de backups: Backups basados en imágenes y basados en archivos.

- **Copia de seguridad basada en imágenes**

  Un backup basado en imágenes lee los bloques de datos sin formato de un volumen Snapshot y los realiza un backup a un archivo conocido como imagen. Se realiza un backup de todos los bloques de datos del volumen Snapshot, incluidos los bloques vacíos, los bloques ocupados por archivos eliminados, los bloques asociados con la partición y los metadatos del sistema de archivos. Los backups de imágenes tienen la ventaja de almacenar toda la información en el volumen Snapshot, independientemente del esquema de partición o del sistema de archivos que contenga.

  La imagen no se almacena en el destino de copia de seguridad como un único archivo, sino que se divide en una serie de fragmentos de datos, que tienen un tamaño de 64 MB. Los fragmentos de datos permiten que SANtricity Cloud Connector utilice varias conexiones con el destino de backup y, de este modo, mejora el rendimiento del proceso de backup.

  Para los backups de StorageGRID y Amazon Web Services (S3), cada fragmento de datos utiliza una clave de cifrado independiente para cifrar el fragmento. La clave es un hash SHA256 que consiste en la combinación de una frase de acceso proporcionada por el usuario y el hash SHA256 de los datos del usuario. Para backups en AltaVault, el conector cloud de SANtricity no cifra los fragmentos de datos mientras AltaVault realiza esta operación.

- **Copia de seguridad basada en archivos**

  Un backup basado en archivos lee los archivos contenidos con una partición de sistema de ficheros y los realiza una copia de seguridad en una serie de fragmentos de datos de 64 MB de tamaño. Un backup basado en archivos no realiza un backup de los archivos eliminados ni de los metadatos de particiones y sistemas de archivos. Al igual que sucede con los backups basados en imágenes, los fragmentos de datos permiten que SANtricity Cloud Connector utilice varias conexiones con el destino de backup, lo que mejora el rendimiento del proceso de backup.

  Para los backups de StorageGRID y Amazon Web Services, cada fragmento de datos utiliza una clave de cifrado independiente para cifrar el fragmento. La clave es un hash SHA256 que consiste en la combinación de frase de contraseña proporcionada por el usuario y el hash SHA256 de los datos del usuario. Para los backups en AltaVault, los fragmentos de datos no están cifrados por SANtricity Cloud Connector porque AltaVault realiza esta operación.

Requisitos del sistema para Cloud Connector

Su sistema debe cumplir con los requisitos de compatibilidad para el conector cloud de SANtricity.

Requisitos de hardware del host

Su hardware debe cumplir con los siguientes requisitos mínimos:

- Al menos 5 GB de memoria; 4 GB para el tamaño máximo de pila configurado
- Se necesitan al menos 5 GB de espacio libre en disco desde la instalación del software

Debe instalar el proxy de servicios web de SANtricity para usar el conector cloud de SANtricity. Puede instalar Web Services Proxy localmente o ejecutar la aplicación de forma remota en un servidor distinto. Para obtener información sobre la instalación del proxy de servicios web de SANtricity, consulte "Temas del proxy de servicios web".

Exploradores compatibles

Los siguientes exploradores son compatibles con la aplicación SANtricity Cloud Connector (se indican versiones mínimas):

- Firefox v31
- Google Chrome v47
- Microsoft Internet Explorer v11
- Microsoft Edge, EdgeHTML 12
- Safari v9

> La documentación de API de la aplicación SANtricity Cloud Connector no se carga cuando se utiliza la configuración de la vista de compatibilidad en el explorador Microsoft Internet Explorer v11. Para asegurarse de que la documentación de API se muestra correctamente bajo el explorador de Microsoft Internet Explorer v11, se recomienda que la configuración Vista de compatibilidad esté deshabilitada.

Cabinas de almacenamiento y firmware de la controladora compatibles

Debe verificar la compatibilidad de las cabinas de almacenamiento y el firmware antes de usar la aplicación SANtricity Cloud Connector.

Para obtener una lista completa y actualizada de todas las cabinas de almacenamiento compatibles y firmware para el conector cloud de SANtricity, consulte "Herramienta de matriz de interoperabilidad de NetApp".

Sistemas operativos compatibles

La aplicación SANtricity Cloud Connector 4.0 es compatible con los sistemas operativos siguientes y compatible con ellos:

Sistema operativo	Versión	Arquitectura
Red Hat Enterprise Linux (RHEL)	7.x.	64 bits
SUSE Linux Enterprise Server (SLES)	12.x.	64 bits

Sistemas de archivos compatibles

Debe utilizar sistemas de archivos compatibles para realizar backups y restauraciones a través de la aplicación Cloud Connector de SANtricity.

Los siguientes sistemas de archivos son compatibles con operaciones de backup y restauración en la aplicación SANtricity Cloud Connector:

- ext2
- ext3
- ext4

Instale el conector SANtricity en la nube

La solución empaquetada de SANtricity Cloud Connector (archivo .bin) sólo está disponible para plataformas RedHat y SUSE Linux.

Puede instalar la aplicación SANtricity Cloud Connector mediante el modo gráfico o el modo de consola en un sistema operativo Linux compatible. Durante el proceso de instalación, debe especificar los números de puerto no SSL y SSL para el conector en nube de SANtricity. Cuando está instalado, el conector en nube de SANtricity se ejecuta como un proceso de daemon.

> La herramienta SANtricity Cloud Connector quedó obsoleta y ya no está disponible para su descarga.

Antes de empezar

Consulte las siguientes notas:

- Si el proxy de servicios web de SANtricity ya está instalado en el mismo servidor que el conector en la nube de SANtricity, se producirán conflictos entre los números de puerto no SSL y los números de puerto SSL. En este caso, elija los números adecuados para el puerto no SSL y el puerto SSL durante la instalación del conector en la nube de SANtricity.
- Si se realiza algún cambio de hardware en el host, vuelva a instalar la aplicación SANtricity Cloud Connector para garantizar la coherencia del cifrado.
- Los backups creados mediante la versión 3.1 de la aplicación SANtricity Cloud Connector no son compatibles con la versión 4.0 de la aplicación SANtricity Cloud Connector. Si planea mantener estas copias de seguridad, debe seguir utilizando su versión anterior del conector SANtricity Cloud. Para garantizar que las versiones 3.1 y 4.0 del conector en nube de SANtricity se instalen correctamente, se deben asignar números de puerto únicos para cada versión de la aplicación.

