NetApp

Legacy solutions

E-Series storage systems

NetApp
January 20, 2026

Table of Contents

Legacy solutions

Cloud connector

Overview of the SANtricity® Cloud Connector

The SANtricity Cloud Connector is a host-based Linux application that enables you to perform full block-based and file-based backup and recovery of E-Series volumes to S3 complaint accounts (for example, Amazon Simple Storage Service and NetApp StorageGRID) and NetApp AltaVault appliance.

Available for installation on RedHat and SUSE Linux platforms, the SANtricity Cloud Connector is a packaged solution (.bin file). After you install SANtricity Cloud Connector, you can configure the application to perform backup and restore jobs for E-Series volumes to an AltaVault appliance or to your existing Amazon S3 or StorageGRID accounts. All jobs performed through the SANtricity Cloud Connector use REST-based APIs.

ⓘ   The SANtricity Cloud Connector tool is deprecated and no longer available for download.

Considerations

When using these procedures, be aware that:

- Configuration and backup/restore jobs described in these procedures apply to the graphical user interface version of the SANtricity Cloud Connector.

- REST API workflows for the SANtricity Cloud Connector application are not described in these procedures. For experienced developers, endpoints are available for each SANtricity Cloud Connector operation under the API documentation. The API documentation is accessible by navigating to `http://<hostname.domain>:<port>/docs` through a browser.

Types of backups

The SANtricity Cloud Connector provides two types of backups: image-based and file-based backups.

- **Image-based backup**

  An image-based backup reads the raw data blocks from a snapshot volume and backs them up to a file known as an image. All of the data blocks on the snapshot volume are backed up, including empty blocks, blocks occupied by deleted files, blocks associated with partitioning, and filesystem metadata. Image backups have the advantage of storing all information with the snapshot volume regardless of the partitioning scheme or filesystems on it.

  The image is not stored on the Backup Target as a single file, but is instead broken up into a series of data chunks, which are 64MB in size. The data chunks allow SANtricity Cloud Connector to use multiple connections to the backup target, thereby improving the performance of the backup process.

  For backups to StorageGRID and Amazon Web Services (S3), each data chunk uses a separate encryption key to encrypt the chunk. The key is a SHA256 hash consisting of the combination of a user supplied passphrase and the SHA256 hash of the user data. For backups to AltaVault, SANtricity Cloud Connector does not encrypt the data chunks as AltaVault performs this operation.

- **File-based backup**

A file-based backup reads the files contained with a filesystem partition and backs them up into a series of data chunks that are 64MB in size. A file-based backup does not back up deleted files or partitioning and filesystem metadata. As with image-based backups, the data chunks allow SANtricity Cloud Connector to use multiple connections to the backup target, thereby improving performance of the backup process.

For backups to StorageGRID and Amazon Web Services, each data chunk uses a separate encryption key to encrypt the chunk. The key is a SHA256 hash consisting of the combination of user-supplied pass phrase and the SHA256 hash of the user data. For backups to AltaVault, the data chunks are not encrypted by SANtricity Cloud Connector because AltaVault performs this operation.

System requirements for SANtricity Cloud Connector

Your system must meet compatibility requirements for the SANtricity Cloud Connector.

Host hardware requirements

Your hardware must meet the following minimum requirements:

- At least 5 GB of memory; 4 GB for the maximum configured heap size
- At least 5 GB of free disk space is required from the software installation

You must install the SANtricity Web Services Proxy to use the SANtricity Cloud Connector. You can install the Web Services Proxy locally or you can run the application remotely on a different sever. For information on installing the SANtricity Web Services Proxy, see the Web Services Proxy topics.

Supported browsers

The following browsers are supported with the SANtricity Cloud Connector application (minimum versions noted):

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

ⓘ API documentation for the SANtricity Cloud Connector application will not load when using the Compatibility View setting within the Microsoft Internet Explorer v11 browser. To ensure the API documentation displays properly under the Microsoft Internet Explorer v11 browser, it is recommended that the Compatibility View setting is disabled.

Compatible storage arrays and controller firmware

You should verify the compatibility of your storage arrays and firmware before using the SANtricity Cloud Connector application.

For a complete and up-to-date listing of all compatible storage arrays and firmware for the SANtricity Cloud Connector, see the NetApp Interoperability Matrix Tool.

Compatible operating systems

The SANtricity Cloud Connector 4.0 application is compatible with and supported on the following operating systems:

Operating System	Version	Architecture
Red Hat Enterprise Linux (RHEL)	7.x	64 bit
SUSE Linux Enterprise Server (SLES)	12.x	64 bit

Supported file systems

You must use supported file systems to perform backups and restores through the SANtricity Cloud Connector application.

