NetApp® SANtricity® Cloud Connector 3.1

User Guide

May 2018 | 215-12513_B0
doccomments@netapp.com

Table of Contents

Deciding whether to use this guide

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.

Understanding the SANtricity Cloud Connector

The SANtricity Cloud Connector is a host-based Linux application that allows you to perform full block-based and file-based backup and recovery of E-Series volumes to S3 complaint accounts (e.g., 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). Once installed, you can configure the SANtricity Cloud Connector 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 utilize REST-based APIs.

Types of backup

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

Image-based backup

This is a type of backup that 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 utilize 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

This is a type of backup that 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 utilize 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 suppled passphrase and the SHA256 hash of the user data. For backups to AltaVault, the data chunks are not encrypted by SANtricity Cloud Connector as AltaVault performs this operation.

Setting up your system

Host hardware requirements

Before installing the SANtricity Cloud Connector, verify your system meets the following host hardware requirements:

- At least 5 GB of memory – 4 GB for the maximum configured heap size
- At least 250 MB of free disk space is required for the software installation

An installation of the SANtricity Web Services Proxy is required for use with the SANtricity Cloud Connector. The Web Services Proxy can be installed locally or ran remotely on a different sever. For information on installing the SANtricity Web Services Proxy, see the NetApp SANtricity Web Services Proxy 2.1 Installation Guide.

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

Compatible storage arrays and controller firmware

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 3.0 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

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

- ext2
- ext3
- ext4

Installing SANtricity Cloud Connector

The Cloud Connector packaged solution (.bin file) is available for RedHat and SUSE Linux platforms only. During the installation process, you must specify the non-SSL and SSL port numbers for the SANtricity Cloud Connector. Once installed, the SANtricity Cloud Connector runs as a daemon process.

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

Installation of Device Mapper Multipath (DM-MP)

Any host running the SANtricity Cloud Connector must also 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 Systems Documentation Center.

Installing 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:

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. Run the following command to initiate 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 Choose Install screen is displayed within the Installer window. The Where Would You Like to Install field displays the following default install folder:

   ```
   /opt/netapp/santricity_cloud_connector
   ```
7. Choose one of the following options:
   a. To accept the default location, click **Next**.
   b. To change the default location, enter a new folder location.

   An Enter the Non SSL Jetty Port Number screen is displayed. A default value of 8080 is assigned to the Non SSL port.

8. Choose one of the following options:
    a. To accept the default Non SSL port number, click **Next**.
    b. To change the default Non SSL port number, enter the new desired port number value.

   The Pre-Installation Summary screen is displayed.

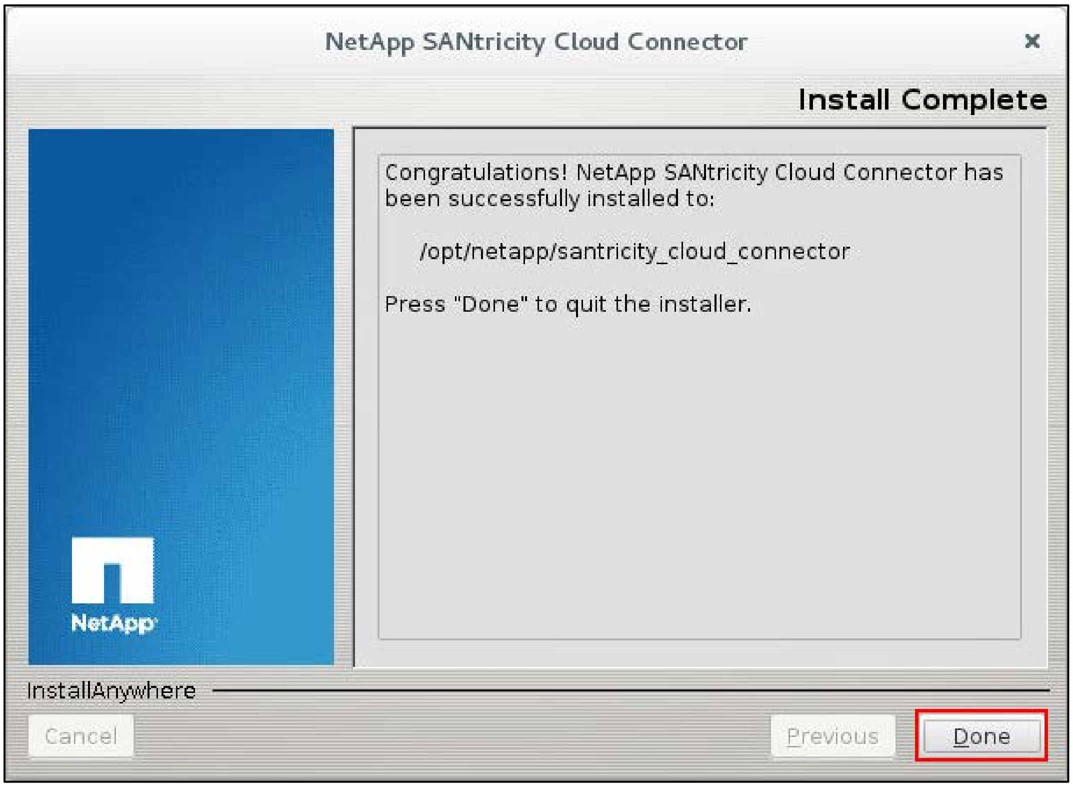
9. Review the displayed Pre-Installation Summary and then click **Install**.

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

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

    The Installation Complete message is displayed.

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



Congratulations! NetApp SANtricity Cloud Connector has been successfully installed to:

/opt/netapp/santricity_cloud_connector

Press "Done" to quit the installer.

Installing 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.

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.

   A Choose Install Folder message with the following default install folder for the SANtricity Cloud Connector is displayed:

   ```
   /opt/netapp/santricity_cloud_connector
   ```

   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. Choose one of the following options:

   a. To accept the default install location, press **Enter**.

   b. 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.

9. Choose one of the following options:

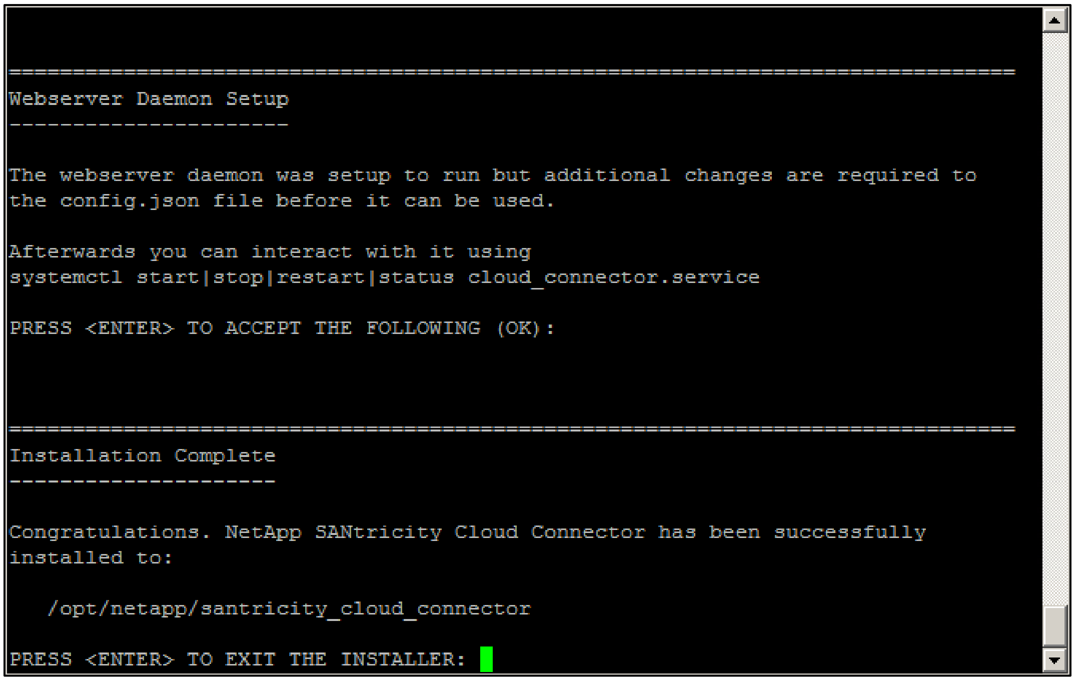
   a. To accept the default Non SSL port number, press Enter.

   b. 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.

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

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



```
================================================================================
Webserver Daemon Setup
----------------------

The webserver daemon was setup to run but additional changes are required to
the config.json file before it can be used.

Afterwards you can interact with it using
systemctl start|stop|restart|status cloud_connector.service

PRESS <ENTER> TO ACCEPT THE FOLLOWING (OK):



================================================================================
Installation Complete
---------------------

Congratulations. NetApp SANtricity Cloud Connector has been successfully
installed to:

   /opt/netapp/santricity_cloud_connector

PRESS <ENTER> TO EXIT THE INSTALLER:
```

The Installation Complete message is displayed.

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

Adding server certificate and CA certificate into a keystore

To avoid receiving untrusted connection alerts when accessing the SANtricity Cloud Connector through a browser, you must add a certificate and trust chain recognized by both the browser and SANtricity Cloud Connector application.

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_connector`.

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 changeit -noprompt

   keytool -import -alias ca-issuing-1 -file issuing-ca-1.cer -keystore
   keystore_cloudconnect.jks -storepass changeit -noprompt