Instalación de Device Mapper Multipath (DM-MP)

Cualquier host que ejecute SANtricity Cloud Connector también debe ejecutar Linux Device Mapper Multipath (DM-MP) y tener instalado el paquete multipath-tools.

El proceso de detección de SANtricity Cloud Connector se basa en el paquete de herramientas multivía para la detección y el reconocimiento de los volúmenes y archivos para el backup o la restauración. Para obtener más información acerca de cómo configurar y configurar Device Mapper, consulte *SANtricity Storage Manager Multipath Drivers Guide* para la versión de SANtricity que está utilizando en "Recursos de documentos de E-Series y SANtricity".

Instale el conector en la nube

Puede instalar SANtricity Cloud Connector en sistemas operativos Linux en modo gráfico o en modo de consola.

Modo gráfico

Puede utilizar el modo gráfico para instalar SANtricity Cloud Connector en un sistema operativo Linux.

Antes de empezar

Designe una ubicación de host para la instalación del conector cloud de SANtricity.

Pasos

1. Descargue el archivo de instalación de SANtricity Cloud Connector en la ubicación del host que desee.
2. Abra una ventana de terminal.
3. Desplácese hasta el archivo de directorio que contiene el archivo de instalación de SANtricity Cloud Connector.
4. Inicie el proceso de instalación de SANtricity Cloud Connector:

   ```
   ./cloudconnector-xxxx.bin -i gui
   ```

   En este comando, `xxxx` designa el número de versión de la aplicación.

   Aparece la ventana Installer.

5. Revise la instrucción Introduction y haga clic en **Siguiente**.

   El contrato de licencia para NetApp, Inc El software se muestra en la ventana del instalador.

6. Acepte los términos del Contrato de licencia y, a continuación, haga clic en **Siguiente**.

   Se muestra la página backups creados con versiones anteriores de SANtricity Cloud Connector.

7. Para reconocer el mensaje copias de seguridad creadas con versiones anteriores de SANtricity Cloud Connector, haga clic en **Siguiente**.

   > Para instalar la versión 4.0 de SANtricity Cloud Connector mientras se mantiene una versión anterior, se deben asignar números de puerto únicos para cada versión de la aplicación.

   La página elegir instalación se muestra en la ventana del instalador. El campo Dónde desea instalar muestra la siguiente carpeta de instalación predeterminada: `opt/netapp/santricity_cloud_connector4/`

8. Seleccione una de las siguientes opciones:
   - Para aceptar la ubicación predeterminada, haga clic en **Siguiente**.
   - Para cambiar la ubicación predeterminada, introduzca una nueva ubicación de carpeta. Se muestra la página introducir el número de puerto no SSL de Jetty. El valor predeterminado de 8080 se asigna al puerto no SSL.
9. Seleccione una de las siguientes opciones:
   - Para aceptar el número de puerto SSL predeterminado, haga clic en **Siguiente**.
   - Para cambiar el número de puerto SSL predeterminado, introduzca el nuevo valor de número de puerto que desee.

10. Seleccione una de las siguientes opciones:
    - Para aceptar el número de puerto no SSL predeterminado, haga clic en **Siguiente**.
    - Para cambiar el número de puerto no SSL predeterminado, introduzca el nuevo valor de número de puerto deseado. Se muestra la página Resumen de preinstalación.
11. Revise el Resumen de preinstalación que se muestra y, a continuación, haga clic en **instalar**.

    Se inicia la instalación del conector en nube de SANtricity y aparece un símbolo del sistema de instalación del demonio del servidor web.

12. Haga clic en **Aceptar** para confirmar el mensaje de instalación de WebServer Daemon.

    Aparece el mensaje Installation Complete (instalación completa).

13. Haga clic en **hecho** para salir del instalador de conexión en la nube de SANtricity.

Modo de consola

Puede utilizar el modo de consola para instalar SANtricity Cloud Connector en un sistema operativo Linux.

Antes de empezar

Designe una ubicación de host para la instalación del conector cloud de SANtricity.

Pasos

1. Descargue el archivo de instalación de SANtricity Cloud Connector en la ubicación del host I/o que desee.
2. Abra una ventana de terminal.
3. Desplácese hasta el archivo de directorio que contiene el archivo de instalación de SANtricity Cloud Connector.
4. Inicie el proceso de instalación de SANtricity Cloud Connector:

    ```
    ./cloudconnector-xxxx.bin –i console
    ```

    En este comando, `xxxx` indica el número de versión de la aplicación.

    Se ha inicializado el proceso de instalación del conector cloud de SANtricity.

5. Pulse **Intro** para continuar con el proceso de instalación.

    Contrato de licencia para usuario final para NetApp, Inc El software se muestra en la ventana del instalador.

    > Para cancelar el proceso de instalación en cualquier momento, escriba `quit` bajo la ventana del instalador.

6. Pulse **Intro** para continuar con cada parte del Contrato de licencia para el usuario final.

    La declaración de aceptación del acuerdo de licencia se muestra en la ventana del instalador.

7. Para aceptar los términos del contrato de licencia para usuario final y proceder con la instalación del conector cloud de SANtricity, introduzca `Y` Y pulse **Intro** en la ventana del instalador.

Se muestra la página backups creados con versiones anteriores de SANtricity Cloud Connector.

> Si no acepta los términos del acuerdo de usuario final, escriba `N` Y pulse **Intro** para finalizar el proceso de instalación del conector en nube de SANtricity.

8. Para reconocer las copias de seguridad creadas con versiones anteriores del mensaje SANtricity Cloud Connector, pulse **Intro**.

> Para instalar la versión 4.0 de SANtricity Cloud Connector mientras se mantiene una versión anterior, se deben asignar números de puerto únicos para cada versión de la aplicación.

Aparece el mensaje elegir carpeta de instalación con la siguiente carpeta de instalación predeterminada para el conector en la nube de SANtricity:`/opt/netapp/santricity_cloud_connector4/`.

