



## **Use SANtricity solutions**

### **E-Series**

NetApp  
January 31, 2022

# Table of Contents

- Use SANtricity solutions . . . . . 1
  - Web services proxy . . . . . 1
  - Remote volume mirroring . . . . . 34
  - Storage plugin for vCenter . . . . . 42
  - Legacy solutions . . . . . 60

# Use SANtricity solutions

## Web services proxy

### SANtricity Web Services Proxy overview

The SANtricity Web Services Proxy is a RESTful API server installed separately on a host system to manage hundreds of new and legacy NetApp E-Series storage systems. The proxy includes SANtricity Unified Manager, which is a web-based interface that provides similar functions.

#### Installation overview

Installing and configuring the Web Services Proxy involves the following steps:

1. [Review installation and upgrade requirements.](#)
2. [Download and install Web Services Proxy file.](#)
3. [Log in to API and Unified Manager.](#)
4. [Configure Web Services Proxy.](#)

#### Find more information

- Unified Manager — The proxy installation includes SANtricity Unified Manager, a web-based interface that provides configuration access to newer E-Series and EF-Series storage systems. For more information, see the Unified Manager online help, which is available from its user interface or from the [Documentation Center](#).
- GitHub repository — GitHub contains a repository for the collection and organization of sample scripts illustrating the use of the NetApp SANtricity Web Services API. To access the repository, see [NetApp Webservices samples](#).
- Representational state transfer (REST) — Web Services is a RESTful API that provides access to virtually all the SANtricity management capabilities, so you should be familiar with REST concepts. For more information, see [Architectural Styles and the Design of Network-based Software Architectures](#).
- JavaScript Object Notation (JSON) — Because data within Web Services is encoded through JSON, you should be familiar with JSON programming concepts. For more information, see [Introducing JSON](#).

## Learn about Web Services

### Web Services and Unified Manager overview

Before you install and configure the Web Services proxy, read the overview of Web Services and SANtricity Unified Manager.

#### Web Services

Web Services is an Application Programming Interface (API) that allows you to configure, manage, and monitor NetApp E-Series and EF-Series storage systems. By issuing API requests, you can complete workflows such as configuration, provisioning, and performance monitoring for E-Series storage systems.

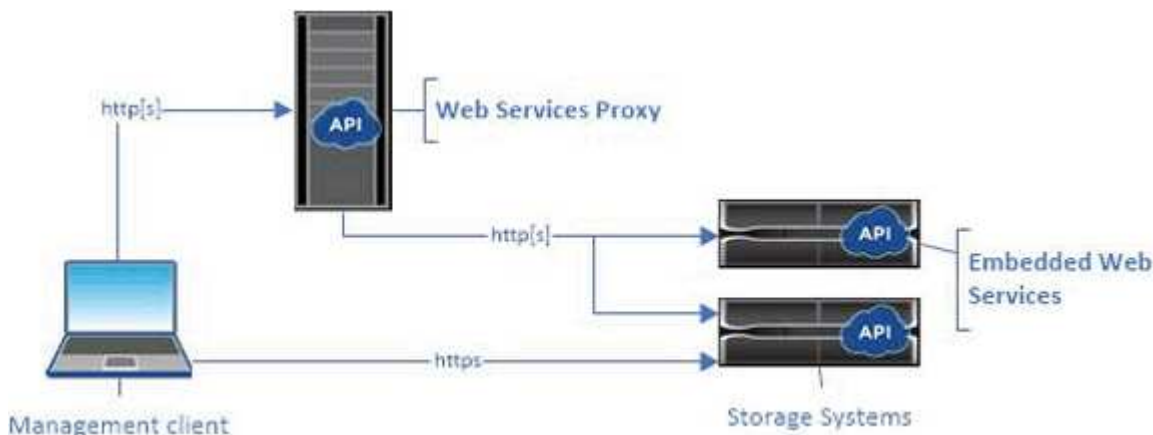
When using the Web Services API to manage storage systems, you should be familiar with the following:

- JavaScript Object Notation (JSON) – Because data within Web Services is encoded through JSON, you should be familiar with JSON programming concepts. For more information, see [Introducing JSON](#).
- Representational state transfer (REST) – Web Services is a RESTful API that provides access to virtually all the SANtricity management capabilities, so you should be familiar with REST concepts. For more information, see [Architectural Styles and the Design of Network-based Software Architectures](#).
- Programming language concepts – Java and Python are the most common programming languages used with the Web Services API, but any programming language that can make HTTP requests is sufficient for API interaction.

Web Services is available in two implementations:

- **Embedded** — A RESTful API server is embedded on each controller of an E2800/EF280 storage system running NetApp SANtricity 11.30 or later versions, an E5700/EF570 running SANtricity 11.40 or later versions, and an EF300 or EF600 running SANtricity 11.60 or later versions. No installation is required.
- **Proxy** — The SANtricity Web Services Proxy is a RESTful API server installed separately on a Windows or Linux server. This host-based application can manage hundreds of new and legacy NetApp E-Series storage systems. In general, you should use the proxy for networks with more than 10 storage systems. The proxy can handle numerous requests more efficiently than the embedded API.

The core of the API is available in both implementations.



The following table provides a comparison of the proxy and the embedded version.

| Consideration | Proxy   | Embedded                                |
|---------------|---|---|
| Installation  | Requires a host system (Linux or Windows). The proxy is available for download at the <a href="#">NetApp Support Site</a> or on <a href="#">DockerHub</a> . | No installation or enablement required. |

| Consideration      | Proxy  | Embedded   |
|--------------------|--|--|
| Security           | Minimal security settings by default.<br><br>Security settings are low so that developers can get started with the API quickly and easily. If desired, you can configure the proxy with the same security profile as the embedded version. | High security settings by default.<br><br>Security settings are high because the API runs directly on the controllers. For example, it does not allow HTTP access, and it disables all SSL and older TLS encryption protocols for HTTPS. |
| Central management | Manages all storage systems from one server.   | Manages only the controller on which it is embedded.   |

### Unified Manager

The proxy installation package includes Unified Manager, a web-based interface that provides configuration access to newer E-Series and EF-Series storage systems, such as the E2800, E5700, EF300, and EF600.



From Unified Manager, you can perform the following batch operations:

- View the status of multiple storage systems from a central view
- Discover multiple storage systems in your network
- Import settings from one storage system to multiple systems
- Upgrade firmware for multiple storage systems

### Compatibility and restrictions

The following compatibility and restrictions apply to using the Web Services Proxy.

| Consideration                | Compatibility or restriction   |
|------------------------------|--|
| HTTP support                 | The Web Services Proxy allows use of HTTP or HTTPS. (The embedded version of Web Services requires HTTPS for security reasons.)  |
| Storage systems and firmware | The Web Services Proxy can manage all E-Series storage systems, including a mixture of older systems and the latest E2800, EF280, E5700, EF570, EF300, and EF600 series systems. |

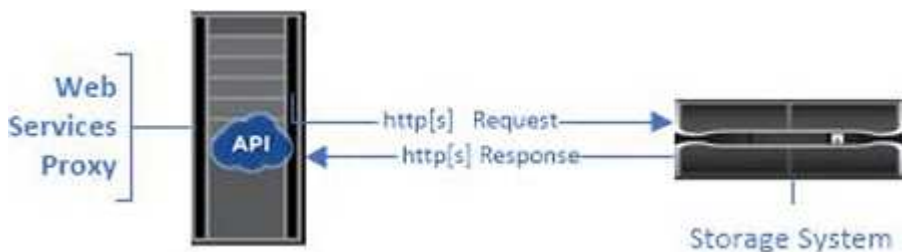
| Consideration                | Compatibility or restriction   |
|------------------------------|--|
| IP Support                   | <p>The Web Services Proxy supports either the IPv4 protocol or IPv6 protocol.</p> <div>  <p>The IPv6 protocol might fail when the Web Services Proxy tries to automatically discover the management address from the controller configuration. Possible causes for the failure include problems during IP address forwarding or IPv6 being enabled on the storage systems but not on the server.</p> </div> |
| NVSRAM file name constraints | <p>The Web Services Proxy uses NVSRAM file names to identify version information accurately. Therefore, you cannot change NVSRAM filenames when they are used with the Web Services Proxy. The Web Services Proxy might not recognize a renamed NVSRAM file as a valid firmware file.</p>  |
| Symbol Web                   | <p>Symbol Web is a URL in the REST API. It provides access to almost all symbol calls. The symbol function is part of the following URL:</p> <pre>http://host:port/devmgr/storage-system/storage array ID/symbol/symbol function</pre> <div>  <p>Symbol-disabled storage systems are supported through the Web Services Proxy.</p> </div>   |

## API basics

In the Web Services API, HTTP communications involve a request-response cycle.

### URL elements in requests

Regardless of the programming language or tool used, each call to the Web Services API has a similar structure, with a URL, HTTP verb, and an Accept header.



All requests include a URL, as in the following example, and contain the elements described in the table.

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

| Area  | Description   |
|---|---|
| HTTP transport<br><br><code>https://</code>                     | <p>The Web Services Proxy enables the use of HTTP or HTTPS.</p> <p>The embedded Web Services requires HTTPS for security reasons.</p>   |
| Base URL and port<br><br><code>webservices.name.com:8443</code> | <p>Each request must be correctly routed to an active instance of Web Services. The FQDN (fully qualified domain name) or the IP address of the instance is required, along with the listening port. By default, Web Services communicates over port 8080 (for HTTP) and port 8443 (for HTTPS).</p> <p>For the Web Services Proxy, both ports can be changed during the proxy installation or in the <code>wsconfig.xml</code> file. Port contention is common on data center hosts running various management applications.</p> <p>For the embedded Web Services, the port on the controller cannot be changed; it defaults to port 8443 for secure connections.</p> |
| API path<br><br><code>devmgr/v2/storage-systems</code>          | <p>A request is made to a specific REST resource or endpoint within the Web Services API. Most endpoints are in the form of:</p> <p><code>devmgr/v2/&lt;resource&gt;/[id]</code></p> <p>The API path consists of three parts:</p> <ul style="list-style-type: none"><li>• <code>devmgr</code> (Device Manager) is the namespace of the Web Services API.</li><li>• <code>v2</code> denotes the version of the API that you are accessing. You can also use <code>utils</code> to access login endpoints.</li><li>• <code>storage-systems</code> is a category within the documentation.</li></ul>   |

### Supported HTTP verbs

Supported HTTP verbs include GET, POST, and DELETE:

- GET requests are used for read-only requests.
- POST requests are used to create and update objects, and also for read requests that might have security implications.

- DELETE requests are typically used to remove an object from management, remove an object entirely, or to reset the state of the object.



Currently, the Web Services API does not support PUT or PATCH. Instead, you can use POST to provide the typical functionality for these verbs.

### Accept headers

When returning a request body, Web Services returns the data in JSON format (unless otherwise specified). Certain clients default to requesting “text/html” or something similar. In these cases, the API responds with an HTTP code 406, denoting that it cannot provide data in this format. As a best practice, you should define the Accept header as “application/json” for any cases in which you expect JSON as the response type. In other cases where a response body is not returned (for example, DELETE), providing the Accept header does not cause any unintended effects.

### Responses

When a request is made to the API, a response returns two critical pieces of information:

- HTTP status code — Indicates whether the request was successful.
- Optional response body — Usually provides a JSON body representing the state of the resource or a body providing more details on the nature of a failure.

You must check the status code and the content-type header to determine what the resulting response body looks like. For HTTP status codes 200-203 and 422, Web Services returns a JSON body with the response. For other HTTP status codes, Web Services generally does not return an additional JSON body, either because the specification does not allow it (204) or because the status is self-explanatory. The table lists common HTTP status codes and definitions. It also indicates whether information associated with each HTTP code is returned in a JSON body.

| HTTP status code                  | Description   | JSON body |
|-----------------------------------|---|-----------|
| 200 OK                            | Denotes a successful response.  | Yes       |
| 201 Created                       | Indicates that an object was created. This code is used in a few rare cases instead of a 200 status.  | Yes       |
| 202 Accepted                      | Indicates that the request is accepted for processing as an asynchronous request, but you must make a subsequent request to get the actual result.  | Yes       |
| 203 Non-Authoritative Information | Similar to a 200 response, but Web Services cannot guarantee that the data is up-to-date (for example, only cached data is available at this time). | Yes       |



| HTTP status code         | Description   | JSON body |
|--------------------------|---|-----------|
| 204 No Content           | Indicates a successful operation, but there is no response body.  | No        |
| 400 Bad Request          | Indicates that the JSON body provided in the request is not valid.  | No        |
| 401 Unauthorized         | Indicates that an authentication failure has occurred. Either no credentials were provided, or the username or password was invalid.  | No        |
| 403 Forbidden            | An authorization failure, which indicates that the authenticated user does not have permission to access the requested endpoint.  | No        |
| 404 Not Found            | Indicates that the requested resource could not be located. This code is valid for nonexistent APIs or nonexistent resources requested by the identifier.                           | No        |
| 422 Unprocessable Entity | Indicates the request is generally well-formed, but either the input parameters are invalid, or the state of the storage system does not allow Web Services to satisfy the request. | Yes       |
| 424 Failed Dependency    | Used in the Web Services Proxy to indicate that the requested storage system is currently inaccessible. Therefore, Web Services cannot satisfy the request.                         | No        |
| 429 Too Many Requests    | Indicates that a request limit was exceeded and should be retried at a later time.  | No        |

### Sample scripts

GitHub contains a repository for the collection and organization of sample scripts illustrating the use of the NetApp SANtricity Web Services API. To access the repository, see [NetApp Webservices samples](#).

