



SANtricity® software

SANtricity® Cloud Connector

Installing and Using

August 2019 | 215-13875_2019-08_en-us
doccomments@netapp.com

Contents

About this Guide	5
Decide whether to use this guide	5
Understand the SANtricity Cloud Connector	5
Types of backup	5
System requirements	6
Host hardware requirements	6
Supported browsers	6
Compatible storage arrays and controller firmware	6
Compatible operating systems	7
Supported file systems	7
Install SANtricity Cloud Connector	8
Install Device Mapper Multipath (DM-MP)	8
Install the SANtricity Cloud Connector on a Linux Operating System in graphical mode	8
Install the SANtricity Cloud Connector on a Linux Operating System in console mode	10
Add server certificate and CA certificate into a keystore	11
Add StorageGRID certificate into a keystore	12
Configure the SANtricity Cloud Connector for the first time	13
Log in to the SANtricity Cloud Connector for the first time	13
Configuration Wizard	13
Set Administrator Password	14
Set Pass Phrase	14
Select Target Type	15
Connect to Web Services Proxy	18
Complete the initial configuration of the SANtricity Cloud Connector	19
Use the SANtricity Cloud Connector	20
Log into the SANtricity Cloud Connector	20
Backups	21
Create a new image-based backup	21
Create a new folder/file-based backup	22
Run Full and Incremental Backups	23
Delete a backup job	24
Restores	24
Create a new image-based restore	25
Create a new file-based restore	25
Delete a restore	26
Modify the SANtricity Cloud Connectors Settings	26
S3 Account Settings	27
Manage Storage Arrays	27
Web Services Settings	28

- Change SANtricity Cloud Connector password 28
- Uninstall the SANtricity Cloud Connector 30**
 - Uninstall the SANtricity Cloud Connector through graphical mode 30
 - Uninstall the SANtricity Cloud Connector through console mode 30
- Copyright 32**
- Trademark 33**
- How to send comments about documentation and receive update notifications 34**

About this Guide

This guide describes how to install, configure, use, and uninstall the NetApp SANtricity Cloud Connector.

Decide whether to use this guide

You use this guide when you want to install, use, or uninstall the SANtricity Cloud Connector.

This guide describes general concepts, setup, installation, configuration, and jobs associated with the SANtricity Cloud Connector application. Configuration and backup/restore job procedures described within this guide apply to the graphical user interface version of the SANtricity Cloud Connector. REST API workflows for the SANtricity Cloud Connector application are not included in this guide. 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.

Understand 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 compliant 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.

Types of backup

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

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

Host hardware requirements

Before installing the SANtricity Cloud Connector, you must make sure that your system meets the following 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 NetApp SANtricity Web Services Proxy Installing and Using guide under the [E-Series Documentation Center](#).

Supported browsers

You must use only supported browsers with the SANtricity Cloud Connector application.

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

Note: 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

You must have a compatible operating system to use the SANtricity Cloud Connector application.

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.

Note: 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.

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

Note: 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 the SANtricity Cloud Connector on a Linux Operating System in graphical mode

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

Before you begin

- You have a designated 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**.

Note: 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 Connector installer.

Install the SANtricity Cloud Connector on a Linux Operating System in console mode

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

Before you begin

- You have a designated 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.

Note: 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.

Note: 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**.

Note: 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 Connector 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

- 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.

Note: 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.
Note: 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.

Steps

1. [Log in to the SANtricity Cloud Connector for the first time](#) on page 13
When initializing the SANtricity Cloud Connector for the first time, you must enter a default password to access the application.
2. [Configuration Wizard](#) on page 13
The Configuration Wizard is displayed upon successful initial login 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

- 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.

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.

Steps

1. [Set Administrator Password](#) on page 14
You can customize the password used for subsequent logins to the SANtricity Cloud Connector through the Set Administrator Password page.