The following file systems are supported for backup and restore operations under the SANtricity Cloud Connector application:

- ext2
- ext3
- ext4

Install SANtricity Cloud Connector

The SANtricity Cloud Connector packaged solution (.bin file) is available for RedHat and SUSE Linux platforms only.

You can install the SANtricity Cloud Connector application through graphical mode or console mode on a compatible Linux operating system. During the installation process, you must specify the non-SSL and SSL port numbers for the SANtricity Cloud Connector. When installed, the SANtricity Cloud Connector runs as a daemon process.

ⓘ The SANtricity Cloud Connector tool is deprecated and no longer available for download.

Before you begin

Review the following notes:

- If SANtricity Web Services Proxy is already installed on the same server as the SANtricity Cloud Connector, conflicts will occur between non-SSL port numbers and SSL port numbers conflicts. In this case, choose appropriate numbers for the non-SSL port and the SSL port during the SANtricity Cloud Connector installation.

- If any hardware changes are performed on your host, re-install the SANtricity Cloud Connector application to ensure encryption consistency.

- Backups created through version 3.1 of the SANtricity Cloud Connector application are not compatible with version 4.0 of the SANtricity Cloud Connector application. If you intend to maintain these backups, you must continue to use your previous version of the SANtricity Cloud Connector. To ensure successful installation of separate 3.1 and 4.0 releases of the SANtricity Cloud Connector, unique port numbers must be assigned for each version of the application.

Install Device Mapper Multipath (DM-MP)

Any host running the SANtricity Cloud Connector also must run Linux Device Mapper Multipath (DM-MP) and have the multipath-tools package installed.

The SANtricity Cloud Connector discovery process relies on the multipath tools package for discovery and recognition of the volumes and files to backup or restore. For more information on how to set up and configure the Device Mapper, see the *SANtricity Storage Manager Multipath Drivers Guide* for the release of SANtricity you are using under the E-Series and SANtricity Document Resources.

Install Cloud Connector

You can install SANtricity Cloud Connector on Linux operating systems in either graphical mode or console mode.

Graphical mode

You can use graphical mode to install the SANtricity Cloud Connector on a Linux operating system.

Before you begin

Designate a host location for the SANtricity Cloud Connector installation.

Steps

1. Download the SANtricity Cloud Connector installation file to the desired host location.
2. Open a terminal window.
3. Navigate to the directory file containing the SANtricity Cloud Connector installation file.
4. Start the SANtricity Cloud Connector installation process:

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

   In this command, `xxxx` designates the version number of the application.

   The Installer window is displayed.

5. Review the Introduction statement, and then click **Next**.

   The License Agreement for NetApp, Inc. Software is displayed within the installer window.

6. Accept the terms of the License Agreement, and then click **Next**.

   The Backups created with previous releases of SANtricity Cloud Connector page is displayed.

7. To acknowledge the Backups created with previous releases of SANtricity Cloud Connector message, click **Next**.

   > ⓘ To install version 4.0 of the SANtricity Cloud Connector while maintaining a previous version, unique port numbers must be assigned for each version of the application.

   The Choose Install page is displayed within the Installer window. The Where Would You Like to Install field displays the following default install folder: `opt/netapp/santricity_cloud_connector4/`

8. Choose one of the following options:

    ◦ To accept the default location, click **Next**.

    ◦ To change the default location, enter a new folder location. An Enter the Non SSL Jetty Port Number page is displayed. A default value of 8080 is assigned to the non-SSL port.

9. Choose one of the following options:

    ◦ To accept the default SSL port number, click **Next**.

    ◦ To change the default SSL port number, enter the new desired port number value.

10. Choose one of the following options:

    ◦ To accept the default Non SSL port number, click **Next**.

    ◦ To change the default Non SSL port number, enter the new desired port number value. The Pre-Installation Summary page is displayed.

11. Review the displayed Pre-Installation Summary, and then click **Install**.

    The installation of the SANtricity Cloud Connector begins and a Webserver Daemon Setup prompt is displayed.

12. Click **OK** to acknowledge the Webserver Daemon Setup prompt.

    The Installation Complete message is displayed.

13. Click **Done** to exit the SANtricity Cloud Connecter installer.

Console mode

You can use the console mode to install the SANtricity Cloud Connector on a Linux operating system.

Before you begin

Designate a host location for the SANtricity Cloud Connector installation.

Steps

1. Download the SANtricity Cloud Connector installation file to the desired IO host location.

2. Open a terminal window.

3. Navigate to the directory file containing the SANtricity Cloud Connector installation file.

4. Start the SANtricity Cloud Connector installation process:

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

In this command, `xxxx` indicates the version number of the application.

