# Storage plugin for vCenter

## E-Series Systems

NetApp
December 19, 2022

# Table of Contents

# 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.

### Available tasks

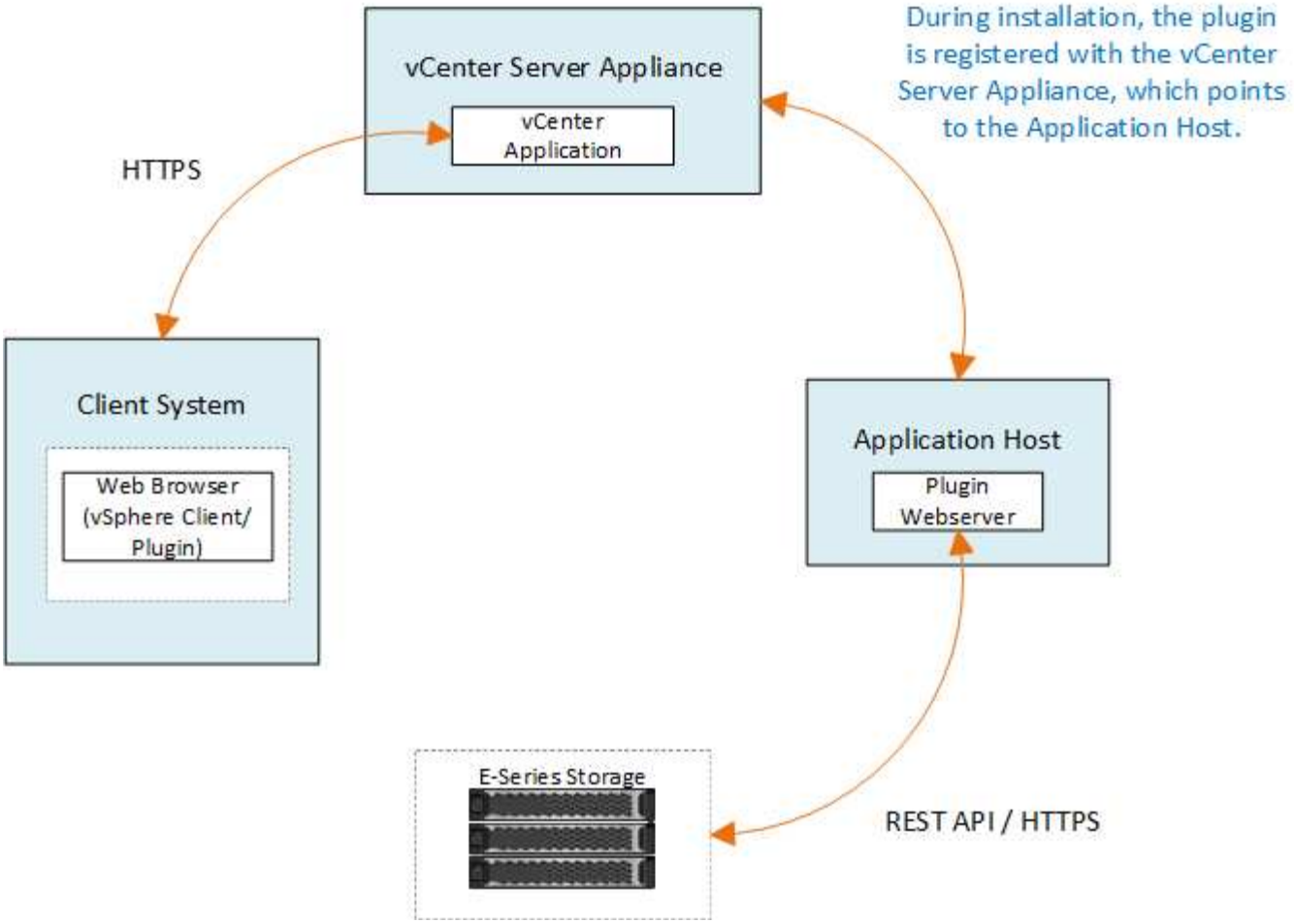
You can use the plugin to perform the following tasks:

- 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 System Manager interface, which is embedded on each controller for a storage array. System Manager provides additional management features; if desired, you can open System Manager by selecting a storage array in the main view of the plugin and then clicking **Launch**.

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.




## Interface overview

When you log in to the plugin, the main page opens to **Manage - All**. From this page, you can view and manage all discovered storage arrays in your network.

### Navigation sidebar

The navigation sidebar displays the following:

- **Manage** — Discover storage arrays in your network, launch System Manager for an array, import settings from one array to multiple arrays, manage array groups, upgrade the SANtricity OS, 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.

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

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

### Supported browsers

The Storage Plugin for vCenter can be accessed from several types of browsers. The following browsers and versions are supported.

- Google Chrome 89 or later

- Mozilla Firefox 80 or later
- Microsoft Edge 90 or later

#### User roles and permissions

To access tasks in the Storage Plugin for vCenter, the user must have read-write permissions. By default, all defined VMware vCenter user IDs have no permissions to perform tasks in the plugin.

### Configuration overview

Configuration involves the following steps:

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 more information about managing datastores in the vSphere Client, see VMware vSphere Documentation.

# 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 | • VMware vCenter Server Appliance supported versions: 6.7U3J, 7.0U1, 7.0U2, 7.0U3, and 8.0.<br>• NetApp SANtricity OS version: 11.60.2 or higher<br>• Supported application host versions: Windows 2016, Windows 2019, Windows 2022.<br><br>For more information on compatibility, see the NetApp Interoperability Matrix Tool. |
| 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. |

| Requirement | Description |
| --- | --- |
| Capacity planning | Storage Plugin for vCenter requires adequate space for execution and logging. Make sure that your system meets the following available disk space requirements:<br>• Required installation space — 275 MB<br>• Storage space — 275 MB + 200 MB (logging)<br>• System memory — 512 MB |
| 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) | To create a DA-enabled volume, the host connection you are planning to use must support DA.<br>• 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).<br>• 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.<br>• 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. |

| Field | Description |
| --- | --- |
| Drive security | To create a secure-enabled volume, a security key must be created for the storage array.<br>• 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).<br>• 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.<br>• 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.

| 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. |

| Field | Description |
| --- | --- |
| Volume Block Size (EF300 and EF600 only) | Shows the block sizes that can be created for the volume:<br>• 512 – 512 bytes<br>• 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.<br><br>**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.<br><br>**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.<br><br>**Amount of time to change segment size** – The amount of time to change a volume's segment size depends on these variables:<br>• The I/O load from the host<br>• The modification priority of the volume<br>• The number of drives in the volume group<br>• The number of drive channels<br>• The processing power of the storage array controllers<br><br>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.<br>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.<br>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. |

| Field | Description |
| --- | --- |
| **DA** | **Yes** appears next to "DA" only if the drives in the pool or volume group support Data Assurance (DA).<br>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. |

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. |

| Field | Description |
| --- | --- |
| Host ports | Do one of the following:<br>• **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.<br>• **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.<br>You can manually enter the host port identifiers or copy/paste them from the utility (one at a time) into the Host ports field.<br>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:<br>• 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.<br>• Leave the field blank if you do not require host authentication.<br>Currently, the only iSCSI authentication method used is CHAP. |

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 |

| Operation | Possible status of the operation | Actions you can take |
|---|---|---|
| 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 |

# Manage certificates

## Certificates overview

Certificate Management in the Storage Plugin for vCenter allows you to create certificate signing requests (CSRs), import certificates, and manage existing certificates.