### Terms and concepts

The following terms apply to the Web Services Proxy.

| Term           | Definition  |
|----------------|---|
| API            | An Application Programming Interface (API) is a set of protocols and methods that enables developers to communicate with devices. The Web Services API is used to communicate with E-Series storage systems.  |
| ASUP           | The AutoSupport (ASUP) feature collects data in a customer support bundle and automatically sends the message file to technical support for remote troubleshooting and problem analysis.  |
| Endpoint       | Endpoints are functions that are available through the API. An endpoint includes an HTTP verb, plus the URI path. In Web Services, endpoints can execute such tasks as discovering storage systems and creating volumes.  |
| HTTP Verb      | An HTTP verb is a corresponding action for an endpoint, such as retrieving and creating data. In Web Services, HTTP verbs include POST, GET, and DELETE.  |
| JSON           | JavaScript Object Notation (JSON) is a structured data format much like XML, which uses a minimal, readable format. Data within Web Services is encoded through JSON.   |
| REST / RESTful | <p>Representational state transfer (REST) is a loose specification that defines an architectural style for an API. Because most REST APIs do not fully adhere to the specification, they are described as “RESTful” or “REST-like.” Generally, a “RESTful” API is agnostic to programming languages and has the following characteristics:</p> <ul style="list-style-type: none"> <li>• HTTP-based, which follows the general semantics of the protocol</li> <li>• Producer and consumer of structured data (JSON, XML, etc.)</li> <li>• Object-oriented (as opposed to operation-oriented)</li> </ul> <p>Web Services is a RESTful API that provides access to virtually all the SANtricity management capabilities.</p> |
| storage system | A storage system is an E-Series array, which includes shelves, controllers, drives, software, and firmware.   |

| Term         | Definition   |
|--------------|--|
| SYMBol API   | SYMBol is a legacy API for managing E-Series storage systems. The underlying implementation of the Web Services API uses SYMBol.   |
| Web Services | Web Services is an API that NetApp designed for developers to manage E-Series storage systems. There are two implementations of Web Services: embedded on the controller and a separate proxy that can be installed on Linux or Windows. |

## Install and configure

### Review installation and upgrade requirements

Before installing the Web Services Proxy, review the installation requirements and upgrade considerations.

#### Installation requirements

You can install and configure the Web Services Proxy on a Windows or Linux host system.

Proxy installation includes the following requirements.

| Requirement          | Description   |
|----------------------|---|
| Hostname limitations | Be sure that the hostname of the server where you plan to install the Web Services Proxy contains only ASCII letters, numerical digits, and hyphens (-). This requirement is due to a limitation of Java Keytool, which is used in generating a self-signed certificate for the server. If the hostname of your server contains any other characters, such as an underscore (_), the Webserver will fail to start after installation. |
| Operating systems    | <p>You can install the proxy on the following operating systems:</p> <ul style="list-style-type: none"> <li>• Linux</li> <li>• Windows</li> </ul> <p>For a complete list of operating systems and firmware compatibility, see the <a href="#">NetApp Interoperability Matrix Tool</a>.</p>  |

| Requirement                      | Description   |
|----------------------------------|---|
| Linux: Additional Considerations | Linux Standard Base libraries (init-functions) are required for the Webserver to function properly. You must install the lsb/insserv packages for your operating system. For more information, refer to the "Additional packages required" section of the Readme file.  |
| Multiple instances               | You can install only one instance of Web Services Proxy on a server; however, you can install the proxy on multiple servers within your network.  |
| Capacity planning                | <p>Web Services Proxy requires adequate space for logging. Make sure that your system meets the following available disk space requirements:</p> <ul style="list-style-type: none"> <li>• Required installation space — 275 MB</li> <li>• Minimum logging space — 200 MB</li> <li>• System memory — 2 GB; heap space is 1 Gb by default</li> </ul> <p>You can use a disk-space monitoring tool to verify available disk drive space for persistent storage and logging.</p> |
| License                          | The Web Services Proxy is a free, standalone product that does not require a license key. However, applicable copyrights and terms of service apply. If you are installing the proxy in either Graphical or Console mode, you must accept the End User License Agreement (EULA).  |

### Upgrade considerations

If you are upgrading from a previous version, be aware that some items are preserved or removed.

- For the Web Services Proxy, previous configuration settings are preserved. These settings include user passwords, all discovered storage systems, server certificates, trusted certificates, and server runtime configuration.
- For Unified Manager, all SANtricity OS files previously loaded in the repository are removed during the upgrade.

### Download and install Web Services Proxy file

Installation involves downloading the file and then installing the proxy package on a Linux or Windows server.

## Download Web Services Proxy files

You can download the installation file and the readme file from the Software download page of the NetApp Support site.

The download package includes the Web Services Proxy and the Unified Manager interface.

### Steps

1. Go to [NetApp Support - Downloads](#).
2. Select **E-Series SANtricity Web Services Proxy**.
3. Follow the instructions to download the file. Make sure you select the correct download package for your server (for example, EXE for Windows; BIN or RPM for Linux).
4. Download the installation file to the server where you want to install the proxy and Unified Manager.

### Install on Windows or Linux server

You can install the Web Services Proxy and Unified Manager using one of three modes (Graphical, Console, or Silent), or by using an RPM file (Linux only).

### Before you begin

- [Review installation requirements](#).
- Make sure you have downloaded the correct installation file (EXE for Windows; BIN for Linux) to the server where you want to install the proxy and Unified Manager.

### Graphical mode install

You can run the installation in Graphical mode for either Windows or Linux. In Graphical mode, the prompts appear in a Windows-style interface.

### Steps

1. Access the folder where you downloaded the installation file.
2. Launch the installation for either Windows or Linux, as follows:

- Windows — Double-click the installation file:

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

- Linux — Run the following command: `santricity_webservices-linux_x64-nn.nn.nn.nnnn.bin`

In the above filenames, `nn.nn.nn.nnnn` represents the version number.

The installation process starts and the NetApp SANtricity Web Services Proxy + Unified Manager splash screen appears.

3. Follow the on-screen prompts.

During the installation, you are prompted to enable several features and enter some configuration parameters. If necessary, you can change any of these selections later in the configuration files.

4. When the Webserver Started message appears, click **OK** to complete the installation.

The Install Complete dialog box appears.

5. Click the check boxes if you want to launch Unified Manager or the interactive API documentation, and then click **Done**.

## Console mode install

You can run the installation in Console mode for either Windows or Linux. In Console mode, the prompts appear in the terminal window.

### Steps

1. Run the following command: `<install filename> -i console`

In the above command, `<install filename>` represents the name of the proxy installation file you downloaded (for example: `santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe`).



To cancel the installation at any time during the installation process, type `QUIT` at the command prompt.

The installation process starts and the Launching Installer — Introduction message appears.

2. Follow the on-screen prompts.

During the installation, you are prompted to enable several features and enter some configuration parameters. If necessary, you can change any of these selections later in the configuration files.

3. When the installation is complete, press **Enter** to exit the installer.

## Silent mode install

You can run the installation in Silent mode for either Windows or Linux. In Silent mode, no return messages or scripts appear in the terminal window.

### Steps

1. Run the following command: `<install filename> -i silent`

In the above command, `<install filename>` represents the name of the proxy installation file you downloaded (for example: `santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe`).

2. Press **Enter**.

The installation process can take several minutes to complete. After successful installation, a command prompt appears in the terminal window.

## RPM command install (Linux only)

For Linux systems that are compatible with the RPM package management system, you can install the Web Services Proxy using an optional RPM file.

### Steps

1. Download the RPM file to the server where you want to install the proxy and Unified Manager.
2. Open a terminal window.

3. Enter the following command:

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



In the above command, nn.nn.nn.nnnn represents the version number.

The installation process can take several minutes to complete. After successful installation, a command prompt appears in the terminal window.

## Log in to API and Unified Manager

Web Services includes API documentation, which enables you to directly interact with the REST API. It also includes Unified Manager, a browser-based interface for managing multiple E-Series storage systems.

### Log in to Web Services API

After you install the Web Services Proxy, you can access the interactive API documentation in a browser.

The API documentation runs with each instance of Web Services, and is also available in a static PDF format from the NetApp Support site. To access the interactive version, you open a browser and enter the URL pointing to where Web Services resides (either a controller for the embedded version or a server for the proxy).



The Web Services API implements the OpenAPI specification (originally called the Swagger specification).

For initial login, you use the "admin" credentials. "Admin" is considered a super administrator with access to all functions and roles.

### Steps

1. Open a browser.
2. Enter the URL for the embedded or proxy implementation:

- Embedded: `https://<controller>:<port>/devmgr/docs/`

In this URL, <controller> is the IP address or FQDN of the controller, and <port> is the management port number of the controller (defaults to 8443).

- Proxy: `http[s]://<server>:<port>/devmgr/docs/`

In this URL, <server> is the IP address or FQDN of the server where the proxy is installed, and <port> is the listening port number (defaults to 8080 for HTTP or 8443 for HTTPS).




If the listening port is already in use, the proxy detects the conflict and prompts you to choose a different listening port.

The API documentation opens in the browser.

3. When the interactive API documentation opens, go to the drop-down menu in the upper right of the page and select **utils**.

4. Click the **Login** category to see the available endpoints.
5. Click the **POST: /login** endpoint, and then click **Try it out**.
6. For first-time login, enter admin for the username and password.
7. Click **Execute**.
8. To access the endpoints for storage management, go to the drop-down menu in the upper right and select **v2**.

The high-level categories for endpoints are displayed. You can navigate the API documentation as described in the table.

| Area           | Description  |
|----------------|--|
| Drop-down menu | <p>At the upper right of the page, a drop-down menu provides options for switching between version 2 of the API documentation (V2), the SYMBol interface (SYMBol V2), and API utilities (utils) for logging in.</p> <div>  <p>Because version 1 of the API documentation was a prerelease and not generally available, V1 is not included in the drop-down menu.</p> </div> |
| Categories     | The API documentation is organized by high-level categories (for example: Administration, Configuration). Click on a category to see the related endpoints.  |
| Endpoints      | Select an endpoint to see its URL paths, required parameters, response bodies, and status codes that the URLs are likely to return.  |
| Try It Out     | <p>Interact with the endpoint directly by clicking <b>Try It Out</b>. This button is provided in each of the expanded views for endpoints.</p> <p>When you click the button, fields appear for entering parameters (if applicable). You can then enter values and click <b>Execute</b>.</p> <p>The interactive documentation uses JavaScript to make the request directly to the API; it is not a test request.</p>  |

### Log in to Unified Manager

After you install the Web Services Proxy, you can access Unified Manager to manage multiple storage systems in a web-based interface.

To access Unified Manager, you open a browser and enter the URL pointing to where the proxy is installed. The following browsers and versions are supported.



| Browser                     | Minimum version |
|-----------------------------|-----------------|
| Google Chrome               | 79              |
| Microsoft Internet Explorer | 11              |
| Microsoft Edge              | 79              |
| Mozilla Firefox             | 70              |
| Safari                      | 12              |

## Steps

1. Open a browser and enter the following URL:

```
http[s]://<server>:<port>/um
```

In this URL, `<server>` represents the IP address or FQDN of the server where the Web Services Proxy is installed, and `<port>` represents the listening port number (defaults to 8080 for HTTP or 8443 for HTTPS).

The Unified Manager login page opens.

2. For first-time login, enter `admin` for the user name, and then set and confirm a password for the admin user.

The password can include up to 30 characters. For further information about users and passwords, see the Access Management section of the Unified Manager online help.

## Configure Web Services Proxy

You can modify the Web Services Proxy settings to meet the unique operating and performance requirements for your environment.

### Stop or restart the Webserver

The Webserver service is started during installation and runs in the background. During some configuration tasks, you might need to stop or restart the Webserver service.

## Steps

1. Do one of the following:
  - For Windows, go to the **Start** menu, select **Administrative Tools > Services**, locate **NetApp SANtricity Web Services** and then select either **Stop** or **Restart**.
  - For Linux, choose the method of stopping and restarting the Webserver for your operating system version. During the installation, a popup dialog indicated what daemon started. For example:

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

The most common method for interacting with the service is by using `systemctl` commands.

## Resolve port conflicts

If the Web Services Proxy is running while another application is available at the defined address or port, you can resolve the port conflict in the wsconfig.xml file.

### Steps

1. Open the wsconfig.xml file, located at:
  - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
  - (Linux) — /opt/netapp/santricity\_web\_services\_proxy
2. Add the following line to the wsconfig.xml file, in which *n* is the port number:

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

The following table shows the attributes that control HTTP ports and HTTPS ports.

| Name    | Description  | Parent Node | Attributes   | Required |
|---------|--|-------------|--|----------|
| config  | The root node for the config                               | Null        | Version - The version of the config schema is currently 1.0. | Yes      |
| sslport | The TCP port to listen for SSL requests. Defaults to 8443. | config      | Clientauth   | No       |
| port    | The TCP port to listen for HTTP request, defaults to 8080. | config      | -  | No       |

3. Save and close the file.
4. Restart the Webserver service so the change takes effect.

## Configure load-balancing and/or high-availability

To use the Web Services Proxy in a highly-available (HA) configuration, you can configure load balancing. In an HA configuration, typically either a single node receives all requests while the others are on stand-by, or requests are load-balanced across all nodes.

The Web Services Proxy can exist in a highly-available (HA) environment, with most APIs operating correctly regardless of the recipient of the request. Metadata tags and folders are two exceptions, because tags and folders are stored in a local database and are not shared between Web Services Proxy instances.

However, there are some known timing issues that occur in a small percentage of requests. Specifically, one instance of the proxy can have newer data faster than a second instance for a small window. The Web Services Proxy includes a special configuration that removes this timing issue. This option is not enabled by

default, because it increases the amount of time it takes to service requests (for data consistency). To enable this option, you must add a property to an .INI file (for Windows) or an .SH file (for Linux).

### Steps

1. Do one of the following:
  - Windows: Open the appserver64.ini file, and then add the `Dload-balance.enabled=true` property.  
  
For example: `vmarg.7=-Dload-balance.enabled=true`
  - Linux: Open the webserver.sh file, and then add the `Dload-balance.enabled=true` property.  
  
For example: `DEBUG_START_OPTIONS="-Dload-balance.enabled=true"`
2. Save your changes.
3. Restart the Webserver service so the change takes effect.

### Disable SYMbol HTTPS

You can disable SYMbol commands (default setting) and send commands over a remote procedure call (RPC). This setting can be changed in the wsconfig.xml file.

By default, the Web Services Proxy sends SYMbol commands over HTTPS for all E2800 series and E5700 series storage systems running SANtricity OS versions 08.40 or later. SYMbol commands sent over HTTPS are authenticated to the storage system. If needed, you can disable HTTPS SYMbol support and send commands over RPC. Whenever SYMbol over RPC is configured, all passive commands to the storage system are enabled without authentication.



When SYMbol over RPC is used, the Web Services Proxy cannot connect to systems with the SYMbol management port disabled.

