Conector de cloud

E-Series storage systems

NetApp
January 20, 2026

Tabla de contenidos

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 SANtricity 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.

Utilice Cloud Connector de SANtricity para crear y gestionar backups de volúmenes de E-Series

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.

Cree nuevas restauraciones basadas en imágenes o en archivos en SANtricity Cloud Connector

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.