### What are certificates?

Certificates are digital files that identify online entities, such as websites and servers, for secure communications on the internet. They ensure that web communications are transmitted in encrypted form, privately and unaltered, only between the specified server and client. Using the Storage Plugin for vCenter, you can manage certificates for the browser on a host management system and the controllers in the discovered storage arrays.

A certificate can be signed by a trusted authority, or it can be self-signed. "Signing" simply means that someone validated the owner's identity and determined that their devices can be trusted.

Storage arrays ship with an automatically generated self-signed certificate on each controller. You can continue to use the self-signed certificates, or you can obtain CA-signed certificates for a more secure connection between the controllers and the host systems.

Although CA-signed certificates provide better security protection (for example, preventing man-in-the-middle attacks), they also require fees that can be expensive if you have a large network. In contrast, self-signed certificates are less secure, but they are free. Therefore, self-signed certificates are most often used for internal testing environments, not in production environments.

### Signed certificates

A signed certificate is validated by a certificate authority (CA), which is a trusted third-party organization. Signed certificates include details about the owner of the entity (typically, a server or website), date of certificate issue and expiration, valid domains for the entity, and a digital signature composed of letters and numbers.

When you open a browser and enter a web address, your system performs a certificate-checking process in the background to determine if you are connecting to a website that includes a valid, CA-signed certificate. Generally, a site that is secured with a signed certificate includes a padlock icon and an https designation in the address. If you attempt to connect to a website that does not contain a CA-signed certificate, your browser

displays a warning that the site is not secure.

The CA takes steps to verify your identity during the application process. They might send an email to your registered business, verify your business address, and perform an HTTP or DNS verification. When the application process is complete, the CA sends you digital files to load on a host management system. Typically, these files include a chain of trust, as follows:

- **Root** — At the top of the hierarchy is the root certificate, which contains a private key used to sign other certificates. The root identifies a particular CA organization. If you use the same CA for all your network devices, you need only one root certificate.
- **Intermediate** — Branching off from the root are the intermediate certificates. The CA issues one or more intermediate certificates to act as middlemen between a protected root and server certificates.
- **Server** — At the bottom of the chain is the server certificate, which identifies your specific entity, such as a website or other device. Each controller in a storage array requires a separate server certificate.

#### Self-signed certificates

Each controller in the storage array includes a pre-installed, self-signed certificate. A self-signed certificate is similar to a CA-signed certificate, except that it is validated by the owner of the entity instead of a third party. Like a CA-signed certificate, a self-signed certificate contains its own private key, and also ensures that data is encrypted and sent over an HTTPS connection between a server and client.

Self-signed certificates are not “trusted” by browsers. Each time you attempt to connect to a website that contains only a self-signed certificate, the browser displays a warning message. You must click a link in the warning message that allows you to proceed to the website; by doing so, you are essentially accepting the self-signed certificate.

#### Management certificate

When you open the plugin, the browser attempts to verify that the management host is a trusted source by checking for a digital certificate. If the browser does not locate a CA-signed certificate, it opens a warning message. From there, you can continue to the website to accept the self-signed certificate for that session. You can also obtain signed, digital certificates from a CA so you no longer see the warning message.

#### Trusted certificates

During a plugin session, you might see additional security messages when you attempt to access a controller that does not have a CA-signed certificate. In this event, you can permanently trust the self-signed certificate or you can import the CA-signed certificates for the controllers so the plugin can authenticate incoming client requests from these controllers.

## Use CA-signed certificates

You can obtain and import CA-signed certificates for secure access to the management system hosting the Storage Plugin for vCenter.

Using CA-signed certificates is a three-step procedure:

- Step 1: Complete a CSR file.
- Step 2: Submit CSR file.
- Step 3: Import management certificates.

### Step 1: Complete a CSR file

You must first generate a certificate signing request (CSR) file, which identifies your organization and the host system where the plugin is running. Alternatively, you can generate a CSR file using a tool such as OpenSSL and skip to Step 2: Submit CSR file.

#### Steps

1. Select **Certificate Management**.
2. From the **Management** tab, select **Complete CSR**.
3. Enter the following information, and then click **Next**:
   - **Organization** — The full, legal name of your company or organization. Include suffixes, such as Inc. or Corp.
   - **Organizational unit (optional)** — The division of your organization that is handling the certificate.
   - **City/Locality** — The city where your host system or business is located.
   - **State/Region (optional)** — The state or region where your host system or business is located.
   - **Country ISO code** — Your country's two-digit ISO (International Organization for Standardization) code, such as US.
4. Enter the following information about the host system where the plugin is running:
   - **Common name** — The IP address or DNS name of the host system where the plugin is running. Make sure this address is correct; it must match exactly what you enter to access the plugin in the browser. Do not include http:// or https://. The DNS name cannot begin with a wildcard.
   - **Alternate IP addresses** — If the common name is an IP address, you can optionally enter any additional IP addresses or aliases for the host system. For multiple entries, use a comma-delimited format.
   - **Alternate DNS names** — If the common name is a DNS name, enter any additional DNS names for the host system. For multiple entries, use a comma-delimited format. If there are no alternate DNS names, but you entered a DNS name in the first field, copy that name here. The DNS name cannot begin with a wildcard.
5. Make sure that the host information is correct. If it is not, the certificates returned from the CA will fail when you try to import them.
6. Click **Finish**.

### Step 2: Submit CSR file

After you create a certificate signing request (CSR) file, you send the generated CSR file to a CA to receive signed, management certificates for the system hosting the plugin.

E-Series systems require PEM format (Base64 ASCII encoding) for signed certificates, which includes the following file types: .pem, .crt, .cer, or .key.

#### Steps

1. Locate the downloaded CSR file.

   The folder location of the download depends on your browser.

2. Submit the CSR file to a CA (for example, Verisign or DigiCert), and request signed certificates in PEM format.

After you submit a CSR file to the CA, do NOT regenerate another CSR file.

Whenever you generate a CSR, the system creates a private and public key pair. The public key is part of the CSR, while the private key is kept in the system's keystore. When you receive the signed certificates and import them, the system ensures that both the private and public keys are the original pair. If the keys do not match, the signed certificates will not work and you must request new certificates from the CA.

#### Step 3: Import management certificates

After you receive signed certificates from the Certificate Authority (CA), import the certificates into the host system where the plugin is installed.

**Before you begin**

- You must have the signed certificates from the CA. These files include the root certificate, one or more intermediate certificates, and the server certificate.
- If the CA provided a chained certificate file (for example, a .p7b file), you must unpack the chained file into individual files: the root certificate, one or more intermediate certificates, and the server certificate. You can use the Windows certmgr utility to unpack the files (right-click and select **All Tasks › Export**). Base-64 encoding is recommended. When the exports are complete, a CER file is shown for each certificate file in the chain.
- You must copy the certificate files to the host system where the plugin is running.

**Steps**

1. Select **Certificate Management**.
2. From the **Management** tab, select **Import**.

   A dialog box opens for importing the certificate files.

3. Click **Browse** to first select the root and intermediate certificate files, and then select the server certificate. If you generated the CSR from an external tool, you must also import the private key file that was created along with the CSR.

   The filenames are displayed in the dialog box.

4. Click **Import**.

**Result**

The files are uploaded and validated. The certificate information displays on the Certificate Management page.

## Reset management certificates

For the management system hosting the Storage Plugin for vCenter, you can revert the management certificate to the original, factory self-signed state.