### Steps

1. Open the wsconfig.xml file, located at:
  - (Windows) — `C:\Program Files\NetApp\SANtricity Web Services Proxy`
  - (Linux) — `/opt/netapp/santricity_web_services_proxy`
2. In the `devicemgt.symbolclientstrategy` entry, replace the `httpsPreferred` value with `rpcOnly`.

For example:

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

3. Save the file.

### Configure cross-origin resource sharing

You can configure cross-origin resource sharing (CORS), which is a mechanism that uses additional HTTP headers to provide a web application running at one origin to have permission to access selected resources from a server at a different origin.

CORS is handled by the cors.cfg file located in the working directory. The CORS configuration is open by default, so cross domain access is not restricted.

If no configuration file is present, CORS is open. But if the cors.cfg file is present, then it is used. If the cors.cfg file is empty, you cannot make a CORS request.

### Steps

1. Open the cors.cfg file, which is located in the working directory.
2. Add the desired lines to the file.

Each line in the CORS configuration file is a regular expression pattern to match. The origin header must match a line in the cors.cfg file. If any line pattern matches the origin header, the request is allowed. The complete origin is compared, not just the host element.

3. Save the file.

Requests are matched on the host and according to protocol, such as the following:

- Match localhost with any protocol — `*localhost*`
- Match localhost for HTTPS only — `https://localhost*`

### Uninstall Web Services Proxy

To remove the Web Services Proxy and Unified Manager, you can use any mode (Graphical, Console, Silent, or RPM file), regardless of what method you used to install the proxy.

#### Graphical mode uninstall

You can run the uninstall in Graphical mode for either Windows or Linux. In Graphical mode, the prompts appear in a Windows-style interface.

### Steps

1. Launch the uninstall for either Windows or Linux, as follows:
  - Windows — Go to the directory that contains the `uninstall_web_services_proxy` uninstall file. The default directory is at the following location: `C:/Program Files/NetApp/SANtricity Web Services Proxy/`. Double-click `uninstall_web_services_proxy.exe`.



Alternatively, you can go to **Control Panel > Programs > Uninstall a program**, and then select "NetApp SANtricity Web Services Proxy."

- Linux — Go to the directory that contains the Web Services Proxy uninstall file. The default directory is at the following location:  
`/opt/netapp/santricity_web_services_proxy/uninstall_web_services_proxy`

2. Run the following command:

```
uninstall_web_services_proxy -i gui
```

The SANtricity Web Services Proxy splash screen appears.

3. From the Uninstall dialog box, click **Uninstall**.

The Uninstaller progress bar appears and shows the progress.

4. When the Uninstall Complete message appears, click **Done**.

### Console mode uninstall

You can run the uninstall in Console mode for either Windows or Linux. In Console mode, the prompts appear in the terminal window.

#### Steps

1. Go to the `uninstall_web_services_proxy` directory.
2. Run the following command:

```
uninstall_web_services_proxy -i console
```

The uninstall process starts.

3. When the uninstall is complete, press **Enter** to exit the installer.

### Silent mode uninstall

You can run the uninstall in Silent mode for either Windows or Linux. In Silent mode, no return messages or scripts appear in the terminal window.

#### Steps

1. Go to the `uninstall_web_services_proxy` directory.
2. Run the following command:

```
uninstall_web_services_proxy -i silent
```

The uninstall process runs, but no return messages or scripts appear in the terminal window. After Web Services Proxy is successfully uninstalled, a command prompt appears in the terminal window.

### RPM command uninstall (Linux only)

You can use an RPM command to uninstall the Web Services Proxy from a Linux system.

#### Steps

1. Open a terminal window.
2. Enter the following command line:

```
rpm -e santricity_webservices
```



The uninstall process might leave files that were not part of the original installation. Manually delete these files to remove Web Services Proxy completely.

## Manage user access in Web Services Proxy

You can manage user access to the Web Services API and Unified Manager for security purposes.

## Overview of access management

Access management includes role-based logins, password encryption, basic authentication, and LDAP integration.

### Role-based access

Role-based access control (RBAC) associates predefined users with roles. Each role grants permissions to a specific level of functionality.

The following table describes each role.

| Role            | Description  |
|-----------------|--|
| security.admin  | SSL and certificate management.  |
| storage.admin   | Full read/write access to storage system configuration.  |
| storage.monitor | Read-only access to view storage system data.  |
| support.admin   | Access to all hardware resources on storage systems and support operations such as AutoSupport (ASUP) retrieval. |

Default user accounts are defined in the `users.properties` file. You can change user accounts by directly modifying the `users.properties` file or by using the Access Management functions in Unified Manager.

The following table lists the user logins available for the Web Services Proxy.

| Predefined user login | Description  |
|-----------------------|--|
| admin                 | A super administrator who has access to all functions and includes all roles. For Unified Manager, you must set the password on first-time login.  |
| storage               | The administrator responsible for all storage provisioning. This user includes the following roles: <code>storage.admin</code> , <code>support.admin</code> , and <code>storage.monitor</code> . This account is disabled until a password is set. |
| security              | The user responsible for security configuration. This user includes the following roles: <code>security.admin</code> and <code>storage.monitor</code> . This account is disabled until a password is set.  |
| support               | The user responsible for hardware resources, failure data, and firmware upgrades. This user includes the following roles: <code>support.admin</code> and <code>storage.monitor</code> . This account is disabled until a password is set.          |

| Predefined user login | Description   |
|-----------------------|---|
| monitor               | A user with read-only access to the system. This user includes only the storage.monitor role. This account is disabled until a password is set.             |
| rw                    | The rw (read/write) user includes the following roles: storage.admin, support.admin, and storage.monitor. This account is disabled until a password is set. |
| ro                    | The ro (read only) user includes only the storage.monitor role. This account is disabled until a password is set.   |

### Password encryption

For each password, you can apply an additional encryption process using the existing SHA256 password encoding. This additional encryption process applies a random set of bytes to each password (salt) for each SHA256 hash encryption. Salted SHA256 encryption is applied to all newly created passwords.



Prior to the Web Services Proxy 3.0 release, passwords were encrypted through SHA256 hashing only. Any existing SHA256 hash-only encrypted passwords retain this encoding and are still valid under the users.properties file. However, SHA256 hash-only encrypted passwords are not as secure as those passwords with salted SHA256 encryption.

### Basic authentication

By default, basic authentication is enabled, which means the server returns a basic authentication challenge. This setting can be changed in the wsconfig.xml file.

### LDAP

Lightweight Directory Access Protocol (LDAP), an application protocol for accessing and maintaining distributed directory information services, is enabled for the Web Services Proxy. LDAP integration allows for user authentication and mapping of roles to groups.

For information on configuring LDAP functionality, refer to configuration options in the Unified Manager interface or in the LDAP section of the interactive API documentation.

### Configure user access

You can manage user access by applying additional encryption to passwords, setting basic authentication, and defining role-based access.

#### Apply additional encryption to passwords

For the highest level of security, you can apply additional encryption to passwords using the existing SHA256 password encoding.

This additional encryption process applies a random set of bytes to each password (salt) for each SHA256 hash encryption. Salted SHA256 encryption is applied to all newly created passwords.

### Steps

1. Open the `users.properties` file, located at:
  - (Windows) — `C:\Program Files\NetApp\SANtricity Web Services Proxy\data/config`
  - (Linux) — `/opt/netapp/santricity_web_services_proxy/data/config`
2. Re-enter the encrypted password as plain text.
3. Run the `securepasswd` command line utility to re-encrypt the password or simply restart the Web Services Proxy. This utility is installed in the root install directory for the Web Services Proxy.



Alternatively, you can salt and hash local user passwords whenever password edits are performed through the Unified Manager.

### Configure basic authentication

By default basic authentication is enabled, which means the server returns a basic authentication challenge. If desired, you can change that setting in the `wsconfig.xml` file.

1. Open the `wsconfig.xml` file, located at:
  - (Windows) — `C:\Program Files\NetApp\SANtricity Web Services Proxy`
  - (Linux) — `/opt/netapp/santricity_web_services_proxy`
2. Modify the following line in the file by specifying `false` (not enabled) or `true` (enabled).

For example: `<env key="enable-basic-auth">true</env>`

3. Save the file.
4. Restart the Webserver service so the change takes effect.

### Configure role-based access

To limit user access to specific functions, you can modify which roles are specified for each user account.

The Web Services Proxy includes role-based access control (RBAC), in which roles are associated with predefined users. Each role grants permissions to a specific level of functionality. You can change the roles assigned to user accounts by directly modifying the `users.properties` file.



You can also change user accounts by using Access Management in Unified Manager. For more information, see the online help available with Unified Manager.

### Steps

1. Open the `users.properties` file, located in:
  - (Windows) — `C:\Program Files\NetApp\SANtricity Web Services Proxy\data/config`
  - (Linux) — `/opt/netapp/santricity_web_services_proxy/data/config`
2. Locate the line for the user account you want to modify (storage, security, monitor, support, rw, or ro).



Do not modify the admin user. This is a super user with access to all functions.

3. Add or remove the specified roles, as desired.

Roles include:



- security.admin — SSL and certificate management.
- storage.admin — Full read/write access to storage system configuration.
- storage.monitor — Read-only access to view storage system data.
- support.admin — Access to all hardware resources on storage systems and support operations such as AutoSupport (ASUP) retrieval.



The storage.monitor role is required for all users, including the administrator.

4. Save the file.

## Manage security and certificates in Web Services Proxy

For security in the Web Services Proxy, you can specify an SSL port designation and you can manage certificates. Certificates identify website owners for secure connections between clients and servers.

### Enable SSL

The Web Services Proxy uses Secure Sockets Layer (SSL) for security, which is enabled during installation. You can change the SSL port designation in the wsconfig.xml file.

#### Steps

1. Open the wsconfig.xml file, located at:
  - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
  - (Linux) — /opt/netapp/santricity\_web\_services\_proxy
2. Add or change the SSL port number, similar to the following example:

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

#### Result

When the server is started with SSL configured, the server looks for the keystore and truststore files.

- If the server does not find a keystore, the server uses the IP address of the first detected non-loopback IPv4 address to generate a keystore and then add a self-signed certificate to the keystore.
- If the server does not find a truststore, or the truststore is not specified, the server uses the keystore as the truststore.

### Bypass certificate validation

To support secure connections, the Web Services Proxy validates the storage systems' certificates against its own trusted certificates. If needed, you can specify that the proxy bypass that validation before connecting to the storage systems.

#### Before you begin

- All storage system connections must be secure.

#### Steps

1. Open the wsconfig.xml file, located at:
  - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
  - (Linux) — /opt/netapp/santricity\_web\_services\_proxy
2. Enter true in the trust.all.arrays entry, as shown in the example:

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

3. Save the file.

## Generate and import a host management certificate

Certificates identify website owners for secure connections between clients and servers. To generate and import Certificate Authority (CA) certificates for the host system where the Web Services Proxy is installed, you can use API endpoints.

To manage certificates for the host system, you perform the following tasks using the API:

- Create a certificate signing request (CSR) for the host system.
- Send the CSR file to a CA, and then wait for them to send you the certificate files.
- Import the signed certificates to the host system.



You can also manage certificates in the Unified Manager interface. For more information, see the online help available in Unified Manager.

### Steps

1. Log in to the [interactive API documentation](#).
2. Go to the drop-down menu in the upper right and then select **v2**.
3. Expand the **Administration** link and scroll down to the **/certificates** endpoints.
4. Generate the CSR file:
  - a. Select **POST:/certificates**, and then select **Try it out**.

The web server regenerates a self-signed certificate. You can then enter information in the fields to define the common name, organization, organization unit, alternate ID, and other information used to generate the CSR.

- b. Add the required information in the **Example values** pane to generate a valid CA certificate, and then execute the commands.



Do not call **POST:/certificates** or **POST:/certificates/reset** again, or you must regenerate the CSR. When you call **POST:/certificates** or **POST:/certificates/reset**, you are generating a new self-signed certificate with a new private key. If you send a CSR that was generated before the last reset of the private key on the server, the new security certificate does not work. You must generate a new CSR and request a new CA certificate.

- c. Execute the **GET:/certificates/server** endpoint to confirm that the current certificate status is the self-signed certificate with the information added from the **POST:/certificates** command.

The server certificate (denoted by the alias `jetty`) is still self-signed at this point.

- d. Expand the **POST:/certificates/export** endpoint, select **Try it out**, enter a file name for the CSR file, and then click **Execute**.
5. Copy and paste the `fileUrl` into a new browser tab to download the CSR file, and then send the CSR file to a valid CA to request a new web server certificate chain.
6. When the CA issues a new certificate chain, use a certificate manager tool to break out the root, intermediate, and web server certificates, and then import them to the Web Services Proxy server:
  - a. Expand the **POST:/sslconfig/server** endpoint and select **Try it out**.
  - b. Enter a name for the CA root certificate in the **alias** field.
  - c. Select **false** in the **replaceMainServerCertificate** field.
  - d. Browse to and select the new CA root certificate.
  - e. Click **Execute**.
  - f. Confirm that the certificate upload was successful.
  - g. Repeat the CA certificate upload procedure for the CA intermediate certificate.
  - h. Repeat the certificate upload procedure for the new web server security certificate file, except in this step, select **true** on the **replaceMainServerCertificate** drop-down.
  - i. Confirm that the web server security certificate import was successful.
  - j. To confirm that the new root, intermediate, and web server certificates are available in the keystore, run **GET:/certificates/server**.
7. Select and expand the **POST:/certificates/reload** endpoint, and then select **Try it out**. When prompted, whether you want to restart both controllers or not, select **false**. ("True" applies only in the case of dual array controllers.) Click **Execute**.

The **/certificates/reload** endpoint usually returns a successful http 202 response. However, the reload of the web server truststore and keystore certificates does create a race condition between the API process and the web server certificate reload process. In rare cases, the web server certificate reload can beat the API processing. In this case, the reload appears to fail even though it completed successfully. If this occurs, continue to the next step anyway. If the reload actually failed, the next step also fails.

8. Close the current browser session to the Web Services Proxy, open a new browser session, and confirm that a new secure browser connection to the Web Services Proxy can be established.

By using an incognito or in-private browsing session, you can open a connection to the server without using any saved data from previous browsing sessions.

## Manage storage systems using Web Services Proxy

To manage storage systems in the network, you must first discover them and then add them to the management list.

### Discover storage systems

You can set automatic discovery or manually discover storage systems.