   keytool -import -trustcacerts -alias cloudconnect -file certnew.cer -
   keystore keystore_cloudconnect.jks -storepass changeit
   ```

6. Access the `config.json` file located under the install directory.

7. Set the `keystore` location and `keystorePassword` under the `config.json` file.

   EXAMPLE

   ~~~
   ```

   {

     "webserver" : {

       "keystore" : "/opt/cloud-connector/cert/keystore_cloudconnect.jks",

       "keystorePassword" : "changeit"

       ...

     },

     ...

   }

   ```
   ~~~

8. Restart the service.

Migrating from SANtricity Cloud Connector v1.0 to v3.1

When migrating from SANtricity Cloud Connector v1.0 to v3.1, you must verify that the WWN values under the metadata files created with v1.0 are uppercase. In order for v3 version of the SANtricity Cloud Connector to restore the v1 backups, the WWN values in the filenames must use uppercase letters (for example, 600A098000A09B140000D91859D59DA7). If the WWN values are lowercase in the filename (for example, 600a098000a09b140000d91859d59da7), the restore operation fails.

1. Access the S3 account bucket or AltaVault NFS mount directory where the SANtricity Cloud Connector backup files are saved.

2. In the `target bucket/directory`, review the following two types of files:

   - `<wwn>-<timestamp>.json`

Example

`600A098000A09B140000D91859D59DA7-1510246767459.json`

- `volinfo-<wwn>.json`

  Example

  `volinfo-600A098000A09B140000D91859D59DA7.json`

3. Choose one of the following options:
   - If the existing WWN values are lowercase, convert each value to uppercase.
   - If the existing WWN are uppercase, no further action is needed.
4. Save the file to apply any changes.

Configuring the SANtricity Cloud Connector for the first time

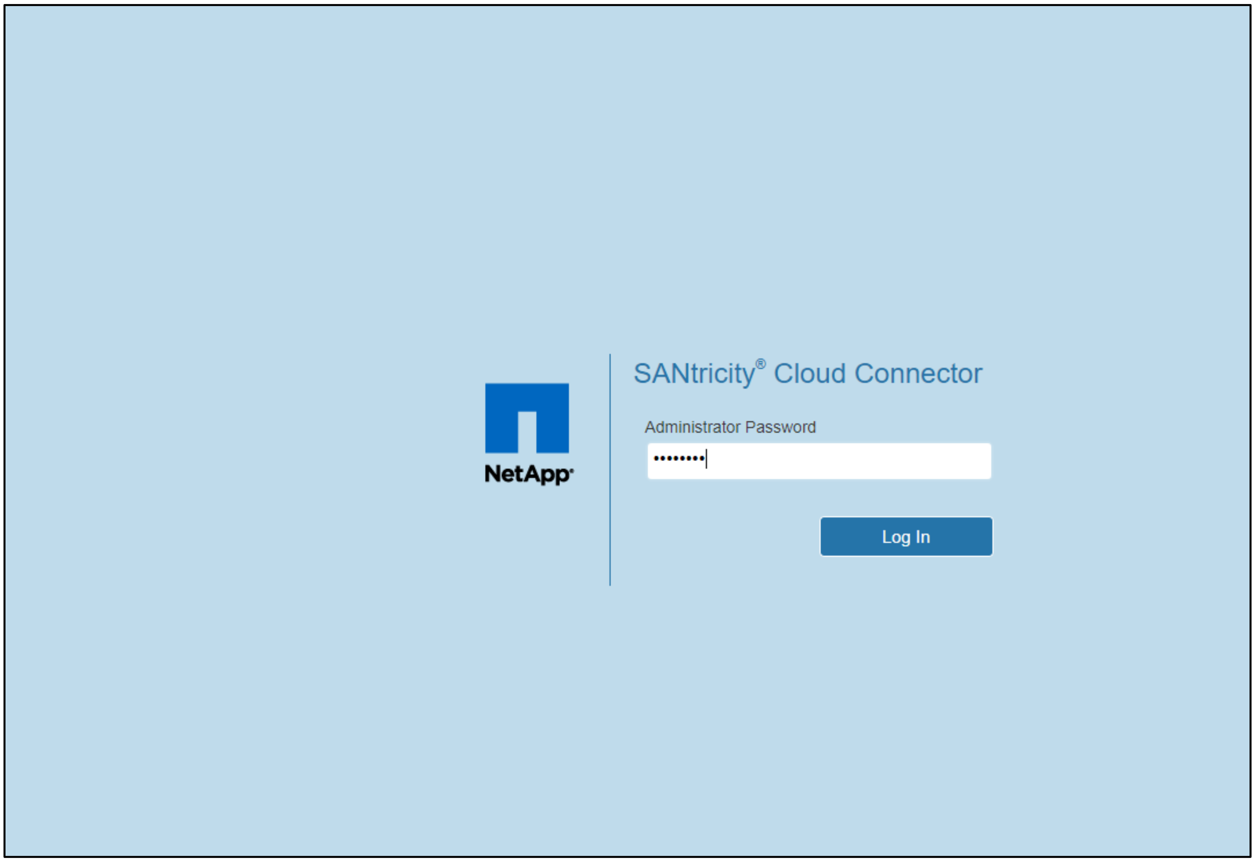
Upon successful installation, you can set up of the SANtricity Cloud Connector application through the configuration wizard. The configuration wizard is displayed after you initially log in to the SANtricity Cloud Connector.

Initial login

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

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

   The initial login screen for the SANtricity Cloud Connector application is displayed.
3. Under the Administrator Password field, enter the default password of "password".



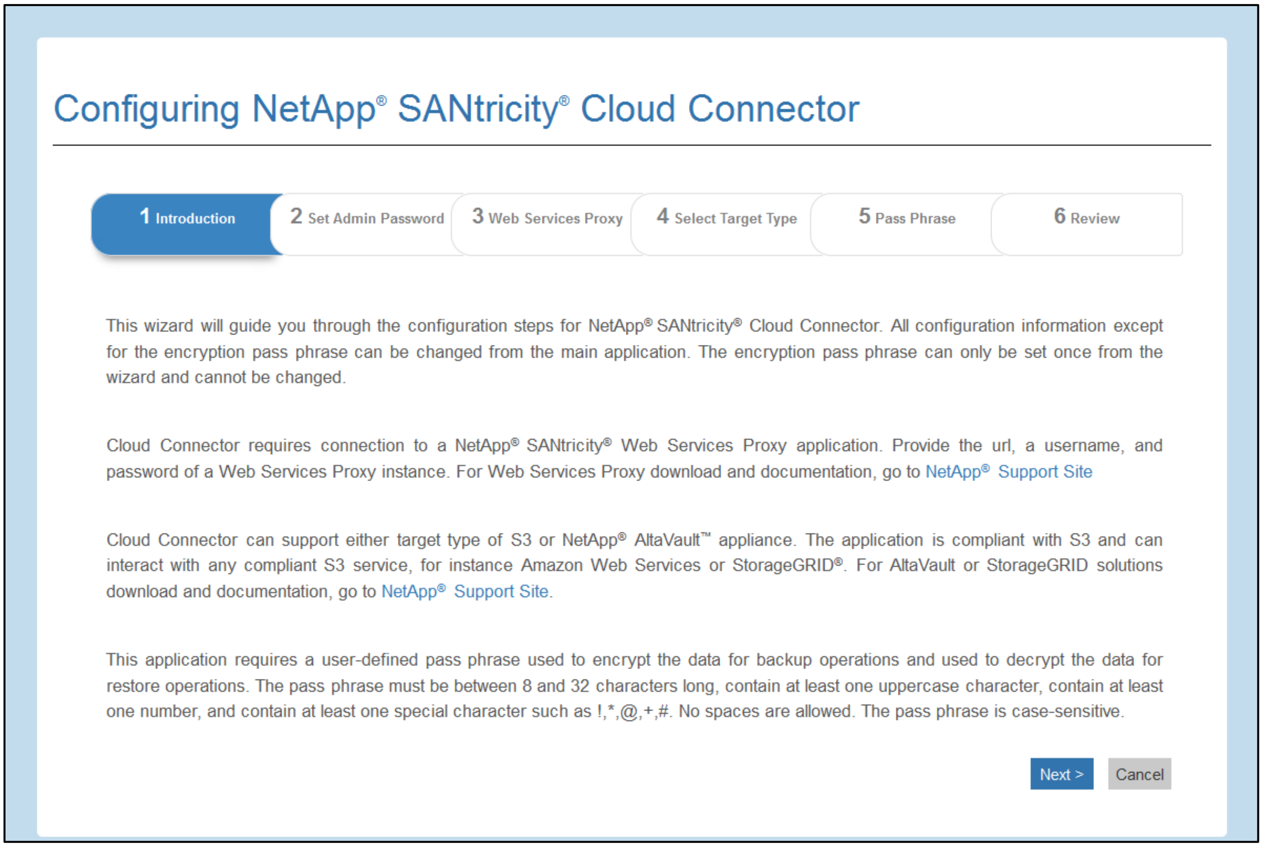
4. Click **Login**.

   The SANtricity Cloud Connector Configuration Wizard is displayed.

Configuration Wizard

The Configuration Wizard is displayed upon successful initial log into the SANtricity Cloud Connector. Through the Configuration Wizard, you can setup the administrator password, Web Services Proxy login management credentials, desired backup target type, and encryption pass phrase for the SANtricity Cloud Connector.

1. Click **Next** to configure the administrator password for the SANtricity Cloud Connector.



This wizard will guide you through the configuration steps for NetApp® SANtricity® Cloud Connector. All configuration information except for the encryption pass phrase can be changed from the main application. The encryption pass phrase can only be set once from the wizard and cannot be changed.

Cloud Connector requires connection to a NetApp® SANtricity® Web Services Proxy application. Provide the url, a username, and password of a Web Services Proxy instance. For Web Services Proxy download and documentation, go to NetApp® Support Site

Cloud Connector can support either target type of S3 or NetApp® AltaVault™ appliance. The application is compliant with S3 and can interact with any compliant S3 service, for instance Amazon Web Services or StorageGRID®. For AltaVault or StorageGRID solutions download and documentation, go to NetApp® Support Site.

This application requires a user-defined pass phrase used to encrypt the data for backup operations and used to decrypt the data for restore operations. The pass phrase must be between 8 and 32 characters long, contain at least one uppercase character, contain at least one number, and contain at least one special character such as !,*,@,+,#. No spaces are allowed. The pass phrase is case-sensitive.

Set Administrator Password

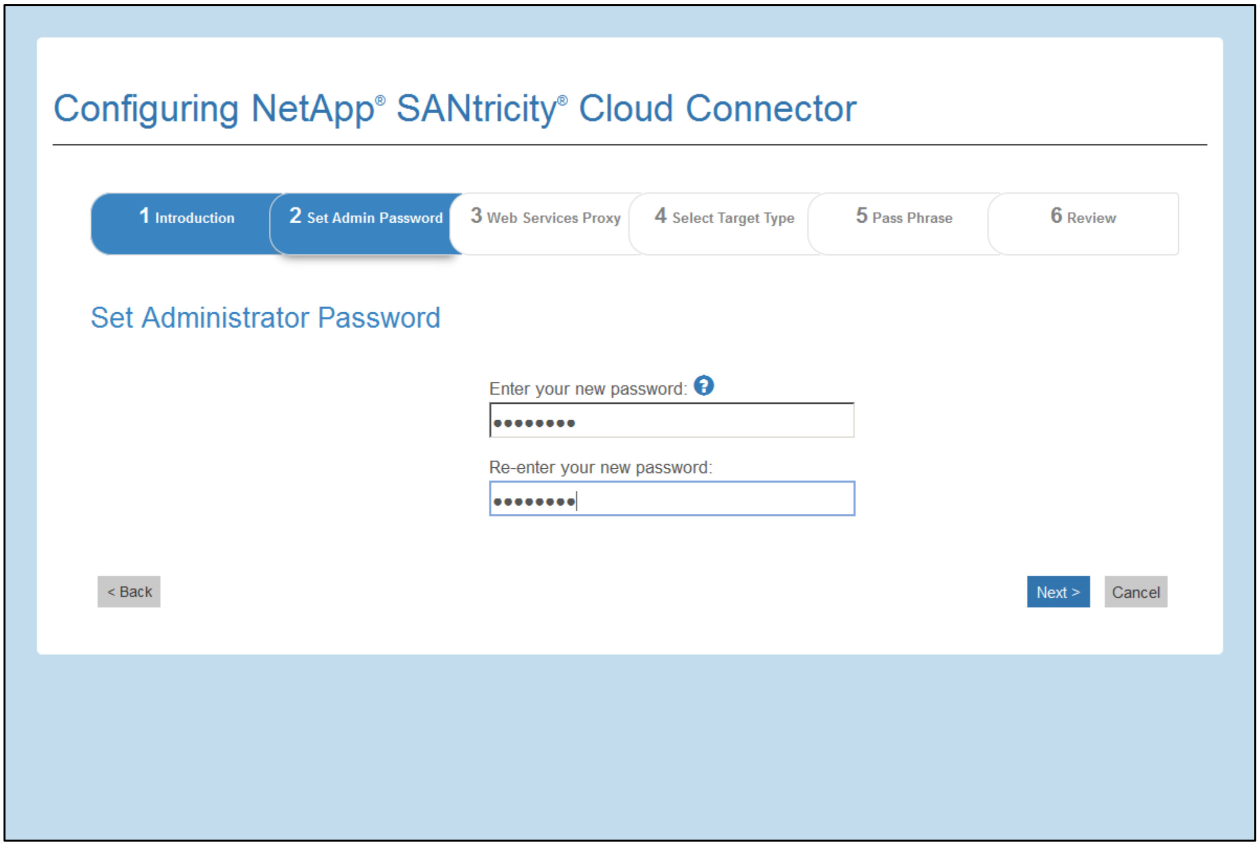
You can customize the password used for subsequent logins to the SANtricity Cloud Connector through the Set Administrator Password screen.

NOTE: 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.

1. Under the Enter your new password field, enter the desired login password for the SANtricity Cloud Connector.

2. Under the Re-enter your new password field, re-enter the password from first field.

3. Click **Next**.



Enter your new password: ●●●●●●●●●

Re-enter your new password: ●●●●●●●●●

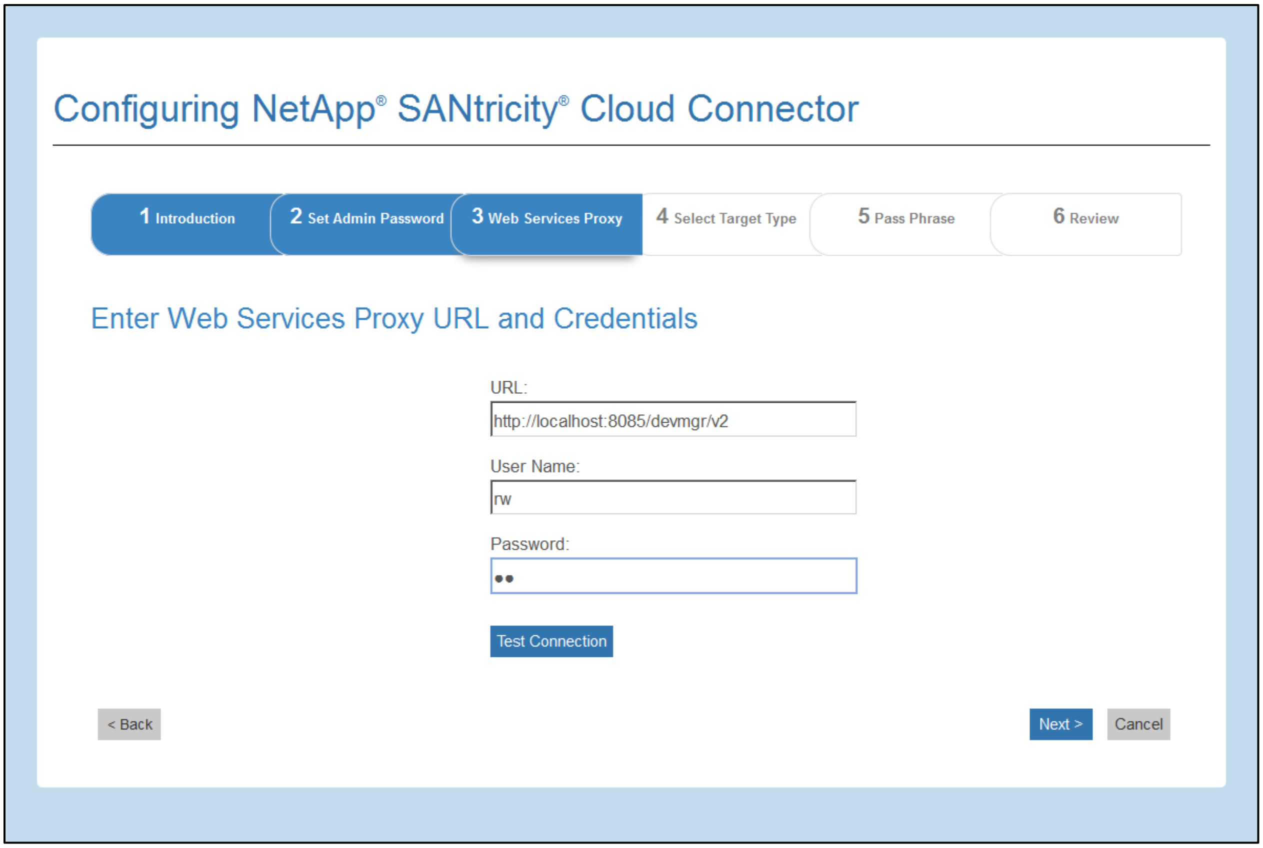