2. [Set Pass Phrase](#) on page 14
Under the Enter the Encryption Pass Phrase page, you can specify an alphanumeric pass phrase between 8 and 32 characters.
3. [Select Target Type](#) on page 15
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.
4. [Connect to Web Services Proxy](#) on page 18
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.
5. [Complete the initial configuration of the SANtricity Cloud Connector](#) on page 19
The final page of the SANtricity Cloud Connector configuration wizard provides a summary of the entered results for your review.

Set Administrator Password

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

About this task

Establishing a password through the Set Administrator Password screen 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.

Note: The user defined administrator password is not set until you complete the configuration wizard.

After you finish

Go to [Set Pass Phrase](#) on page 14.

Set Pass Phrase

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

About this task

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.

After you finish

Go to [Select Target Type](#) on page 15.

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

- You have an established AltaVault mount point, Amazon AWS account, or StorageGRID account.

Step

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.

Choices

- [AltaVault Appliance](#) on page 15
After selecting the AltaVault appliance option under the `Select the Target Type` page, configuration options for the AltaVault target type are displayed.
- [Amazon AWS Account](#) on page 16
After selecting the Amazon AWS option under the `Select the Target Type` page, configuration options for the Amazon AWS target type are displayed.
- [StorageGRID Account](#) on page 17
After selecting the StorageGRID option under the `Select the Target Type` page, configuration options for the StorageGRID target type are displayed.

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.

About this task

You specify your AltaVault appliance as the target type under the AltaVault appliance page of the configuration wizard.

Steps

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

Note: 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` checkbox to create a backup of the configuration database on the selected target type.

Note: 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.

After you finish

Go to [Web Services Proxy](#) on page 18.

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.

About this task

You specify your Amazon AWS credentials under the Amazon AWS account page of the configuration wizard.

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.

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

Note: 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.

After you finish

Go to [Web Services Proxy](#) on page 18.

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.

About this task

You specify your StorageGRID credentials for the target type under the StorageGRID account page of the configuration wizard.

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.
Note: 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.
Important: It is recommended you enable this setting to ensure that data from the backup target can be restored if the database is lost.
Note: 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.
Note: 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](#) on page 12.
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.

After you finish

Go to [Web Services Proxy](#) on page 18.

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

- 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, 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.

Steps

1. [Select Storage Arrays](#) on page 18
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.
2. [Select Hosts](#) on page 19
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.

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

- You have storage arrays configured to your SANtricity Web Services Proxy application.

Note: 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.

Note: 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.

After you finish

Go to [Select Hosts](#) on page 19.

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

- 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.

After you finish

Go to [Complete the initial configuration of the SANtricity Cloud Connector](#) on page 19.

Complete the initial configuration of the SANtricity Cloud Connector

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

About this task

You verify all information entered through the configuration wizard to complete the initial setup of your SANtricity Cloud Connector application.

Step

1. 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.

Use the SANtricity Cloud Connector

You can access the Backups, Restore, Settings, and Events functions in the left navigation panel of the SANtricity Cloud Connector application.

All functionality for the SANtricity Cloud Connector application is available through the left navigation panel of the landing page. The Backups option displays the Backups page, which allows you to create new image-based or file-based backup jobs. Conversely, the Restore option displays the Restore page, which allows you to create new image-based or file-based restore jobs. All SANtricity Cloud Connector application-related events are viewable through the Events page. Finally, settings for the SANtricity Cloud Connector application are configurable through the various Settings options available under the left navigation panel.

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

Steps

1. [Log into the SANtricity Cloud Connector](#) on page 20
You can access the graphical user interface for the SANtricity Cloud Connector application through the configured server in a supported browser.
2. [Backups](#) on page 21
You can use the Backups page of the SANtricity Cloud Connector application to create and process backups of E-Series volumes. The SANtricity Cloud Connector application allows you to create image-based or file-based backups and then perform those operations immediately or at a later time. In addition, you can chose 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.
3. [Restores](#) on page 24
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.
4. [Modify the SANtricity Cloud Connectors Settings](#) on page 26
The Settings button in the left navigation panel section of the SANtricity Cloud Connector landing page allows you to modify the application's current configurations for the S3 account, managed storage arrays and hosts, and Web Services Proxy credentials. In addition, you also can change the password for the SANtricity Cloud Connector application through the Settings option.