## Automatically discover storage systems

You can specify that storage systems are automatically discovered in the network by modifying the settings in the `wsconfig.xml` file. By default, IPv6 automatic discovery is disabled and IPv4 is enabled.

You only need to provide one management IP or DNS address to add a storage system. The server automatically discovers all management paths when the paths are either not configured or the paths are configured and rotatable.



If you attempt to use an IPv6 protocol to automatically discover storage systems from the controller configuration after an initial connection has been made, the process might fail. Possible causes for the failure include problems during IP address forwarding or IPv6 being enabled on the storage systems, but not being enabled on the server.

### Before you begin

Before enabling IPv6 discovery settings, verify that your infrastructure supports IPv6 connectivity to the storage systems to mitigate any connection issues.

### Steps

1. Open the `wsconfig.xml` file, located at:
  - (Windows) — `C:\Program Files\NetApp\SANtricity Web Services Proxy`
  - (Linux) — `/opt/netapp/santricity_web_services_proxy`
2. In the autodiscover strings, change settings from `true` to `false`, as desired. See the following example.

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



When the paths are configured, but not configured so that the server can route to the addresses, intermittent connection errors happen. If you cannot set the IP addresses to be routable from the host, turn off auto discovery (change the settings to `false`).

3. Save the file.

## Discover and add storage systems using API endpoints

You can use API endpoints to discover and add storage systems to the managed list. This procedure creates a management connection between the storage system and the API.



This task describes how to discover and add storage systems using the REST API, so you can manage these systems in the interactive API documentation. However, you might want to manage storage systems in the Unified Manager instead, which provides an easy-to-use interface. For more information, see the online help available with Unified Manager.

### Before you begin

For storage systems with SANtricity versions 11.30 and later, the legacy management interface for SYMBol must be enabled in the SANtricity System Manager interface. Otherwise, the Discovery endpoints fail. You can find this setting by opening System Manager, and then going to **Settings > System > Additional Settings > Change Management Interface**.

### Steps

1. Log in to the [interactive API documentation](#).
2. Discover storage systems, as follows:
  - a. From the API documentation, make sure **V2** is selected in the drop-down, and then expand the **Storage-Systems** category.
  - b. Click the **POST: /discovery** endpoint, and then click **Try it out**.
  - c. Enter the parameters as described in the table.

|                   |  |
|-------------------|--|
| startIP<br>endIP  | Replace string with the starting and ending IP address range for one or more storage systems in the network.   |
| useAgents         | Set this value to either: <ul style="list-style-type: none"> <li>• true = Use in-band agents for the network scan.</li> <li>• false = Do not use in-band agents for the network scan.</li> </ul> |
| connectionTimeout | Enter the seconds allowed for the scan before the connection times out.  |
| maxPortsToUse     | Enter a maximum number of ports used for the network scan.   |

- d. Click **Execute**.



API actions execute without user prompts.

The discovery process runs in the background.

- e. Make sure the code returns a 202.
  - f. Under **Response Body**, locate the value returned for the requestId. You need the Request ID to view the results in the next step.
3. View discovery results, as follows:
    - a. Click the **GET: /discovery** endpoint, and then click **Try it out**.
    - b. Enter the Request ID from the previous step. If you leave the **Request ID** blank, the endpoint defaults to the last request ID executed.
    - c. Click **Execute**.
    - d. Make sure the code returns 200.
    - e. In the response body, locate your Request ID and the strings for storageSystems. The strings look similar to the following example:

```

"storageSystems": [
  {
    "serialNumber": "123456789",
    "wwn": "000A011000AF00000000000001A0C000E",
    "label": "EF570_Array",
    "firmware": "08.41.10.01",
    "nvsram": "N5700-841834-001",
    "ipAddresses": [
      "10.xxx.xx.213",
      "10.xxx.xx.214"
    ],
  },

```

f. Write down the values for wwn, label, and ipAddresses. You need them for the next step.

4. Add storage systems, as follows:

- a. Click the **POST: /storage-system** endpoint, and then click **Try it out**.
- b. Enter the parameters as described in the table.

|                     |  |
|---------------------|--|
| id                  | Enter a unique name for this storage system. You can enter the label (displayed in the response for GET: /discovery), but the name can be any string you choose. If you do not provide a value for this field, Web Services automatically assigns a unique identifier. |
| controllerAddresses | Enter the IP addresses displayed in the response for GET: /discovery. For dual controllers, separate the IP addresses with a comma. For example:<br><br>"IP address 1", "IP address 2"   |
| validate            | Enter <code>true</code> , so you can receive confirmation that Web Services can connect to the storage system.   |
| password            | Enter the administrative password for the storage system.  |
| wwn                 | Enter the WWN of the storage system (displayed in the response for GET: /discovery).   |

- c. Remove all strings after "enableTrace": `true`, so that the entire string set is similar to the following example:

```
{
  "id": "EF570_Array",
  "controllerAddresses": [
    "Controller-A-Mgmt-IP", "Controller-B-Mgmt_IP"
  ],
  "validate": true,
  "password": "array-admin-password",
  "wwn": "000A011000AF00000000000001A0C000E",
  "enableTrace": true
}
```

d. Click **Execute**.

e. Make sure the code response is 201, which indicates that the endpoint executed successfully.

The **Post: /storage-systems** endpoint is queued. You can view the results using the **GET: /storage-systems** endpoint in the next step.

5. Confirm the list addition, as follows:

a. Click the **GET: /storage-system** endpoint.

No parameters are required.

b. Click **Execute**.

c. Make sure that the code response is 200, which indicates that the endpoint executed successfully.

d. In the response body, look for the storage system details. The returned values indicate that it was successfully added to the list of managed arrays, similar to the following example:

```
[
  {
    "id": "EF570_Array",
    "name": "EF570_Array",
    "wwn": "000A011000AF00000000000001A0C000E",
    "passwordStatus": "valid",
    "passwordSet": true,
    "status": "optimal",
    "ip1": "10.xxx.xx.213",
    "ip2": "10.xxx.xx.214",
    "managementPaths": [
      "10.xxx.xx.213",
      "10.xxx.xx.214"
    ]
  }
]
```

## Scale up the number of managed storage systems

By default, the API can manage up to 100 storage systems. If you need to manage more, you must bump the memory requirements for the server.

The server is set to use 512 MB of memory. For every 100 extra storage systems in your network, add 250 MB to that number. Do not add more memory than what you physically have. Allow enough extra for your operating system and other applications.



The default cache size is 8,192 events. The approximate data usage for the MEL events cache is 1MB for each 8,192 events. Therefore, by retaining the defaults, cache usage should be approximately 1MB for a storage system.



In addition to memory, the proxy uses network ports for each storage system. Linux and Windows consider network ports as file handles. As a security measure, most operating systems limit the number of open file handles that a process or a user can have open at one time. Especially in Linux environments, where open TCP connections are considered to be file handles, the Web Services Proxy can easily exceed this limit. Because the fix is system dependent, you should refer to your operating system's documentation for how to raise this value.

### Steps

1. Do one of the following:
  - On Windows, go to the `appserver64.init` file. Locate the line, `vmarg.3=-Xmx512M`
  - On Linux, go to the `webserver.sh` file. Locate the line, `JAVA_OPTIONS="-Xmx512M"`
2. To increase the memory, replace 512 with the desired memory in MB.
3. Save the file.

## Manage automatic polling for Web Services Proxy statistics

You can configure automatic polling for all disk and volume statistics on discovered storage systems.

### Overview of statistics

Statistics provide information about the data collection rates and performance of the storage systems.

The Web Services Proxy provides access to the following types of statistics:

- Raw statistics — Total counters for data points at the time of data collection. Raw statistics can be used for total read operations or total write operations.
- Analyzed statistics — Calculated information for an interval. Examples of analyzed statistics are read input/output operations (IOPs) per second or write throughput.

Raw statistics are linear, typically requiring at least two collected data points to derive usable data from them. The analyzed statistics are a derivation of the raw statistics, which provide important metrics. Many values that can be derived from the raw statistics are shown in a usable, point-in-time format in the analyzed statistics for your convenience.

You can retrieve raw statistics regardless of whether the automatic polling is enabled or not. You can add the



`usecache=true` query string to the end of the URL to retrieve cached statistics from the last poll. Using cached results greatly increases the performance of statistics retrieval. However, multiple calls at a rate equal to or less than the configured polling interval cache retrieves the same data.

## Statistics functionality

The Web Services Proxy provides API endpoints that enable the retrieval of raw and analyzed controller and interface statistics from supported hardware models and software versions.

### Raw Statistics APIs

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

### Analyzed Statistics APIs

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

These URLs retrieve analyzed statistics from the last poll and are only available when polling is enabled. These URLs include the following input-output data:

- Operations per second
- Throughput in megabytes per second
- Response times in milliseconds

The calculations are based on the differences between statistical polling iterations, which are the most common measures of storage performance. These statistics are preferable to unanalyzed statistics.



When the system starts, there is no previous statistics collection to use to calculate the various metrics, so analyzed statistics require at least one polling cycle after startup to return data. In addition, if the cumulative counters are reset, the next polling cycle will have unpredictable numbers for the data.

## Configure polling intervals

To configure polling intervals, you modify the `wsconfig.xml` file to specify a polling interval in seconds.



Because the statistics are cached in memory, you might see an increase of about 1.5 MB of memory-use for each storage system.

## Before you begin

- The storage systems must be discovered by the proxy.

## Steps

1. Open the wsconfig.xml file, located at:
  - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
  - (Linux) — /opt/netapp/santricity\_web\_services\_proxy
2. Add the following line inside the `<env-entries>` tag, in which `n` is the number of seconds for the interval between polling requests:

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

For example, if 60 is entered, polling starts at 60-second intervals. That is, the system requests polling to start 60 seconds after the prior polling period was completed (regardless of the duration of the prior polling period). All statistics are time-stamped with the exact time they were retrieved. The system uses the time stamp or time difference on which to base the 60-second calculation.

3. Save the file.

## Manage AutoSupport using Web Services Proxy

You can configure AutoSupport (ASUP), which collects data and then automatically sends that data to technical support for remote troubleshooting and problem analysis.

### Overview of AutoSupport (ASUP)

The AutoSupport (ASUP) feature automatically transmits messages to NetApp based on manual and schedule-based criteria.

Each AutoSupport message is a collection of log files, configuration data, state data, and performance metrics. By default, AutoSupport transmits the files listed in the following table to the NetApp Support team once each week.

| File Name            | Description   |
|----------------------|---|
| x-headers-data.txt   | A .txt file containing the X-header information.              |
| manifest.xml         | An .xml file detailing the contents of the message.           |
| arraydata.xml        | An .xml file containing the list of client persisted data.    |
| appserver-config.txt | A .txt file containing application server configuration data. |
| wsconfig.txt         | A .txt file containing the web service configuration data.    |

| File Name                | Description  |
|--------------------------|--|
| host-info.txt            | A .txt file containing information about the host environment.   |
| server-logs.7z           | A .7z file containing every available webserver log file.  |
| client-info.txt          | A .txt file with arbitrary key/value pairs for application-specific counters such as method and webpage hits.  |
| webservices-profile.json | <p>These files contain Webservices profile data and Jersey monitoring statistical data. By default, Jersey monitoring statistics are enabled. You can enable and disable them in the wsconfig.xml file, as follows:</p> <ul style="list-style-type: none"> <li>• <b>Enable:</b> <code>&lt;env key="enable.jersey.statistics"&gt;true&lt;/env&gt;</code></li> <li>• <b>Disable:</b> <code>&lt;env key="enable.jersey.statistics"&gt;false&lt;/env&gt;</code></li> </ul> |

## Configure AutoSupport

AutoSupport is enabled by default at installation; however, you can change that setting or modify the delivery types.

### Enable or disable AutoSupport

The AutoSupport feature is enabled or disabled during the initial installation of the Web Services Proxy, but you can change that setting in the ASUPConfig file.

You can enable or disable AutoSupport through the ASUPConfig.xml file, as described in the steps below. Alternatively, you can enable or disable this feature through the API using **Configuration** and **POST/asup**, and then entering "true" or "false."

1. Open the ASUPConfig.xml file in the working directory.
2. Locate the lines for `<asupdata enabled="(Boolean)" timestamp=>`
3. Enter `true` (enable) or `false` (disable). For example:

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



The timestamp entry is superfluous.

4. Save the file.

## Configure AutoSupport delivery method

You can configure the AutoSupport feature to use HTTPS, HTTP, or SMTP delivery methods. HTTPS is the default delivery method.

1. Access the ASUPConfig.xml file in the working directory.
2. In the string, `<delivery type="n">`, enter 1, 2, or 3 as described in the table:

| Value | Description   |
|-------|---|
| 1     | <b>HTTPS</b> (default)<br><br><code>&lt;delivery type="1"&gt;</code>  |
| 2     | <b>HTTP</b><br><br><code>&lt;delivery type="2"&gt;</code>   |
| 3     | <b>SMTP</b> — To properly configure the AutoSupport delivery type to SMTP, you must include the SMTP mail server address, along with the sender and recipient user emails, similar to the following example:<br><br><pre>&lt;delivery type="3"&gt; &lt;smtp&gt; &lt;mailserver&gt;smtp.example.com&lt;/mailserver&gt; &lt;sender&gt;user@example.com&lt;/sender&gt; &lt;replyto&gt;user@example.com&lt;/replyto&gt; &lt;/smtp&gt; &lt;/delivery&gt;</pre> |

## Remote volume mirroring

### Remote Storage Volumes overview

Use the SANtricity® Remote Storage Volumes feature to import data from a remote storage device directly to a local E-Series volume. This feature helps streamline the process for equipment upgrades and provides data migration capabilities to move data from non-E-Series devices to E-Series systems.

### Configuration overview

The Remote Storage Volumes feature is available with SANtricity System Manager on selected submodel IDs. To use this feature, you must configure a remote storage system and an E-Series storage system to

communicate with each other.

Use the following workflow:

1. [Review requirements and restrictions.](#)
2. [Configure hardware.](#)
3. [Import remote storage.](#)

### Find more information

- Online help, available in the System Manager user interface or in the [Documentation Center](#).
- For additional technical information on the Remote Storage Volumes feature, see the [Remote Storage Volumes Technical Report](#).

## Requirements and restrictions for remote storage

Before configuring the Remote Storage Volumes feature, review the following requirements and restrictions.