9. Seleccione una de las siguientes opciones:
   - Para aceptar la ubicación de instalación predeterminada, pulse **Intro**.
   - Para cambiar la ubicación de instalación predeterminada, introduzca la nueva ubicación de la carpeta. Se muestra el mensaje Enter the Non SSL Jetty Port Number. Se asigna un valor predeterminado de 8080 al puerto no SSL.
10. Seleccione una de las siguientes opciones:
    - Para aceptar el número de puerto SSL predeterminado, pulse **Siguiente**.
    - Para cambiar el número de puerto SSL predeterminado, introduzca el nuevo valor de número de puerto que desee.
11. Seleccione una de las siguientes opciones:
    - Para aceptar el número de puerto no SSL predeterminado, pulse **Intro**.
    - Para cambiar el número de puerto no SSL predeterminado, introduzca el nuevo valor de número de puerto. Aparecerá el resumen de pasos previos a la instalación del conector de cloud de SANtricity.
12. Revise el Resumen de preinstalación que se muestra y pulse **Intro**.
13. Pulse **Intro** para confirmar el mensaje de instalación de Webserver Daemon.

    Aparece el mensaje Installation Complete (instalación completa).

14. Pulse **Intro** para salir del instalador de conexiones de la nube de SANtricity.

Añada certificado de servidor y certificado de CA a un almacén de claves

Para usar una conexión https segura desde el explorador al host de SANtricity Cloud Connector, puede aceptar el certificado autofirmado del host SANtricity Cloud Connector o añadir un certificado y una cadena de confianza reconocidos por el explorador y la aplicación SANtricity Cloud Connector.

Antes de empezar

La aplicación SANtricity Cloud Connector debe estar instalada en un host.

Pasos

1. Detenga el servicio con `systemctl` comando.
2. Desde la ubicación de instalación predeterminada, acceda al directorio de trabajo.

La ubicación de instalación predeterminada para el conector en cloud de SANtricity es `/opt/netapp/santricity_cloud_connector4`.

3. Con el `keytool` Cree el certificado de servidor y la solicitud de firma de certificación (CSR).

   EJEMPLO

   ```
   keytool -genkey -dname "CN=host.example.com, OU=Engineering, O=Company,
   L=<CITY>, S=<STATE>, C=<COUNTRY>" -alias cloudconnect -keyalg "RSA"
   -sigalg SHA256withRSA -keysize 2048 -validity 365 -keystore
   keystore_cloudconnect.jks -storepass changeit
   keytool -certreq -alias cloudconnect -keystore keystore_cloudconnect.jks
   -storepass changeit -file cloudconnect.csr
   ```

4. Envíe la CSR generada a la entidad de certificación (CA) que elija.

   La entidad de certificación firma la solicitud de certificado y devuelve un certificado firmado. Además, recibe un certificado de la propia CA. Este certificado de CA debe importarse al almacén de claves.

5. Importe el certificado y la cadena de certificados de CA al almacén de claves de la aplicación: `/<install Path>/working/keystore`

   EJEMPLO

   ```
   keytool -import -alias ca-root -file root-ca.cer -keystore
   keystore_cloudconnect.jks -storepass <password> -noprompt
   keytool -import -alias ca-issuing-1 -file issuing-ca-1.cer -keystore
   keystore_cloudconnect.jks -storepass <password> -noprompt
   keytool -import -trustcacerts -alias cloudconnect -file certnew.cer
   -keystore keystore_cloudconnect.jks -storepass <password>
   ```

6. Reinicie el servicio.

Añada el certificado StorageGRID a un almacén de claves

Si está configurando StorageGRID como tipo de destino para la aplicación SANtricity Cloud Connector, primero debe añadir un certificado StorageGRID al almacén de claves del conector en la nube de SANtricity.

Antes de empezar

- Tiene un certificado StorageGRID firmado.
- Tiene la aplicación SANtricity Cloud Connector instalada en un host.

Pasos

1. Detenga el servicio con `systemctl` comando.
2. Desde la ubicación de instalación predeterminada, acceda al directorio de trabajo.

La ubicación de instalación predeterminada para el conector en cloud de SANtricity es `/opt/netapp/santricity_cloud_connector4`.

3. Importe el certificado StorageGRID al almacén de claves de la aplicación: `/<install Path>/working/keystore`

   EJEMPLO

   ```
   opt/netapp/santricity_cloud_connector4/jre/bin/keytool -import
   -trustcacerts -storepass changeit -noprompt -alias StorageGrid_SSL -file
   /home/ictlabsg01.cer -keystore
   /opt/netapp/santricity_cloud_connector/jre/lib/security/cacerts
   ```

4. Reinicie el servicio.

Configure por primera vez el conector SANtricity Cloud

Una vez instalado correctamente, puede configurar la aplicación SANtricity Cloud Connector con el asistente de configuración. El asistente de configuración se muestra después de iniciar sesión inicialmente en el conector cloud de SANtricity.

Inicie sesión en el conector cloud de SANtricity por primera vez

Al inicializar SANtricity Cloud Connector por primera vez, debe introducir una contraseña predeterminada para acceder a la aplicación.

Antes de empezar

Asegúrese de que tiene acceso a un navegador conectado a Internet.

Pasos

1. Abra un explorador compatible.
2. Conéctese al servidor de conector Cloud de SANtricity configurado (p. ej., `http://localhost:8080/`).

   Aparece la página de inicio de sesión inicial de la aplicación SANtricity Cloud Connector.

3. En el campo Administrator Password, introduzca la contraseña predeterminada de `password`.
4. Haga clic en **Iniciar sesión**.

   Aparece el asistente de configuración del conector de cloud de SANtricity.

Uso del Asistente de configuración

El asistente de configuración aparece cuando se inicia sesión correctamente en el conector cloud de SANtricity.

Con el asistente de configuración, configuró la contraseña de administrador, las credenciales de gestión de inicio de sesión de Web Services Proxy, el tipo de destino de backup deseado y la frase de contraseña de cifrado para el conector cloud de SANtricity.

Paso 1: Establecer la contraseña de administrador

Puede personalizar la contraseña utilizada para los inicios de sesión posteriores en SANtricity Cloud Connector a través de la página establecer contraseña de administrador.

Establecer una contraseña a través de la página definir contraseña de administrador reemplaza efectivamente la contraseña predeterminada utilizada durante el inicio de sesión inicial para la aplicación SANtricity Cloud Connector.