The installation process for the SANtricity Cloud Connector is initialized.

5. Press **Enter** to proceed with the installation process.

The End User License Agreement for NetApp, Inc. Software is displayed within the installer window.

ⓘ   To cancel the installation process at any time, type `quit` under the installer window.

6. Press **Enter** to proceed through each portion of the End User License Agreement.

   The License Agreement acceptance statement is displayed under the installer window.

7. To accept the terms of the End User License Agreement and proceed with the installation of the SANtricity Cloud Connector, enter `Y` and press **Enter** under the installer window.

   The Backups created with previous releases of SANtricity Cloud Connector page is displayed.

   > ⓘ If you do not accept the terms of the End User Agreement, type `N` and press **Enter** to terminate the installation process for the SANtricity Cloud Connector.

8. To acknowledge the Backups created with previous releases of SANtricity Cloud Connector message, press **Enter**.

   > ⓘ To install version 4.0 of the SANtricity Cloud Connector while maintaining a previous version, unique port numbers must be assigned for each version of the application.

   A Choose Install Folder message with the following default install folder for the SANtricity Cloud Connector is displayed:`/opt/netapp/santricity_cloud_connector4/`.

9. Choose one of the following options:
   - To accept the default install location, press **Enter**.
   - To change the default install location, enter the new folder location. An Enter the Non SSL Jetty Port Number message is displayed. A default value of 8080 is assigned to the Non SSL port.

10. Choose one of the following options:
    - To accept the default SSL port number, press **Next**.
    - To change the default SSL port number, enter the new desired port number value.

11. Choose one of the following options:
    - To accept the default Non SSL port number, press **Enter**.
    - To change the default Non SSL port number, enter the new port number value. The Pre-Installation Summary for the SANtricity Cloud Connector is displayed.

12. Review the displayed Pre-Installation Summary, and press **Enter**.

13. Press **Enter** to acknowledge the Webserver Daemon Setup prompt.

    The Installation Complete message is displayed.

14. Press **Enter** to exit the SANtricity Cloud Connecter installer.

Add server certificate and CA certificate into a keystore

To use a secure https connection from the browser to the SANtricity Cloud Connector host, you can accept the self-signed certificate from the SANtricity Cloud Connector host or add a certificate and a trust chain recognized by both the browser and the SANtricity Cloud Connector application.

Before you begin

The SANtricity Cloud Connector application must be installed on a host.

Steps

1. Stop the service using the `systemctl` command.

2. From the default install location, access the working directory.

   > ⓘ The default install location for the SANtricity Cloud Connector is `/opt/netapp/santricity_cloud_connector4`.

3. Using the `keytool` command, create your server certificate, and certificate signing request (CSR).

   EXAMPLE

   ```
   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. Send the generated CSR to the certificate authority (CA) of your choosing.

   The certificate authority signs the certificate request and returns a signed certificate. In addition, you receive a certificate from the CA itself. This CA certificate must be imported into your keystore.

5. Import the certificate and the CA certificate chain into the application keystore: `/<install Path>/working/keystore`

   EXAMPLE

   ```
   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. Restart the service.

Add StorageGRID certificate into a keystore

If you are configuring StorageGRID as the target type for the SANtricity Cloud Connector application, you must first add a StorageGRID certificate into the SANtricity Cloud Connector keystore.

Before you begin

- You have a signed StorageGRID certificate.
- You have the SANtricity Cloud Connector application installed on a host.

Steps

1. Stop the service using the `systemctl` command.

2. From the default install location, access the working directory.

> ⓘ The default install location for the SANtricity Cloud Connector is
> `/opt/netapp/santricity_cloud_connector4`.