### Hardware requirements

#### Supported protocols

For the initial release of the Remote Storage Volumes feature, support is only available for iSCSI and IPv4 protocols.

Refer to the [NetApp Interoperability Matrix Tool](#) for up-to-date support and configuration information between the host and E-Series (destination) array used for the Remote Storage Volumes feature.

#### Storage system requirements

The E-Series storage system must include:

- Two controllers (duplex mode)
- iSCSI connections for both E-Series controllers to communicate with the remote storage system through one or more iSCSI connections
- SANtricity OS 11.71 or greater
- Remote Storage feature enabled in the Submodel ID (SMID)

The remote system can be either an E-Series storage system or a system from another vendor. It must include iSCSI-capable interfaces.

### Volume requirements

Volumes used for imports must meet the requirements for size, status, and other criteria.

#### Remote storage volume

The source volume of an import is called a "remote storage volume." This volume must meet the following criteria:

- Cannot be part of another import
- Must have an online status

After the import begins, the controller firmware creates a remote storage volume in the background. Due to that background process, the remote storage volume is not manageable in System Manager and can only be used for the import operation.

After it is created, the remote storage volume is treated like any other standard volume on the E-Series system with the following exceptions:

- Can be used as proxies to the remote storage device.
- Cannot be used as candidates for other volume copies or snapshots.
- Cannot have the Data Assurance setting changed while the import is in progress.
- Cannot be mapped to any hosts, because they are reserved strictly for the import operation.

Each remote storage volume is associated with only one remote storage object; however, one remote storage object can be associated with multiple remote storage volumes. The remote storage volume is uniquely identified using a combination of the following:

- Remote storage object identifier
- Remote storage device LUN number

#### **Target volume candidates**

The target volume is the destination volume on the local E-Series system.

The destination volume must meet the following criteria:

- Must be a RAID/DDP volume.
- Must have a capacity that is equal to or larger than the remote storage volume.
- Must have a block size that is the same as the remote storage volume.
- Must have a valid state (optimal).
- Cannot have any of the following relationships: volume copy, snapshot copies, asynchronous or synchronous mirroring.
- Cannot be undergoing any reconfiguration operations: Dynamic Volume Expansion, Dynamic Capacity Expansion, Dynamic Segment Size, Dynamic RAID Migration, Dynamic Capacity Reduction, or Defragmentation.
- Cannot be mapped to a host before the import starts (however, it can be mapped after import completes).
- Cannot have Flash Read Cached (FRC) enabled.

System Manager automatically checks these requirements as part of the Import Remote Storage wizard. Only volumes that meet all the requirements are displayed for destination volume selection.

#### **Restrictions**

The Remote Storage feature has the following restrictions:

- Mirroring must be disabled.
- Destination volume on the E-Series system must not have snapshots.

- Destination volume on the E-Series system must not be mapped to any hosts before the import is started.
- Destination volume on the E-Series system must have resource-provisioning disabled.
- Direct mappings of the remote storage volume to a host or multiple hosts are not supported.
- Web Services Proxy is not supported.
- iSCSI CHAP secrets are not supported.
- SMcli is not supported.
- VMware Datastore is not supported.
- Only one storage system in the relationship/import pair can be upgraded at a time when there is an import pair present.

## Preparation for production imports

You should perform a test or "dry run" import before production imports to verify proper storage and fabric configuration.

Many variables can impact the import operation and completion time. To ensure a production import is successful and to get a duration estimate, you can use these test imports to ensure all connections are working as expected and the import operation is completing in an appropriate amount of time. You can then make adjustments to achieve the desired results before the production import is initiated.

## Configure hardware for Remote Storage Volumes

The E-Series storage system must be configured to communicate with the remote storage system through the supported iSCSI protocol.

### Configure remote storage device and E-Series array

Before proceeding to the SANtricity System Manager to configure the Remote Storage Volumes feature, do the following:

1. Manually establish a cabled connection between the E-Series system and the remote storage system such that the two systems can be configured to communicate via iSCSI.
2. Configure the iSCSI ports such that the E-Series system and the remote storage system can communicate successfully with each other.
3. Obtain the IQN of the E-Series system.
4. Make the E-Series system visible to the remote storage system. If the remote storage system is an E-Series system, then create a host using the IQN of the destination E-Series system as the connection information for the host port.
5. If the remote storage device is in use by a host/application:
  - Stop I/O to the remote storage device.
  - Unmap/unmount the remote storage device.
6. Map the remote storage device to the host defined for the E-Series storage system.
7. Obtain the LUN number of the device used for the mapping.



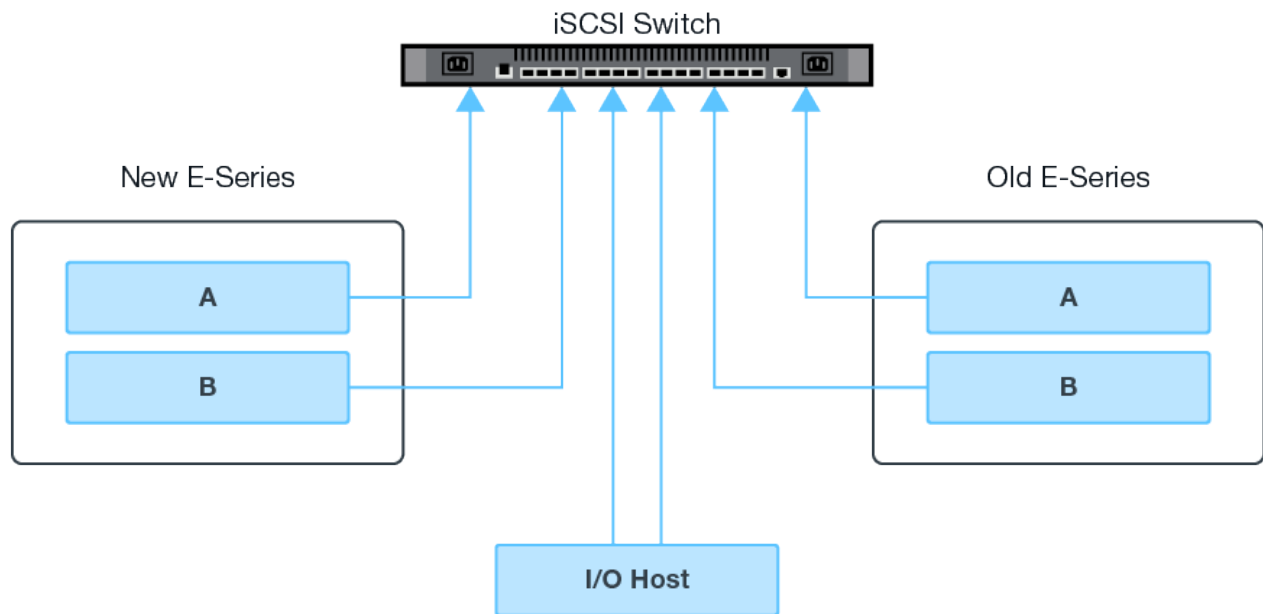
Recommended: Back up the remote source volume before starting the import process.

## Cable the storage arrays

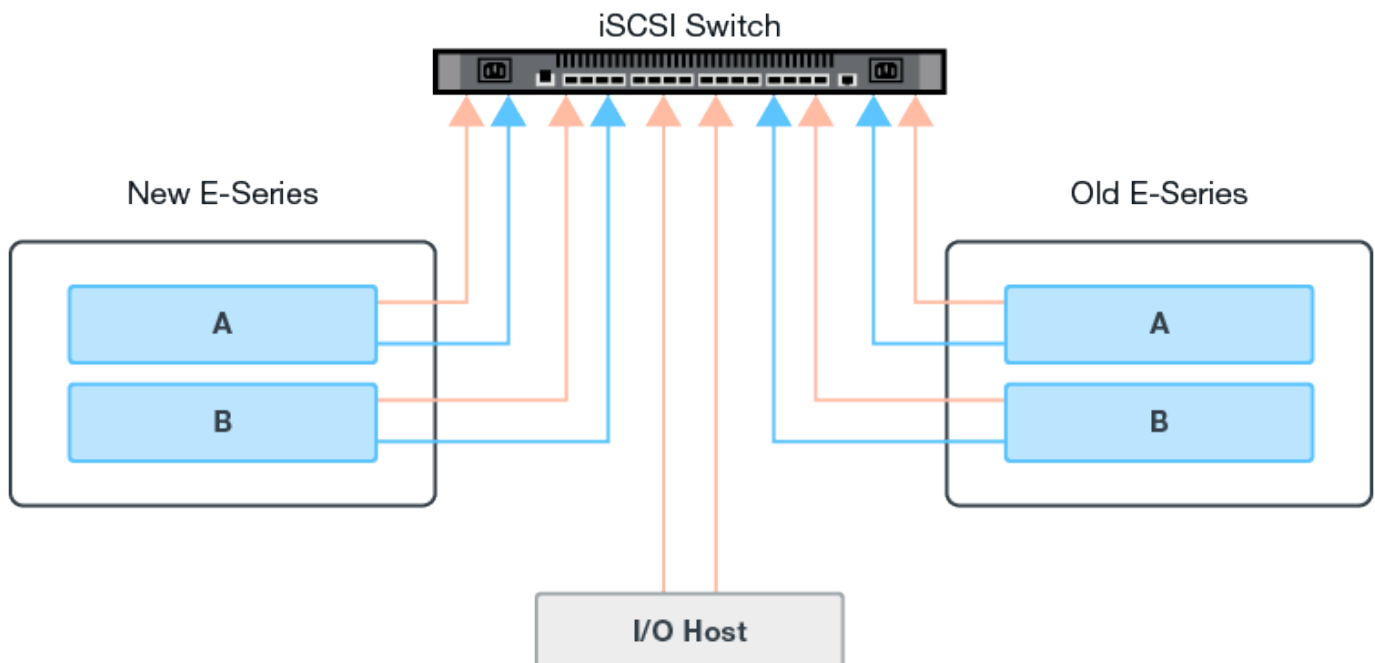
As part of the setup process, the storage arrays and I/O host must be cabled to the iSCSI-compatible interface.

The following diagrams provide examples of how to cable the systems such that they perform Remote Storage Volume operations over an iSCSI connection.

### Fabric Connection - Use Case 1



### Fabric Connection - Use Case 2





## Configure the iSCSI ports

You must configure the iSCSI ports to ensure communication between the target (local E-Series storage array) and source (remote storage array).

The iSCSI ports can be configured multiple ways based on your subnet. The following are a few examples on how to configure the iSCSI ports for use with the Remote Storage Volumes feature.

| Source A       | Source B       | Target A       | Target B       |
|----------------|----------------|----------------|----------------|
| 10.10.1.100/22 | 10.10.2.100/22 | 10.10.1.101/22 | 10.10.2.101/22 |

| Source A       | Source B       | Target A       | Target B       |
|----------------|----------------|----------------|----------------|
| 10.10.0.100/16 | 10.10.0.100/16 | 10.10.0.101/16 | 10.10.0.101/16 |

## Import remote storage

To initiate a storage import from a remote system to a local E-Series storage system, use the Import Remote Storage wizard in the SANtricity System Manager user interface.

### What you'll need

- The E-Series storage system must be configured to communicate with the remote storage system. See [Configure hardware](#).
- For the remote storage system, gather the following information:
  - iSCSI IQN
  - iSCSI IP addresses
  - LUN number of the remote storage device (source volume)
- For the local E-Series storage system, create or select a volume to be used for the data import. The target volume must meet the following requirements:
  - Matches the block size of the remote storage device (the source volume).
  - Has a capacity that is equal to or larger than the remote storage device.
  - Has a state of Optimal and is available. For a full list of requirements, see [Requirements and restrictions](#).
- Recommended: Back up volumes on the remote storage system before starting the import process.

### About this task

In this task, you create a mapping between the remote storage device and a volume on the local E-Series storage system. When you finish the configuration, the import begins.



Because many variables can impact the import operation and its completion time, you should first perform smaller “test” imports. Use these tests to ensure that all connections work as expected and that the import operation completes in an appropriate amount of time.

### Steps

1. From the SANtricity System Manager, click **Storage > Remote Storage**.

2. Click **Import Remote Storage**.

A wizard for importing remote storage is displayed.

3. In Step 1a of the Configure Source panel, enter connection information.

- a. Under the **Name** field, enter the name for the remote storage device.
- b. Under the **iSCSI connection properties**, enter the following for the remote storage device: IQN, IP address, and the port number (default is 3260).

If you want to add another iSCSI connection, click **+Add another IP address** to include an additional IP address for the remote storage. When you are done, click **Next**.

After you click Next, Step 1b of the Configure Source panel is displayed.

4. Under the **LUN** field, select the desired source LUN for the remote storage device, and then click **Next**.

The Configure Target panel opens and displays volume candidates to serve as the target for the import. Some volumes do not display in the list of candidates due to block size, capacity, or volume availability.

5. From the table, select a target volume on the E-Series storage system. If needed, use the slider to change the import priority. Click **Next**. Confirm the operation in the next dialog box by typing `continue`, and then clicking **Continue**.

If the target volume has a capacity that is larger than the source volume, that additional capacity is not reported to the host connected to the E-Series system. To use the new capacity, you must perform a file system expansion operation on the host after the import operation completes and is disconnected.

After you confirm the configuration in the dialog, the Review panel is displayed.

6. From the Review screen, verify the specified remote storage device, target, and import settings are accurate. Click **Finish** to complete the creation of the remote storage.

Another dialog box opens asking if you want to initiate another import.

7. If needed, click **Yes** to create another remote storage import. Clicking Yes returns to Step 1a of the Configure Source panel, where you can select the existing configuration or add a new one. If you do not want to create another import, click **No** to exit the dialog.

Once the import process begins, the entire target volume is overwritten with the copied data. If the host writes any new data to the target volume during this process, that new data is propagated back to the remote device (source volume).

8. View the progress of the operation in the View Operations dialog under the Remote Storage panel.

The time required to complete the import operation depends on the size of the remote storage system, the priority setting for the import, and the amount of I/O load on both storage systems and their associated volumes. Once the import is complete, the local volume is a duplicate of the remote storage device.

9. When you are ready to break the relationship between the two volumes, select **Disconnect** on the import object from the Operations in Progress view. Once the relationship is disconnected, performance of the local volume returns to normal and is no longer impacted by the remote connection.