Pasos

1. En la página definir contraseña de administrador, introduzca la contraseña de inicio de sesión que desee para el conector en nube de SANtricity en el campo **Introduzca la nueva contraseña de administrador**.
2. En el campo **Volver a introducir la nueva contraseña de administrador**, vuelva a introducir la contraseña del primer campo.
3. Haga clic en **Siguiente**.

   Se acepta la configuración de contraseña para el conector en nube de SANtricity y se muestra la página establecer frase de contraseña en el asistente de configuración.

   > La contraseña de administrador definida por el usuario no se establece hasta que finalice el asistente de configuración.

Paso 2: Configurar la frase de contraseña

En la página Enter the Encryption pass phrase, puede especificar una frase de contraseña alfanumérica de entre 8 y 32 caracteres.

Se requiere una frase de contraseña especificada por el usuario como parte de la clave de cifrado de datos que utiliza la aplicación SANtricity Cloud Connector.

Pasos

1. En el campo **define a pass phrase**, introduzca la frase de contraseña que desee.
2. En el campo **Volver a introducir la frase de contraseña**, vuelva a introducir la frase de contraseña en el primer campo.
3. Haga clic en **Siguiente**.

   La frase de contraseña introducida para la aplicación SANtricity Cloud Connector se acepta y se muestra la página Seleccionar tipo de objetivo para el asistente de configuración.

Paso 3: Seleccione el tipo de destino

Las funcionalidades de backup y restauración están disponibles para los tipos de destino de Amazon S3, AltaVault y StorageGRID mediante el conector Cloud de SANtricity. Puede especificar el tipo de destino de almacenamiento deseado para la aplicación SANtricity Cloud Connector, en la página Select the Target Type.

Antes de empezar

Compruebe que dispone de uno de los siguientes elementos: Punto de montaje de AltaVault, cuenta de Amazon AWS o cuenta de StorageGRID.

Pasos

1. En el menú desplegable, seleccione una de las siguientes opciones:

- Amazon AWS
- AltaVault
- StorageGRID

  En el Asistente de configuración se muestra una página Tipo de destino para la opción seleccionada.

2. Consulte las instrucciones de configuración adecuadas para AltaVault, Amazon AWS o StorageGRID.

Configuración del dispositivo AltaVault

Después de seleccionar la opción AltaVault Appliance en la página Select the Target Type, se muestran las opciones de configuración para el tipo de destino AltaVault.

Antes de empezar

- Tiene la ruta de montaje NFS para un dispositivo AltaVault.
- Ha especificado el dispositivo AltaVault como tipo de destino.

Pasos

1. En el campo **Ruta de montaje NFS**, introduzca el punto de montaje para el tipo de destino AltaVault.

   Los valores del campo **Ruta de montaje de NFS** deben seguir el formato de ruta de Linux.

2. Active la casilla de verificación **Guardar una copia de seguridad de la base de datos de configuración en este destino** para crear una copia de seguridad de la base de datos de configuración en el tipo de destino seleccionado.

   Si se detecta una configuración de base de datos existente en el tipo de objetivo especificado al probar la conexión, tiene la opción de reemplazar la información de configuración de la base de datos existente en el host Cloud Connector de SANtricity con la nueva información de backup introducida en el asistente de configuración.

3. Haga clic en **probar conexión** para probar la conexión para los ajustes de AltaVault especificados.
4. Haga clic en **Siguiente**.

   El tipo de destino especificado para el conector cloud SANtricity se acepta y la página proxy de servicios web se muestra en el asistente de configuración.

5. Continúe con "Paso 4: Conectarse a Web Services Proxy".

Configure la cuenta de Amazon AWS

Después de seleccionar la opción Amazon AWS en la página Select the Target Type, se muestran las opciones de configuración para el tipo de destino de Amazon AWS.

Antes de empezar

- Tiene una cuenta de Amazon AWS establecida.
- Especificó Amazon AWS como tipo de destino.

Pasos

1. En el campo **ID de clave de acceso**, introduzca el identificador de acceso del destino de Amazon AWS.

2. En el campo **clave de acceso secreta**, introduzca la clave de acceso secreta del destino.
3. En el campo **Nombre de bloque**, introduzca el nombre de segmento del destino.
4. Seleccione la casilla de verificación **Guardar una copia de seguridad de la base de datos de configuración en este destino** para crear una copia de seguridad de la base de datos de configuración en el tipo de destino seleccionado.

   Se recomienda activar esta opción para garantizar que los datos del destino de copia de seguridad se puedan restaurar si se pierde la base de datos.

   Si se detecta una configuración de base de datos existente en el tipo de objetivo especificado al probar la conexión, tiene la opción de reemplazar la información de configuración de la base de datos existente en el host Cloud Connector de SANtricity con la nueva información de backup introducida en el asistente de configuración.

5. Haga clic en **probar conexión** para verificar las credenciales de Amazon AWS introducidas.
6. Haga clic en **Siguiente**.

   El tipo de destino especificado para el conector cloud de SANtricity se acepta y la página proxy de servicios web se muestra en el asistente de configuración.

7. Continúe con "Paso 4: Conectarse a Web Services Proxy".

Configure la cuenta de StorageGRID

Después de seleccionar la opción StorageGRID en la página Select the Target Type, se muestran las opciones de configuración para el tipo de destino StorageGRID.

Antes de empezar

- Tiene una cuenta de StorageGRID establecida.
- Tiene un certificado StorageGRID firmado en el almacén de claves del conector cloud de SANtricity.
- Especificó StorageGRID como el tipo de destino.

Pasos

1. En el campo **URL**, introduzca la dirección URL del servicio cloud de Amazon S3
2. En el campo **ID de clave de acceso**, introduzca el ID de acceso del destino S3.
3. En el campo **clave de acceso secreta**, introduzca la clave de acceso secreta del destino S3.
4. En el campo **Nombre de bloque**, introduzca el nombre de bloque para el destino S3.
5. Para utilizar el acceso al estilo de ruta, seleccione la casilla de verificación **usar acceso al estilo de ruta**.

   Si no está seleccionada, se utiliza el acceso al estilo de host virtual.

6. Seleccione la casilla de verificación **Guardar una copia de seguridad de la base de datos de configuración en este destino** para crear una copia de seguridad de la base de datos de configuración en el tipo de destino seleccionado.

   Se recomienda activar esta opción para garantizar que los datos del destino de copia de seguridad se puedan restaurar si se pierde la base de datos.