The password setup for the SANtricity Cloud Connector is accepted and the Web Services Proxy screen is displayed under the Configuration Wizard.

NOTE: The user defined administrator password will not be set until you complete the configuration wizard.

Web Services Proxy

Connection to the SANtricity Web Services Proxy is required for the SANtricity Cloud Connector application. 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 screen.

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



Enter Web Services Proxy URL and Credentials

URL: http://localhost:8085/devmgr/v2

User Name: rw

Password: ●●

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

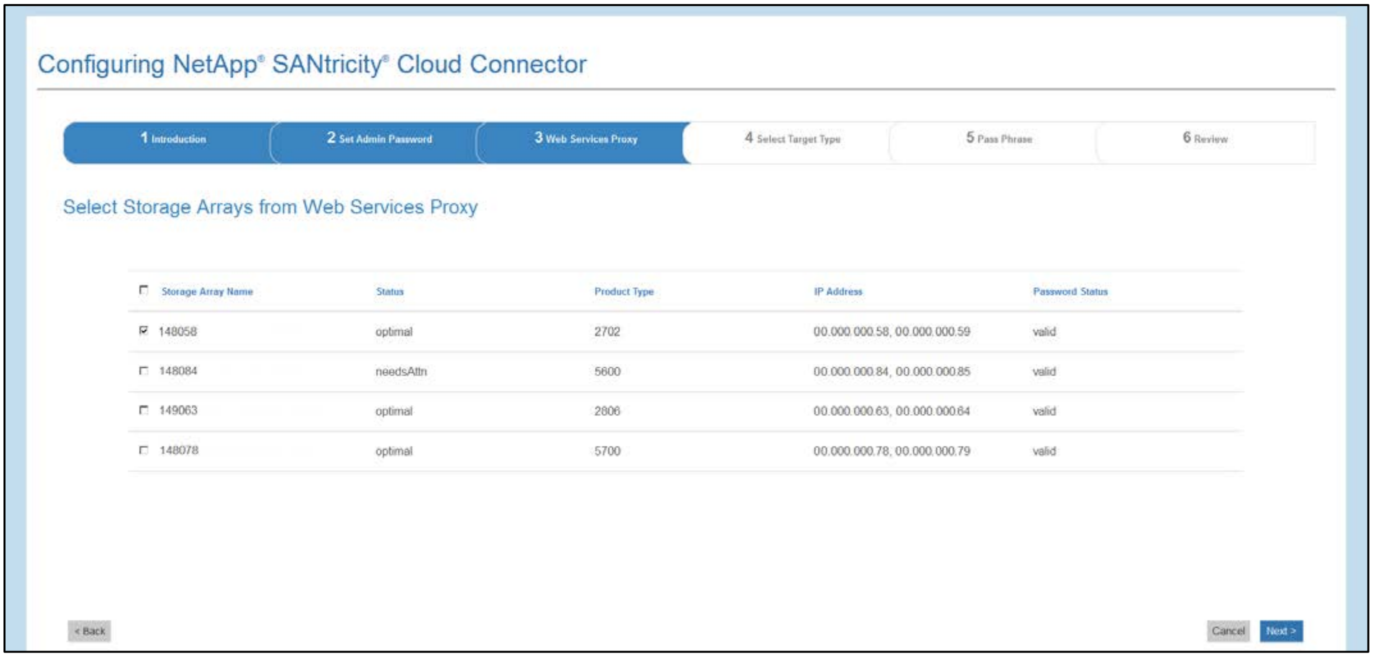
Select Storage Arrays

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 screen. Through this screen, you can select which storage arrays the SANtricity Cloud Connector uses for backup and restore jobs.

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

   NOTE: When selecting a storage array under the Select Storage Arrays screen, the listed array status is retained throughout the SANtricity Cloud Connector application and not updated dynamically.

2. Click **Next**.



Select Storage Arrays from Web Services Proxy

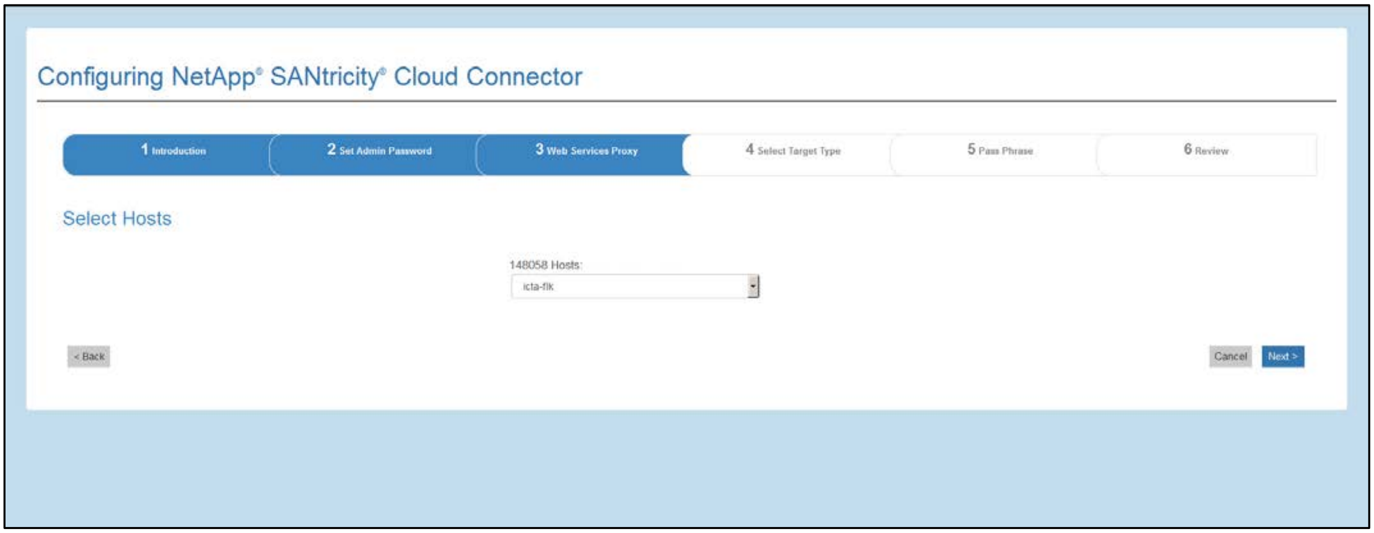
☐ Storage Array Name	Status	Product Type	IP Address	Password Status
☑ 148058	optimal	2702	00.000.000.58, 00.000.000.59	valid
☐ 148084	needsAttn	5600	00.000.000.84, 00.000.000.85	valid
☐ 149063	optimal	2806	00.000.000.63, 00.000.000.64	valid
☐ 148078	optimal	5700	00.000.000.78, 00.000.000.79	valid

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

Select Hosts

Based on the Web Services Proxy-hosted storage arrays selected through the Configuration Wizard, you can select an available host for the SANtricity Cloud Connector application through the Select Hosts screen.

1. Under the drop-down field for the listed storage array, select the desired host.
2. Repeat step 1 for any additional storage arrays listed under the Select Host screen.
3. Click **Next**.



Select Hosts

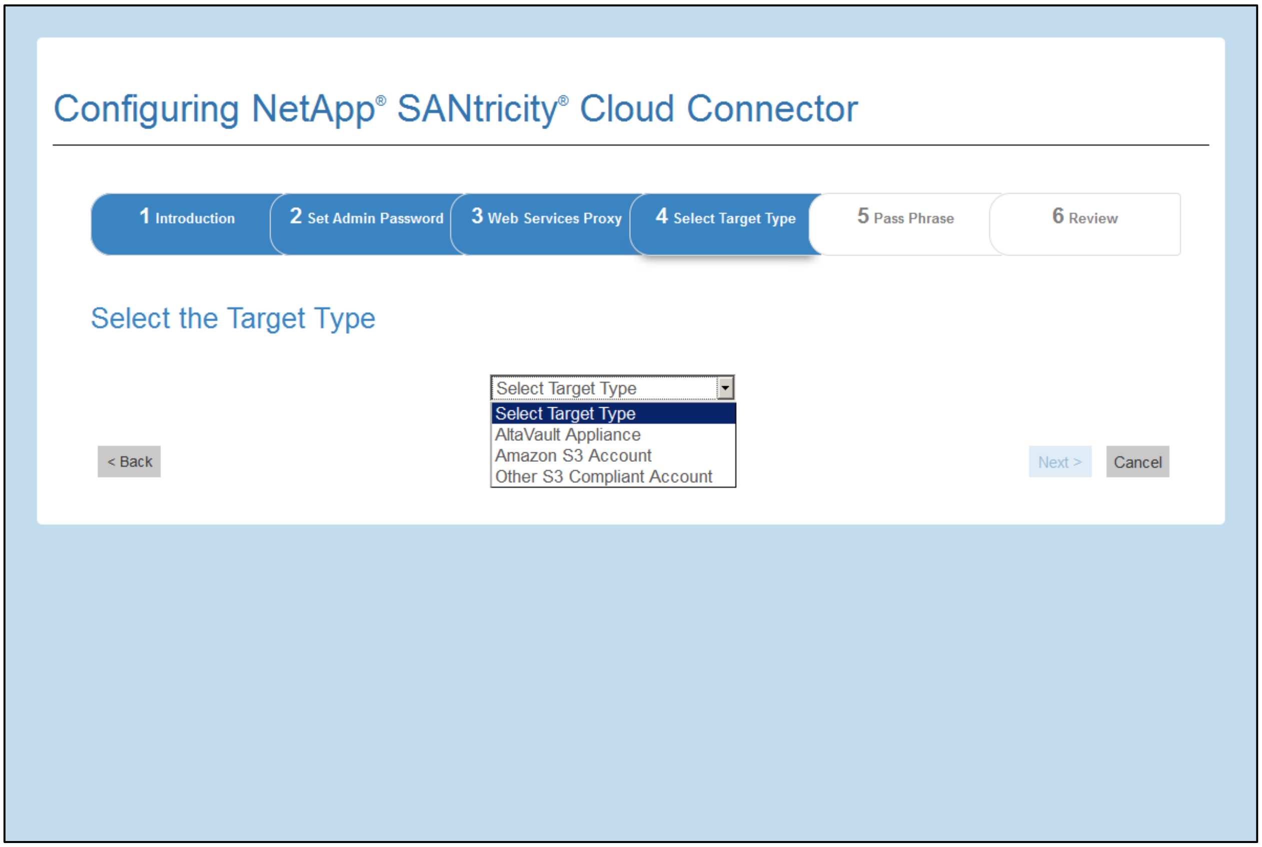
148058 Hosts: icta-flk

The selected host for the SANtricity Cloud Connector is accepted and the Select Target Type screen is displayed under the Configuration Wizard.

Select Target Type

Backup and restore capabilities are available for Amazon S3, S3-compliant and AltaVault 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 screen.

1. Under the dropdown field, select one of the following options:
    - AltaVault Appliance
    - Amazon S3 Account
    - Other S3 Compliant Account



AltaVault Appliance

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

1. Under the NFS Mount Path, enter the mount point for the AltaVault target type.
2. Click **Next**.

   The specified target type for the SANtricity Cloud Connector is accepted and the Pass Phrase screen is displayed under the Configuration Wizard.

Amazon S3 Account

After selecting the Amazon S3 Account option under the Select the Target Type screen, configuration options for the Amazon S3 target type are displayed.

1. Under the Access Key ID field, enter the access ID for the S3 target.
2. Enter the access key for the S3 target under the Secret Access Key field.
3. Under the Bucket Name field, enter the bucket name for the S3 target.
4. Click **Test Connection** to verify the entered Amazon S3 credentials.
5. Click **Next**.

   The specified target type for the SANtricity Cloud Connector is accepted and the Pass Phrase screen is displayed under the Configuration Wizard.

Other S3 Compliance Account

After selecting the Other S3 Compliant Account option under the Select the Target Type screen, configuration options for the S3-compliant target type are displayed.

1. Enter the URL for the Amazon S3 cloud service under the URL field.
2. Under the Access Key ID field, enter the access ID for the S3 target.
3. Enter the access key for the S3 target under the Secret Access Key field.
4. Under the Bucket Name field, enter the bucket name for the S3 target.
5. Click Test Connection to verify the entered S3 credentials.

   NOTE: Some S3-compliant accounts may require secured HTTP connections. For details on how to add a CA certificate into a keystore, refer to Adding server certificate and CA certificate into a keystore.

6. Click **Next**.

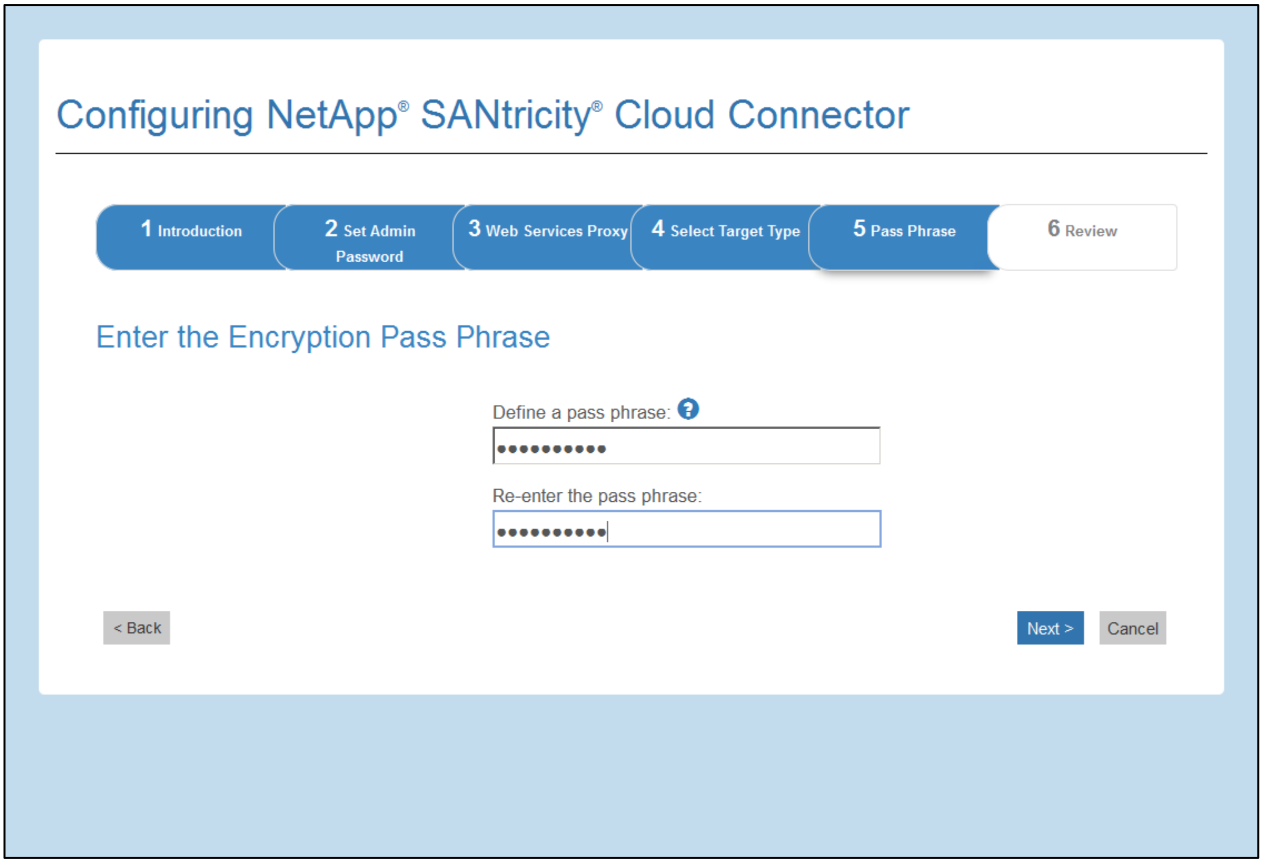
   The specified target type for the SANtricity Cloud Connector is accepted and the Pass Phrase screen is displayed under the Configuration Wizard.

Pass Phrase

A user-specified pass phrase is required as part of the data encryption key used by the SANtricity Cloud Connector application. Under the Enter the Encryption Pass Phrase screen, you can specify an alphanumeric pass phrase between 8 and 32 characters with at least one special character.