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.

Before you begin

- 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.

Backups

You can use the **Backups** page of the SANtricity Cloud Connector application to create and process backups of E-Series volumes. The SANtricity Cloud Connector application allows you to 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.

Steps

1. [Create a new image-based backup](#) on page 21
You can create new image-based backups through the **Create** function on the **Backups** page of the SANtricity Cloud Connector application.
2. [Create a new folder/file-based backup](#) on page 22
You can create new folder/file-based backups through the **Create** function on the **Backups** page of the SANtricity Cloud Connector application.
3. [Run Full and Incremental Backups](#) on page 23
You can perform full and incremental backups through the **Run** function on the **Backups** page. Incremental backups are only available for file-based backups.
4. [Delete a backup job](#) on page 24
You can use the **Delete** function to delete a selected backup item from the result list section of the **Backups** page.

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

- 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.

Note: 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.

Note: 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

- You have storage arrays from the Web Services Proxy registered to the SANtricity Cloud Connector.

About this task

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`, 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.

Note: 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](#) on page 7.

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.

Note: 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.

Note: 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

- 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**.

Note: 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.

Note: 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

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

Before you begin

- You have a backup with a status of Completed, Failed, or Canceled.

About this task

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

Steps

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

Note: 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.

Restores

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.

Steps

1. [Create a new image-based restore](#) on page 25
You can create new image-based restores through the Create function on the Restore page of the SANtricity Cloud Connector application.
2. [Create a new file-based restore](#) on page 25
You can create new file-based restores through the Create function in the Restore page of the SANtricity Cloud Connector application.
3. [Delete a restore](#) on page 26
You can use the Delete function to delete a selected restore item from the result list section of the Restore page.

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

- 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

- You have an 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

- You have 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**.

Note: You cannot delete a suspended restore.

The selected restore is deleted.

Modify the SANtricity Cloud Connectors Settings

The `Settings` button in the left navigation panel section of the SANtricity Cloud Connector landing page allows you to modify the application's current configurations for the S3 account, managed storage arrays and hosts, and Web Services Proxy credentials. In addition, you also can change the password for the SANtricity Cloud Connector application through the `Settings` option.

Choices

- [S3 Account Settings](#) on page 27
You can modify existing S3 settings for the SANtricity Cloud Connector application in the `S3 Account Settings` window.
- [Manage Storage Arrays](#) on page 27
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.
- [Web Services Settings](#) on page 28
You can modify existing Web Services Proxy settings for the SANtricity Cloud Connector application in the `Web Services Proxy Settings` window.
- [Change SANtricity Cloud Connector password](#) on page 28
You can change the password for the SANtricity Cloud Connector application in the `Change Password` screen.

S3 Account Settings

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

About this task

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` field, 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.

About this task

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 Arrays` field, type `REMOVE`.
 - b. Click **Remove**.

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

Web Services 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 need 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.

Choices

- [Uninstall the SANtricity Cloud Connector through graphical mode](#) on page 30
You can use the graphical mode to uninstall the SANtricity Cloud Connector on a Linux operating system.
- [Uninstall the SANtricity Cloud Connector through console mode](#) on page 30
You can use the console mode to uninstall the SANtricity Cloud Connector on a Linux operating system.

Uninstall the SANtricity Cloud Connector through 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 the SANtricity Cloud Connector through 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.

Copyright

Copyright © 2019 NetApp, Inc. All rights reserved. Printed in the U.S.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).

Trademark

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

doccomments@netapp.com

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 1395 Crossman Ave., Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277