> Si se detecta una configuración de base de datos existente en el tipo de objetivo especificado al probar la conexión, tiene la opción de reemplazar la información de configuración de la base de datos existente en el host Cloud Connector de SANtricity con la nueva información de backup introducida en el asistente de configuración.

7. Haga clic en **probar conexión** para verificar las credenciales de S3 introducidas.

> Es posible que algunas cuentas compatibles con S3 requieran conexiones HTTP seguras. Para obtener información sobre cómo colocar un certificado StorageGRID en el almacén de claves, consulte "Añada el certificado StorageGRID a un almacén de claves".

8. Haga clic en **Siguiente**.

   El tipo de destino especificado para el conector cloud de SANtricity se acepta y la página proxy de servicios web se muestra en el asistente de configuración.

9. Continúe con "Paso 4: Conectarse a Web Services Proxy".

Paso 4: Conectarse al proxy de servicios web

La información de inicio de sesión y conexión para el proxy de servicios web que se utiliza junto con el conector cloud de SANtricity se introduce a través de la página Enter Web Services Proxy URL and Credentials.

Antes de empezar

Asegúrese de contar con una conexión establecida con el proxy de servicios web de SANtricity.

Pasos

1. En el campo **URL**, introduzca la URL del proxy de servicios web utilizado para el conector en nube de SANtricity.
2. En el campo **Nombre de usuario**, introduzca el nombre de usuario para la conexión del proxy de servicios web.
3. En el campo **Contraseña**, introduzca la contraseña para la conexión de proxy de servicios web.
4. Haga clic en **probar conexión** para verificar la conexión de las credenciales de proxy de servicios web introducidas.
5. Después de verificar las credenciales de proxy de servicios web introducidas mediante la conexión de prueba.
6. Haga clic en **Siguiente**

   Las credenciales de proxy de servicios web para el conector cloud de SANtricity se aceptan y la página Seleccionar cabinas de almacenamiento se muestra en el asistente de configuración.

Paso 5: Seleccione las cabinas de almacenamiento

Según las credenciales del proxy de servicios web de SANtricity introducidas mediante el asistente de configuración, se muestra una lista de las cabinas de almacenamiento disponibles en la página Seleccionar cabinas de almacenamiento. A través de esta página, puede seleccionar las cabinas de almacenamiento que el conector cloud de SANtricity utiliza para trabajos de backup y restauración.

Antes de empezar

Asegúrese de que haya cabinas de almacenamiento configuradas en la aplicación SANtricity Web Services Proxy.

> Las cabinas de almacenamiento inaccesibles observadas en la aplicación SANtricity Cloud Connector provocará excepciones de API en el archivo de registro. Este es el comportamiento esperado de la aplicación SANtricity Cloud Connector cada vez que se extrae una lista de volúmenes desde una cabina inaccesible. Para evitar estas excepciones de API en el archivo de registro, es posible resolver el problema raíz directamente con la cabina de almacenamiento o quitar la cabina de almacenamiento afectada de la aplicación SANtricity Web Services Proxy.

Pasos

1. Seleccione cada casilla de comprobación junto a la cabina de almacenamiento que desee asignar a la aplicación SANtricity Cloud Connector para operaciones de backup y restauración.
2. Haga clic en **Siguiente**.

   Se aceptan las matrices de almacenamiento seleccionadas y se muestra la página Seleccionar hosts en el Asistente de configuración.

   > Debe configurar una contraseña válida para todas las cabinas de almacenamiento seleccionadas en la página Seleccionar cabinas de almacenamiento. Es posible configurar contraseñas de las cabinas de almacenamiento mediante la documentación de la API de SANtricity Web Services Proxy.

Paso 6: Seleccione hosts

Según las cabinas de almacenamiento alojadas en el proxy de servicios web seleccionadas mediante el asistente de configuración, puede seleccionar un host disponible para asignar los volúmenes candidatos de backup y restaurar a la aplicación SANtricity Cloud Connector a través de la página Select hosts.

Antes de empezar

Asegúrese de contar con un host disponible a través del proxy de servicios web de SANtricity.

Pasos

1. En el menú desplegable de la cabina de almacenamiento enumerada, seleccione el host deseado.
2. Repita el paso 1 para todas las cabinas de almacenamiento adicionales que aparecen en la página Seleccionar host.
3. Haga clic en **Siguiente**.

   Se acepta el host seleccionado para el conector en nube de SANtricity y se muestra la página revisar en el asistente de configuración.

Paso 7: Revise la configuración inicial

En la última página del asistente de configuración de SANtricity Cloud Connector, se proporciona un resumen de los resultados introducidos para su revisión.

Revise los resultados de los datos de configuración validados.

- Si todos los datos de configuración se validan y establecen correctamente, haga clic en **Finalizar** para completar el proceso de configuración.

- Si no se puede validar alguna sección de los datos de configuración, haga clic en **Atrás** para ir a la página correspondiente del asistente de configuración y revisar los datos enviados.

Inicie sesión en el conector cloud de SANtricity

Puede acceder a la interfaz gráfica de usuario para la aplicación SANtricity Cloud Connector a través del servidor configurado en un explorador compatible. Asegúrese de tener una cuenta de conector de cloud de SANtricity establecida.

Pasos

1. En un explorador compatible, conéctese al servidor configurado de SANtricity Cloud Connector (por ejemplo, `http://localhost:8080/`).

   Aparece la página de inicio de sesión de la aplicación SANtricity Cloud Connector.

2. Introduzca la contraseña de administrador configurada.
3. Haga clic en **Inicio de sesión**.

   Aparece la página de destino de la aplicación SANtricity Cloud Connector.

Completos

Puede acceder a la opción backups en el panel de navegación izquierdo de la aplicación Cloud Connector de SANtricity. La opción backups muestra la página backups, que permite crear nuevos trabajos de backup basados en imágenes o basados en archivos.

Utilice la página **copias de seguridad** de la aplicación SANtricity Cloud Connector para crear y procesar copias de seguridad de los volúmenes E-Series. Es posible crear backups basados en imágenes o archivos y, luego, ejecutar esas operaciones de inmediato o más adelante. Además, puede elegir entre realizar backups completos o backups incrementales en función del último backup completo realizado. Puede realizarse un máximo de seis backups incrementales en función del último backup completo realizado mediante la aplicación Cloud Connector de SANtricity.