3. Import the StorageGRID certificate into the application keystore: `/<install Path>/working/keystore`

   EXAMPLE

   ```
   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. Restart the service.

Configure the SANtricity Cloud Connector for the first time

Upon successful installation, you can set up the SANtricity Cloud Connector application through the configuration wizard. The configuration wizard is displayed after you initially log in to the SANtricity Cloud Connector.

Log in to the SANtricity Cloud Connector for the first time

When initializing the SANtricity Cloud Connector for the first time, you must enter a default password to access the application.

Before you begin
Make sure you have access to an internet-connected browser.

Steps
1. Open a supported browser.
2. Connect to the configured SANtricity Cloud Connector server (e.g., `http://localhost:8080/`).

   The initial login page for the SANtricity Cloud Connector application is displayed.

3. In the Administrator Password field, enter the default password of `password`.
4. Click **Log In**.

   The SANtricity Cloud Connector Configuration Wizard is displayed.

Using the Configuration Wizard

The Configuration Wizard is displayed upon successful initial login to the SANtricity Cloud Connector.

Through the Configuration Wizard, you set up the administrator password, Web Services Proxy login management credentials, desired backup target type, and encryption pass phrase for the SANtricity Cloud Connector.

Step 1: Set administrator password

You can customize the password used for subsequent logins to the SANtricity Cloud Connector through the Set Administrator Password page.

Establishing a password through the Set Administrator Password page effectively replaces the default password used during the initial login for the SANtricity Cloud Connector application.

Steps

1. On the Set Administrator Password page, enter the desired login password for the SANtricity Cloud Connector in the **Enter the new administrator password** field.

2. In the **Re-enter the new administrator password** field, re-enter the password from first field.

3. Click **Next**.

   The password setup for the SANtricity Cloud Connector is accepted and the Set Pass Phrase page is displayed under the Configuration Wizard.

   > ⓘ The user defined administrator password is not set until you complete the configuration
   >   wizard.

Step 2: Set pass phrase

Under the Enter the Encryption Pass Phrase page, you can specify an alphanumeric pass phrase between 8 and 32 characters.

A user-specified pass phrase is required as part of the data encryption key used by the SANtricity Cloud Connector application.

Steps

1. In the **Define a pass phrase** field, enter the desired pass phrase.

2. In the **Re-enter your pass phrase** field, re-enter the pass phrase from the first field.

3. Click **Next**.

   The entered pass phrase for the SANtricity Cloud Connector application is accepted and the Select Target Type page for the configuration wizard is displayed.

Step 3: Select target type

Backup and restore capabilities are available for Amazon S3, AltaVault, and StorageGRID target types through the SANtricity Cloud Connector. You can specify the desired storage target type for the SANtricity Cloud Connector application under the Select the Target Type page.

Before you begin

Make sure you have one of the following: AltaVault mount point, Amazon AWS account, or StorageGRID account.

Steps

1. In the dropdown menu, select one of the following options:

   ◦ Amazon AWS

   ◦ AltaVault

◦ StorageGRID

    A Target Type page for the selected option is displayed in the Configuration Wizard.

  2. Refer to the appropriate configuration instructions for AltaVault, Amazon AWS, or StorageGRID.

Configure AltaVault appliance

After selecting the AltaVault appliance option under the Select the Target Type page, configuration options for the AltaVault target type are displayed.

Before you begin

- You have the NFS mount path for an AltaVault appliance.
- You specified AltaVault appliance as the target type.

Steps

1. In the **NFS Mount Path** field, enter the mount point for the AltaVault target type.

   > ℹ️ Values in the **NFS Mount Path** field must follow the Linux path format.

2. Select the **Save a backup of the configuration database on this target** check box to create a backup of the configuration database on the selected target type.

   > ℹ️ If an existing database configuration is detected on the specified target type when testing the connection, you have the option of replacing the existing database configuration information on the SANtricity Cloud Connector host with the new backup information entered under the configuration wizard.

3. Click **Test Connection** to test the connection for the specified AltaVault settings.

4. Click **Next**.

   The specified target type for the SANtricity Cloud Connector is accepted and the Web Services Proxy page is displayed in the Configuration Wizard.

5. Proceed to "Step 4: Connect to Web Services Proxy."

Configure Amazon AWS account

After selecting the Amazon AWS option under the Select the Target Type page, configuration options for the Amazon AWS target type are displayed.

Before you begin

- You have an established Amazon AWS account.
- You specified Amazon AWS as the target type.

Steps

1. In the **Access Key ID** field, enter the access ID for the Amazon AWS target.

2. In the **Secret Access Key** field, enter the secret access key for the target.

3. In the **Bucket Name** field, enter the bucket name for the target.

4. Select the **Save a backup of the configuration database on this target** checkbox to create a backup of

the configuration database on the selected target type.

> ⓘ It is recommended you enable this setting to ensure that data from the backup target can be restored if the database is lost.

> ⓘ If an existing database configuration is detected on the specified target type when testing the connection, you have the option of replacing the existing database configuration information on the SANtricity Cloud Connector host with the new backup information entered under the configuration wizard.

5. Click **Test Connection** to verify the entered Amazon AWS credentials.

6. Click **Next**.

   The specified target type for the SANtricity Cloud Connector is accepted, and the Web Services Proxy page is displayed under the Configuration Wizard.

7. Proceed to "Step 4: Connect to Web Services Proxy."

Configure StorageGRID account

After selecting the StorageGRID option under the Select the Target Type page, configuration options for the StorageGRID target type are displayed.

Before you begin
- You have an established StorageGRID account.
- You have a signed StorageGRID certificate in the SANtricity Cloud Connector keystore.
- You specified StorageGRID as the target type.

Steps
1. In the **URL** field, enter the URL for the Amazon S3 cloud service

2. In the **Access Key ID** field, enter the access ID for the S3 target.

