



# **Get started**

## **E-Series Systems**

NetApp  
January 30, 2023

This PDF was generated from <https://docs.netapp.com/us-en/e-series/vcenter-plugin/san-spvc-ic-reqs.html> on January 30, 2023. Always check docs.netapp.com for the latest.

# Table of Contents

- Get started ..... 1
  - Review installation and upgrade requirements ..... 1
  - Install or upgrade the Storage Plugin for vCenter ..... 2
  - Configure plugin access permissions ..... 3
  - Log in and navigate the Storage Plugin for vCenter ..... 6
  - Discover storage arrays in the plugin ..... 6
  - Provision storage in the plugin ..... 8
  - View status ..... 16

# Get started

## Review installation and upgrade requirements

Before installing or upgrading the SANtricity Storage Plugin for vCenter, review the installation requirements and upgrade considerations.

### Installation requirements

You can install and configure the Storage Plugin for vCenter on a Windows host system. Plugin installation includes the following requirements.

Requirement	Description
Supported versions	<ul style="list-style-type: none"><li>• VMware vCenter Server Appliance supported versions: 6.7U3J, 7.0U1, 7.0U2, 7.0U3, and 8.0.</li><li>• NetApp SANtricity OS version: 11.60.2 or higher</li><li>• Supported application host versions: Windows 2016, Windows 2019, Windows 2022.</li></ul> <p>For more information on compatibility, see the <a href="#">NetApp Interoperability Matrix Tool</a>.</p>
Multiple instances	You can install only one instance of Storage Plugin for vCenter on a Windows host and can only register it to one vCSA.
Capacity planning	<p>Storage Plugin for vCenter requires adequate space for execution and 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>• Storage space — 275 MB + 200 MB (logging)</li><li>• System memory — 512 MB</li></ul>
License	The Storage Plugin for vCenter is a free, standalone product that does not require a license key. However, applicable copyrights and terms of service apply.

### Upgrade considerations

If you are upgrading from a previous version, be aware that the plugin must be unregistered from the vCSA prior to the upgrade.

- During the upgrade, most of the plugin's previous configuration settings are preserved. These settings include user passwords, all discovered storage systems, server certificates, trusted certificates, and server runtime configuration.
- The upgrade process does not preserve the **vcenter.properties** files, so you must unregister the plugin prior to the upgrade. Once the upgrade is successful, you can then register the plugin again to the vCSA.

- All SANtricity OS files previously loaded in the repository are removed during the upgrade.

## Install or upgrade the Storage Plugin for vCenter

Follow these steps to install the Storage Plugin for vCenter and verify the plugin registration. You can also upgrade the plugin using these instructions.

### Review installation prerequisites

Be sure that your systems meet the requirements in [Review installation and upgrade requirements](#).



The upgrade process does not preserve the **vcenter.properties** files. If you are upgrading, you must unregister the plugin prior to the upgrade. Once the upgrade is successful, you can then register the plugin again to the vCSA.

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



During an upgrade, you are not prompted for configuration parameters.



During installation, you are prompted for certificate validation. 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. To learn more about certificates, refer to the online help available from the plugin interface.

4. When the Webserver Started message appears, click **OK** to complete the installation, and then click **Done**.
5. Verify that the application server was installed successfully by running the **services.msc** command.
6. Verify that the Application Server (vCP) service, **NetApp SANtricity Storage Plugin for vCenter**, was installed and the service has started.



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.

## 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, you must unregister the plugin from the current vCSA and uninstall it from the application host. You can then 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 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 89 or later
  - Mozilla Firefox 80 or later
  - Microsoft Edge 90 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.



Some operations are not available when a storage array has a non-optimal status.

## 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.

### 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).

## Step 1: Enter network addresses for discovery

### 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.

## Step 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.

### 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.
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 <b>Yes</b> 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 <b>Yes</b> 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	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.

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	<p>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.</p> <p>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.</p>
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)	<p>Shows the block sizes that can be created for the volume:</p> <ul style="list-style-type: none"> <li>• 512 – 512 bytes</li> <li>• 4K – 4,096 bytes</li> </ul>

Field	Description
Segment Size	<p>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><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><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><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 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>When you change the segment size for a volume, I/O performance is affected, but your data remains available.</p>
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**.

## Step 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. 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.
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 <b>X</b> 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 <b>Set CHAP initiator secret</b> 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.

### Step 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.

### 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 [Step 1: 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](#)

# View status

You can view system status from the Storage Plugin for vCenter or from the vSphere Client.

1. Open the plugin from within the vSphere Client.
2. View status from the following panels:
  - **Storage array status** — Go to the **Manage-All** panel. For each discovered array, the row provides a Status column.
  - **Operations in progress** — Click **Operations** on the side panel to view all long-running tasks, such as importing settings. You can also view long-running operations from the Provisioning drop-down. For each operation listed on the Operations in Progress dialog, a percentage of completion and estimated time remaining to complete the operation are shown. In some cases, you can stop an operation or place it at a higher or lower priority. If desired, use the links in the Actions column to stop or change priority for an operation.



Read all cautionary text provided in the dialog boxes, particularly when stopping an operation.

Operations that might appear for the plugin are listed in the following table. Additional operations might also appear in the System Manager interface.

Operation	Possible status of the operation	Actions you can take
Volume create (thick pool volumes larger than 64TiB only)	In progress	none
Volume delete (thick pool volumes larger than 64TiB only)	In progress	none
Add capacity to pool or volume group	In progress	none
Change a RAID level for a volume	In progress	none
Reduce capacity for a pool	In progress	none
Check the time remaining on an instant availability format (IAF) operation for pool volumes	In progress	none
Check the data redundancy of a volume group	In progress	none
Initialize a volume	In progress	none
Increase capacity for a volume	In progress	none
Change segment size for a volume	In progress	none

## Copyright information

Copyright © 2023 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## 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.