> Todas las marcas de hora de los trabajos de backup y restauración que se enumeran en la aplicación SANtricity Cloud Connector utilizan la hora local.

Cree un nuevo backup basado en imágenes

Puede crear nuevos backups basados en imágenes mediante la función Create en la página backups de la aplicación Cloud Connector de SANtricity.

Antes de empezar

Asegúrese de tener cabinas de almacenamiento del proxy de servicios web registrado en el conector cloud de SANtricity.

Pasos

1. En la página copias de seguridad, haga clic en **Crear**.

   Aparecerá la ventana Create Backup.

2. Seleccione **Crear una copia de seguridad basada en imágenes**.

3. Haga clic en **Siguiente**.

   Se muestra una lista de los volúmenes E-Series disponibles en la ventana Create Backup.

4. Seleccione el volumen de E-Series deseado y haga clic en **Siguiente**.

   Aparecerá la página **Nombre de la copia de seguridad y descripción** de la ventana de confirmación Crear copia de seguridad.

5. Para modificar el nombre de la copia de seguridad generada automáticamente, introduzca el nombre deseado en el campo **Nombre de trabajo**.
6. Si es necesario, agregue una descripción para la copia de seguridad en el campo **Descripción del trabajo**.

   Debe introducir una descripción del trabajo que permita identificar fácilmente el contenido de la copia de seguridad.

7. Haga clic en **Siguiente**.

   En la página **Review backup information** de la ventana Create Backup se muestra un resumen de la copia de seguridad basada en imagen seleccionada.

8. Revise la copia de seguridad seleccionada y haga clic en **Finalizar**.

   Aparecerá la página de confirmación de la ventana Create Backup.

9. Seleccione una de las siguientes opciones:
   - **SÍ** — inicia una copia de seguridad completa para la copia de seguridad seleccionada.
   - **NO** — no se realiza una copia de seguridad completa para la copia de seguridad basada en imagen seleccionada.

     Un backup completo para el backup basado en imágenes seleccionado se puede realizar más tarde mediante la función Run de la página backups.

10. Haga clic en **Aceptar**.

    El backup para el volumen E-Series seleccionado se inicia, y el estado de la tarea se muestra en la sección de lista de resultados de la página backups.

Cree una nueva copia de seguridad basada en archivos/carpetas

Puede crear nuevos backups basados en archivos/carpetas mediante la función Create en la página backups de la aplicación Cloud Connector de SANtricity.

Antes de empezar

Asegúrese de tener cabinas de almacenamiento del proxy de servicios web registrado en el conector cloud de SANtricity.

Una copia de seguridad basada en archivos realiza una copia de seguridad incondicional de todos los archivos del sistema de archivos especificado. No obstante, puede realizar una restauración selectiva de archivos y carpetas.

Pasos

1. En la página copias de seguridad, haga clic en **Crear**.

   Aparecerá la ventana Create Backup.

2. Seleccione **Crear una copia de seguridad basada en carpeta/archivo**.
3. Haga clic en **Siguiente**.

   En la ventana Create Backup se muestra una lista de los volúmenes que contienen sistemas de archivos disponibles para la copia de seguridad.

4. Seleccione el volumen deseado y haga clic en **Siguiente**.

   En la ventana Crear copia de seguridad se muestra una lista de los sistemas de archivos disponibles en el volumen seleccionado.

   > Si su sistema de archivos no aparece, compruebe que el tipo de sistema de archivos es compatible con la aplicación SANtricity Cloud Connector. Para obtener más información, consulte "Sistemas de archivos compatibles".

5. Seleccione el sistema de ficheros que desee que contenga la carpeta o los archivos que desea realizar la copia de seguridad y haga clic en **Siguiente**.

   Aparecerá la página **Nombre de la copia de seguridad y descripción** de la ventana de confirmación Crear copia de seguridad.

6. Para modificar el nombre de la copia de seguridad generada automáticamente, introduzca el nombre deseado en el campo **Nombre de trabajo**.
7. Si es necesario, agregue una descripción para la copia de seguridad en el campo **Descripción del trabajo**.

   > Debe introducir una descripción del trabajo que permita identificar fácilmente el contenido de la copia de seguridad.

8. Haga clic en **Siguiente**.

   Un resumen de la copia de seguridad basada en archivos/carpeta seleccionada se muestra en la página **revisar información de copia de seguridad** de la ventana Crear copia de seguridad.

9. Revise la copia de seguridad basada en archivos/carpeta seleccionada y haga clic en **Finalizar**.

   Aparecerá la página de confirmación de la ventana Create Backup.

10. Seleccione una de las siguientes opciones:
    - **SÍ** — inicia una copia de seguridad completa para la copia de seguridad seleccionada.
    - **NO** — no se realiza una copia de seguridad completa para la copia de seguridad seleccionada.

    > También se puede realizar un backup completo para el backup basado en archivos seleccionado más adelante mediante la función Run en la página backups.

11. Haga clic en **Cerrar**.

Se inicia el backup del volumen E-Series seleccionado, y el estado de la tarea se muestra en la sección de lista de resultados de la página Backup.

Ejecución de copias de seguridad completas e incrementales

Los backups completos e incrementales se pueden realizar con la función Run en la página backups. Los backups incrementales solo están disponibles para backups basados en archivos.

Antes de empezar

Asegúrese de haber creado una tarea de backup a través de SANtricity Cloud Connector.

Pasos

1. En la ficha copias de seguridad, seleccione el trabajo de copia de seguridad deseado y haga clic en **Ejecutar**.

   > Un backup completo se realiza automáticamente siempre que se selecciona una tarea de backup basado en imágenes o una tarea de backup sin un backup inicial realizado previamente.

   Aparecerá la ventana Run Backup.

2. Seleccione una de las siguientes opciones:
   - **Full** — realiza una copia de seguridad de todos los datos de la copia de seguridad basada en archivos seleccionada.
   - **Incremental** — copia de seguridad de los cambios realizados sólo desde la última copia de seguridad realizada.

     > Se puede realizar un número máximo de seis backups incrementales en función del último backup completo a través de la aplicación Cloud Connector de SANtricity.

3. Haga clic en **Ejecutar**.

   Se inicia la solicitud de respaldo.