1. Under the Define a pass phrase field, enter the desired pass phrase.
2. Under 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 review screen for the configuration wizard is displayed.



Configuring NetApp® SANtricity® Cloud Connector

Enter the Encryption Pass Phrase

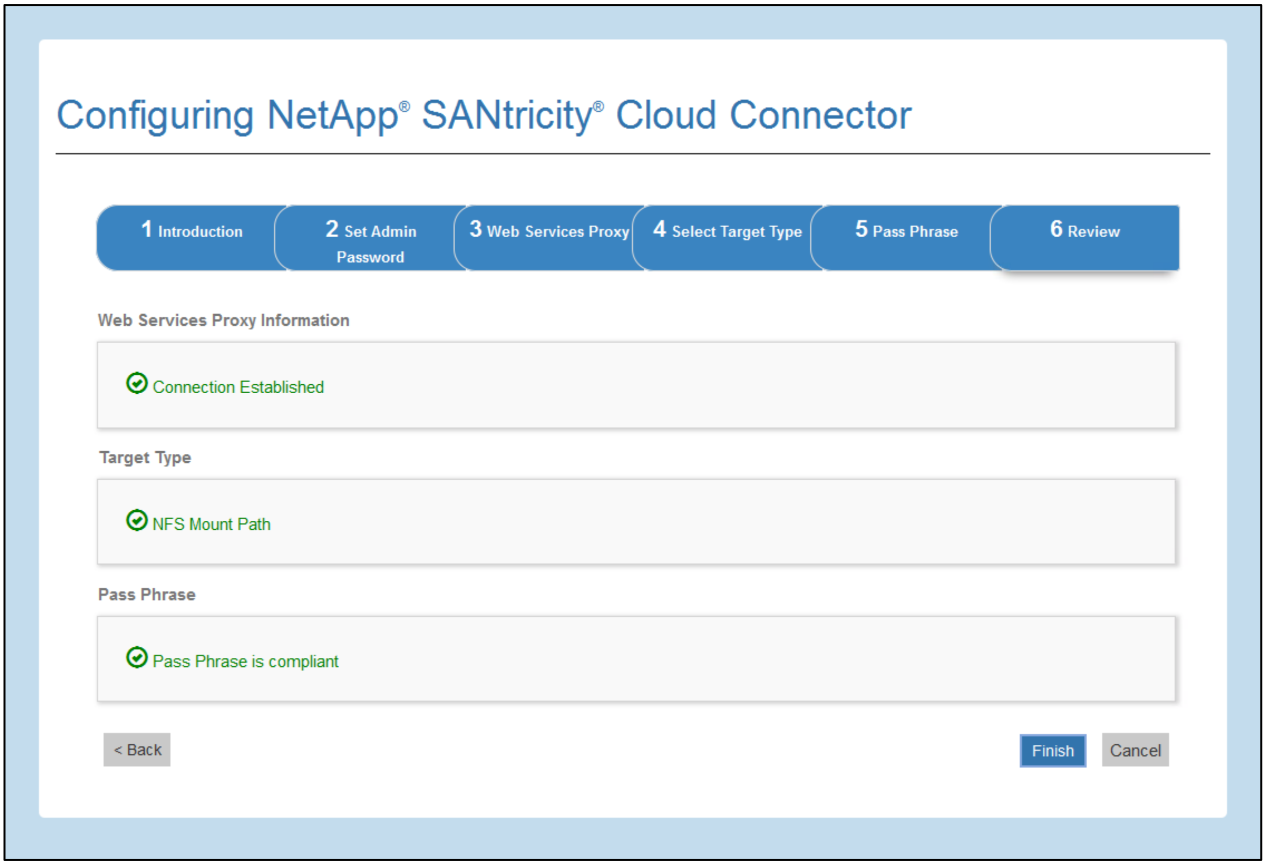
Define a pass phrase: ●●●●●●●●●●●

Re-enter the pass phrase: ●●●●●●●●●●●

Completing the initial configuration of the SANtricity Cloud Connector

The final screen of the SANtricity Cloud Connector configuration wizard performs a validation on the entered configuration data and provides a summary of the results for your review.

1. Review the results of the validated configuration data.
2. If all configuration data is successfully validated and established, click **Finish** to complete the configuration process.
3. If any section of the configuration data cannot be validated, click **Back** to navigate to the applicable screen of the configuration wizard to revise the submitted data.


Configuring NetApp® SANtricity® Cloud Connector

Web Services Proxy Information

✓ Connection Established

Target Type

✓ NFS Mount Path

Pass Phrase

✓ Pass Phrase is compliant

Using the SANtricity Cloud Connector

Functionality for the SANtricity Cloud Connector application is centralized under a single landing page comprised of the three tabs, Backup, Restore, and Events. The Backup tab allows you to create new image-based or file-based backup jobs. Conversely, the Restore tab allows you to create new image-based or file-based restore jobs. All SANtricity Cloud Connector application-related events are viewable through the Events tab.

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

Logging into the SANtricity Cloud Connector

You can access the graphical user interface for the SANtricity Cloud Connector application through the configured server under a supported browser.

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

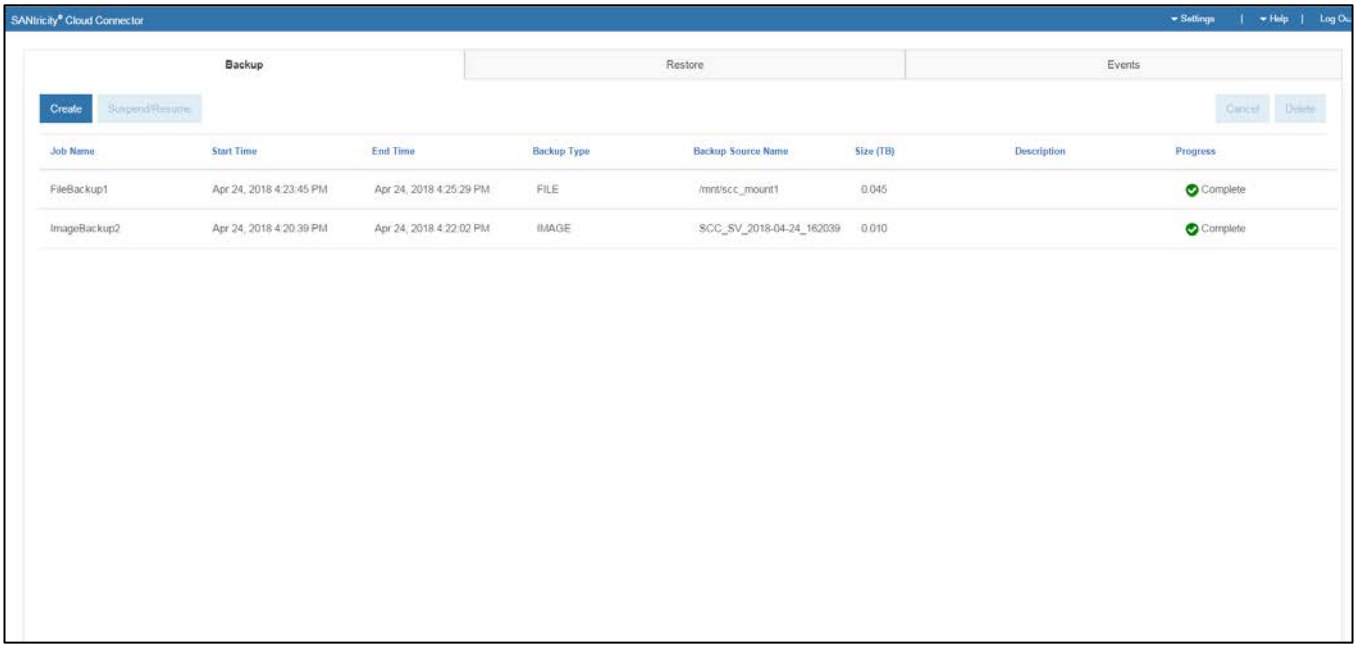
   The initial login screen for the SANtricity Cloud Connector application is displayed.

2. Enter your configured administrator password.
3. Click **Login**.

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

Backup jobs

The SANtricity Cloud Connector uses the concept of jobs to perform the actual backup of an E-Series volume. The SANtricity Cloud Connector application utilizes backup data in the form of snapshots of an E-Series volume. You can utilize the Backup tab of the SANtricity Cloud Connector application to create and process backup jobs of E-Series volumes.



Job Name	Start Time	End Time	Backup Type	Backup Source Name	Size (TB)	Description	Progress
FileBackup1	Apr 24, 2018 4:23:45 PM	Apr 24, 2018 4:25:29 PM	FILE	/mnt/scc_mount1	0.045		✓ Complete
ImageBackup2	Apr 24, 2018 4:20:39 PM	Apr 24, 2018 4:22:02 PM	IMAGE	SCC_SV_2018-04-24_162039	0.010		✓ Complete

Creating a new image-based backup job

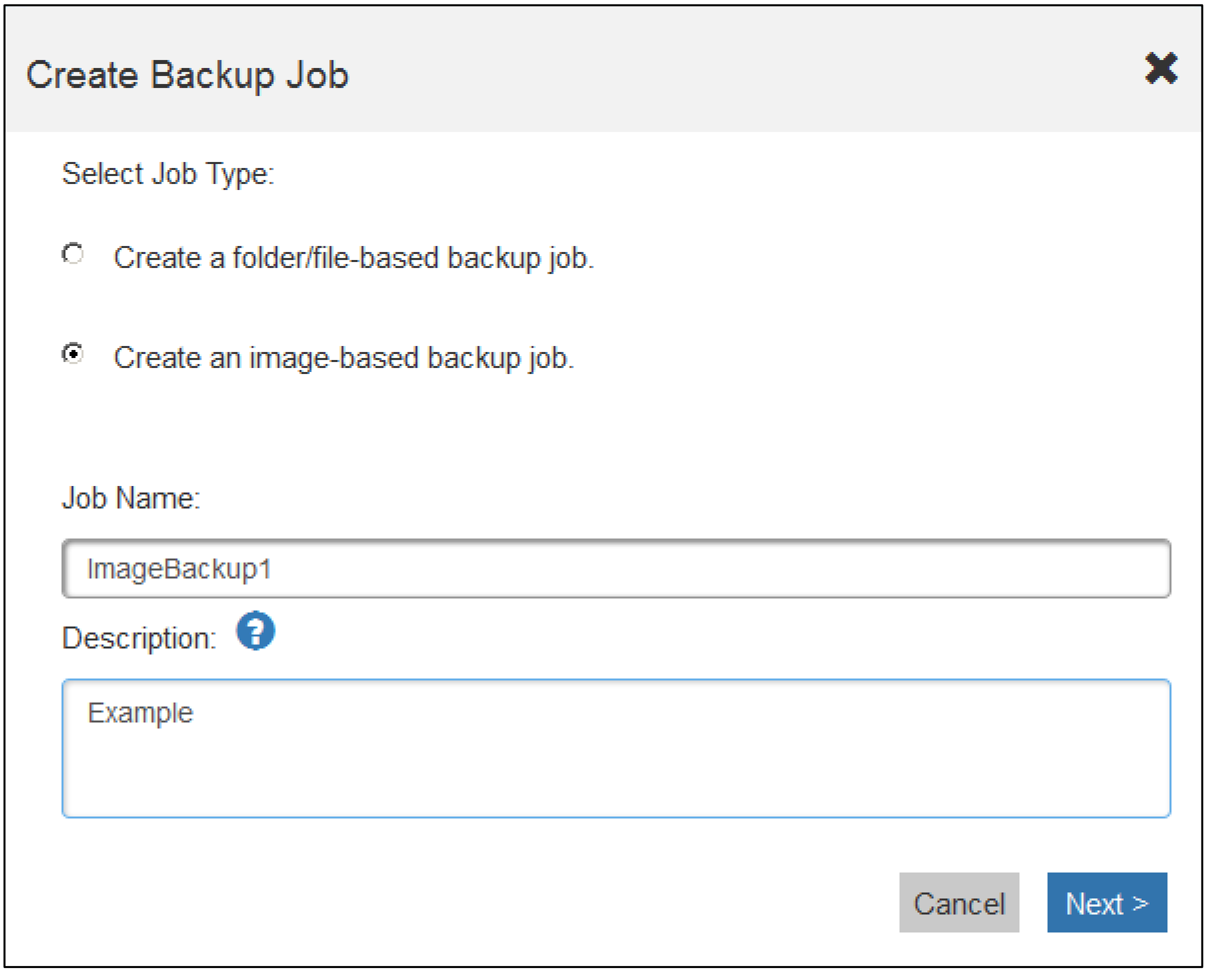
You can create new image-based backup jobs through the Create function in the Backup tab of the SANtricity Cloud Connector application.

1. In the Backup tab of the SANtricity Cloud Connector application, click **Create.**

   The Create Backup Job window is displayed.

2. In the Create Backup Job window, select **Create an image-based backup job**.
3. To modify the auto-generated backup job name, enter the desired name in the Job Name field.
4. If needed, add a description for the backup job in the Job Description field.

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



Create Backup Job

Select Job Type:

○ Create a folder/file-based backup job.

● Create an image-based backup job.

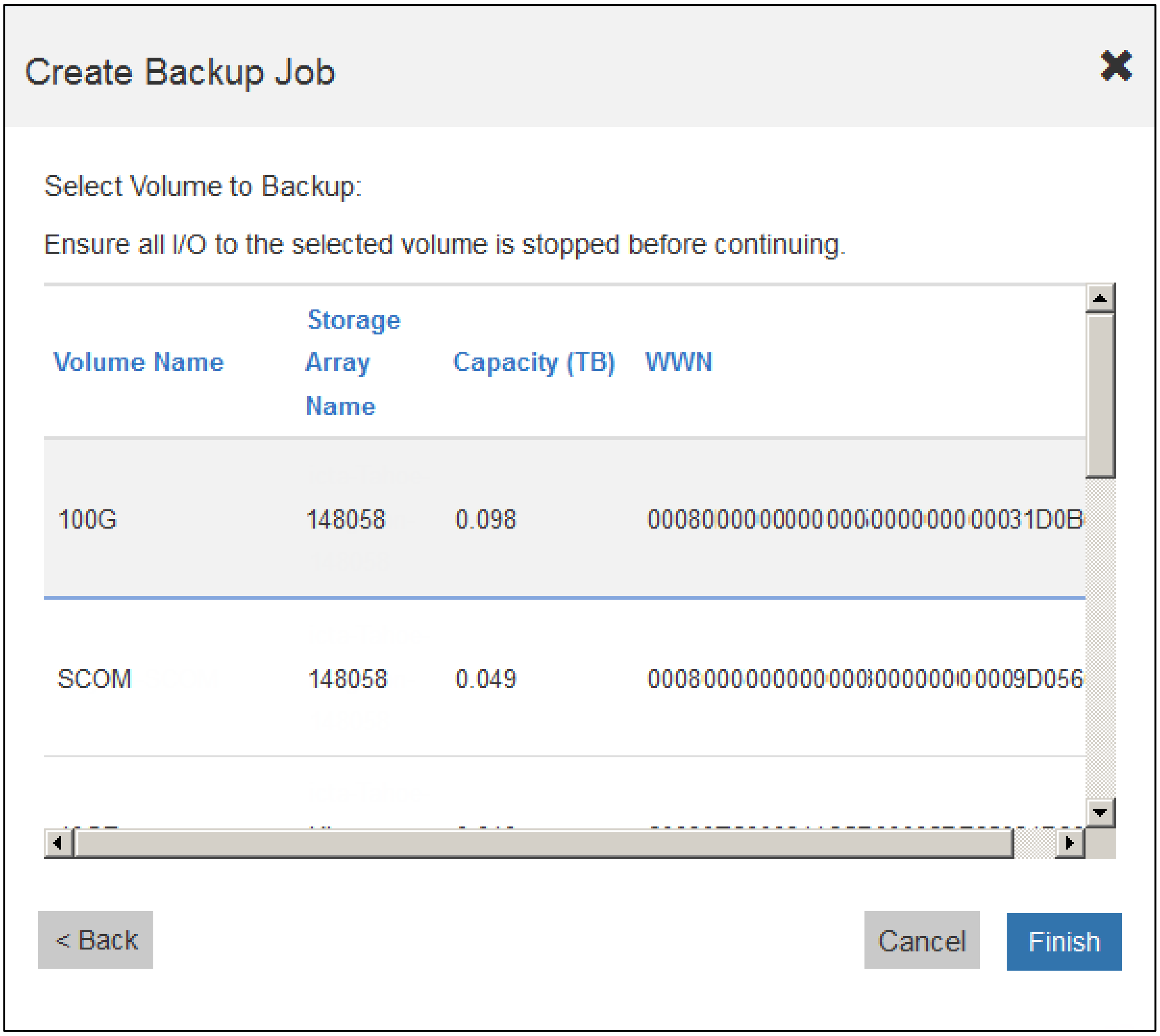
Job Name: ImageBackup1

Description: Example

5. Click **Next**.

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

6. In the Create Backup Job window, select the desired E-Series volume and click **Finish**.


Create Backup Job
Select Volume to Backup:
Ensure all I/O to the selected volume is stopped before continuing.
< Back
Cancel
Finish

Volume Name	Storage Array Name	Capacity (TB)	WWN
100G	148058	0.098	00080000000000000000000000031D0B
SCOM	148058	0.049	00080000000000000000000000009D056

The backup job for the selected E-Series volume is initiated and a Create Backup Job confirmation window is displayed.

7. In the Create Backup Job confirmation window, select one of the following options:
   a. **No –** Closes the Create Backup Job confirmation window.
   b. **Yes** – The Create Backup Job window is displayed. Repeat steps 2-6 to create another backup job.
8. Click **Close**.

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