## Manage import progress

After the import process begins, you can view and take action on its progress.

For each import operation, the Operations in Progress page displays a percentage of completion and estimated time remaining. Actions include changing the import priority, stopping and resuming operations, and disconnecting from the operation.



You can also view Operations in Progress from the Home page (**Home > Show operations in progress**).

### Steps

1. In SANtricity System Manager, go to the Remote Storage page and select **View Operations**.

The Operations in Progress dialog is displayed.

2. If desired, use the links in the Actions column to stop and resume, change priority, or disconnect from an operation.
  - **Change Priority** – Select **Change Priority** to change the processing priority of an operation that is in progress or pending. Apply a priority to the operation and then click **OK**.
  - **Stop** – Select **Stop** to pause the copying of data from the remote storage device. The relationship between the import pair is still intact, and you can select **Resume** when you are ready to continue the import operation.
  - **Resume** – Select **Resume** to begin a stopped or failed process from where it left off. Next, apply a priority to the Resume operation, and then click **OK**.

The Resume operation does **not** restart the import from the beginning. If you want to restart the process from the beginning, you must select **Disconnect**, and then re-create the import through the Import Remote Storage wizard.

- **Disconnect** – Select **Disconnect** to break the relationship between the source and destination volumes for an import operation that has stopped, completed, or failed.

## Modify remote storage connection settings

You can edit, add, or delete connection settings for any remote storage configuration through the View/Edit Settings option.

Making changes to connection properties will affect in-progress imports. To avoid disruptions, only make changes to connection properties when imports are not running.

### Steps

1. From the Remote Storage screen of the SANtricity System Manager, select the desired Remote Storage object under the result list section.
2. Click **View/Edit Settings**.

The Remote Storage Settings screen is displayed.

3. Click the **Connection Properties** tab.

The configured IP address and port settings for the remote storage import are displayed.

4. Perform one of the following actions:

- **Edit** – Click **Edit** next to the corresponding line item for the remote storage object. Enter the revised IP address and/or port information in the fields.
- **Add** – Click **Add**, and then enter the new IP address and port information in the fields provided. Click **Add** to confirm, and then the new connection appears in the list of remote storage objects.
- **Delete** – Select the desired connection from the list and then click **Delete**. Confirm the operation by typing `delete` in the provided field and then click **Delete**. The connection is removed from the list of remote storage objects.

5. Click **Save**.

The modified connection settings are applied to the remote storage object.

## Remove remote storage object

After an import completes, you can remove a remote storage object if you no longer want data copied between the local and remote devices.

### Steps

1. Make sure that no imports are associated with the remote storage object you plan to remove.
2. From the Remote Storage screen of the SANtricity System Manager, select the desired Remote Storage object under the result list section.
3. Click **Remove**.

The Confirm Remove Remote Storage Connection dialog is displayed.

4. Confirm the operation by typing `remove` and then clicking **Remove**.

The selected Remote Storage object is removed.

## Storage plugin for vCenter

### Overview of the Storage Plugin for vCenter

The SANtricity Storage Plugin for vCenter provides integrated management of E-Series storage arrays from within a VMware vSphere Client session.

The following functions are available in the Plugin for vCenter:

- View and manage discovered storage arrays in the network.
- Perform batch operations on groups of multiple storage arrays.
- Perform upgrades on the software OS.
- Import settings from one storage array to another.
- Configure volumes, SSD cache, hosts, host clusters, pools, and volume groups.
- Launch the System Manager interface for additional management tasks on an array.



The plugin is not a direct replacement for the SANtricity System Manager software. System Manager is still required for performing certain storage administration tasks on a single array.

The plugin requires a VMware vCenter Server Appliance deployed in the VMware environment and an application host to install and run the plugin webserver.

Refer to the following figure for more information on communications in the vCenter environment.

[vcenter communication] | [../media/vcenter\\_communication.png](#)

## Configuration overview

1. [Install and register the plugin.](#)
2. [Configure plugin access permissions.](#)
3. [Log in to the plugin interface.](#)
4. [Discover storage arrays.](#)
5. [Provision storage.](#)

## Find more information

- For online help, see the user interface of the Storage Plugin for vCenter.
- For more information about managing datastores in the vSphere Client, see [VMware vSphere Documentation](#).

## Install the Storage Plugin for vCenter

You can install the Storage Plugin for vCenter and verify the plugin registration.

### Review installation prerequisites

Be sure that your systems meet the following requirements:

- VMware vCenter Server Appliance supported versions: 6.7U3J, 7.0U1, or 7.0U2
- NetApp SANtricity OS version: 11.60.2 or higher
- Supported application host versions: Windows 2016 or Windows 2019
- CPU requirements for the host system:
  - System memory: 1.5GB
  - Storage space: 275 MB + 200 MB (logging)

### Install the plugin software

To install the plugin software:

1. Copy the installer file to the host that will be used as the application server, and then access the folder where you downloaded the installer.
2. Double-click the installation file:

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

In the above filename, `nn.nn.nn.nnnn` represents the version number.

3. When the installation starts, follow the on-screen prompts.

During the installation, you are prompted to enter some configuration parameters.

- a. On the first screen, select your preferred language for the software and click **OK**.
- b. In the Introduction screen, click **Next**.
- c. In the Copyright screen, click **Next**.
- d. In the License Agreement screen, select the box for accepting the terms and then click **Next**.
- e. Select the folder where you want to install the software and then click **Next**.
- f. In the Certificate Validation screen, keep the checkbox selected if you want to enforce certificate validation between the plugin and the storage arrays. With this enforcement, the storage array certificates are checked to be trusted against the plugin. If the certificates are not trusted, then they are not allowed to be added to the plugin. If you want to override certificate validation, deselect the checkbox so that all storage arrays can be added to the plugin using self-signed certificates. Click **Next**.

To learn more about certificates, refer to the online help available from the plugin interface.

- g. In the HTTPS Web Service Port screen, leave the default at 8445, or if necessary, change the port number. Click **Next**.
- h. In the Pre-Installation Summary screen, click **Next** to install the files.
- i. When the Webserver Started message appears, click **OK** to complete the installation.
- j. Click **Done**.



If necessary, you can change the Certificate Validation and Web Service Port settings after installation. From the installation directory, open the `wsconfig.xml` file. To remove the Certificate Validation on storage arrays, change the `env` key, `trust.all.arrays`, to `true`. To change the Web Services port, modify the `sslport` value to the desired port value ranging from 0-65535. Ensure that the port number used is not binding to another process. When you are done, save the changes and restart the plugin webserver. If the port value of the plugin webserver is changed after registering the plugin to a vCSA, then you must unregister and re-register the plugin so the vCSA is communicating on the changed port to the plugin webserver.

4. Verify that the application server was installed successfully by running the **services.msc** command.
5. Verify that the Application Server (vCP) service, **NetApp SANtricity Storage Plugin for vCenter**, was installed and the service has started.

## Register the plugin with a vCenter Server Appliance

After the plugin software is installed, register the plugin with a vCSA.



The plugin can only be registered to one vCSA at a time. To register to a different vCSA, then you must un-register the plugin from the current vCSA and uninstall it from the application host. Then you can re-install the plugin and register it to the other vCSA.

1. Open a prompt through the command line and navigate to the following directory:

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

2. Execute the **vcenter-register.bat** file:

```
vcenter-register.bat ^  
-action registerPlugin ^  
-vcenterHostname <vCenter FQDN> ^  
-username <Administrator username> ^
```

3. Verify that the script was successful.

The logs are saved to %install\_dir%/working/logs/vc-registration.log.

## Verify the plugin registration

After the plugin is installed and the registration script has executed, verify that the plugin successfully registered with the vCenter Server Appliance.

1. Open the vSphere Client to the vCenter Server Appliance.
2. On the menu bar, select **Administrator > Client Plugins**.
3. Make sure the SANtricity Storage Plugin for vCenter is listed as **Enabled**.

If the plugin is listed as Disabled with an error message stating that it cannot communicate with the application server, verify that the port number defined for the application server is enabled to pass through any firewalls that might be in use. The default application server Transmission Control Protocol (TCP) port number is 8445.

## Configure plugin access permissions

You can configure access permissions for the Storage Plugin for vCenter, which includes users, roles, and privileges.

### Review required vSphere privileges

To access the plugin within the vSphere Client, you must be assigned to a role that has the appropriate vSphere privileges. Users with the “Configure datastore” vSphere privilege have read-write access to the plugin, while users with the “Browse datastore” privilege have read-only access. If a user has neither of these privileges, the plugin displays an “Insufficient Privileges” message.

| Plugin access type     | vSphere privilege required |
|------------------------|----------------------------|
| Read-Write (Configure) | Datastore.Configure        |
| Read-Only (View)       | Datastore.Browse           |

### Configure Storage Administrator roles

To provide read/write privileges for plugin users, you can create, clone, or edit a role. For more information about configuring roles in the vSphere Client, see the following topic in the VMware Doc Center:

- [Create a Custom Role](#)

## Access role actions

1. From the home page of the vSphere Client, select **Administrator** from the access control area.
2. Click **Roles** from the access control area.
3. Perform one of the following actions:
  - **Create new role:** Click on the **Create Role** action icon.
  - **Clone role:** Select an existing role and click on the **Clone Role** action icon.
  - **Edit existing role:** Select an existing role and click on the **Edit Role** action icon.



The Administrator role is not editable.

The appropriate wizard appears, depending on the above selection.

## Create a new role

1. In the Privileges list, select the access permissions to assign to this role.

To allow Read-Only access to the plugin, select **Datastore > Browse datastore**. To allow Read-Write access, select **Datastore > Configure datastore**.

2. Assign other privileges for the list if needed, and then click **Next**.
3. Name the role and provide a description.
4. Click **Finish**.

## Clone a role

1. Name the role and provide a description.
2. Click **OK** to finish the wizard.
3. Select the cloned role from the list, and then click on **Edit Role**.
4. In the Privileges list, select the access permissions to assign to this role.

To allow Read-Only access to the plugin, select **Datastore > Browse datastore**. To allow Read-Write access, select **Datastore > Configure datastore**.

5. Click **Next**.
6. Update the name and description, if desired.
7. Click **Finish**.

## Edit an existing role

1. In the Privileges list, select the access permissions to assign to this role.

To allow Read-Only access to the plugin, select **Datastore > Browse datastore**. To allow Read-Write access, select **Datastore > Configure datastore**.

2. Click **Next**.
3. Update the name or description, if desired.
4. Click **Finish**.



## Set permissions for vCenter Server Appliance

After setting privileges for a role, you must then add a permission to the vCenter Server Appliance. This permission allows a given user or group access to the plugin.

1. From the menu dropdown list, select **Hosts and Clusters**.
2. Select the **vCenter Server Appliance** from the access control area.
3. Click the **Permissions** tab.
4. Click the **Add Permission** action icon.
5. Select the appropriate domain and user/group.
6. Select the role created that allows for the read/write plugin privilege.
7. Enable the **Propagate to Children** option, if needed.
8. Click **OK**.



You can select an existing permission and modify it to use the created role. **However, be aware that the role must have the same privileges along with read/write plugin privileges as to avoid a regress in permissions.**

To access the plugin, you must log in to the vSphere Client under the user account that has the read/write privileges for the plugin.

For more information about managing permissions, see the following topics in the VMware Doc Center:

- [Managing Permissions for vCenter Components](#)
- [Best Practices for Roles and Permissions](#)

## Log in and navigate the Storage Plugin for vCenter

You can log in to the Storage Plugin for vCenter to navigate the user interface.

1. Before you log in to the plugin, make sure you are using one of the following browsers:
  - Google Chrome 79 or later
  - Mozilla Firefox 70 or later
  - Microsoft Edge 79 or later
2. Log in to the vSphere Client under the user account that has read/write privileges for the plugin.
3. From the vSphere Client Home page, click **SANtricity Storage Plugin for vCenter**.

The plugin opens within a vSphere Client window. The plugin's main page opens to **Manage-All**.

4. Access storage management tasks from the navigation sidebar on the left:
  - **Manage** – Discover storage arrays in your network, open System Manager for an array, import settings from one array to multiple arrays, manage array groups, upgrade the OS software, and provision storage.
  - **Certificate Management** – Manage certificates to authenticate between browsers and clients.
  - **Operations** – View the progress of batch operations, such as importing settings from one array to another.

- **Support** – View technical support options, resources, and contacts.

## Discover storage arrays in the plugin

To display and manage storage resources, you must use the Storage Plugin for vCenter interface to discover the IP addresses of arrays in your network.

### Step 1: Enter network addresses for discovery

#### Before you begin

- You must know the network IP addresses (or range of addresses) of the array controllers.
- The storage arrays must be correctly set up and configured, and you must know the storage array login credentials (user name and password).

#### Steps

1. From the Manage page, select **Add/Discover**.

The Enter Network Address Range dialog box appears.

2. Do one of the following:
  - To discover one array, select the **Discover a single storage array** radio button, and then enter the IP address for one of the controllers in the storage array.
  - To discover multiple storage arrays, select the **Discover all storage arrays within a network range** radio button, and then enter the starting network address and ending network address to search across your local sub-network.
3. Click **Start Discovery**.

As the discovery process begins, the dialog box displays the storage arrays as they are discovered. The discovery process might take several minutes to complete.

If no manageable arrays are discovered, verify that the storage arrays are properly connected to your network and their assigned addresses are within range. Click **New Discovery Parameters** to return to the Add/Discover page.

4. Select the checkbox next to any storage array that you want to add to your management domain.

The system performs a credential check on each array that you are adding to the management domain. You might need to resolve any issues with untrusted certificates before proceeding.

5. Click **Next** to proceed to the next step in the wizard.

If the storage arrays have valid certificates, go to [Step 3: Provide passwords](#).

If any storage arrays do not have valid certificates, the Resolve Self-Signed Certificates dialog box appears. Go to [Step 2: Resolve untrusted certificates during discovery](#).

If you want to import CA-signed certificates, cancel out of the discovery wizard and click **Certificate Management** from the left panel. Refer to the online help for further instructions.

## Step 2: Resolve untrusted certificates during discovery

You must resolve any certificate issues before proceeding with the discovery process.