**About this task**

This task deletes the current management certificate from the host system where the Storage Plugin for vCenter is running. After the certificate is reset, the host system reverts to using the self-signed certificate.

**Steps**

1. Select **Certificate Management**.

2. From the **Management** tab, select **Reset**.

   A Confirm Reset Management Certificate dialog box opens.

3. Type reset in the field, and then click **Reset**.

   After your browser refreshes, the browser might block access to the destination site and report that the site is using HTTP Strict Transport Security. This condition arises when you switch back to self-signed certificates. To clear the condition that is blocking access to the destination, you must clear the browsing data from the browser.

**Result**

The system reverts to using the self-signed certificate from the server. As a result, the system prompts users to manually accept the self-signed certificate for their sessions.

## Import certificates for arrays

If necessary, you can import certificates for the storage arrays so they can authenticate with the system hosting the Storage Plugin for vCenter. Certificates can be signed by a certificate authority (CA) or can be self-signed.

**Before you begin**

If you are importing trusted certificates, the certificates must be imported for the storage array controllers using System Manager.

**Steps**

1. Select **Certificate Management**.
2. Select the **Trusted** tab.

   This page shows all certificates reported for the storage arrays.

3. Select either **Import › Certificates** to import a CA certificate or **Import › Self-signed storage array certificates** to import a self-signed certificate.
4. To limit the view, you can use the **Show certificates that are…** filtering field or you can sort the certificate rows by clicking one of the column heads.
5. In the dialog box, select the certificate and then click **Import**.

   The certificate is uploaded and validated.

## View certificates

You can view summary information for a certificate, which includes the organization using the certificate, the authority that issued the certificate, the period of validity, and the fingerprints (unique identifiers).

**Steps**

1. Select **Certificate Management**.
2. Select one of the following tabs:
   - **Management** — Shows the certificate for the system hosting the plugin. A management certificate can

be self-signed or approved by a certificate authority (CA). It allows secure access to the plugin.

- **Trusted** — Shows certificates that the plugin can access for storage arrays and other remote servers, such as an LDAP server. The certificates can be issued from a certificate authority (CA) or can be self-signed.

3. To see more information about a certificate, select its row, select the ellipses at the end of the row, and then click **View** or **Export**.

## Export certificates

You can export a certificate to view its complete details.

### Before you begin

To open the exported file, you must have a certificate viewer application.

### Steps

1. Select **Certificate Management**.
2. Select one of the following tabs:
   - **Management** — Shows the certificate for the system hosting the plugin. A management certificate can be self-signed or approved by a certificate authority (CA). It allows secure access to the plugin.
   - **Trusted** — Shows certificates that the plugin can access for storage arrays and other remote servers, such as an LDAP server. The certificates can be issued from a certificate authority (CA) or can be self-signed.
3. Select a certificate from the page, and then click the ellipses at the end of the row.
4. Click **Export**, and then save the certificate file.
5. Open the file in your certificate viewer application.

## Delete trusted certificates

You can delete one or more certificates that are no longer needed, such as an expired certificate.

### Before you begin

Import the new certificate before deleting the old one.

Be aware that deleting a root or intermediate certificate can impact multiple storage arrays, since these arrays can share the same certificate files.

### Steps

1. Select **Certificate Management**.
2. Select the **Trusted** tab.
3. Select one or more certificates in the table, and then click **Delete**.

   The Delete function is not available for pre-installed certificates.

   The Confirm Delete Trusted Certificate dialog box opens.

4. Confirm the deletion, and then click **Delete**.

The certificate is removed from the table.

## Resolve untrusted certificates

From the Certificate page, you can resolve untrusted certificates by importing a self-signed certificate from the storage array or by importing a certificate authority (CA) certificate that has been issued by a trusted third party.

**Before you begin**

If you plan to import a CA-signed certificate, make sure that:

- You have generated a certificate signing request (.CSR file) for each controller in the storage array and sent it to the CA.
- The CA returned trusted certificate files.
- The certificate files are available on your local system.

**About this task**

Untrusted certificates occur when a storage array attempts to establish a secure connection to the plugin, but the connection fails to confirm as secure. You might need to install additional trusted CA certificates if any of the following are true:

- You recently added a storage array.
- One or both certificates are expired or revoked.
- One or both certificates are missing a root or intermediate certificate.

**Steps**

1. Select **Certificate Management**.
2. Select the **Trusted** tab.

   This page shows all certificates reported for the storage arrays.

3. Select either **Import › Certificates** to import a CA certificate or **Import › Self-Signed storage array certificates** to import a self-signed certificate.
4. To limit the view, you can use the **Show certificates that are…** filtering field or you can sort the certificate rows by clicking one of the column heads.
5. In the dialog box, select the certificate, and then click **Import**.

   The certificate is uploaded and validated.

# Manage arrays

## Array management overview

Use the Add/Discover feature to find and add the storage arrays you want to manage in the Storage plugin for vCenter. From the Manage page, you can also rename, remove, and provide new passwords for these discovered arrays.

## Considerations for discovering arrays

For the plugin to display and manage storage resources, you must discover the storage arrays you want to manage in your organization's network. You can discover and then add a single array or multiple arrays.

#### Multiple storage arrays

If you choose to discover multiple arrays, you enter a network IP address range and then the system attempts individual connections to each IP address in that range. Any storage array successfully reached appears in the plugin and you can then add them to your management domain.

#### Single storage array

If you choose to discover a single array, you enter the single IP address for one of the controllers in the storage array and then add that array to your management domain.

> The plugin discovers and displays only the single IP address or IP address within a range assigned to a controller. If there are alternate controllers or IP addresses assigned to these controllers that fall outside of this single IP address or IP address range, then the plugin will not discover or display them. However, once you add the storage array, all associated IP addresses will be discovered and displayed in the Manage view.

#### User credentials

You must supply the administrator password for each storage array you want to add.

#### Certificates

As part of the discovery process, the system verifies that the discovered storage arrays are using certificates by a trusted source. The system uses two types of certificate-based authentication for all connections that it establishes with the with the browser:

- **Trusted certificates** — You might need to install additional trusted certificates supplied by the Certificate Authority if one or both controller certificates are expired, revoked, or missing a certificate in its chain.
- **Self-signed certificates** — Arrays can also use self-signed certificates. If you attempt to discover arrays without importing signed certificates, the plugin provides an additional step that allows you to accept the self-signed certificate. The storage array's self-signed certificate will be marked as trusted and the storage array will be added to the plugin. If you do not trust the connections to the storage array, select **Cancel** and validate the storage array's security certificate strategy before adding the storage array to the plugin.

## Storage array status

When you open the Storage Plugin for vCenter, communication with each storage array is established and the status for each storage array is displayed.

From the **Manage - All** page, you can view the status of the storage array and the status of the storage array connection.

| Status | Indicates |
| --- | --- |
| Optimal | The storage array is in an optimal state. There are no certificate issues and the password is valid. |
| Invalid Password | An invalid storage array password was provided. |

| Status | Indicates |
| --- | --- |
| Untrusted Certificate | One or more connections with the storage array is untrusted because the HTTPS certificate is either self-signed and has not been imported, or the certificate is CA-signed and the root and intermediate CA certificates have not been imported. |
| Needs Attention | There is a problem with the storage array that requires your intervention to correct it. |
| Lockdown | The storage array is in a locked-down state. |
| Unknown | The storage array has never been contacted. This can happen when the plugin is starting up and has not yet made contact with the storage array, or the storage array is offline and has never been contacted since the plugin was started. |
| Offline | The plugin had previously contacted the storage array, but now has lost all connection to it. |

**Plugin interface compared to System Manager**

You can use Storage Plugin for vCenter for basic operating tasks on your storage array; however, there might be times when you need to launch System Manager to perform tasks not available in the plugin.