Creating a new folder/file-based backup job

You can create new folder/file-based backup jobs through the Create function in the Backup tab of the SANtricity Cloud Connector application.

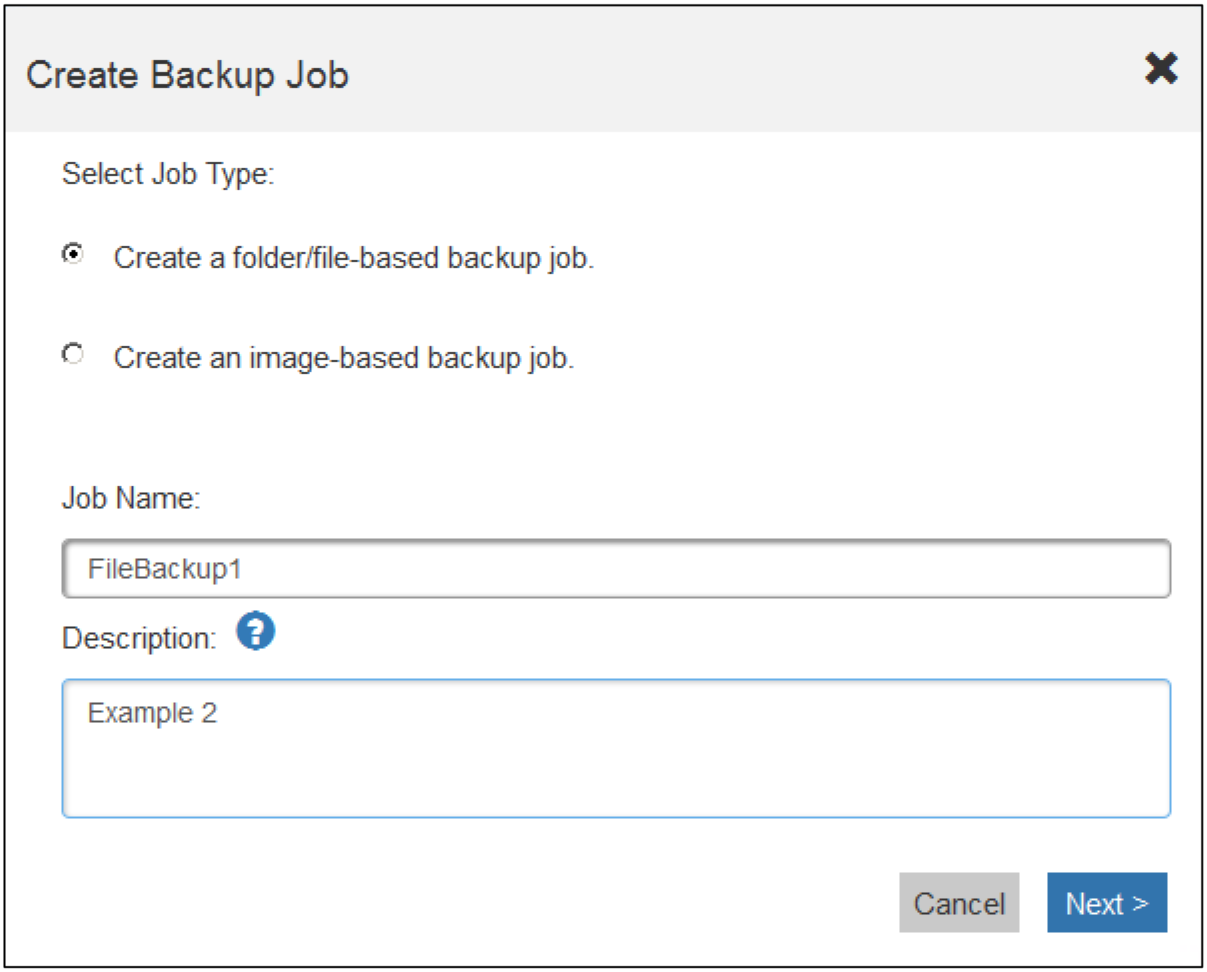
NOTE: A file-based backup unconditionally backs up all files on the filesystem you specify. However, you can perform a selective restore of files and folders.

1. In the Backup tab of the SANtricity Cloud Connector application, click **Create**.

   The Create Backup Job window is displayed.

2. Select **Create a folder/file-based backup job**.
3. To modify the auto-generated backup job name, enter the desired name in the Job Name field.
4. If needed, add a description for the backup job in the Job Description field.

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



● Create a folder/file-based backup job.

○ Create an image-based backup job.

Job Name: FileBackup1

Description: Example 2

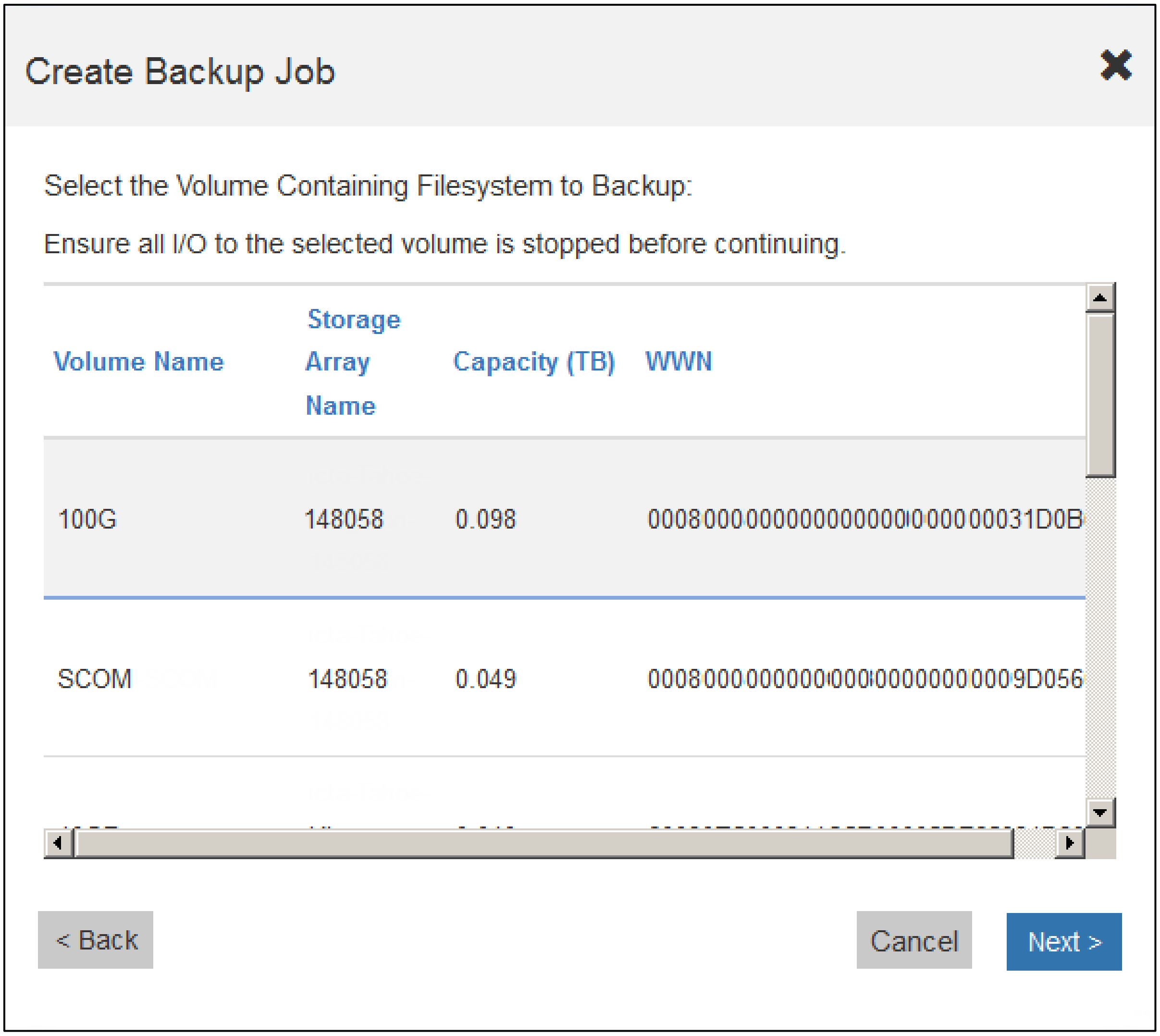
5. Click **Next**.

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

6. Select the desired volume in the Create Backup Job window and click **Next**.

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

7. Select the desired volume to backup in the Create Backup Job window and click **Next**.



Select the Volume Containing Filesystem to Backup:

Ensure all I/O to the selected volume is stopped before continuing.

Volume Name	Storage Array Name	Capacity (TB)	WWN
100G	148058	0.098	00080000000000000000000000031D0B
SCOM	148058	0.049	00080000000000000000000000009D056

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

8. Select the desired file system in the Create Backup Job window and click **Finish**.

   The backup job for the selected file system is initiated, and a Create Backup Job confirmation window is displayed.

9. In the Create Backup Job confirmation window, select one of the following options:

   a. **No –** Closes the Create Backup Job confirmation window.

   b. **Yes** – The Create Backup Job window is displayed. Repeat steps 2-8 to create another backup job.

10. Click **Close**.

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

Deleting a backup job

You can use the Delete function to delete a selected backup job item from the result list section of the Backup tab.

NOTE: The Delete function does not delete backup data at the specified target location for the selected backup job.

1. In the Backup tab of the SANtricity Cloud Connector application, select the desired backup job and click **Delete**.

   The Confirm Delete window is displayed.

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

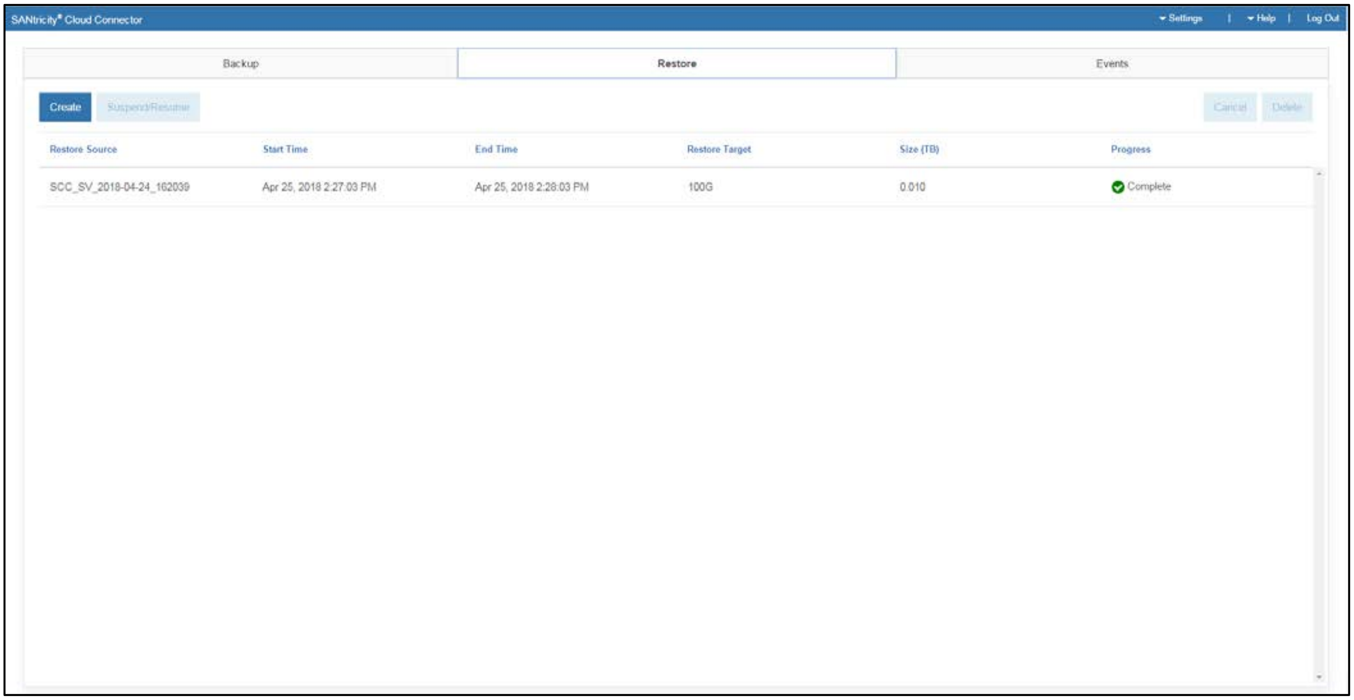
3. Click **Confirm**.

   The selected backup job is deleted.

   NOTE: You cannot delete a suspended backup job.

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 utilize the Restore tab of the SANtricity Cloud Connector application to create and process restore jobs.



Restore Source	Start Time	End Time	Restore Target	Size (TB)	Progress
SCC_SV_2018-04-24_162039	Apr 25, 2018 2:27:03 PM	Apr 25, 2018 2:28:03 PM	100G	0.010	✓ Complete

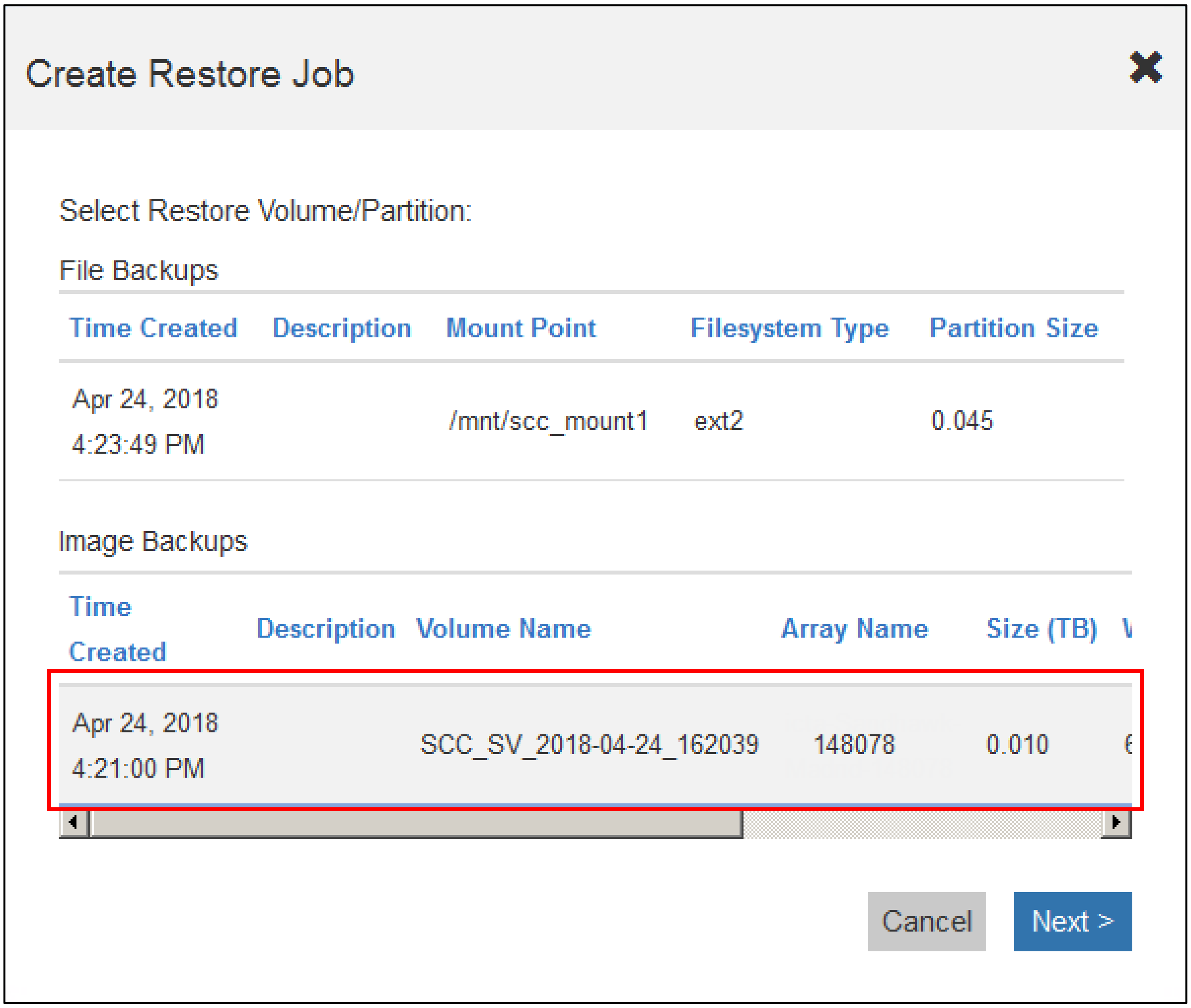
Creating a new image-based restore job

You can create new image-based restore jobs through the Create function in the Restore tab of the SANtricity Cloud Connector application.

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

   The Create Restore Job window is displayed.

2. In the Create Restore Job window, select the desired volume in the Image Backups section.



Create Restore Job

Select Restore Volume/Partition:

File Backups

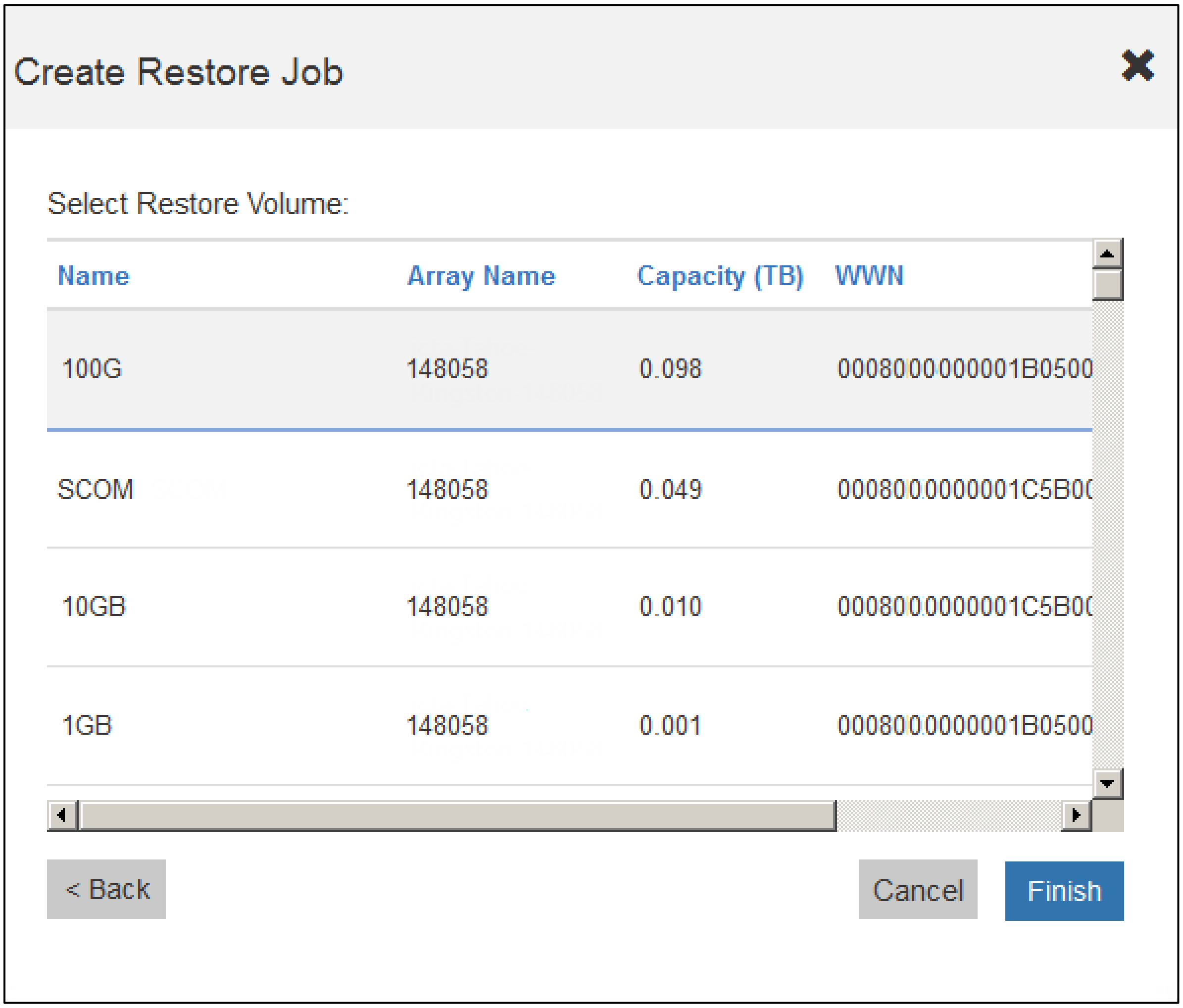
Time Created	Description	Mount Point	Filesystem Type	Partition Size
Apr 24, 2018 4:23:49 PM		/mnt/scc_mount1	ext2	0.045

Image Backups

Time Created	Description	Volume Name	Array Name	Size (TB)
Apr 24, 2018 4:21:00 PM		SCC_SV_2018-04-24_162039	148078	0.010

3. Click **Next**.

   The Select Restore Volume/Partition screen is displayed in the Create Restore Job window.



Select Restore Volume:

Name	Array Name	Capacity (TB)	WWN
100G	148058	0.098	0008000000001B0500
SCOM	148058	0.049	0008000000001C5B0
10GB	148058	0.010	0008000000001C5B0
1GB	148058	0.001	0008000000001B0500

4. Select the desired host volume and click **Finish**.

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

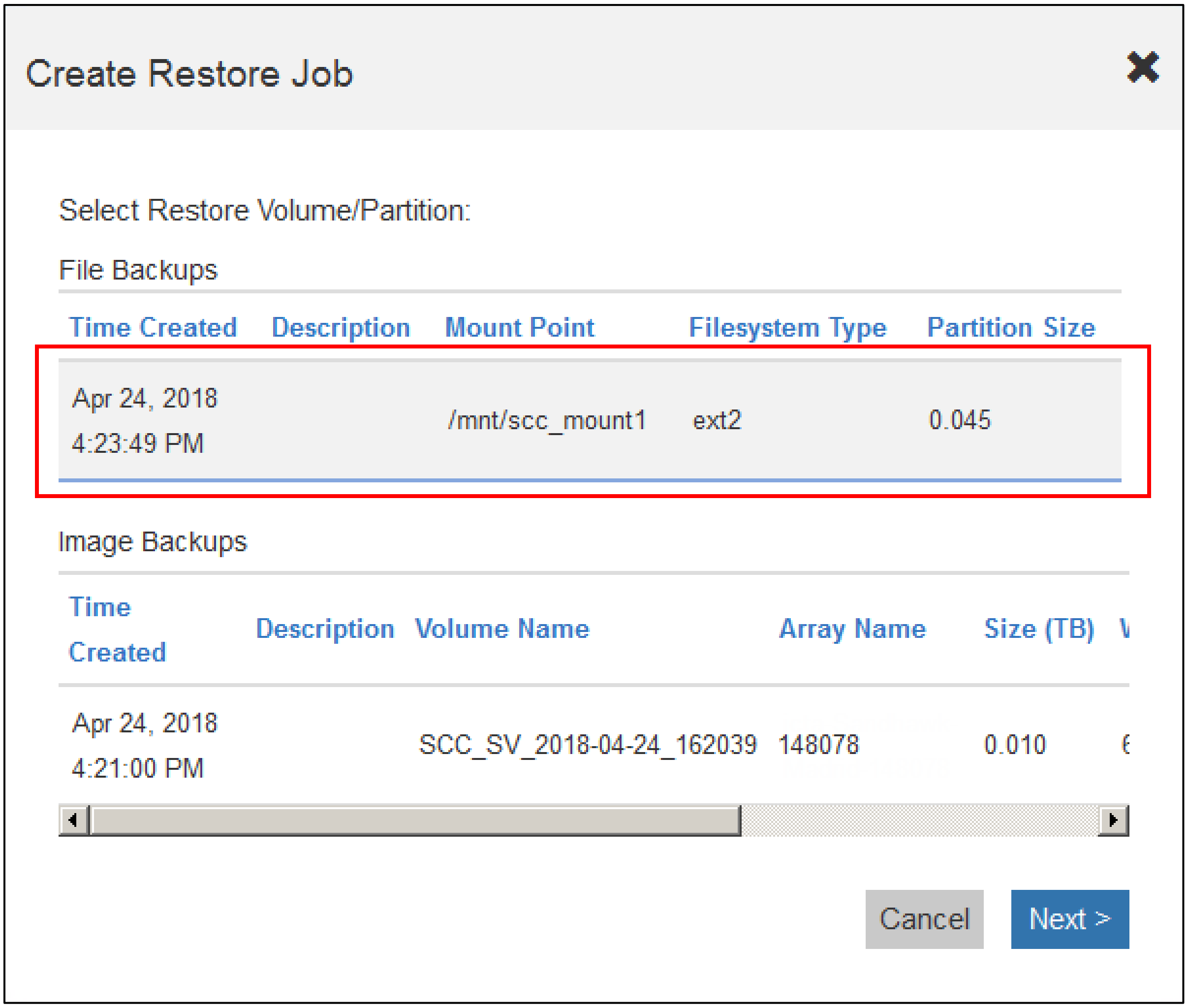
Creating a new file-based restore job

You can create new file-based restore jobs through the Create function in the Restore tab of the SANtricity Cloud Connector application.

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

   The Create Restore Job window is displayed.

2. In the Create Restore Job window, select the desired file-based backup in the File Backups section.