Eliminar un trabajo de backup

La función Delete elimina los datos de los que se ha realizado una copia de seguridad en la ubicación de destino especificada para la copia de seguridad seleccionada junto con el conjunto de copia de seguridad.

Antes de empezar

Asegúrese de que hay una copia de seguridad con el estado completado, fallido o Cancelado.

Pasos

1. En la página copias de seguridad, seleccione la copia de seguridad deseada y haga clic en **Eliminar**.

   > Si se selecciona un backup base completo para eliminar, también se eliminan todos los backups incrementales asociados.

   Aparece la ventana Confirmar eliminación.

2. En el campo **Escriba delete**, escriba `DELETE` para confirmar la acción de eliminación.

3. Haga clic en **Eliminar**.

   Se elimina el backup seleccionado.

Restauraciones

Puede acceder a la opción Restore en el panel de navegación izquierdo de la aplicación Cloud Connector de SANtricity. La opción Restore muestra la página Restore, que permite crear nuevos trabajos de restauración basados en imágenes o basados en archivos.

El conector de cloud de SANtricity utiliza el concepto de trabajos para realizar la restauración real de un volumen de E-Series. Antes de realizar una restauración, debe identificar qué volumen E-Series se utilizará para la operación. Después de añadir un volumen E-Series para restaurar al host de SANtricity Cloud Connector, puede usar el `Restore` Página de la aplicación Cloud Connector de SANtricity para crear y procesar restauraciones.

> Todas las marcas de hora de los trabajos de backup y restauración que se enumeran en la aplicación SANtricity Cloud Connector utilizan la hora local.

Crear una nueva restauración basada en imágenes

Puede crear nuevas restauraciones basadas en imágenes mediante la función Crear en la página Restore de la aplicación Cloud Connector de SANtricity.

Antes de empezar

Asegúrese de tener disponible un backup basado en imágenes mediante SANtricity Cloud Connector.

Pasos

1. En la página Restaurar de la aplicación SANtricity Cloud Connector, haga clic en **Crear**.

   Aparecerá la ventana Restore (Restaurar).

2. Seleccione el backup que desee.
3. Haga clic en **Siguiente**.

   La página Select Backup Point aparece en la ventana Restore.

4. Seleccione el backup completado que desee.
5. Haga clic en **Siguiente**.

   La página Select Restore Target aparece en la ventana Restore.

6. Seleccione el volumen de restauración y haga clic en **Siguiente**.

   La página Review se muestra en la ventana Restore.

7. Revise la operación de restauración seleccionada y haga clic en **Finalizar**.

   La restauración para el volumen de host objetivo seleccionado se inicia, y el estado de la tarea se muestra en la sección de lista de resultados de la página Restore.

Crear una nueva restauración basada en archivos

Puede crear nuevas restauraciones basadas en archivos mediante la función Crear en la página Restore de la aplicación Cloud Connector de SANtricity.

Antes de empezar

Asegúrese de tener disponible un backup basado en archivos mediante el conector cloud de SANtricity.

Pasos

1. En la página Restaurar de la aplicación SANtricity Cloud Connector, haga clic en **Crear**.

   Aparecerá la ventana Restore (Restaurar).

2. En la ventana Restore, seleccione el backup basado en archivos que desee.
3. Haga clic en **Siguiente**.

   La página Select Backup Point aparece en la ventana Create Restore Job.

4. En la página Select Backup Point, seleccione la copia de seguridad completada que desee.
5. Haga clic en **Siguiente**.

   Se muestra una lista de la página sistemas de archivos o carpetas/archivos disponibles en la ventana Restore.

6. Seleccione las carpetas o archivos que desee restaurar y haga clic en **Siguiente**.

   La página Select Restore Target aparece en la ventana Restore.

7. Seleccione el volumen de restauración y haga clic en **Siguiente**.

   La página Review se muestra en la ventana Restore.

8. Revise la operación de restauración seleccionada y haga clic en **Finalizar**.

   La restauración para el volumen de host objetivo seleccionado se inicia, y el estado de la tarea se muestra en la sección de lista de resultados de la página Restore.

Eliminar una restauración

Puede utilizar la función Eliminar para eliminar un elemento de restauración seleccionado de la sección de lista de resultados de la página Restaurar.

Antes de empezar

Asegúrese de que hay un trabajo de restauración con el estado completado, fallido o Cancelado.

Pasos

1. En la página Restaurar, haga clic en **Eliminar**.

   Aparece la ventana Confirmar eliminación.

2. En el campo **Escriba delete**, escriba `delete` para confirmar la acción de eliminación.
3. Haga clic en **Eliminar**.

No se puede eliminar una restauración suspendida.

Se elimina la restauración seleccionada.

Modifique la configuración de SANtricity Cloud Connector

La opción Configuración permite modificar las configuraciones actuales de la aplicación para la cuenta de S3, las cabinas y los hosts gestionados, y las credenciales del proxy de servicios web. También puede cambiar la contraseña de la aplicación SANtricity Cloud Connector mediante la opción Configuración.

Modifique la configuración de la cuenta de S3

Puede modificar la configuración de S3 existente para la aplicación SANtricity Cloud Connector en la ventana S3 Account Settings.

Antes de empezar

Al modificar la configuración de etiqueta de bloque de S3 o URL, tenga en cuenta que afectará el acceso a los backups existentes configurados a través del conector cloud de SANtricity.

Pasos

1. En la barra de herramientas de la izquierda, haga clic en **Configuración > Configuración**.

   Aparecerá la página Configuración - Configuración.

2. Haga clic en **Ver/editar configuración** para la configuración de la cuenta de S3.

   Se mostrará la página S3 Account Settings.

3. En el archivo URL, introduzca la URL para el servicio cloud de S3.
4. En el campo **ID de clave de acceso**, introduzca el ID de acceso del destino S3.
5. En el campo **clave de acceso secreta**, introduzca la clave de acceso para el destino S3.
6. En el campo **S3 Bucket Name**, introduzca el nombre del bloque para el destino S3.
7. Seleccione la casilla de verificación **usar acceso de estilo de ruta** si es necesario.
8. Haga clic en **probar conexión** para verificar la conexión para las credenciales S3 introducidas.
9. Haga clic en **Guardar** para aplicar las modificaciones.