System Manager is an embedded application on the storage array's controller, which is connected to the network through an Ethernet management port. System Manager includes all array-based functions.

The following table helps you decide whether you can use the plugin interface or the System Manager interface for a particular storage array task.

| Function | Plugin interface | System Manager interface |
| --- | --- | --- |
| Batch operations on groups of multiple storage arrays | Yes | No. Operations are performed on a single array. |
| Upgrades for the SANtricity OS firmware | Yes. One or more arrays in a batch operation. | Yes. Single array only. |
| Import settings from one array to multiple arrays | Yes | No |
| Host and host cluster management (create, assign volumes, update, and delete) | Yes | Yes |
| Pools and volume group management (create, update, enable security, and delete) | Yes | Yes |
| Volume management (create, resize, update, and delete) | Yes | Yes |
| SSD Cache management (create, update, and delete) | Yes | Yes |

| Function | Plugin interface | System Manager interface |
|---|---|---|
| Mirroring and snapshot management | No | Yes |
| Hardware management (view controller status, configure port connections, take controller offline, enable hot spares, erase drives, etc.) | No | Yes |
| Manage alerts (email, SNMP, and syslog) | No | Yes |
| Security key management | No | Yes |
| Certificate management for controllers | No | Yes |
| Access management for controllers (LDAP, SAML, etc.) | No | Yes |
| AutoSupport management | No | Yes |

## Discover storage arrays

To display and manage storage resources in the Storage Plugin for vCenter, you must 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.
- Storage array passwords must be set up using System Manager's Access Management tile.

**About this task**

Array discovery is a multi-step procedure:

- Step 1: Enter network addresses for discovery
- Step 2: Resolve untrusted certificates during discovery
- Step 3: Provide passwords

### Step 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.

**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 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.
6. 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 dialogs and go to Import certificates for arrays.

### Step 2: Resolve untrusted certificates during discovery

If necessary, you must resolve any certificate issues before proceeding with the discovery process.

During discovery, if any storage arrays show an "Untrusted Certificates" status, the Resolve Self-Signed Certificates dialog box appears. You can resolve untrusted certificates in this dialog, or you can import CA certificates (see Import certificates for arrays).

#### Steps

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 card in the wizard. The self-signed certificates will be 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 to the plugin.

### 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.

#### Steps

1. Optionally, if you have previously configured groups for the arrays, you can use the drop-down to select a

group for the discovered arrays.

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

> It can take several minutes for the system to connect to the specified storage arrays.

**Result**

The storage arrays are added to your management domain and associated with the selected group (if specified).

> You can use the Launch option to open the browser-based System Manager for one or more storage arrays when you want to perform management operations.

## Rename storage array

You can change the storage array's name displayed on the Manage page of the Storage Plugin for vCenter.

**Steps**

1. From the **Manage** page, select the checkbox to the left of the storage array name.
2. Select the ellipses at the far right of the row, and then select **Rename storage array** from the pop-up menu.
3. Enter the new name and click **Save**.

## Change storage array passwords

You can update the passwords used for viewing and accessing storage arrays in the Storage Plugin for vCenter.

**Before you begin**

You must know the current password for the storage array, which is set in System Manager.

**About this task**

In this task, you enter the current password for a storage array so you can access it in the plugin. This might be necessary if the array password was changed in System Manager.

**Steps**

1. From the **Manage** page, select one or more storage arrays.
2. Select **Uncommon Tasks › Provide storage array passwords**.
3. Enter the password or passwords for each storage array, and then click **Save**.

## Remove storage arrays

You can remove one or more storage arrays if you no longer want to manage it from the Storage Plugin for vCenter.

**About this task**

You cannot access any of the storage arrays you remove. You can, however, establish a connection to any of the removed storage arrays by pointing a browser directly to its IP address or host name.

Removing a storage array does not affect the storage array or its data in any way. If a storage array is accidentally removed, it can be added again.

**Steps**

1. From the **Manage** page, select one or more storage arrays that you want to remove.
2. Select **Uncommon Tasks › Remove storage arrays**.

   The storage array is removed from all the views in the plugin interface.

### Launch System Manager

To manage a single array, use the Launch option to open SANtricity System Manager in a new browser window.

System Manager is an embedded application on the storage array's controller, which is connected to the network through an Ethernet management port. System Manager includes all array-based functions. To access System Manager, you must have an out-of-band connection to a network management client with a web browser.

**Steps**

1. From the **Manage** page, select one or more storage arrays that you want to manage.
2. Click **Launch**.

   The system opens a new tab in the browser, and then displays the System Manager login page.

3. Enter your username and password, and then click **Log in**.

# Import settings

## Import settings overview

The Import Settings feature is a batch operation that allows you to replicate the settings in a single storage array (the source) to multiple arrays (the targets) in the Storage Plugin for vCenter.

#### Settings available for import

The following configurations can be imported from one array to another:

- **Alerts** — Alerting methods to send important events to administrators using email, a syslog server, or an SNMP server.
- **AutoSupport** — A feature that monitors the health of a storage array and sends automatic dispatches to technical support.
- **Directory services** — A method of user authentication that is managed through an LDAP (Lightweight Directory Access Protocol) server and directory service, such as Microsoft's Active Directory.
- **System settings** — Configurations relating to the following:

    - Media scan settings for a volume
    - SSD settings
    - Automatic load balancing (does not include host connectivity reporting)
- **Storage configuration** — Configurations relating to the following:
    - Volumes (thick and non-repository volumes only)
    - Volume groups and pools
    - Hot spare drive assignments

### Configuration workflow

To import settings, follow this workflow:

1. On a storage array to be used as the source, configure the settings using System Manager.
2. On the storage arrays to be used as the targets, back up their configuration using System Manager.
3. From the plugin interface, go to the **Manage** page and import the settings.
4. From the Operations page, review the results of the Import Settings operation.

### Requirements for replicating storage configurations

Before importing a storage configuration from one storage array to another, review the requirements and guidelines.

#### Shelves

- The shelves where the controllers reside must be identical on the source and target arrays.
- Shelf IDs must be identical on the source and target arrays.
- Expansion shelves must be populated in the same slots with the same drive types (if the drive is used in the configuration, the location of unused drives does not matter).

#### Controllers

- The controller type can be different between the source and target arrays, but the RBOD enclosure type must be identical.
- The HICs, including the DA capabilities of the host, must be identical between the source and target arrays.
- Importing from a duplex to simplex configuration is not supported; however, importing from simplex to duplex is allowed.
- FDE settings are not included in the import process.

#### Status

- The target arrays must be in Optimal status.
- The source array does not need to be in Optimal status.

#### Storage

- Drive capacity may vary between the source and target arrays, as long as the volume capacity on the target is larger than the source. (A target array might have newer, larger capacity drives that would not be fully configured into volumes by the replication operation.)

- Disk pool volumes 64 TB or larger on the source array will prevent the import process on the targets.

## Import alert settings

You can import alert configurations from one storage array to other storage arrays. This batch operation saves time when you need to configure multiple arrays in the network.

### Before you begin

Make sure that:

- Alerts are configured in System Manager (**Settings › Alerts**) for the storage array you want to use as the source.
- The existing configuration for the target storage arrays are backed up in System Manager (**Settings › System › Save Storage Array Configuration**).
- You have reviewed the requirements for replicating storage configurations in Import settings overview.