3. In the **Secret Access Key** field, enter the secret access key for the S3 target.

4. In the **Bucket Name** field, enter the bucket name for the S3 target.

5. To use path style access, select the **Use path-style access** checkbox.

> ⓘ If unchecked, virtual host-style access is used.

6. Select the **Save a backup of the configuration database on this target** checkbox to create a backup of the configuration database on the selected target type.

> ⓘ It is recommended you enable this setting to ensure that data from the backup target can be restored if the database is lost.

> ⓘ If an existing database configuration is detected on the specified target type when testing the connection, you have the option of replacing the existing database configuration information on the SANtricity Cloud Connector host with the new backup information entered in the configuration wizard.

7. Click **Test Connection** to verify the entered S3 credentials.

> (i) Some S3-compliant accounts may require secured HTTP connections. For information on placing a StorageGRID certificate in the keystore, see Add StorageGRID certificate into a keystore.

8. Click **Next**.

   The specified target type for the SANtricity Cloud Connector is accepted and the Web Services Proxy page is displayed under the Configuration Wizard.

9. Proceed to "Step 4: Connect to Web Services Proxy."

Step 4: Connect to Web Services Proxy

Login and connection information for the Web Services Proxy used in conjunction with the SANtricity Cloud Connector is entered through the Enter Web Services Proxy URL and Credentials page.

Before you begin

Make sure you have an established connection to the SANtricity Web Services Proxy.

Steps

1. In the **URL** field, enter the URL for the Web Services Proxy used for the SANtricity Cloud Connector.
2. In the **User Name** field, enter the user name for the Web Services Proxy connection.
3. In the **Password** field, enter the password for the Web Services Proxy connection.
4. Click **Test Connection** to verify the connection for the entered Web Services Proxy credentials.
5. After verifying the entered Web Services Proxy credentials through the test connection.
6. Click **Next**

   The Web Services Proxy credentials for the SANtricity Cloud Connector is accepted and the Select Storage Arrays page is displayed in the Configuration Wizard.

Step 5: Select storage arrays

Based on the SANtricity Web Services Proxy credentials entered through the Configuration Wizard, a list of available storage arrays is displayed under the Select Storage Arrays page. Through this page, you can select which storage arrays the SANtricity Cloud Connector uses for backup and restore jobs.

Before you begin

Make sure you have storage arrays configured to your SANtricity Web Services Proxy application.

> (i) Unreachable storage arrays observed by the SANtricity Cloud Connector application will result in API exceptions in the log file. This is the intended behavior of the SANtricity Cloud Connector application whenever a volume list is pulled from an unreachable array. To avoid these API exceptions in the log file, you can resolve the root issue directly with the storage array or remove the affected storage array from the SANtricity Web Services Proxy application.

Steps

1. Select each checkbox next to the storage array that you want to assign to the SANtricity Cloud Connector application for backup and restore operations.

2. Click **Next**.

   The selected storage arrays are accepted, and the Select Hosts page is displayed in the Configuration Wizard.

   > ⓘ You must configure a valid password for any storage array selected under the Select Storage Arrays page. You can configure storage array passwords through the SANtricity Web Services Proxy API Documentation.

Step 6: Select hosts

Based on the Web Services Proxy-hosted storage arrays selected through the Configuration Wizard, you can select an available host to map backup and restore candidate volumes to the SANtricity Cloud Connector application through the Select Hosts page.

Before you begin

Make sure you have a host available through the SANtricity Web Services Proxy.

Steps

1. In the drop-down menu for the listed storage array, select the desired host.

2. Repeat step 1 for any additional storage arrays listed under the Select Host page.

3. Click **Next**.

   The selected host for the SANtricity Cloud Connector is accepted and the Review page is displayed in the Configuration Wizard.

Step 7: Review the initial configuration

The final page of the SANtricity Cloud Connector configuration wizard provides a summary of the entered results for your review.

Review the results of the validated configuration data.

- If all configuration data is successfully validated and established, click **Finish** to complete the configuration process.

- If any section of the configuration data cannot be validated, click **Back** to navigate to the applicable page of the configuration wizard to revise the submitted data.

Log into the SANtricity Cloud Connector

You can access the graphical user interface for the SANtricity Cloud Connector application through the configured server in a supported browser. Make sure you have an established SANtricity Cloud Connector account.

Steps

1. In a supported browser, connect to the configured SANtricity Cloud Connector server (for example, `http://localhost:8080/`).

   The login page for the SANtricity Cloud Connector application is displayed.

2. Enter your configured administrator password.

3. Click **Login**.

   The landing page for the SANtricity Cloud Connector application is displayed.

Use SANtricity Cloud Connector to create and manage E-Series volume backups

You can access the Backups option in the left navigation panel of the SANtricity Cloud Connector application. The Backups option displays the Backups page, which allows you to create new image-based or file-based backup jobs.

Use the **Backups** page of the SANtricity Cloud Connector application to create and process backups of E-Series volumes. You can create image-based or file-based backups and then perform those operations immediately or at a later time. In addition, you can choose to perform full backups or incremental backups based on the last performed full backup. A maximum of six incremental backups can be performed based on the last full backup performed through the SANtricity Cloud Connector application.

> ⓘ All timestamps for backup and restore jobs listed under the SANtricity Cloud Connector
> application use local time.

Create a new image-based backup

You can create new image-based backups through the Create function on the Backups page of the SANtricity Cloud Connector application.

Before you begin

Make sure you have storage arrays from the Web Services Proxy registered to the SANtricity Cloud Connector.

Steps

1. In the Backups page, click **Create**.

   The Create Backup window is displayed.

2. Select **Create an image-based backup**.