Create Restore Job

Select Restore Volume/Partition:

File Backups

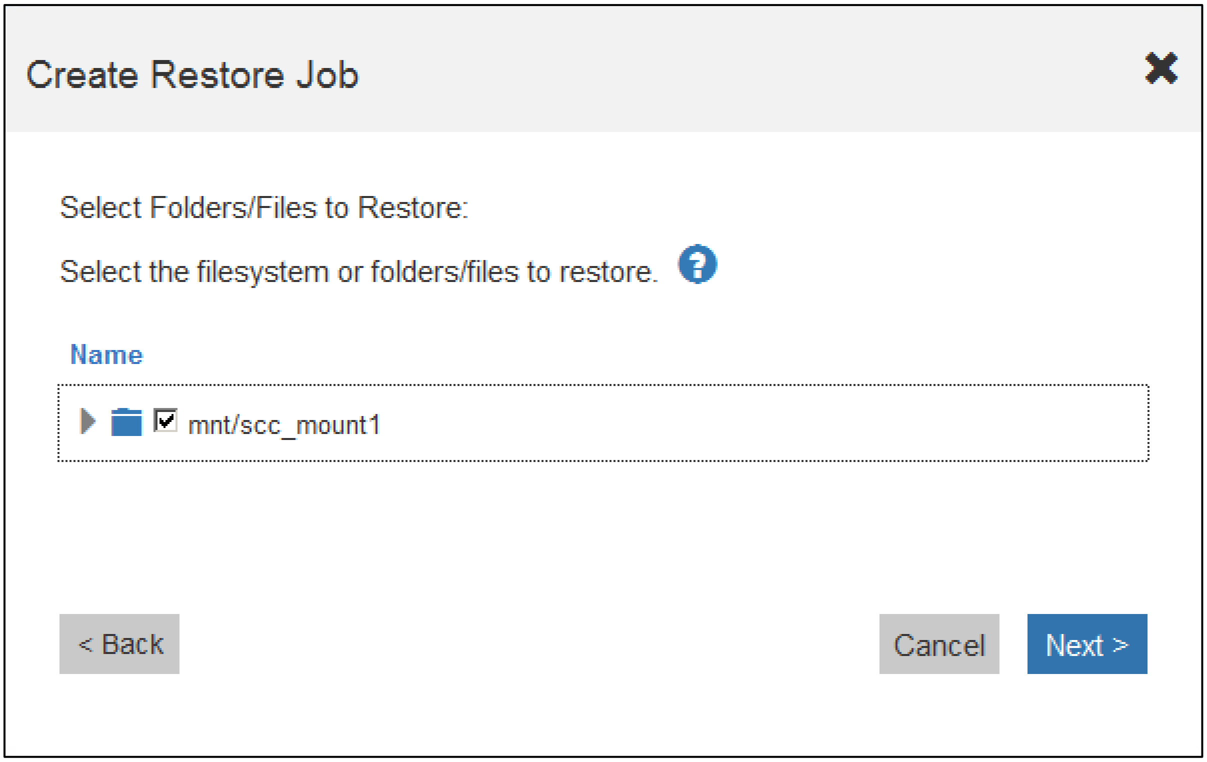
Time Created	Description	Mount Point	Filesystem Type	Partition Size
Apr 24, 2018 4:23:49 PM		/mnt/scc_mount1	ext2	0.045

Image Backups

Time Created	Description	Volume Name	Array Name	Size (TB)
Apr 24, 2018 4:21:00 PM		SCC_SV_2018-04-24_162039	148078	0.010

3. Click **Next**.

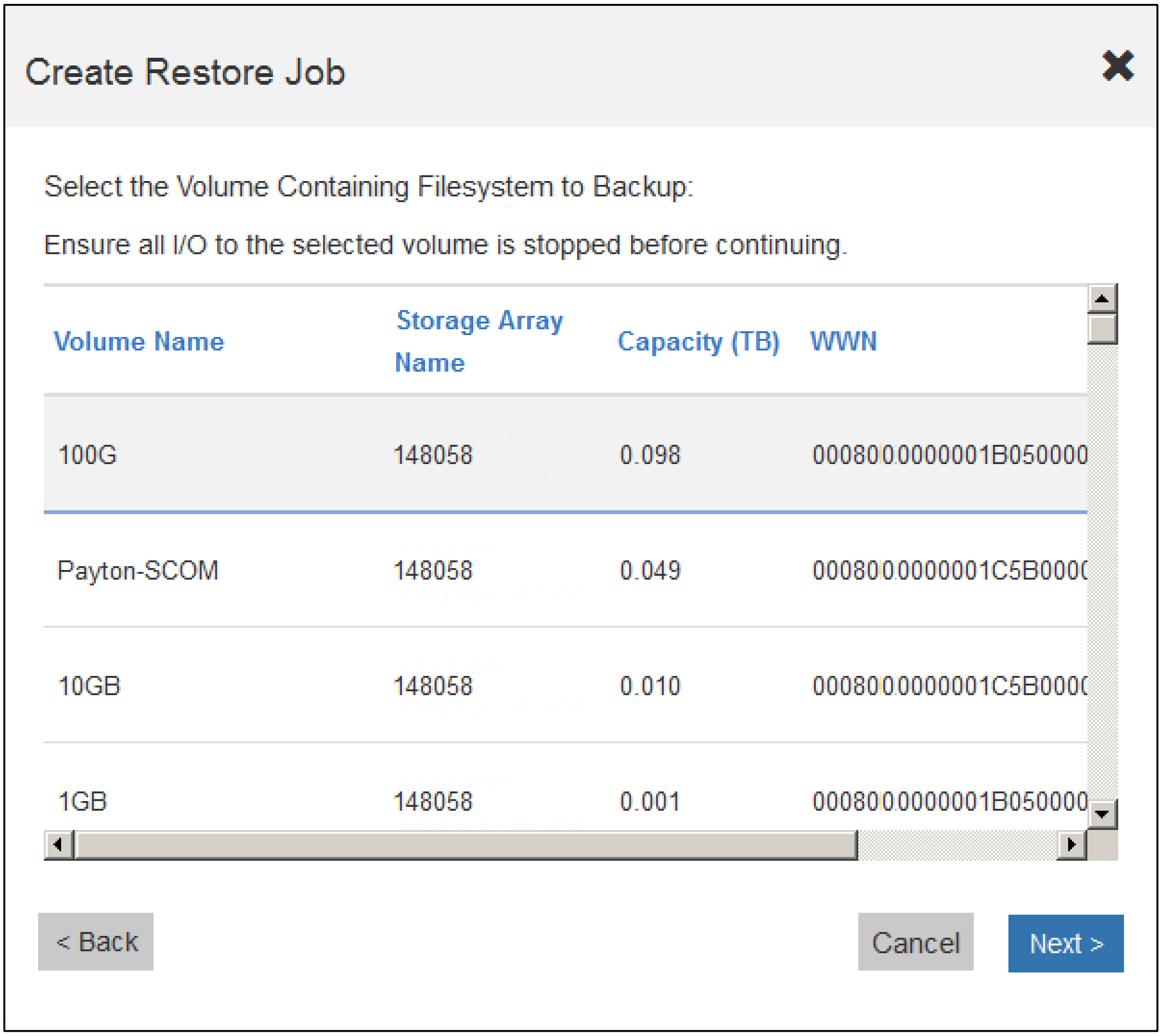
   The Select Folders/Files to Restore screen is displayed in the Create Restore Job window.


Create Restore Job
✖
Select Folders/Files to Restore:
Select the filesystem or folders/files to restore.
Name
☑ mnt/scc_mount1
< Back
Cancel
Next >

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

   A list of available volumes for the selected folder or file is displayed in the Create Restore Job window.

5. Select the desired restore volume for the restore job and click **Next**.



Create Restore Job

Select the Volume Containing Filesystem to Backup:

Ensure all I/O to the selected volume is stopped before continuing.

Volume Name	Storage Array Name	Capacity (TB)	WWN
100G	148058	0.098	0008000000001B050000
Payton-SCOM	148058	0.049	0008000000001C5B000
10GB	148058	0.010	0008000000001C5B000
1GB	148058	0.001	0008000000001B050000

A list of available restore partitions for the selected volume is displayed in the Create Restore window.

NOTE: The partition where the files are restored must be formatted. If the SANtricity Cloud Connector detects a non-formatted partition, the restore job stops and a user alert is displayed.

6. Select the desired restore partition for the restore job and click **Finish**.

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

Deleting a restore job

You can use the Delete function to delete a selected restore job item from the result list section of the Backup tab.

1. In the Restore tab of the SANtricity Cloud Connector application, select the desired restore job and click **Delete**.

   The Confirm Delete window is displayed.

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

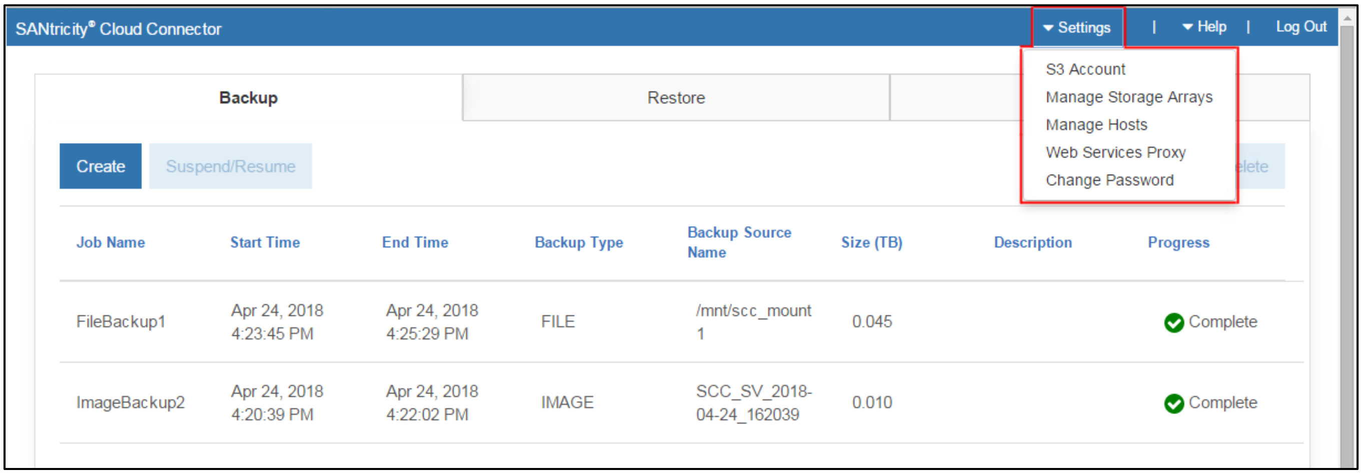
3. Click **Confirm**.

   The selected restore is deleted.

   NOTE: You cannot delete a suspended restore job.

Modifying the SANtricity Cloud Connectors Settings

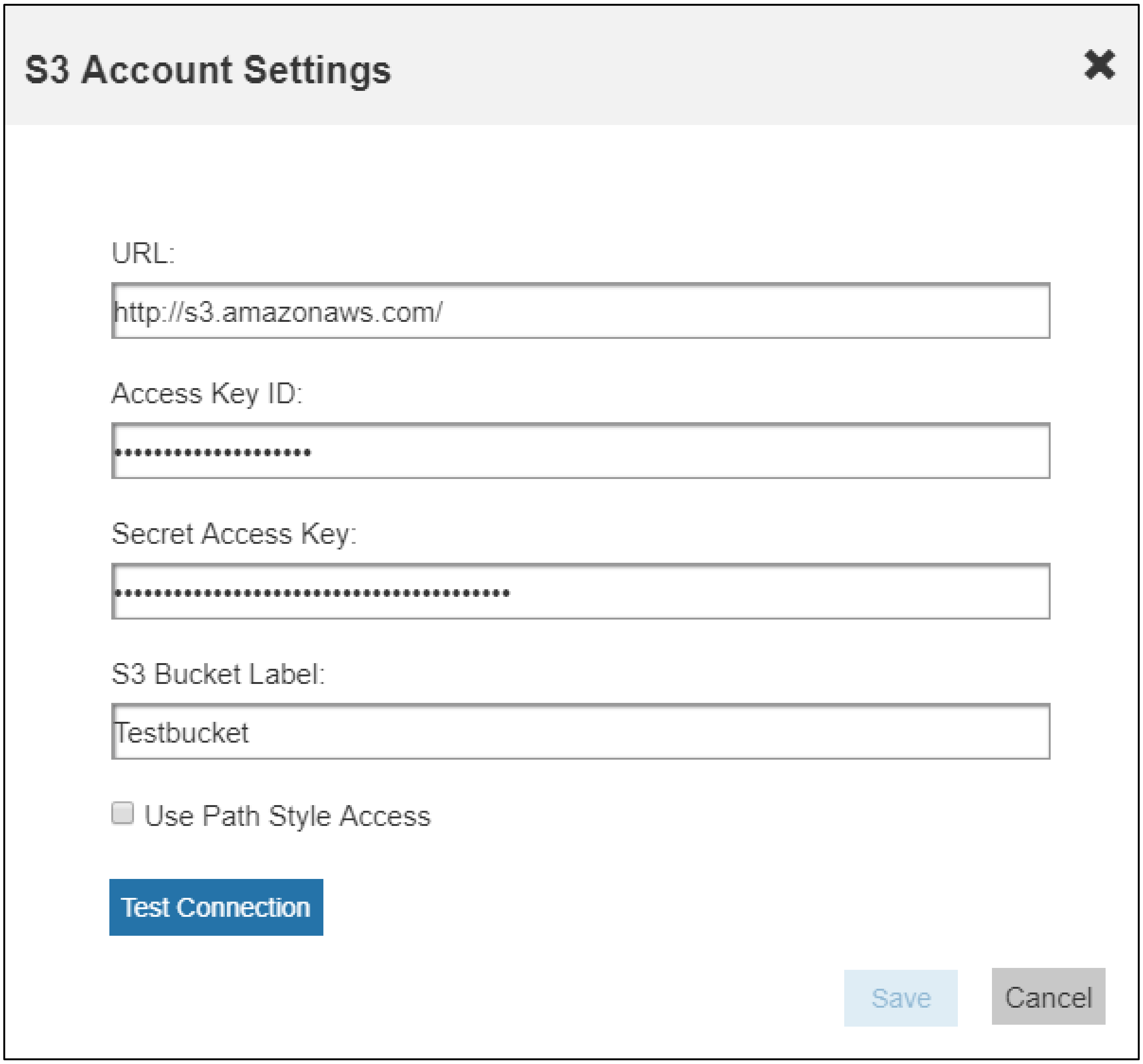
The Settings button in the top toolbar section of the SANtricity Cloud Connector landing page allows you to modify the application's current configurations for the S3 account, managed storage arrays and hosts, and Web Services Proxy credentials. In addition, you also can change the password for the SANtricity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



Job Name	Start Time	End Time	Backup Type	Backup Source Name	Size (TB)	Description	Progress
FileBackup1	Apr 24, 2018 4:23:45 PM	Apr 24, 2018 4:25:29 PM	FILE	/mnt/scc_mount1	0.045		✓ Complete
ImageBackup2	Apr 24, 2018 4:20:39 PM	Apr 24, 2018 4:22:02 PM	IMAGE	SCC_SV_2018-04-24_162039	0.010		✓ Complete

S3 Account Settings

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



S3 Account Settings

URL: http://s3.amazonaws.com/

Access Key ID: ••••••••••••••••••••

Secret Access Key: ••

S3 Bucket Label: Testbucket

☐ Use Path Style Access

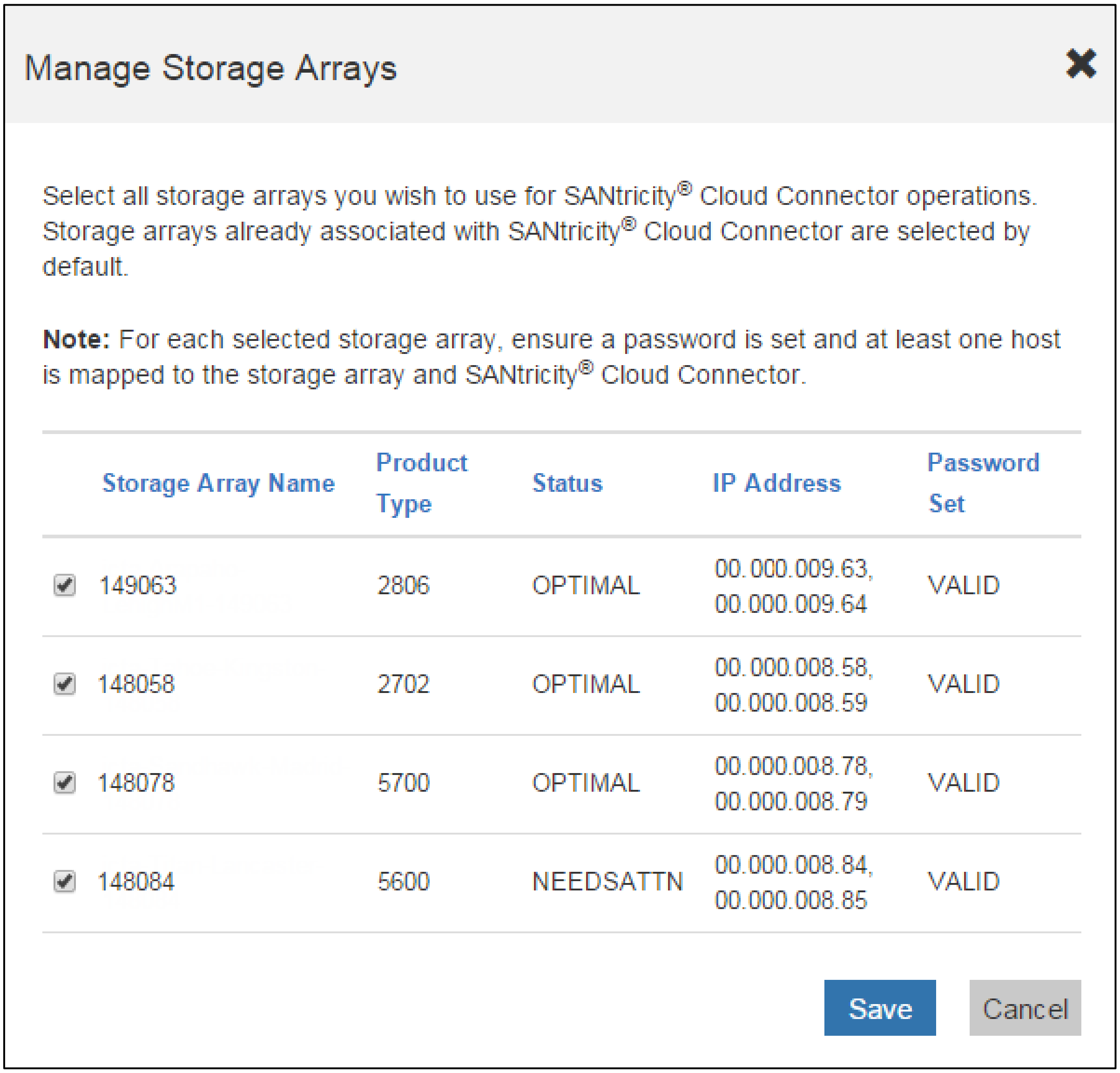
NOTE: Before modifying the URL or S3 Bucket Label settings, be aware that access to any existing backups configured through the SANtricity Cloud Connector will be affected.

1. In the top toolbar, click **Settings > S3 Account**.
2. In the URL file, enter the URL for the S3 cloud service.
3. In the Access Key ID field, enter the access ID for the S3 target.
4. In the Secret Access Key field, enter the access key for the S3 target in the Secret Access Key field.
5. In the S3 Bucket Name field, enter the bucket name for the S3 target.
6. Select the **Use Path Style Access** check box if needed.
7. Click **Test Connection** to verify the connection for the entered S3 credentials.
8. 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 mapped to the SANtricity Cloud Connector host in the Manage Storage Arrays screen. When accessing the Manage Storage Arrays window, any box unchecked by default indicates the corresponding storage array can be added to the SANtricity Cloud Connector host. Conversely, any checkboxes selected by default under the Manage Storage Arrays window indicates the corresponding storage array is already registered with the SANtricity Cloud Connector.



Manage Storage Arrays

Select all storage arrays you wish to use for SANtricity® Cloud Connector operations. Storage arrays already associated with SANtricity® Cloud Connector are selected by default.