1. If the Resolve Self-Signed Certificates dialog box opens, review the information displayed for the untrusted certificates. For more information, you can also click the ellipses at the far end of the table and select **View** from the pop-up menu.
2. Do one of the following:
  - If you trust the connections to the discovered storage arrays, click **Next** and then click **Yes** to confirm and continue to the next dialog in the wizard. The self-signed certificates are marked as trusted and the storage arrays will be added to the plugin.
  - If you do not trust the connections to the storage arrays, select **Cancel** and validate each storage array's security certificate strategy before adding any of them.
3. Click **Next** to proceed to the next step in the wizard.

## Step 3: Provide passwords

As the last step for discovery, you must enter the passwords for the storage arrays that you want to add to your management domain.

1. For each discovered array, enter its admin password in the fields.
2. Click **Finish**.

It can take several minutes for the system to connect to the specified storage arrays. When the process is finished, the storage arrays are added to your management domain and associated with the selected group (if specified).

## Provision storage in the plugin

To provision storage, you create volumes, assign volumes to hosts, and then assign volumes to datastores.



For more information about storage provisioning, see the online help available from the plugin interface.

### Create volumes

Volumes are data containers that manage and organize the storage space on your storage array. You create volumes from the storage capacity available on your storage array, which helps organize your system's resources. The concept of "volumes" is similar to using folders/directories on a computer to organize files for quick access.

Volumes are the only data layer visible to hosts. In a SAN environment, volumes are mapped to logical unit numbers (LUNs). These LUNs hold the user data that is accessible using one or more of the host access protocols supported by the storage array.

### Steps

1. From the Manage page, select the storage array.
2. Select **Provisioning > Manage Volumes**.

3. Select **Create > Volumes**.

The Select Host dialog box appears.

4. From the drop-down list, select a specific host or host cluster to which you want to assign volumes, or choose to assign the host or host cluster at a later time.
5. To continue the volume creation sequence for the selected host or host cluster, click **Next**.

The Select Workload dialog box appears. A workload contains volumes with similar characteristics, which are optimized based on the type of application the workload supports. You can define a workload or you can select existing workloads.

6. Do one of the following:
  - Select the **Create volumes for an existing workload** option and then select the workload from the drop-down list.
  - Select the **Create a new workload** option to define a new workload for a supported application or for “Other” applications, and then following these steps:
    - a. From the drop-down list, select the name of the application you want to create the new workload for. Select one of the “Other” entries if the application you intend to use on this storage array is not listed.
    - b. Enter a name for the workload you want to create.
7. Click **Next**. If your workload is associated with a supported application type, enter the information requested; otherwise, go to the next step.

The Add/Edit Volumes dialog box appears. In this dialog, you create volumes from eligible pools or volume groups. For each eligible pool and volume group, the number of drives available and the total free capacity appears. For some application-specific workloads, each eligible pool or volume group shows the proposed capacity based on the suggested volume configuration and shows the remaining free capacity in GiB. For other workloads, the proposed capacity appears as you add volumes to a pool or volume group and specify the reported capacity.

8. Before you begin adding volumes, read the guidelines in the following table.

| Field         | Description  |
|---------------|--|
| Free capacity | Because volumes are created from pools or volume groups, the pool or volume group you select must have sufficient free capacity. |

| Field                 | Description   |
|-----------------------|---|
| Data Assurance (DA)   | <p>To create a DA-enabled volume, the host connection you are planning to use must support DA.</p> <ul style="list-style-type: none"> <li>• If you want to create a DA-enabled volume, select a pool or volume group that is DA capable (look for Yes next to "DA" in the pool and volume group candidates table).</li> <li>• DA capabilities are presented at the pool and volume group level. DA protection checks for and corrects errors that might occur as data is transferred through the controllers down to the drives. Selecting a DA-capable pool or volume group for the new volume ensures that any errors are detected and corrected.</li> <li>• If any of the host connections on the controllers in your storage array do not support DA, the associated hosts cannot access data on DA-enabled volumes.</li> </ul>                               |
| Drive security        | <p>To create a secure-enabled volume, a security key must be created for the storage array.</p> <ul style="list-style-type: none"> <li>• If you want to create a secure-enabled volume, select a pool or volume group that is secure capable (look for Yes next to "Secure-capable" in the pool and volume group candidates table).</li> <li>• Drive security capabilities are presented at the pool and volume group level. Secure-capable drives prevent unauthorized access to the data on a drive that is physically removed from the storage array. A secure-enabled drive encrypts data during writes and decrypts data during reads using a unique encryption key.</li> <li>• A pool or volume group can contain both secure-capable and non-secure-capable drives, but all drives must be secure-capable to use their encryption capabilities.</li> </ul> |
| Resource provisioning | <p>To create a resource-provisioned volume, all drives must be NVMe drives with the Deallocated or Unwritten Logical Block Error (DULBE) option.</p>  |

9. Choose one of these actions based on whether you selected Other or an application-specific workload in the previous step:

- **Other** – Click **Add new volume** in each pool or volume group that you want to use to create one or more volumes.
- **Application-specific workload** – Either click **Next** to accept the system-recommended volumes and

characteristics for the selected workload, or click **Edit Volumes** to change, add, or delete the system-recommended volumes and characteristics for the selected workload.

The following fields appear.

| Field                                    | Description   |
|--|---|
| Volume Name                              | A volume is assigned a default name during the volume creation sequence. You can either accept the default name or provide a more descriptive one indicating the type of data stored in the volume.   |
| Reported Capacity                        | Define the capacity of the new volume and the capacity units to use (MiB, GiB, or TiB). For thick volumes, the minimum capacity is 1 MiB, and the maximum capacity is determined by the number and capacity of the drives in the pool or volume group.<br>Capacity in a pool is allocated in 4-GiB increments. Any capacity that is not a multiple of 4 GiB is allocated but not usable. To make sure that the entire capacity is usable, specify the capacity in 4-GiB increments. If unusable capacity exists, the only way to regain it is to increase the capacity of the volume. |
| Volume Type                              | If you selected Application-specific workload, the Volume Type field appears. This indicates the type of volume that was created for an application-specific workload.  |
| Volume Block Size (EF300 and EF600 only) | Shows the block sizes that can be created for the volume: <ul style="list-style-type: none"><li>• 512 – 512 bytes</li><li>• 4K – 4,096 bytes</li></ul>  |

| Field        | Description  |
|--------------|--|
| Segment Size | <p data-bbox="863 157 1490 296">Shows the setting for segment sizing, which only appears for volumes in a volume group. You can change the segment size to optimize performance.</p> <p data-bbox="863 327 1490 636"><b>Allowed segment size transitions</b> – The system determines the segment size transitions that are allowed. Segment sizes that are inappropriate transitions from the current segment size are unavailable on the drop-down list. Allowed transitions usually are double or half of the current segment size. For example, if the current volume segment size is 32 KiB, a new volume segment size of either 16 KiB or 64 KiB is allowed.</p> <p data-bbox="863 667 1490 976"><b>SSD Cache-enabled volumes</b> – You can specify a 4-KiB segment size for SSD Cache-enabled volumes. Make sure you select the 4-KiB segment size only for SSD Cache-enabled volumes that handle small-block I/O operations (for example, 16 KiB I/O block sizes or smaller). Performance might be impacted if you select 4 KiB as the segment size for SSD Cache-enabled volumes that handle large block sequential operations.</p> <p data-bbox="863 1008 1490 1108"><b>Amount of time to change segment size</b> – The amount of time to change a volume's segment size depends on these variables:</p> <ul data-bbox="889 1140 1442 1409" style="list-style-type: none"> <li>• The I/O load from the host</li> <li>• The modification priority of the volume</li> <li>• The number of drives in the volume group</li> <li>• The number of drive channels</li> <li>• The processing power of the storage array controllers</li> </ul> <p data-bbox="863 1440 1490 1541">When you change the segment size for a volume, I/O performance is affected, but your data remains available.</p> |

| Field          | Description   |
|----------------|---|
| Secure-capable | <p><b>Yes</b> appears next to "Secure-capable" only if the drives in the pool or volume group are encryption-capable.</p> <p>Drive Security prevents unauthorized access to the data on a drive that is physically removed from the storage array. This option is available only when the Drive Security feature has been enabled, and a security key is set up for the storage array.</p> <p>A pool or volume group can contain both secure-capable and non-secure-capable drives, but all drives must be secure-capable to use their encryption capabilities.</p> |
| DA             | <p><b>Yes</b> appears next to "DA" only if the drives in the pool or volume group support Data Assurance (DA).</p> <p>DA increases data integrity across the entire storage system. DA enables the storage array to check for errors that might occur as data is transferred through the controllers down to the drives. Using DA for the new volume ensures that any errors are detected.</p>  |

10. To continue the volume creation sequence for the selected application, click **Next**.
11. In the last step, review a summary of the volumes you intend to create and make any necessary changes. To make changes, click **Back**. When you are satisfied with your volume configuration, click **Finish**.

## Create host access and assign volumes

A host can be created automatically or manually:

- **Automatic** — Automatic host creation for SCSI-based (not NVMe-oF) hosts is initiated by the Host Context Agent (HCA). The HCA is a utility that you can install on each host attached to the storage array. Each host that has the HCA installed pushes its configuration information to the storage array controllers through the I/O path. Based on the host information, the controllers automatically create the host and the associated host ports and set the host type. If needed, you can make any additional changes to the host configuration. After the HCA performs its automatic detection, the host is automatically configured with the following attributes:
  - The host name derived from the system name of the host.
  - The host identifier ports that are associated with the host.
  - The Host Operating System Type of the host.



Host Context Agent software for Linux and Windows is available from [NetApp Support - Downloads](#).



Hosts are created as stand-alone hosts; the HCA does not automatically create or add to host clusters.



- **Manual** – During manual host creation, you associate host port identifiers by selecting them from a list or manually entering them. After you create a host, you can assign volumes to it or add it to a host cluster if you plan to share access to volumes.

## Using the HCA to auto-discover the host

You can allow the Host Context Agent (HCA) to automatically detect the hosts, and then verify that the information is correct.

### Steps

1. From the Manage page, select the storage array with the host connection.
2. Select **Provisioning > Configure Hosts**.

The Configure Hosts page opens.

3. Select **Storage > Hosts**.

The table lists the automatically created hosts.

4. Verify that the information provided by the HCA is correct (name, host type, host port identifiers).
5. If you need to change any of the information, select the host, and then click **View/Edit Settings**.

## Manually creating the host

### Before you begin

Read the following guidelines:

- You must already have added or discovered storage arrays within your environment.
- You must define the host identifier ports that are associated with the host.
- Make sure that you provide the same name as the host's assigned system name.
- This operation does not succeed if the name you choose is already in use.
- The length of the name cannot exceed 30 characters.

### Steps

1. From the Manage page, select the storage array with the host connection.
2. Select **Provisioning > Configure Hosts**.

The Configure Hosts page opens.

3. Click **Create > Host**.

The Create Host dialog box appears.

4. Select the settings for the host as appropriate.

| Field | Description                   |
|-------|-------------------------------|
| Name  | Type a name for the new host. |

| Field                      | Description  |
|----------------------------|--|
| Host operating system type | Select the operating system that is running on the new host from the drop-down list.   |
| Host interface type        | (Optional) If you have more than one type of host interface supported on your storage array, select the host interface type that you want to use.  |
| Host ports                 | <p>Do one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Select I/O Interface.</b> Generally, the host ports should have logged in and be available from the drop-down list. You can select the host port identifiers from the list.</li> <li>• <b>Manual add.</b> If a host port identifier is not displayed in the list, it means that the host port has not logged in. An HBA utility or the iSCSI initiator utility may be used to find the host port identifiers and associate them with the host.</li> </ul> <p>You can manually enter the host port identifiers or copy/paste them from the utility (one at a time) into the Host ports field.</p> <p>You must select one host port identifier at a time to associate it with the host, but you can continue to select as many identifiers that are associated with the host. Each identifier is displayed in the Host ports field. If necessary, you also can remove an identifier by selecting the X next to it.</p> |

| Field                     | Description   |
|---------------------------|---|
| Set CHAP initiator secret | <p>(Optional) If you selected or manually entered a host port with an iSCSI IQN, and if you want to require a host that tries to access the storage array to authenticate using Challenge Handshake Authentication Protocol (CHAP), select the Set CHAP initiator secret checkbox. For each iSCSI host port you selected or manually entered, do the following:</p> <ul style="list-style-type: none"> <li>• Enter the same CHAP secret that was set on each iSCSI host initiator for CHAP authentication. If you are using mutual CHAP authentication (two-way authentication that enables a host to validate itself to the storage array and for a storage array to validate itself to the host), you also must set the CHAP secret for the storage array at initial setup or by changing settings.</li> <li>• Leave the field blank if you do not require host authentication.</li> </ul> <p>Currently, the only iSCSI authentication method used is CHAP.</p> |

5. Click **Create**.

6. If you need to update the host information, select the host from the table and click **View/Edit Settings**.

After the host is successfully created, the system creates a default name for each host port configured for the host (user label). The default alias is <Hostname\_Port Number>. For example, the default alias for the first port created for host IPT is IPT\_1.

7. Next, you must assign a volume to a host or a host cluster so it can be used for I/O operations. Select **Provisioning > Configure Hosts**.

The Configure Hosts page opens.

8. Select the host or host cluster to which you want to assign volumes, and then click **Assign Volumes**.

A dialog box appears that lists all the volumes that can be assigned. You can sort any of the columns or type something in the Filter box to make it easier to find particular volumes.

9. Select the check box next to each volume that you want to assign or select the check box in the table header to select all volumes.

10. Click **Assign** to complete the operation.

The system performs the following actions:

- The assigned volume receives the next available LUN number. The host uses the LUN number to access the volume.
- The user-supplied volume name appears in volume listings associated to the host. If applicable, the

factory-configured access volume also appears in volume listings associated to the host.

## Create a datastore in vSphere Client

To create a datastore in the vSphere Client, see the following topic in the VMware Doc Center:

- [Create a VMFS Datastore in the vSphere Client](#)

### Increase capacity of existing datastore by increasing volume capacity

You can increase the reported capacity (the capacity reported to hosts) of a volume by using the free capacity that is available in the pool or volume group. To learn more about pools and volume groups, see the online help for the plugin.

#### Before you begin

Make sure that:

- Enough free capacity is available in the volume's associated pool or volume group.
- The volume is Optimal and not in any state of modification.
- No hot spare drives are in use in the volume. (Applies only to volumes in volume groups.)