### About this task

You can select email, SNMP, or syslog alerts for the import operation:

- **Email alerts** — A mail server address and the email addresses of the alert recipients.
- **Syslog alerts** — A syslog server address and a UDP port.
- **SNMP alerts** — A community name and IP address for the SNMP server.

### Steps

1. From the Manage page, click **Actions › Import Settings**.

   The Import Settings wizard opens.

2. In the Select Settings dialog, select either **Email alerts**, **SNMP alerts**, or **Syslog alerts**, and then click **Next**.

   A dialog box opens for selecting the source array.

3. In the Select Source dialog, select the array with the settings you want to import, and then click **Next**.
4. In the Select Targets dialog, select one or more arrays to receive the new settings.

   Storage arrays with firmware below 8.50 are not available for selection. In addition, an array does not appear in this dialog if the plugin cannot communicate with that array (for example, if it is offline or if it has certificate, password, or networking problems).

5. Click **Finish**.

   The Operations page displays the results of the import operation. If the operation fails, you can click on its row to see more information.

### Result

The target storage arrays are now configured to send alerts to administrators through email, SNMP, or syslog.

## Import AutoSupport settings

You can import an AutoSupport configuration from one storage array to other storage arrays. This batch operation saves time when you need to configure multiple arrays in the network.

### Before you begin

Make sure that:

- AutoSupport is configured in System Manager (**Support › Support Center**) for the storage array you want to use as the source.
- The existing configuration for the target storage arrays are backed up in System Manager (**Settings › System › Save Storage Array Configuration**).
- You have reviewed the requirements for replicating storage configurations in Import settings overview.

### About this task

Imported settings include the separate features (Basic AutoSupport, AutoSupport OnDemand, and Remote Diagnostics), the maintenance window, delivery method, and dispatch schedule.

### Steps

1. From the Manage page, click **Actions › Import Settings**.

   The Import Settings wizard opens.

2. In the Select Settings dialog, select **AutoSupport** and then click **Next**.

   A dialog box opens for selecting the source array.

3. In the Select Source dialog, select the array with the settings you want to import, and then click **Next**.
4. In the Select Targets dialog, select one or more arrays to receive the new settings.

   Storage arrays with firmware below 8.50 are not available for selection. In addition, an array does not appear in this dialog if the plugin cannot communicate with that array (for example, if it is offline or if it has certificate, password, or networking problems).

5. Click **Finish**.

   The Operations page displays the results of the import operation. If the operation fails, you can click on its row to see more information.

### Result

The target storage arrays are now configured with the same AutoSupport settings as the source array.

## Import directory services settings

You can import a directory services configuration from one storage array to other storage arrays. This batch operation saves time when you need to configure multiple arrays in the network.

### Before you begin

Make sure that:

- Directory services are configured in System Manager (**Settings › Access Management**) for the storage array you want to use as the source.
- The existing configuration for the target storage arrays are backed up in System Manager (**Settings › System › Save Storage Array Configuration**).
- You have reviewed the requirements for replicating storage configurations in Import settings overview.

**About this task**

Imported settings include the domain name and URL of an LDAP (Lightweight Directory Access Protocol) server, along with the mappings for the LDAP server's user groups to the storage array's predefined roles.

**Steps**

1. From the Manage page, click **Actions › Import Settings**.

   The Import Settings wizard opens.

2. In the Select Settings dialog, select **Directory services** and then click **Next**.

   A dialog box opens for selecting the source array.

3. In the Select Source dialog, select the array with the settings you want to import, and then click **Next**.
4. In the Select Targets dialog, select one or more arrays to receive the new settings.

   Storage arrays with firmware below 8.50 are not available for selection. In addition, an array does not appear in this dialog if the plugin cannot communicate with that array (for example, if it is offline or if it has certificate, password, or networking problems).

5. Click **Finish**.

   The Operations page displays the results of the import operation. If the operation fails, you can click on its row to see more information.

**Result**

The target storage arrays are now configured with the same directory services as the source array.

## Import system settings

You can import the system settings from one storage array to other storage arrays. This batch operation saves time when you need to configure multiple arrays in the network.

**Before you begin**

Make sure that:

- System settings are configured in System Manager for the storage array you want to use as the source.
- The existing configuration for the target storage arrays are backed up in System Manager (**Settings › System › Save Storage Array Configuration**).
- You have reviewed the requirements for replicating storage configurations in Import settings overview.

**About this task**

Imported settings include media scan settings for a volume, SSD settings for controllers, and automatic load balancing (does not include host connectivity reporting).

**Steps**

1. From the Manage page, click **Actions › Import Settings**.

   The Import Settings wizard opens.

2. In the Select Settings dialog, select **System** and then click **Next**.

   A dialog box opens for selecting the source array.

3. In the Select Source dialog, select the array with the settings you want to import, and then click **Next**.
4. In the Select Targets dialog, select one or more arrays to receive the new settings.

   > Storage arrays with firmware below 8.50 are not available for selection. In addition, an array does not appear in this dialog if the plugin cannot communicate with that array (for example, if it is offline or if it has certificate, password, or networking problems).

5. Click **Finish**.

   The Operations page displays the results of the import operation. If the operation fails, you can click on its row to see more information.

**Result**

The target storage arrays are now configured with the same system settings as the source array.

## Import storage configuration settings

You can import the storage configuration from one storage array to other storage arrays. This batch operation saves time when you need to configure multiple arrays in the network.

**Before you begin**

Make sure that:

- Storage is configured in System Manager for the storage array you want to use as the source.
- The existing configuration for the target storage arrays are backed up in System Manager (**Settings › System › Save Storage Array Configuration**).
- You have reviewed the requirements for replicating storage configurations in Import settings overview.
- The source and target arrays must meet these requirements:
  - The shelves where the controllers reside must be identical.
  - Shelf IDs must be identical.
  - Expansion shelves must be populated in the same slots with the same drive types.
  - The RBOD enclosure type must be identical.
  - The HICs, including the Data Assurance capabilities of the host, must be identical.
  - The target arrays must be in Optimal status.

- The volume capacity on the target array is larger than the source array's capacity.

- You understand the following restrictions:
  - Importing from a duplex to simplex configuration is not supported; however, importing from simplex to duplex is allowed.
  - Disk pool volumes 64 TB or larger on the source array will prevent the import process on the targets.

**About this task**

Imported settings include configured volumes (thick and non-repository volumes only), volume groups, pools, and hot spare drive assignments.

**Steps**

1. From the Manage page, click **Actions › Import Settings**.

   The Import Settings wizard opens.

2. In the Select Settings dialog, select **Storage configuration** and then click **Next**.

   A dialog box opens for selecting the source array.

3. In the Select Source dialog, select the array with the settings you want to import, and then click **Next**.
4. In the Select Targets dialog, select one or more arrays to receive the new settings.

   Storage arrays with firmware below 8.50 are not available for selection. In addition, an array does not appear in this dialog if the plugin cannot communicate with that array (for example, if it is offline or if it has certificate, password, or networking problems).

5. Click **Finish**.

   The Operations page displays the results of the import operation. If the operation fails, you can click on its row to see more information.

**Result**

The target storage arrays are now configured with the same storage configuration as the source array.

# Manage array groups

## Array groups overview

You can manage your physical and virtualized infrastructure in the Storage Plugin for vCenter by grouping a set of storage arrays. You might want to group storage arrays to make it easier to run monitoring or reporting jobs.