Note: For each selected storage array, ensure a password is set and at least one host is mapped to the storage array and SANtricity® Cloud Connector.

	Storage Array Name	Product Type	Status	IP Address	Password Set
☑	149063	2806	OPTIMAL	00.000.009.63, 00.000.009.64	VALID
☑	148058	2702	OPTIMAL	00.000.008.58, 00.000.008.59	VALID
☑	148078	5700	OPTIMAL	00.000.008.78, 00.000.008.79	VALID
☑	148084	5600	NEEDSATTN	00.000.008.84, 00.000.008.85	VALID

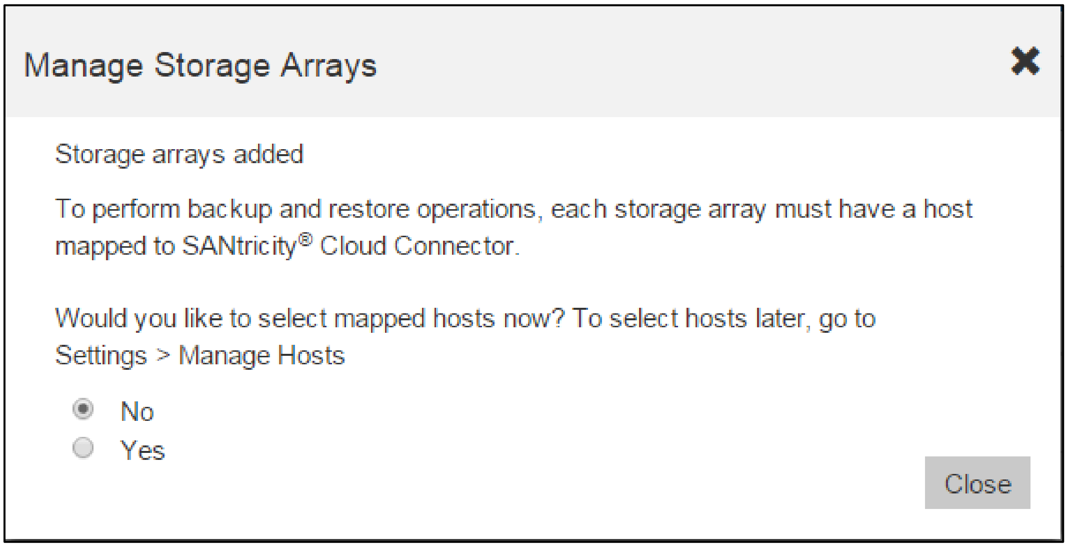
1. In the top toolbar, click **Manage Storage Arrays**.

   The Manage Storage Arrays screen is displayed.

2. To add storage arrays to the SANtricity Cloud Connector, select each box next to the desired storage arrays from the result list, and click **Save**.

   NOTE: When selecting a storage array under the Manage Storage Arrays screen, the listed array status is retained throughout the SANtricity Cloud Connector application and not updated dynamically.

The selected storage arrays are added to the SANtricity Cloud Connector host and a confirmation window is displayed.



Manage Storage Arrays

Storage arrays added

To perform backup and restore operations, each storage array must have a host mapped to SANtricity® Cloud Connector.

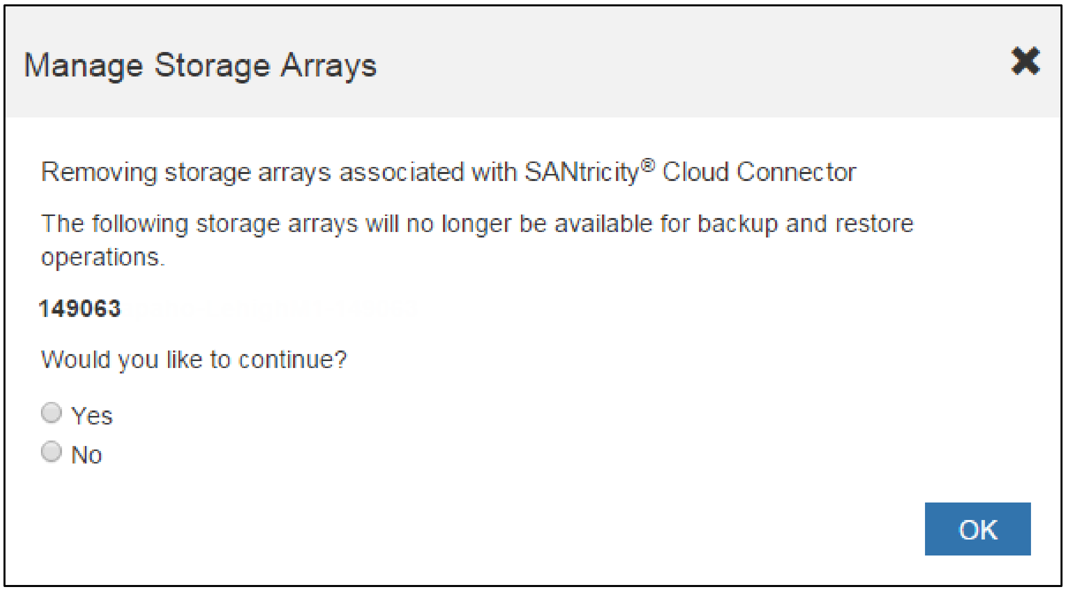
Would you like to select mapped hosts now? To select hosts later, go to Settings > Manage Hosts

● No
○ Yes

a. From the confirmation window, select one of the following Manage Host options:

  - **No –** Decline to select a host for the selected storage array and close the Manage Storage Arrays window.
  - **Yes** – The Manage Hosts window is displayed, allowing you to select a host for the storage array. Refer to the Manage Hosts section for details on how to configure the host for a selected storage array.

3. To remove an existing storage array from the SANtricity Cloud Connector host, uncheck each box next to the desired storage arrays from the bottom result list, and click **Save**.



Manage Storage Arrays

Removing storage arrays associated with SANtricity® Cloud Connector

The following storage arrays will no longer be available for backup and restore operations.

149063 [redacted]

Would you like to continue?

○ Yes
○ No

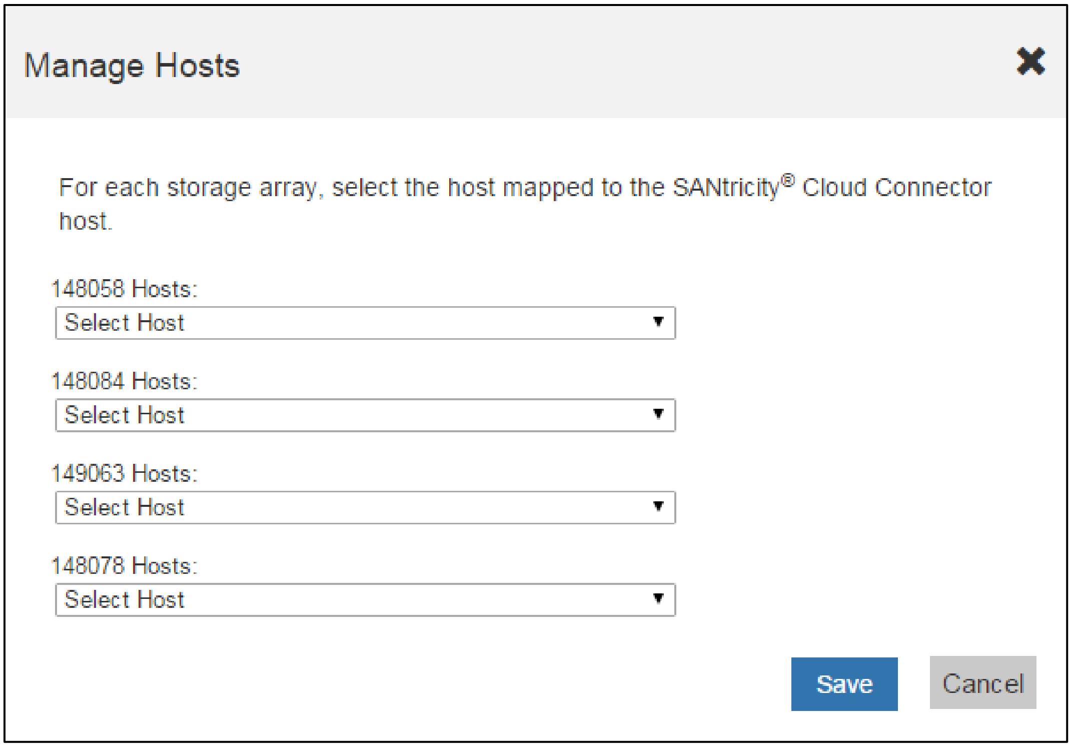
The selected storage arrays are removed from the SANtricity Cloud Connector host and a confirmation window is displayed.

a. From the confirmation window, select one of the following Manage Host options:

- **No –** The confirmation window closes, and the Manage Storage Arrays window is displayed.
- **Yes** – The confirmation window and the Manage Storage Arrays window close.

Manage Hosts

You can modify the host for each storage array mapped to the SANtricity Cloud Connector application in the Manage Hosts screen.



Manage Hosts

For each storage array, select the host mapped to the SANtricity® Cloud Connector host.

148058 Hosts: Select Host

148084 Hosts: Select Host

149063 Hosts: Select Host

148078 Hosts: Select Host

NOTE: If a host for a storage array is not currently mapped to the SANtricity Cloud Connector, Select Host is displayed under the corresponding drop-down field within the Manage Host screen.

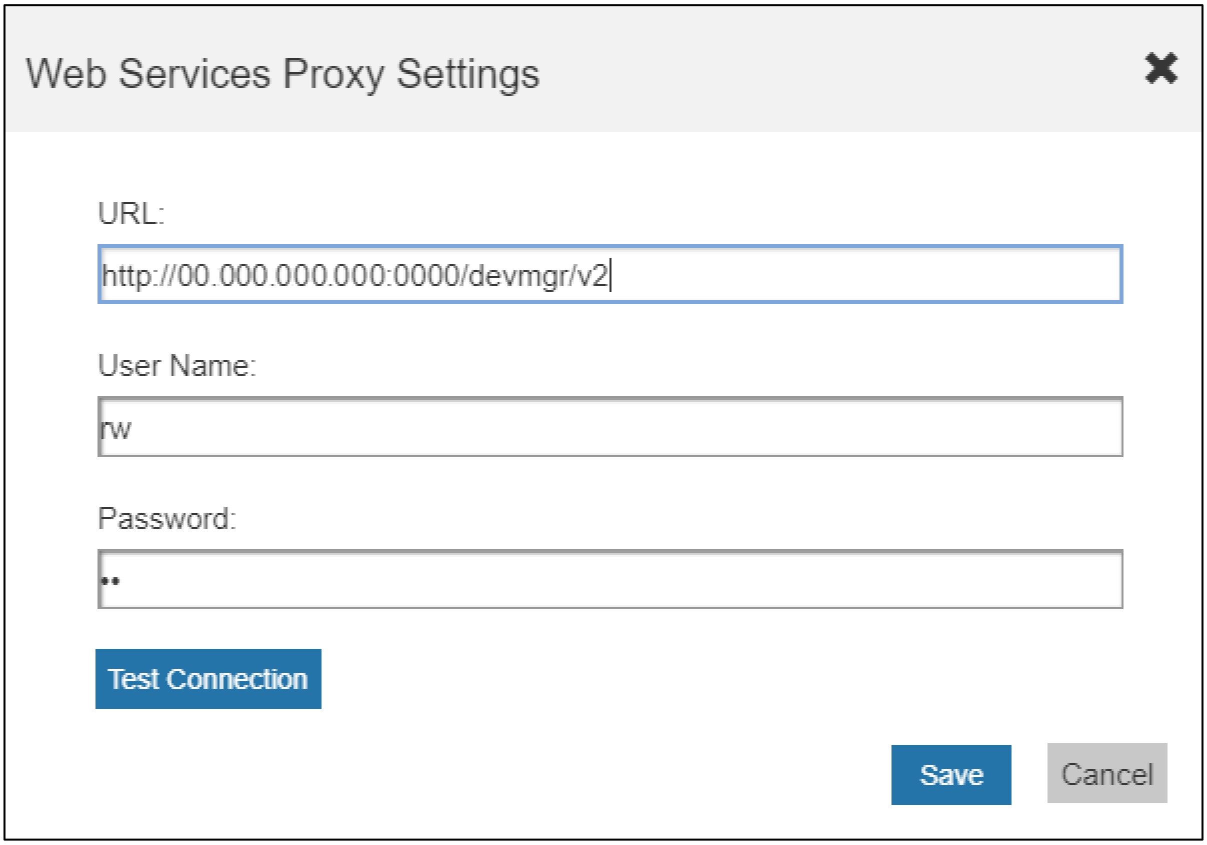
1. In the top toolbar, click **Manage Hosts**.

   The Manage Hosts screen is displayed.
2. To map a host to the SANtricity Cloud Connector, select the desired host option under the drop-down field for the corresponding storage array.
3. To remove an existing mapped host, select the **Select host** option under the drop-down field for the desired storage array.
4. Click **Save**.

   All changes made in the Manage Host screen are saved and applied to the SANtricity Cloud Connector application.

Web Services Settings

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



Web Services Proxy Settings

URL: http://00.000.000.000:0000/devmgr/v2

User Name: rw

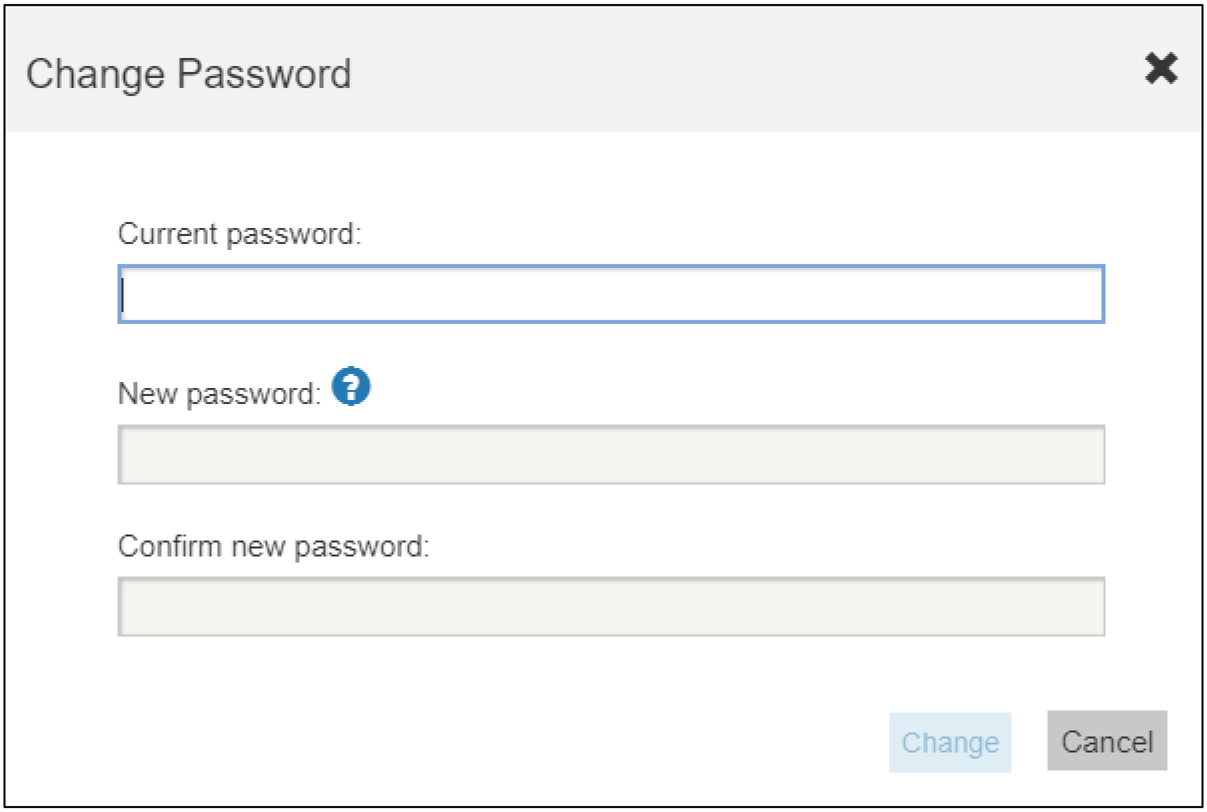
Password: ••

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

   NOTE: The Web Services Proxy used with the SANtricity Cloud Connector needs to have the appropriate arrays added.

Change SANtricity Cloud Connector password

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



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

Uninstalling the SANtricity Cloud Connector

Uninstalling the SANtricity Cloud Connector on a Linux Operating System through graphical mode

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

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:

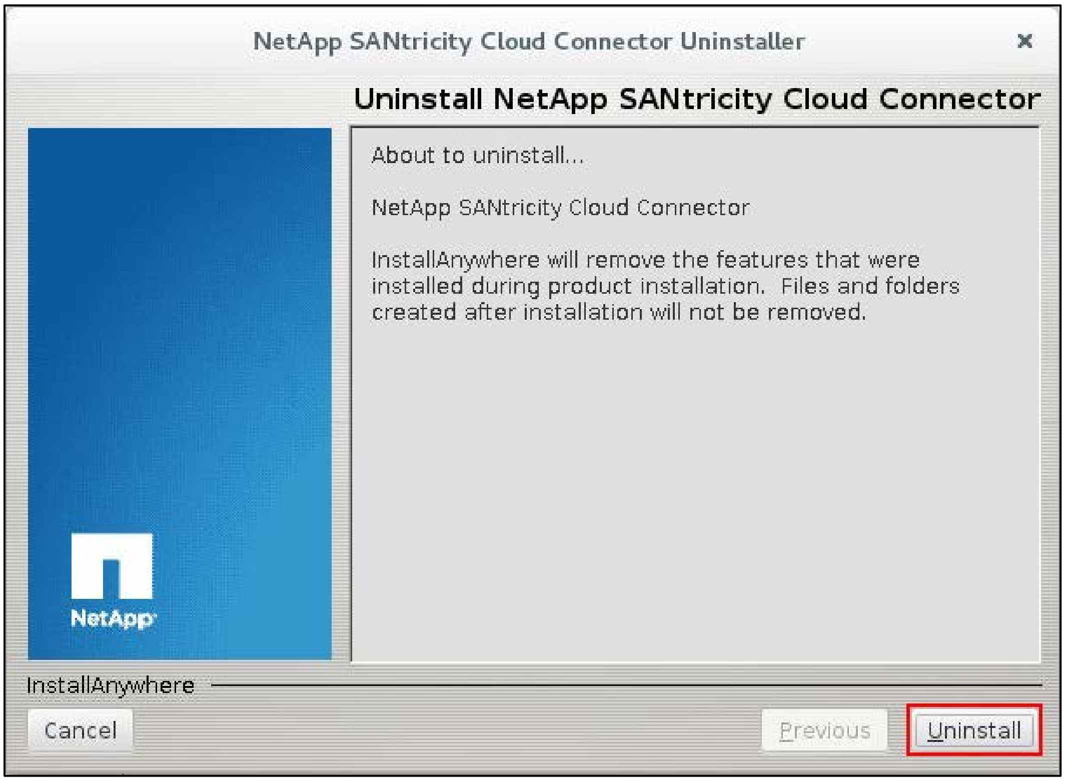
   ```
   /opt/netapp/santricity_cloud_connector/uninstall_cloud_connector
   ```

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

   ```
   ./uninstall_cloud_connector –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.