Increasing the capacity of a volume is supported only on certain operating systems. If you increase the volume capacity on a host operating system that does not support LUN expansion, the expanded capacity is unusable, and you cannot restore the original volume capacity.

#### Steps

1. Navigate to the plugin within vSphere Client.
2. Within the plugin, select the desired storage array.
3. Click on **Provisioning** and select **Manage Volumes**.
4. Select the volume for which you want to increase capacity, and then select **Increase Capacity**.

The Confirm Increase Capacity dialog box appears.

5. Select **Yes** to continue.

The Increase Reported Capacity dialog box appears.

This dialog box displays the volume's current reported capacity and the free capacity available in the volume's associated pool or volume group.

6. Use the **Increase reported capacity by adding...** box to add capacity to the current available reported capacity. You can change the capacity value to display in either mebibytes (MiB), gibibytes (GiB), or tebibytes (TiB).
7. Click **Increase**.
8. View the Recent Tasks pane for the progress of the increase capacity operation that is currently running for the selected volume. This operation can be lengthy and could affect system performance.
9. After the volume capacity is complete, you must manually increase the VMFS size to match as described in the following topic:
  - [Increase VMFS Datastore Capacity in the vSphere Client](#)

## Increase capacity of existing datastore by adding volumes

1. You can increase the capacity of a datastore by adding volumes. Follow the steps in *Create volumes*.
2. Next, assign the volumes to the desired host to increase the datastore's capacity. See the following topic:
  - [Increase VMFS Datastore Capacity in the vSphere Client](#)

## Remove the Storage Plugin for vCenter

You can remove the plugin from the vCenter Server Appliance and uninstall the plugin webserver from the application host.

These are two distinct steps that you can perform in any order. However, if you choose to remove the plugin webserver from the application host before unregistering the plugin, the registration script is removed during that process and you cannot use Method 1 to unregister.

### Unregister the plugin from a vCenter Server Appliance

To unregister the plugin from a vCenter Server Appliance, select one of these methods:

- Method 1: Executing the registration script
- Method 2: Using the vCenter Server Mob pages

#### Method 1: Executing the registration script

1. Open a prompt through the command line and navigate to the following directory:

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

2. Execute the `vcenter-register.bat` file:

```
vcenter-register.bat ^  
  
-action unregisterPlugin ^  
  
-vcenterHostname <vCenter FQDN> ^  
  
-username <Administrator Username> ^
```

3. Verify that the script is successful.

The logs are saved to `%install_dir%/working/logs/vc-registration.log`.

#### Method 2: Using the vCenter Server Mob pages

1. Open a web browser and enter the following url:

```
https://<FQDN of vCenter Server>/mob
```

2. Log in under the administrator credentials.
3. Look for the property name of `extensionManager` and click the link associated with that property.
4. Expand the properties list by clicking the **More...** link at the bottom of the list.

5. Verify that the extension `plugin.netapp.eseries` is in the list.
6. If it is present, then click the Method `UnregisterExtension`.
7. Enter the value `plugin.netapp.eseries` in the dialog and click **Invoke Method**.
8. Close the dialog and refresh the web browser.
9. Verify that the `plugin.netapp.eseries` extension is not on the list.



This procedure unregisters the plugin from the vCenter Server Appliance; however, it does not remove plugin package files from the server. To remove package files, use SSH to access the vCenter Server Appliance and navigate to the following directory:

```
etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity/
```

Then remove the directory associated with the plugin.

### Remove the plugin webserver from the Application host

To remove the plugin software from the application host, follow these steps:

1. From the application server, navigate to the **Control Panel**.
2. Go to **Apps & Features**, and then select **SANtricity Storage Plugin for vCenter**.
3. Click **Uninstall/Change**.

A confirmation dialog opens.

4. Click **Uninstall**.

A confirmation message is displayed when the uninstall is complete.

5. Click **Done**.

## Legacy solutions

### Cloud connector

#### Overview of the SANtricity® Cloud Connector

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

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

## Considerations

When using these procedures, be aware that:

- Configuration and backup/restore jobs described in these procedures apply to the graphical user interface version of the SANtricity Cloud Connector.
- REST API workflows for the SANtricity Cloud Connector application are not described in these procedures. For experienced developers, endpoints are available for each SANtricity Cloud Connector operation under the API documentation. The API documentation is accessible by navigating to <http://<hostname.domain>:<port>/docs> through a browser.

## Types of backups

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

### • Image-based backup

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

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

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

### • File-based backup

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

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

## System requirements for Cloud Connector

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

### Host hardware requirements

Your hardware must meet the following minimum requirements:

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

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

### Supported browsers

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

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



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

### Compatible storage arrays and controller firmware

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

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

### Compatible operating systems

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

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

### Supported file systems

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

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

- ext2
- ext3



- ext4

## Install SANtricity Cloud Connector

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

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

### Before you begin

Review the following notes:

- If SANtricity Web Services Proxy is already installed on the same server as the SANtricity Cloud Connector, conflicts will occur between non-SSL port numbers and SSL port numbers conflicts. In this case, choose appropriate numbers for the non-SSL port and the SSL port during the SANtricity Cloud Connector installation.
- If any hardware changes are performed on your host, re-install the SANtricity Cloud Connector application to ensure encryption consistency.
- Backups created through version 3.1 of the SANtricity Cloud Connector application are not compatible with version 4.0 of the SANtricity Cloud Connector application. If you intend to maintain these backups, you must continue to use your previous version of the SANtricity Cloud Connector. To ensure successful installation of separate 3.1 and 4.0 releases of the SANtricity Cloud Connector, unique port numbers must be assigned for each version of the application.

## Install Device Mapper Multipath (DM-MP)

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

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

## Install Cloud Connector

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

### Graphical mode

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

### Before you begin

Designate a host location for the SANtricity Cloud Connector installation.

### Steps

1. Download the SANtricity Cloud Connector installation file to the desired host location.
2. Open a terminal window.

3. Navigate to the directory file containing the SANtricity Cloud Connector installation file.
4. Start the SANtricity Cloud Connector installation process:

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

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

The Installer window is displayed.

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

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

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

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

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



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

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

8. Choose one of the following options:

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

9. Choose one of the following options:

- To accept the default SSL port number, click **Next**.
- To change the default SSL port number, enter the new desired port number value.

10. Choose one of the following options:

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

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

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

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

The Installation Complete message is displayed.

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

## Console mode

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

### Before you begin

Designate a host location for the SANtricity Cloud Connector installation.

### Steps

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

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

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

The installation process for the SANtricity Cloud Connector is initialized.

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

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



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

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

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

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

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



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

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



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

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

9. Choose one of the following options:
  - To accept the default install location, press **Enter**.

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

10. Choose one of the following options:

- To accept the default SSL port number, press **Next**.
- To change the default SSL port number, enter the new desired port number value.

11. Choose one of the following options:

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

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

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

The Installation Complete message is displayed.

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

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

#### Steps

1. Stop the service using the `systemctl` command.
2. From the default install location, access the working directory.



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

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

#### EXAMPLE

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

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

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

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

#### EXAMPLE

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

6. Restart the service.

#### Add StorageGRID certificate into a keystore

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

#### Before you begin

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

#### Steps

1. Stop the service using the `systemctl` command.
2. From the default install location, access the working directory.



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

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

#### EXAMPLE

```
opt/netapp/santricity_cloud_connector4/jre/bin/keytool -import
-trustcacerts -storepass changeit -noprompt -alias StorageGrid_SSL -file
/home/ictlabs01.cer -keystore
/opt/netapp/santricity_cloud_connector/jre/lib/security/cacerts
```

4. Restart the service.

## Configure the SANtricity Cloud Connector for the first time

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

### Log in to the SANtricity Cloud Connector for the first time

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

### Before you begin

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

### Steps

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

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

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

The SANtricity Cloud Connector Configuration Wizard is displayed.

### Using the Configuration Wizard

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

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

### Step 1: Set administrator password

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

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

### Steps

1. On the Set Administrator Password page, enter the desired login password for the SANtricity Cloud Connector in the **Enter the new administrator password** field.
2. In the **Re-enter the new administrator password** field, re-enter the password from first field.
3. Click **Next**.

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



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

## Step 2: Set pass phrase

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

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

### Steps

1. In the **Define a pass phrase** field, enter the desired pass phrase.
2. In the **Re-enter your pass phrase** field, re-enter the pass phrase from the first field.
3. Click **Next**.

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

## Step 3: Select target type

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

### Before you begin

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

### Steps

1. In the dropdown menu, select one of the following options:
  - Amazon AWS
  - AltaVault
  - StorageGRID

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

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

## Configure AltaVault appliance

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

### Before you begin

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

### Steps

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



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

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



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

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

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

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

## Configure Amazon AWS account

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

### Before you begin

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

### Steps

1. In the **Access Key ID** field, enter the access ID for the Amazon AWS target.
2. In the **Secret Access Key** field, enter the secret access key for the target.
3. In the **Bucket Name** field, enter the bucket name for the target.
4. Select the **Save a backup of the configuration database on this target** checkbox to create a backup of the configuration database on the selected target type.



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



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

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

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



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

## Configure StorageGRID account

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

### Before you begin

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

### Steps

1. In the **URL** field, enter the URL for the Amazon S3 cloud service
2. In the **Access Key ID** field, enter the access ID for the S3 target.
3. In the **Secret Access Key** field, enter the secret access key for the S3 target.
4. In the **Bucket Name** field, enter the bucket name for the S3 target.
5. To use path style access, select the **Use path-style access** checkbox.



If unchecked, virtual host-style access is used.

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



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



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

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



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

8. Click **Next**.

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

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

## Step 4: Connect to Web Services Proxy

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

## Before you begin

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

### Steps

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

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

## Step 5: Select storage arrays

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

### Before you begin

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



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

### Steps

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

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



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

## Step 6: Select hosts

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

### Before you begin

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

## Steps

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

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

## Step 7: Review the initial configuration

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

Review the results of the validated configuration data.

- If all configuration data is successfully validated and established, click **Finish** to complete the configuration process.
- If any section of the configuration data cannot be validated, click **Back** to navigate to the applicable page of the configuration wizard to revise the submitted data.

## Log into the SANtricity Cloud Connector

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

## Steps

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

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

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

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

## Backups

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

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



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

### Create a new image-based backup

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

#### Before you begin

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

#### Steps

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

The Create Backup window is displayed.

2. Select **Create an image-based backup**.
3. Click **Next**.

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

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

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

5. To modify the auto-generated backup name, enter the desired name in the **Job Name** field.
6. If needed, add a description for the backup in the **Job Description** field.



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

7. Click **Next**.

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

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

The confirmation page of the Create Backup window is displayed.

9. Select one of the following options:
  - **YES** — Initiates a full backup for the selected backup.
  - **NO** — A full backup for the selected image-based backup is not performed.



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

10. Click **OK**.

The backup for the selected E-Series volume is initiated, and the status for the task is displayed under the

result list section of the Backups page.

### Create a new folder/file-based backup

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

#### Before you begin

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

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

#### Steps

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

The Create Backup window is displayed.

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

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

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

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



If your filesystem does not appear, verify your filesystem type is supported by the SANtricity Cloud Connector application. For more information, refer to [Supported file systems](#).

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

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

6. To modify the auto-generated backup name, enter the desired name in the **Job Name** field.
7. If needed, add a description for the backup in the **Job Description** field.



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.



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

#### 11. Click **Close**.

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

### Run Full and Incremental Backups

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

#### Before you begin

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

#### Steps

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



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.



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

3. Click **Run**.

The backup request is initiated.

### Delete a backup job

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

#### Before you begin

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

#### Steps

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



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

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

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



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

### Create a new image-based restore

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

### Before you begin

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

### Steps

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

The Restore window is displayed.

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

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

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

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

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

The Review page is displayed in the Restore window.

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

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

## Create a new file-based restore

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

### Before you begin

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

### Steps

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

The Restore window is displayed.

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

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

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

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

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

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

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

The Review page is displayed in the Restore window.

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

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

## Delete a restore

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

### Before you begin

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

### Steps

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

The Confirm Delete window is displayed.

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





You cannot delete a suspended restore.

The selected restore is deleted.

## Modify the SANtricity Cloud Connector settings

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

### Modify S3 Account settings

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

#### Before you begin

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

#### Steps

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

The Settings - Configuration page is displayed.

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

The S3 Account Settings page is displayed.

3. In the URL file, enter the URL for the S3 cloud service.
4. In the **Access Key ID** field, enter the access ID for the S3 target.
5. In the **Secret Access Key** field, enter the access key for the S3 target.
6. In the **S3 Bucket Name** field, enter the bucket name for the S3 target.
7. Select the **Use Path Style Access** check box if needed.
8. Click **Test Connection** to verify the connection for the entered S3 credentials.
9. Click **Save** to apply the modifications.

The modified S3 account settings are applied.

### Manage storage arrays

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

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

#### Steps

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

The Settings - Storage Arrays screen is displayed.

2. To add storage arrays to the SANtricity Cloud Connector, click **Add**.
  - a. In the Add Storage Arrays window, select each checkbox next to the desired storage arrays from the result list.
  - b. Click **Add**.

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

3. To modify the host for an added storage array, click **Edit** for the line item in the result list section of the Settings - Storage Arrays screen.
  - a. In the Associated Host drop-down menu, select the desired host for the storage array.
  - b. Click **Save**.

The selected host is assigned to the storage array.

4. To remove an existing storage array from the SANtricity Cloud Connector host, select the desired storage arrays from the bottom result list, and click **Remove**.
  - a. In the Confirm Remove Storage Array field, type REMOVE.
  - b. Click **Remove**.

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

### Modify Web Services Proxy settings

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

#### Before you begin

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

#### Steps

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

The Settings - Configuration screen is displayed.

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

The Web Services Proxy settings screen is displayed.

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

## Change SANtricity Cloud Connector password

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

### Steps

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

The Settings - Configuration screen is displayed.

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

The Change Password screen is displayed.

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

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

## Uninstall the SANtricity Cloud Connector

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

### Uninstall using graphical mode

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

### Steps

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

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

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

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

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

The uninstall process for the SANtricity Cloud Connector is initialized.

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

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

## Uninstall using console mode

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

### Steps

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

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

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

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

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

The uninstall process for the SANtricity Cloud Connector is initialized.

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

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

## Copyright Information

Copyright © 2022 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.