NetApp E-Series

SANtricity Storage Plugin for vCenter, Version 1.10

Installation and Configuration

May 2021 | PN 215-15257

TABLE OF CONTENTS

1 Overview

This guide describes how to install and configure the SANtricity Storage Plugin for vCenter.

The Plugin for vCenter provides integrated management of E-Series storage arrays from within a VMware vSphere Client session. The vSphere Client is a single management interface that you can use to manage the VMware infrastructure and all your day-to-day storage needs.

The following functions are available in the Plugin for vCenter:

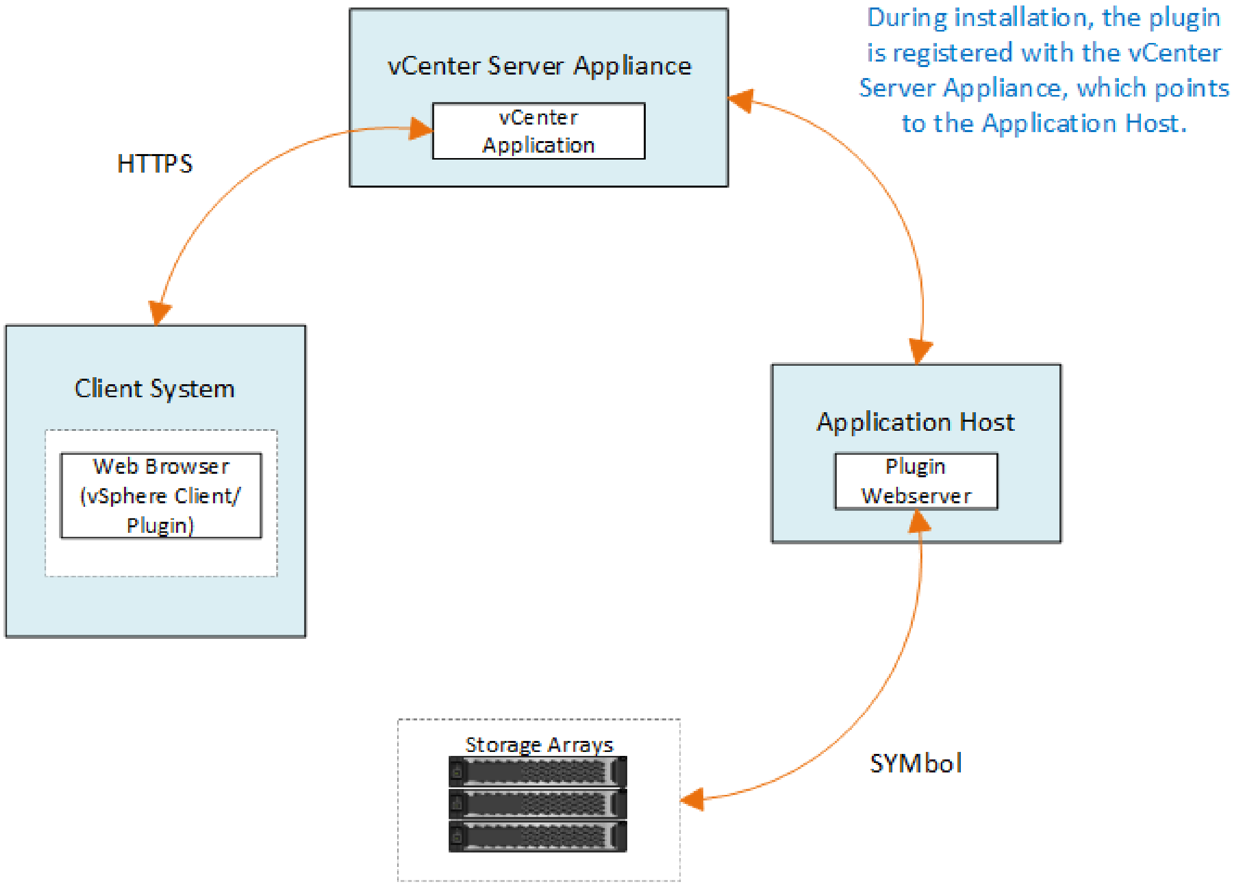
- View and manage discovered storage arrays in the network.
- Perform batch operations on groups of multiple storage arrays.
- Perform upgrades on the software OS.
- Import settings from one storage array to another.
- Configure volumes, SSD cache, hosts, host clusters, pools, and volume groups.
- Launch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

Note: 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.