   Se aplicará la configuración de cuenta de S3 modificada.

Gestione las cabinas de almacenamiento

Es posible añadir o quitar cabinas de almacenamiento del proxy de servicios web registrado en el host del conector cloud de SANtricity en la página gestionar cabinas de almacenamiento.

La página gestionar cabinas de almacenamiento muestra una lista de las cabinas de almacenamiento del proxy de servicios web disponible para el registro con el host del conector cloud de SANtricity.

Pasos

1. En la barra de herramientas de la izquierda, haga clic en **Configuración > matrices de almacenamiento**.

Se muestra la pantalla Configuración - cabinas de almacenamiento.

2. Para agregar matrices de almacenamiento al conector en nube de SANtricity, haga clic en **Agregar**.
   a. En la ventana Add Storage Arrays, seleccione cada casilla de comprobación junto a las cabinas de almacenamiento que desee en la lista de resultados.
   b. Haga clic en **Agregar**.

      La cabina de almacenamiento seleccionada se añade al conector cloud de SANtricity y se muestra en la sección Lista de resultados de la pantalla Configuración - cabinas de almacenamiento.

3. Para modificar el host para una matriz de almacenamiento agregada, haga clic en **Editar** para el elemento de línea de la sección de lista de resultados de la pantalla Configuración - matrices de almacenamiento.
   a. En el menú desplegable Host asociado, seleccione el host que desea para la cabina de almacenamiento.
   b. Haga clic en **Guardar**.

      El host seleccionado se asigna a la cabina de almacenamiento.

4. Para eliminar una cabina de almacenamiento existente del host de SANtricity Cloud Connector, seleccione las cabinas de almacenamiento que desee en la lista de resultados inferior y haga clic en **Quitar**.
   a. En el campo Confirmar eliminación de cabina de almacenamiento, escriba `REMOVE`.
   b. Haga clic en **Quitar**.

      La cabina de almacenamiento seleccionada se quita del host de SANtricity Cloud Connector.

Modifique la configuración del proxy de servicios web

Puede modificar la configuración del proxy de servicios web existente para la aplicación SANtricity Cloud Connector de la ventana Configuración del proxy de servicios web.

Antes de empezar

El proxy de servicios web que se utiliza con el conector cloud de SANtricity debe añadir las cabinas adecuadas y establecer la contraseña correspondiente.

Pasos

1. En la barra de herramientas de la izquierda, haga clic en **MENU:Settings[Configuration]**.

   Aparecerá la pantalla Configuración - Configuración.

2. Haga clic en **Ver/editar configuración** para Web Services Proxy.

   Se muestra la pantalla de configuración del proxy de servicios web.

3. En el campo URL, introduzca la URL del proxy de servicios web utilizado para el conector cloud de SANtricity.
4. En el campo User Name, introduzca el nombre de usuario para la conexión del proxy de servicios web.
5. En el campo Password, introduzca la contraseña de la conexión del proxy de servicios web.
6. Haga clic en **probar conexión** para verificar la conexión de las credenciales de proxy de servicios web introducidas.

7. Haga clic en **Guardar** para aplicar las modificaciones.

Cambie la contraseña de SANtricity Cloud Connector

Puede cambiar la contraseña de la aplicación SANtricity Cloud Connector en la pantalla Cambiar contraseña.

Pasos

1. En la barra de herramientas de la izquierda, haga clic en **MENU:Settings[Configuration]**.

   Aparecerá la pantalla Configuración - Configuración.

2. Haga clic en **Cambiar contraseña** para el conector SANtricity en la nube.

   Se mostrará la pantalla Cambiar contraseña.

3. En el campo Contraseña actual, introduzca su contraseña actual para la aplicación SANtricity conector Cloud.
4. En el campo Nueva contraseña, introduzca su nueva contraseña para la aplicación SANtricity conector Cloud.
5. En el campo Confirm new password, vuelva a introducir la nueva contraseña.
6. Haga clic en **Cambiar** para aplicar la nueva contraseña.

   La contraseña modificada se aplica a la aplicación SANtricity Cloud Connector.

Desinstale el conector de cloud de SANtricity

Puede desinstalar el conector cloud de SANtricity mediante el desinstalador gráfico o el modo de consola.

Desinstale utilizando el modo gráfico

Puede utilizar el modo gráfico para desinstalar SANtricity Cloud Connector de un sistema operativo Linux.

Pasos

1. Desde una ventana de terminal, desplácese hasta el directorio que contiene el archivo de desinstalación del conector de cloud de SANtricity.

   El archivo de desinstalación para el conector cloud de SANtricity está disponible en la siguiente ubicación de directorio predeterminada:

   ```
   /opt/netapp/santricity_cloud_connector4/uninstall_cloud_connector4
   ```

2. En el directorio que contiene el archivo de desinstalación del conector de cloud de SANtricity, ejecute el siguiente comando:

   ```
   ./uninstall_cloud_connector4 -i gui
   ```

   Se ha inicializado el proceso de desinstalación para el conector cloud de SANtricity.

3. En la ventana de desinstalación, haga clic en **Desinstalar** para continuar con la desinstalación del conector en la nube de SANtricity.

   El proceso de desinstalación ha finalizado y la aplicación SANtricity Cloud Connector se desinstala en el sistema operativo Linux.

Desinstale mediante el modo de consola

Puede utilizar el modo de consola para desinstalar el conector en nube de SANtricity en un sistema operativo Linux.

Pasos

1. Desde una ventana de terminal, desplácese hasta el directorio que contiene el archivo de desinstalación del conector de cloud de SANtricity.

   El archivo de desinstalación para el conector cloud de SANtricity está disponible en la siguiente ubicación de directorio predeterminada:

   ```
   /opt/netapp/santricity_cloud_connector4/uninstall_cloud_connector4
   ```

2. En el directorio que contiene el archivo de desinstalación del conector de cloud de SANtricity, ejecute el siguiente comando:

   ```
   ./uninstall_cloud_connector4 -i console
   ```

   Se ha inicializado el proceso de desinstalación para el conector cloud de SANtricity.

3. En la ventana de desinstalación, pulse **Intro** para continuar con la desinstalación del conector en nube de SANtricity.

   El proceso de desinstalación ha finalizado y la aplicación SANtricity Cloud Connector se desinstala en el sistema operativo Linux.