Types of storage array groups:

- **All group** — The All group is the default group and includes all the storage arrays discovered in your organization. The All group can be accessed from the main view.
- **User-created group** — A user-created group includes the storage arrays that you manually select to add to that group. User-created groups can be accessed from the main view.

## Create storage array group

You create storage groups, and then add storage arrays to the groups. The storage group defines which drives provide the storage that makes up the volume.

### Steps

1. From the Manage page, select **Manage Groups › Create storage array group**.
2. In the **Name** field, type a name for the new group.
3. Select the storage arrays that you want to add to the new group.
4. Click **Create**.

## Add storage array to group

You can add one or more storage arrays to a user-created group.

### Steps

1. From the main view, select **Manage**, and then select the group that you want to add storage arrays to.
2. Select **Manage Groups › Add storage arrays to group**.
3. Select the storage arrays that you want to add to the group.
4. Click **Add**.

## Rename storage array group

You can change the name of a storage array group when the current name is no longer meaningful or applicable.

### About this task

Keep these guidelines in mind.

- A name can consist of letters, numbers, and the special characters underscore (_), hyphen (-), and pound (#). If you choose any other characters, an error message appears. You are prompted to choose another name.
- Limit the name to 30 characters. Any leading and trailing spaces in the name are deleted.
- Use a unique, meaningful name that is easy to understand and remember.
- Avoid arbitrary names or names that would quickly lose their meaning in the future.

### Steps

1. From the main view, select **Manage**, and then select the storage array group you want to rename.
2. Select **Manage Groups › Rename storage array group**.
3. In the **Group Name** field, type a new name for the group.
4. Click **Rename**.

## Remove storage arrays from group

You can remove one or more managed storage arrays from a group if you no longer want to manage it from a specific storage group.

### About this task

Removing storage arrays from a group does not affect the storage array or its data in any way. If your storage array is managed by System Manager, you can still manage it using your browser. If a storage array is accidentally removed from a group, it can be added again.

### Steps

1. From the Manage page, select **Manage Groups › Remove storage arrays from group**.
2. From the drop-down, select the group that contains the storage arrays you want to remove, and then click the check box next to each storage array that you want to remove from the group.
3. Click **Remove**.

## Delete storage array group

You can remove one or more storage array groups that are no longer needed.

### About this task

This operation deletes only the storage array group. Storage arrays associated with the deleted group remain accessible through the Manage All view or any other group it is associated with.

### Steps

1. From the Manage page, select **Manage Groups › Delete storage array group**.
2. Select one or more storage array groups that you want to delete.
3. Click **Delete**.

# Upgrade OS software

## Upgrade overview

In the Storage Plugin for vCenter, you can manage SANtricity software and NVSRAM upgrades for multiple storage arrays of the same type.

### Upgrade workflow

The following steps provide a high-level workflow for performing software upgrades:

1. You download the latest SANtricity OS file from the support site (a link is available from the Support page). Save the file on the management host system (the host where you access the plugin in a browser), and then unzip the file.
2. In the plugin, you can load the SANtricity OS software file and the NVSRAM file into the repository (an area of the server where files are stored).
3. After the files are loaded in the repository, you can then select the file to be used in the upgrade. From the Upgrade SANtricity OS Software page, you select the OS software file and the NVSRAM file. After you select a software file, a list of compatible storage arrays appear on this page. You then select the storage

arrays that you want to upgrade with the new software. (You cannot select incompatible arrays.)

4. You can then begin an immediate software transfer and activation, or you can choose to stage the files for activation at a later time. During the upgrade process, the plugin performs the following tasks:
   - Performs a health check on the storage arrays to determine if any conditions exist that might prevent the upgrade from completing. If any arrays fail the health check, you can skip that particular array and continue the upgrade for the others, or you can stop the entire process and troubleshoot the arrays that did not pass.
   - Transfers the upgrade files to each controller.
   - Reboots the controllers and activates the new OS software, one controller at a time. During activation, the existing OS file is replaced with the new file.

You can also specify that the software is activated at a later time.

### Upgrade considerations

Before you upgrade multiple storage arrays, review the key considerations as part of your planning.

#### Current versions

You can view the current SANtricity OS software versions from the Manage page of the Storage Plugin for vCenter for each discovered storage array. The version is shown in the SANtricity OS Software column. The controller firmware and NVSRAM information is available in a pop-up dialog box when you click on the OS version in each row.

#### Other components requiring upgrade

As part of the upgrade process, you might also need to upgrade the host's multipath/failover driver or the HBA driver so that the host can interact with the controllers correctly. For compatibility information, refer to the Interoperability Matrix Tool.

#### Dual controllers

If a storage array contains two controllers and you have a multipath driver installed, the storage array can continue to process I/O while the upgrade occurs. During the upgrade, the following process occurs:

1. Controller A fails over all its LUNs to controller B.
2. Upgrade occurs on controller A.
3. Controller A takes back its LUNs and all of controller B's LUNs.
4. Upgrade occurs on controller B.

After the upgrade completes, you might need to manually redistribute volumes between the controllers to ensure volumes return to the correct owning controller.

## Perform pre-upgrade health check

A health check runs as part of the upgrade process, but you also can run a health check separately before you begin. The health check assesses components of the storage array to make sure that the upgrade can proceed.

### Steps

1. From the main view, select **Manage**, and then select **Upgrade Center › Pre-Upgrade Health Check**.

   The Pre-Upgrade Health Check dialog box opens and lists all the discovered storage systems.

2. If needed, filter or sort the storage systems in the list, so you can view all systems that are not currently in the Optimal state.
3. Select the check boxes for the storage systems that you want to run through the health check.
4. Click **Start**.

   The progress is shown in the dialog box while the health check is performed.

5. When the health check completes, you can click on the ellipses (…) to the right of each row to view more information and perform other tasks.

If any arrays fail the health check, you can skip that particular array and continue the upgrade for the others, or you can stop the entire process and troubleshoot the arrays that did not pass.

## Upgrade SANtricity OS

Upgrade one or more storage arrays with the latest software and NVSRAM to make sure that you have all the latest features and bug fixes. Controller NVSRAM is a controller file that specifies the default settings for the controllers.

**Before you begin**

Make sure that:

- The latest SANtricity OS files are available on the host system where the plugin is running.
- You know whether you want to activate your software upgrade now or later. You might choose to activate later for these reasons:
  - **Time of day** — Activating the software can take a long time, so you might want to wait until I/O loads are lighter. The controllers fail over during activation, so performance might be lower than usual until the upgrade completes.
  - **Type of package** — You might want to test the new OS software on one storage array before you upgrade the files on other storage arrays.

**Risk of data loss or risk of damage to the storage array** — Do not make changes to the storage array while the upgrade is occurring. Maintain power to the storage array.

**Steps**

1. If your storage array contains only one controller or a multipath driver is not in use, stop I/O activity to the storage array to prevent application errors. If your storage array has two controllers and you have a multipath driver installed, you do not need to stop I/O activity.
2. From the main view, select **Manage**, and then select one or more storage arrays that you want to upgrade.
3. Select **Upgrade Center › Upgrade › SANtricity OS › Software**.

   The Upgrade SANtricity OS software page appears.

4. Download the latest SANtricity OS software package from the Support site to your local machine.

a. Click Add new file to software repository
b. Click the link for finding the latest SANtricity OS downloads.
c. Click the **Download Latest Release** link.
d. Follow the remaining instructions to download the OS file and the NVSRAM file to your local machine.

> Digitally signed firmware is required in version 8.42 and above. If you attempt to download unsigned firmware, an error is displayed and the download is aborted.