Figure 1) Communication details.


vCenter Server Appliance
vCenter Application
During installation, the plugin is registered with the vCenter Server Appliance, which points to the Application Host.
HTTPS
Client System
Web Browser (vSphere Client/ Plugin)
Application Host
Plugin Webserver
Storage Arrays
SYMbol

2 Installation

Follow the instructions in this section to install the plugin.

2.1 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)

2.2 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**.

   Note: 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.

2.3 Register the plugin with a vCenter Server Appliance

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

Note: 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.

To register the plugin:

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`.

2.4 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.

3 User Access

Follow the instructions in this section to configure access permissions for the plugin's users.

3.1 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

3.2 Configure Storage Administrator role

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:
   – 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.

   Note: 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**.

3.3 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**.

Note: 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

4 Login and Navigation

Follow the instructions in this section to log in to the plugin and 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 75 or later
   - Mozilla Firefox 60 or later
   - Microsoft Edge 44 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.

5 Storage Array Discovery

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

5.1 Enter network addresses for discovery

As the first step to discovering storage arrays, you enter a single IP address or a range of IP addresses to search across the local sub-network. The Add/Discover feature opens a wizard that guides you through the process of discovery.

1. Before you begin, make sure that:
   - You know the network IP addresses (or range of addresses) of the array controllers.
   - The storage arrays are correctly set up and configured, and you know the storage array login credentials (user name and password).
2. From the Manage page, select **Add/Discover**.

   The Enter Network Address Range dialog box appears.
3. 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.
4. 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.

5. 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.

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

   If the storage arrays have valid certificates, go to “Provide passwords” on page 9.

   If any storage arrays do not have valid certificates, the Step 2: Resolve Self-Signed Certificates dialog box appears. Go to the next section, “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.

5.2 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.

5.3 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).

6 Storage Provisioning

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

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

6.1 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.

To create a volume:

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.

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

Data Assurance (DA)	To create a DA-enabled volume, the host connection you are planning to use must support DA. • 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). • 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. • 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.
Drive security	To create a secure-enabled volume, a security key must be created for the storage array. • 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). • 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. • 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.
Resource provisioning	To create a resource-provisioned volume, all drives must be NVMe drives with the Deallocated or Unwritten Logical Block Error (DULBE) option.

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.

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. 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: • 512 – 512 bytes • 4K – 4,096 bytes
Segment Size	Shows the setting for segment sizing, which only appears for volumes in a volume group. You can change the segment size to optimize performance. **Allowed segment size transitions** – 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. **SSD Cache-enabled volumes** – 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. **Amount of time to change segment size** – The amount of time to change a volume's segment size depends on these variables: • The I/O load from the host • The modification priority of the volume • The number of drives in the volume group • The number of drive channels • The processing power of the storage array controllers When you change the segment size for a volume, I/O performance is affected, but your data remains available.
Secure-capable	**Yes** appears next to "Secure-capable" only if the drives in the pool or volume group are encryption-capable. 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. 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.
DA	**Yes** appears next to "DA" only if the drives in the pool or volume group support Data Assurance (DA). 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.
Resource provisioned (EF300 and EF600 only)	**Yes** appears next to "Resource provisioned" only if the drives support this option. Resource Provisioning is a feature available in the EF300 and EF600 storage arrays, which allows volumes to be put in use immediately with no background initialization process.

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**.

6.2 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.

  Note: Host Context Agent software for Linux and Windows is available from https://mysupport.netapp.com/site/downloads.

  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.

  Note: 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.

To verify host information:

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

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

   The Configure Hosts page opens.
4. Click **Create > Host**.

The Create Host dialog box appears.

5. Select the settings for the host as appropriate.

Name	Type a name for the new host.
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	Do one of the following: • **Select I/O Interface**. 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. • **Manual add**. 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. You can manually enter the host port identifiers or copy/paste them from the utility (one at a time) into the Host ports field. 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.
Set CHAP initiator secret	(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: • 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. • Leave the field blank if you do not require host authentication. Currently, the only iSCSI authentication method used is CHAP.

6. Click **Create**.

7. 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`.

8. 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.

9. 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.

10. 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.

11. 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.

6.3 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.)

Keep in mind any future capacity requirements that you might have for other volumes in this pool or volume group. Make sure that you allow enough free capacity.

Note: 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.

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 the section, “Create volumes” on page 10.
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

7 Plugin Removal

Follow these instructions to remove the plugin from the vCenter Server Appliance and to 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.

7.1 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.

Note: 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.

7.2 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**.

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

Trademark Information