3. Click **Next**.

   A list of available E-Series volumes is displayed in the Create Backup window.

4. Select the desired E-Series volume and click **Next**.

   The **Name the backup and provide a description** page of Create Backup confirmation window is displayed.

5. To modify the auto-generated backup name, enter the desired name in the **Job Name** field.

6. If needed, add a description for the backup in the **Job Description** field.

> ⓘ You should enter a job description that allows you to easily identify the contents of the
> backup.

7. Click **Next**.

A summary of the selected image-based backup is displayed under the **Review backup information** page of the Create Backup window.

8. Review the selected backup and click **Finish**.

   The confirmation page of the Create Backup window is displayed.

9. Select one of the following options:

   ◦ **YES** — Initiates a full backup for the selected backup.

   ◦ **NO** — A full backup for the selected image-based backup is not performed.

   > ⓘ   A full backup for the selected image-based backup can be performed at a later time through the Run function on the Backups page.

10. Click **OK**.

    The backup for the selected E-Series volume is initiated, and the status for the task is displayed under the result list section of the Backups page.

Create a new folder/file-based backup

You can create new folder/file-based backups through the Create function on the Backups page of the SANtricity Cloud Connector application.

Before you begin

Make sure you have storage arrays from the Web Services Proxy registered to the SANtricity Cloud Connector.

A file-based backup unconditionally backs up all files on the filesystem you specify. However, you can perform a selective restore of files and folders.

Steps

1. In the Backups page, click **Create**.

   The Create Backup window is displayed.

2. Select **Create a folder/file-based backup**.

3. Click **Next**.

   A list of volumes containing file systems available for backup is displayed in the Create Backup window.

4. Select the desired volume and click **Next**.

   A list of available filesystems on the selected volume is displayed in the Create Backup window.

   > ⓘ   If your filesystem does not appear, verify your filesystem type is supported by the SANtricity Cloud Connector application. For more information, refer to Supported file systems.

5. Select the desired filesystem containing the folder or files to backup, and click **Next**.

   The **Name the backup and provide a description** page of Create Backup confirmation window is displayed.

6. To modify the auto-generated backup name, enter the desired name in the **Job Name** field.

7. If needed, add a description for the backup in the **Job Description** field.

> (i) You should enter a job description that allows you to easily identify the contents of the backup.

8. Click **Next**.

   A summary of the selected folder/file-based backup is displayed under the **Review backup information** page of the Create Backup window.

9. Review the selected folder/file-based backup and click **Finish**.

   The confirmation page of the Create Backup window is displayed.

10. Select one of the following options:

    ◦ **YES** — Initiates a full backup for the selected backup.

    ◦ **NO** — A full backup for the selected backup is not performed.

    > (i) A full backup for the selected file-based backup can also be performed at a later time through the Run function on the Backups page.

11. Click **Close**.

    The backup for the selected E-Series volume is initiated, and the status for the task is displayed under the result list section of the Backup page.

Run Full and Incremental Backups

You can perform full and incremental backups through the Run function on the Backups page. Incremental backups are only available for file-based backups.

Before you begin

Make sure you have created a backup job through the SANtricity Cloud Connector.

Steps

1. In the Backups tab, select the desired backup job and click **Run**.

   > (i) A full backup is performed automatically whenever an image-based backup job or a backup job without a previously performed initial backup is selected.

   The Run Backup window is displayed.

2. Select one of the following options:

   ◦ **Full** — Backs up all data for the selected file-based backup.

   ◦ **Incremental** — Backs up changes made only since the last performed backup.

   > (i) A maximum number of six incremental backups can be performed based on the last full backup performed through the SANtricity Cloud Connector application.

3. Click **Run**.

   The backup request is initiated.

Delete a backup job

The Delete function deletes backed up data at the specified target location for the selected backup along with backup set.

Before you begin

Make sure there is a backup with a status of Completed, Failed, or Canceled.

Steps

1. In the Backups page, select the desired backup and click **Delete**.

   > (i) If a full base backup is selected for deletion, all associated incremental backups are also deleted.

   The Confirm Delete window is displayed.

2. In the **Type delete** field, type `DELETE` to confirm the delete action.
3. Click **Delete**.

   The selected backup is deleted.

Create new image-based or file-based restores in SANtricity Cloud Connector

You can access the Restore option in the left navigation panel of the SANtricity Cloud Connector application. The Restore option displays the Restore page, which allows you to create new image-based or file-based restore jobs.

The SANtricity Cloud Connector uses the concept of jobs to perform the actual restore of an E-Series volume. Before performing a restore, you must identify which E-Series volume will be used for the operation. After you add an E-Series volume for restore to the SANtricity Cloud Connector host, you can use the `Restore` page of the SANtricity Cloud Connector application to create and process restores.

> (i) All timestamps for backup and restore jobs listed under the SANtricity Cloud Connector application use local time.

Create a new image-based restore

You can create new image-based restores through the Create function on the Restore page of the SANtricity Cloud Connector application.

Before you begin

Make sure you have an image-based backup available through the SANtricity Cloud Connector.

Steps

1. In the Restore page of the SANtricity Cloud Connector application, click **Create**.

The Restore window is displayed.

2. Select the desired backup.
3. Click **Next**.

   The Select Backup Point page is displayed in the Restore window.

4. Select the desired completed backup.
5. Click **Next**.

   The Select Restore Target page is displayed in the Restore window.

6. Select the restore volume and click **Next**.

   The Review page is displayed in the Restore window.

7. Review the selected restore operation and click **Finish**.

   The restore for the selected target host volume is initiated, and the status for the task is displayed in the result list section of the Restore page.