Uninstall NetApp SANtricity Cloud Connector

About to uninstall...

NetApp SANtricity Cloud Connector

InstallAnywhere will remove the features that were installed during product installation. Files and folders created after installation will not be removed.

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

Uninstalling the SANtricity Cloud Connector on a Linux Operating System through console mode

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

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:

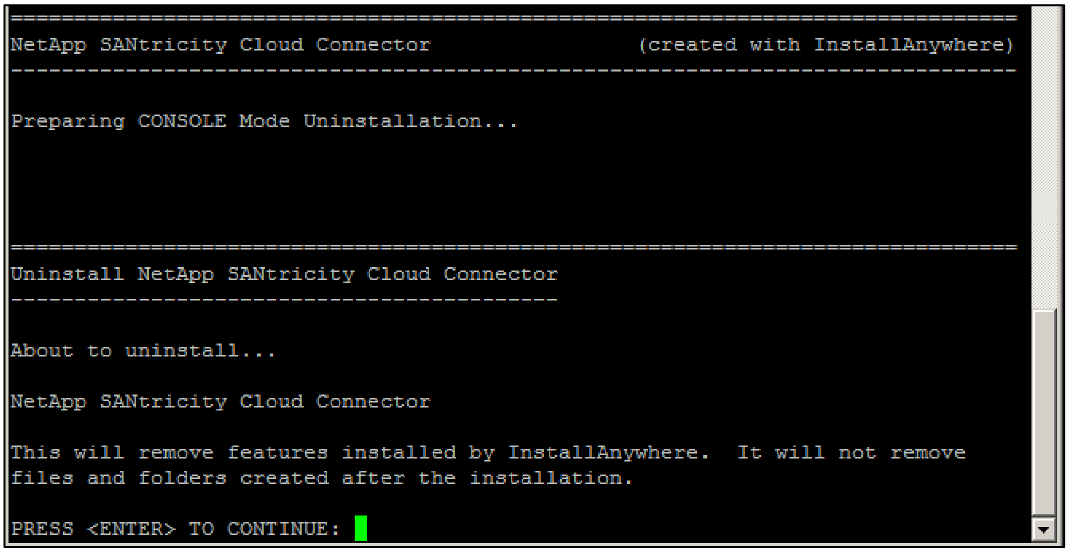
   ```
   /opt/netapp/santricity_cloud_connector/uninstall_cloud_connector
   ```

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

   ```
   ./uninstall_cloud_connector –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.



```
===============================================================================
NetApp SANtricity Cloud Connector                (created with InstallAnywhere)
-------------------------------------------------------------------------------

Preparing CONSOLE Mode Uninstallation...




===============================================================================
Uninstall NetApp SANtricity Cloud Connector
-------------------------------------------

About to uninstall...

NetApp SANtricity Cloud Connector

This will remove features installed by InstallAnywhere.  It will not remove
files and folders created after the installation.

PRESS <ENTER> TO CONTINUE:
```

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

Copyright information

Trademark information

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 your comments

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., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

NetApp®