5. Select the OS software file and the NVSRAM file that you want to use to upgrade the controllers:
   a. From the drop-down, select the OS file that you downloaded to your local machine.

      If there are multiple files available, the files are sorted from newest date to oldest date.

      > The software repository lists all software files associated with the plugin. If you do not see the file that you want to use, you can click the link, **Add new file to software repository**, to browse to the location where the OS file that you want to add resides.

   b. From the **Select an NVSRAM file** drop-down, select the controller file that you want to use.

      If there are multiple files, the files are sorted from newest date to oldest date.

6. In the Compatible Storage Array table, review the storage arrays that are compatible with the OS software file that you selected, and then select the arrays you want to upgrade.
   - The storage arrays that you selected in the Manage view and that are compatible with the selected firmware file are selected by default in the Compatible Storage Array table.
   - The storage arrays that cannot be updated with the selected firmware file are not selectable in the Compatible Storage Array table as indicated by the status **Incompatible**.
7. (Optional) To transfer the software file to the storage arrays without activating them, select the **Transfer the OS software to the storage arrays, mark it as staged, and activate at a later time** check box.
8. Click **Start**.
9. Depending on whether you chose to activate now or later, do one of the following:
   - Type `TRANSFER` to confirm that you want to transfer the proposed OS software versions on the arrays you selected to upgrade, and then click **Transfer**. To activate the transferred software, select **Upgrade Center › Activate Staged SANtricity OS Software**.
   - Type `UPGRADE` to confirm that you want to transfer and activate the proposed OS software versions on the arrays you selected to upgrade, and then click **Upgrade**.

     The system transfers the software file to each storage array you selected to upgrade and then activates that file by initiating a reboot.

     The following actions occur during the upgrade operation:

   - A pre-upgrade health check runs as part of the upgrade process. The pre-upgrade health check assesses all storage array components to make sure that the upgrade can proceed.
   - If any health check fails for a storage array, the upgrade stops. You can click the ellipsis (…) and select **Save Log** to review the errors. You can also choose to override the health check error and then click **Continue** to proceed with the upgrade.

- You can cancel the upgrade operation after the pre-upgrade health check.

10. (Optional) Once the upgrade has completed, you can see a list of what was upgraded for a specific storage array by clicking the ellipsis (…) and then selecting **Save Log**.

    The file is saved in the Downloads folder for your browser with the name `upgrade_log-<date>. json`.

## Activate staged OS software

You can choose to activate the software file immediately or wait until a more convenient time. This procedure assumes you chose to activate the software file at a later time.

### About this task

You can transfer the firmware files without activating them. You might choose to activate later for these reasons:

- **Time of day** — Activating the software can take a long time, so you might want to wait until I/O loads are lighter. The controllers reboot and fail over during activation so performance might be lower than usual until the upgrade completes.
- **Type of package** — You might want to test the new software and firmware on one storage array before upgrading the files on other storage arrays.

> ⓘ You cannot stop the activation process after it starts.

### Steps

1. From the main view, select **Manage**. If necessary, click the **Status** column to sort, at the top of the page, all storage arrays with a status of "OS Upgrade (awaiting activation)."
2. Select one or more storage arrays that you want to activate software for, and then select **Upgrade Center › Activate Staged SANtricity Software**.

   The following actions occur during the upgrade operation:

   - A pre-upgrade health check runs as part of the activate process. The pre-upgrade health check assesses all storage array components to make sure that the activation can proceed.
   - If any health check fails for a storage array, the activation stops. You can click the ellipsis (…) and select **Save Log** to review the errors. You can also choose to override the health check error and then click **Continue** to proceed with the activation.
   - You can cancel the activate operation after the pre-upgrade health check.

     On successful completion of the pre-upgrade health check, activation occurs. The time it takes to activate depends on your storage array configuration and the components that you are activating.

3. (Optional) After the activation is complete, you can see a list of what was activated for a specific storage array by clicking the ellipsis (…) and then selecting **Save Log**.

   The file is saved in the Downloads folder for your browser with the name `activate_log-<date>. json`.

## Clear staged OS software

You can remove staged OS software to ensure that a pending version is not inadvertently activated at a later time. Removing the staged OS software does not affect the current version that is running on the storage arrays.

**Steps**

1. From the main view, select **Manage**, and then select **Upgrade Center › Clear Staged SANtricity Software**.

   The Clear Staged SANtricity Software dialog box opens and lists all the discovered storage systems with pending software or NVSRAM.

2. If needed, filter or sort the storage systems in the list, so you can view all systems that have staged software.
3. Select the check boxes for the storage systems with pending software that you want cleared.
4. Click **Clear**.

   The status of the operation is shown in the dialog box.

## Manage software repository

You can view and manage a software repository, which lists all software files associated with the Storage Plugin for vCenter.

**Before you begin**

If you are using the repository to add SANtricity OS files, make sure that the OS files are available on your local system.

**About this task**

You can use the Manage SANtricity OS Software Repository option to import one or more OS files to the host system where the plugin is running. You can also choose to delete one or more OS files that are available in the software repository.

**Steps**

1. From the main view, select **Manage**, and then select **Upgrade Center › Manage SANtricity Software Repository**.

   The Manage SANtricity OS Software Repository dialog appears.

2. Perform one of the following actions:
   - **Import:**
     a. Click **Import**.
     b. Click **Browse**, and then navigate to the location where the OS files you want to add reside. OS files have a filename similar to `N2800-830000-000.dlp`.
     c. Select one or more OS files that you want to add, and then click **Import**.
   - **Delete:**
     a. Select one or more OS files that you want to remove from the software repository.

b. Click **Delete**.

**Result**

If you selected import, the file(s) are uploaded and validated. If you selected delete, the files are removed from the software repository.

# Provision storage

## Provisioning overview

In the Storage Plugin for vCenter, you can create data containers, called volumes, so the host can access storage on the array.

### Volume types and characteristics

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, including FC, iSCSI, and SAS.

Each volume in a pool or volume group can have its own individual characteristics based on what type of data will be stored in it. Some of these characteristics include:

- **Segment size** — A segment is the amount of data in kilobytes (KiB) that is stored on a drive before the storage array moves to the next drive in the stripe (RAID group). The segment size is equal to or less than the capacity of the volume group. The segment size is fixed and cannot be changed for pools.
- **Capacity** — You create a volume from the free capacity available in either a pool or volume group. Before you create a volume, the pool or volume group must already exist, and it must have enough free capacity to create the volume.
- **Controller ownership** — All storage arrays can have either one or two controllers. On a single- controller array, a volume's workload is managed by a single controller. On a dual-controller array, a volume will have a preferred controller (A or B) that "owns" the volume. In a dual- controller configuration, volume ownership is automatically adjusted using the Automatic Load Balancing feature to correct any load balance issues when workloads shift across the controllers. Automatic load balancing provides automated I/O workload balancing and ensures that incoming I/O traffic from the hosts is dynamically managed and balanced across both controllers.
- **Volume assignment** — You can give hosts access to a volume either when you create the volume or at a later time. All host access is managed through a logical unit number (LUN). Hosts detect LUNs that are, in turn, assigned to volumes. If you are assigning a volume to multiple hosts, use clustering software to make sure that the volume is available to all of the hosts.

  The host type can have specific limits on how many volumes the host can access. Keep this limitation in mind when you create volumes for use by a particular host.