Create a new file-based restore

You can create new file-based restores through the Create function in the Restore page of the SANtricity Cloud Connector application.

Before you begin

Make sure you have a file-based backup available through the SANtricity Cloud Connector.

Steps

1. In the Restore page of the SANtricity Cloud Connector application, click **Create**.

   The Restore window is displayed.

2. In the Restore window, select the desired file-based backup.
3. Click **Next**.

   The Select Backup Point page is displayed in the Create Restore Job window.

4. In the Select Backup Point page, select the desired completed backup.
5. Click **Next**.

   A list of available filesystems or folders/files page is displayed in the Restore window.

6. Select the desired folders or files to restore and click **Next**.

   The Select Restore Target page is displayed in the Restore window.

7. Select the restore volume and click **Next**.

   The Review page is displayed in the Restore window.

8. Review the selected restore operation and click **Finish**.

The restore for the selected target host volume is initiated, and the status for the task is displayed in the result list section of the Restore page.

Delete a restore

You can use the Delete function to delete a selected restore item from the result list section of the Restore page.

Before you begin

Make sure there is a restore job with a status of Completed, Failed or Canceled.

Steps

1. In the Restore page, click **Delete**.

   The Confirm Delete window is displayed.

2. In the **Type delete** field, type `delete` to confirm the delete action.

3. Click **Delete**.

   (i)   You cannot delete a suspended restore.

   The selected restore is deleted.

Modify the SANtricity Cloud Connector settings

The Settings option allows you to modify the application's current configurations for the S3 account, managed storage arrays and hosts, and Web Services Proxy credentials. You can also change the password for the SANtricity Cloud Connector application through the Settings option.

Modify S3 Account settings

You can modify existing S3 settings for the SANtricity Cloud Connector application in the S3 Account Settings window.

Before you begin

When modifying the URL or S3 Bucket Label settings, be aware that access to any existing backups configured through the SANtricity Cloud Connector will be affected.

Steps

1. In the left toolbar, click **Settings > Configuration**.

   The Settings - Configuration page is displayed.

2. Click **View/Edit Settings** for S3 Account Settings.

   The S3 Account Settings page is displayed.

3. In the URL file, enter the URL for the S3 cloud service.

4. In the **Access Key ID** field, enter the access ID for the S3 target.

5. In the **Secret Access Key** field, enter the access key for the S3 target.

6. In the **S3 Bucket Name** field, enter the bucket name for the S3 target.

7. Select the **Use Path Style Access** check box if needed.

8. Click **Test Connection** to verify the connection for the entered S3 credentials.

9. Click **Save** to apply the modifications.

   The modified S3 account settings are applied.

Manage storage arrays

You can add or remove storage arrays from the Web Services Proxy registered to the SANtricity Cloud Connector host in the Manage Storage Arrays page.

The Manage Storage Arrays page displays a list of storage arrays from the Web Services Proxy available for registration with the SANtricity Cloud Connector host.

Steps

1. In the left toolbar, click **Settings > Storage Arrays**.

   The Settings - Storage Arrays screen is displayed.

2. To add storage arrays to the SANtricity Cloud Connector, click **Add**.

   a. In the Add Storage Arrays window, select each checkbox next to the desired storage arrays from the result list.

   b. Click **Add**.

   The selected storage array is added to the SANtricity Cloud Connector and displays in the result list section of the Settings - Storage Arrays screen.

3. To modify the host for an added storage array, click **Edit** for the line item in the result list section of the Settings - Storage Arrays screen.

   a. In the Associated Host drop-down menu, select the desired host for the storage array.

   b. Click **Save**.

   The selected host is assigned to the storage array.

4. To remove an existing storage array from the SANtricity Cloud Connector host, select the desired storage arrays from the bottom result list, and click **Remove**.

   a. In the Confirm Remove Storage Array field, type `REMOVE`.

   b. Click **Remove**.

   The selected storage array is removed from the SANtricity Cloud Connector host.

Modify Web Services Proxy settings

You can modify existing Web Services Proxy settings for the SANtricity Cloud Connector application in the Web Services Proxy Settings window.

Before you begin

The Web Services Proxy used with the SANtricity Cloud Connector needs to have the appropriate arrays added and the corresponding password set.

Steps

1. In the left toolbar, click **Settings › Configuration**.

   The Settings - Configuration screen is displayed.

2. Click **View/Edit Settings** for Web Services Proxy.

   The Web Services Proxy settings screen is displayed.

3. In the URL field, enter the URL for the Web Services proxy used for the SANtricity Cloud Connector.
4. In the User Name field, enter the user name for the Web Services Proxy connection.
5. In the Password field, enter the password for the Web Services Proxy connection.
6. Click **Test Connection** to verify the connection for the entered Web Services Proxy credentials.
7. Click **Save** to apply the modifications.

Change SANtricity Cloud Connector password

You can change the password for the SANtricity Cloud Connector application in the Change Password screen.

Steps

1. In the left toolbar, click **Settings › Configuration**.

   The Settings - Configuration screen is displayed.

2. Click **Change Password** for SANtricity Cloud Connector.

   The Change Password screen is displayed.

3. In the Current password field, enter your current password for the SANtricity Cloud Connector application.
4. In the New Password field, enter your new password for the SANtricity Cloud Connector application.
5. In the Confirm new password field, re-enter the new password.
6. Click **Change** to apply the new password.

   The modified password is applied to the SANtricity Cloud Connector application.

Uninstall the SANtricity Cloud Connector

You can uninstall the SANtricity Cloud Connector through the graphical uninstaller or console mode.

Uninstall using graphical mode

You can use the graphical mode to uninstall the SANtricity Cloud Connector on a Linux operating system.

Steps

1. From a terminal window, navigate to the directory containing the SANtricity Cloud Connector uninstall file.

The uninstall file for the SANtricity Cloud Connector is available at the following default directory location:

```
/opt/netapp/santricity_cloud_connector4/uninstall_cloud_connector4
```

2. From the directory containing the SANtricity Cloud Connector uninstall file, run the following command:

```
./uninstall_cloud_connector4 -i gui
```

The uninstall process for the SANtricity Cloud Connector is initialized.

3. In the uninstall window, click **Uninstall** to proceed with uninstalling the SANtricity Cloud Connector.

The uninstall process is completed, and the SANtricity Cloud Connector application is uninstalled in the Linux operating system.

Uninstall using console mode

You can use the console mode to uninstall the SANtricity Cloud Connector on a Linux operating system.

Steps

1. From a terminal window, navigate to the directory containing the SANtricity Cloud Connector uninstall file.

The uninstall file for the SANtricity Cloud Connector is available at the following default directory location:

```
/opt/netapp/santricity_cloud_connector4/uninstall_cloud_connector4
```

2. From the directory containing the SANtricity Cloud Connector uninstall file, run the following command:

```
./uninstall_cloud_connector4 -i console
```

The uninstall process for the SANtricity Cloud Connector is initialized.

3. In the uninstall window, press **Enter** to proceed with uninstalling the SANtricity Cloud Connector.

The uninstall process is completed, and the SANtricity Cloud Connector application is uninstalled in the Linux operating system.