- **Resource provisioning** — For EF600 or EF300 storage arrays, you can specify that volumes be put in use immediately with no background initialization process. A resource-provisioned volume is a thick volume in an SSD volume group or pool, where drive capacity is allocated (assigned to the volume) when the volume

is created, but the drive blocks are deallocated (unmapped).

- **Descriptive name** — You can name a volume whatever name you like, but we recommend making the name descriptive.

During volume creation, each volume is allocated capacity and is assigned a name, segment size (volume groups only), controller ownership, and volume-to-host assignment. Volume data is automatically load balanced across controllers, as needed.

## Capacity for volumes

The drives in your storage array provide the physical storage capacity for your data. Before you can begin storing data, you must configure the allocated capacity into logical components known as pools or volume groups. You use these storage objects to configure, store, maintain, and preserve data on your storage array.

#### Capacity to create and expand volumes

You can create volumes from either the unassigned capacity or free capacity in a pool or volume group.

- When you create a volume from unassigned capacity, you can create a pool or volume group and the volume at the same time.
- When you create a volume from free capacity, you are creating an additional volume on an already existing pool or volume group.After you expand the volume capacity, you must manually increase the file system size to match. How you do this depends on the file system you are using. See your host operating system documentation for details.

The plugin interface does not provide an option to create thin volumes.

#### Reported capacity for volumes

The reported capacity of the volume is equal to the amount of physical storage capacity allocated. The entire amount of physical storage capacity must be present. The physically allocated space is equal to the space that is reported to the host.

You normally set the volume's reported capacity to be the maximum capacity to which you think the volume will grow. Volumes provide high and predictable performance for your applications mainly because all of the user capacity is reserved and allocated upon creation.

#### Capacity limits

The minimum capacity for a volume is 1 MiB, and the maximum capacity is determined by the number and capacity of the drives in the pool or volume group.

When increasing reported capacity for a volume, keep the following guidelines in mind:

- You can specify up to three decimal places (for example, 65.375 GiB).
- Capacity needs to be less than (or equal to) the maximum available in the volume group. When you create a volume, some additional capacity is pre-allocated for Dynamic Segment Size (DSS) migration. DSS migration is a feature of the software that allows you to change the segment size of a volume.
- Volumes larger than 2 TiB are supported by some host operating systems (maximum reported capacity is determined by the host operating system). In fact, some host operating systems support up to 128 TiB volumes. Refer to your host operating system documentation for additional details.

## Application-specific workloads

When creating a volume, you select a workload to customize the storage array configuration for a specific application.

A workload is a storage object that supports an application. You can define one or more workloads, or instances, per application. For some applications, the system configures the workload to contain volumes with similar underlying volume characteristics. These volume characteristics are optimized based on the type of application the workload supports. For example, if you create a workload that supports a Microsoft SQL Server application and then subsequently create volumes for that workload, the underlying volume characteristics are optimized to support Microsoft SQL Server.

During volume creation, the system prompts you to answer questions about a workload's use. For example, if you are creating volumes for Microsoft Exchange, you are asked how many mailboxes you need, what your average mailbox capacity requirements are, and how many copies of the database you want. The system uses this information to create an optimal volume configuration for you, which can be edited as needed. Optionally, you can skip this step in the volume creation sequence.

### Types of workloads

You can create two types of workloads: application-specific and other.

- **Application-specific** — When you are creating volumes using an application-specific workload, the system may recommend an optimized volume configuration to minimize contention between application workload I/O and other traffic from your application instance. Volume characteristics like I/O type, segment size, controller ownership, and read and write cache are automatically recommended and optimized for workloads that are created for the following application types.
  - Microsoft SQL Server
  - Microsoft Exchange Server
  - Video Surveillance applications
  - VMware ESXi (for volumes to be used with Virtual Machine File System)

    You can review the recommended volume configuration and edit, add, or delete the system-recommended volumes and characteristics using the Add/Edit Volumes dialog box.
- **Other (or applications without specific volume creation support)** — Other workloads use a volume configuration that you must manually specify when you want to create a workload that is not associated with a specific application, or if the system does not have built-in optimization for the application you intend to use on the storage array. You must manually specify the volume configuration using the Add/Edit Volumes dialog box.

### Application and workload views

To view applications and workloads, launch System Manager. From that interface, you can view information associated with an application-specific workload in a couple of different ways:

- You can select the Applications & Workloads tab in the Volumes tile to view the storage array's volumes grouped by workload and the application type the workload is associated with.
- You can select the Applications & Workloads tab in the Performance tile to view performance metrics (latency, IOPS, and MBs) for logical objects. The objects are grouped by application and associated workload. By collecting this performance data at regular intervals, you can establish baseline measurements and analyze trends, which can help as you investigate problems related to I/O performance.

## Create storage

In the Storage Plugin for vCenter, you create storage by first creating a workload for a specific application type. Next, you add storage capacity to the workload by creating volumes with similar underlying volume characteristics.

### Step 1: Create workloads

A workload is a storage object that supports an application. You can define one or more workloads, or instances, per application.

#### About this task

For some applications, the system configures the workload to contain volumes with similar underlying volume characteristics. These volume characteristics are optimized based on the type of application the workload supports. For example, if you create a workload that supports a Microsoft SQL Server application and then subsequently create volumes for that workload, the underlying volume characteristics are optimized to support Microsoft SQL Server.

The system recommends an optimized volume configuration only for the following application types:

- Microsoft SQL Server
- Microsoft Exchange Server
- Video Surveillance
- VMware ESXi (for volumes to be used with Virtual Machine File System)

#### Steps

1. From the Manage page, select the storage array.
2. Select **Provisioning › Manage Volumes**.
3. Select **Create › Workload**.

   The Create Application Workload dialog box appears.

4. Use the drop-down list to select the type of application that you want to create the workload for and then type a workload name.
5. Click **Create**.

### Step 2: Create volumes

You create volumes to add storage capacity to an application-specific workload, and to make the created volumes visible to a specific host or host cluster.

#### About this task

Most application types default to a user-defined volume configuration, while other types have a smart configuration applied at volume creation. For example, if you are creating volumes for a Microsoft Exchange application, you are asked how many mailboxes you need, what your average mailbox capacity requirements are, and how many copies of the database you want. The system uses this information to create an optimal volume configuration for you, which can be edited as needed.

You can create volumes from **Provisioning › Manage Volumes › Create › Volumes** or from **Provisioning › Configure Pools and Volume Groups › Create › Volumes**. The procedure is the same for either selection.

The process to create a volume is a multi-step procedure.

#### Step 2a: Select host for a volume

In the first step, you can select a specific host or host cluster for the volume, or you can choose to assign the host later.

**Before you begin**

Make sure that:

- Valid hosts or host clusters have been defined (go to **Provisioning › Configure Hosts**).
- Host port identifiers have been defined for the host.
- The host connection must support Data Assurance (DA) if you plan to create DA-enabled volumes. 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.

**About this task**

Keep these guidelines in mind when you assign volumes:

- A host's operating system can have specific limits on how many volumes the host can access. Keep this limitation in mind when you create volumes for use by a particular host.
- You can define one assignment for each volume in the storage array.
- Assigned volumes are shared between controllers in the storage array.
- The same logical unit number (LUN) cannot be used twice by a host or a host cluster to access a volume. You must use a unique LUN.
- If you want to speed the process for creating volumes, you can skip the host assignment step so that newly created volumes are initialized offline.

> Assigning a volume to a host will fail if you try to assign a volume to a host cluster that conflicts with an established assignment for a host in the host clusters.

**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.

#### Step 2b: Select a workload for a volume

In the second step, you select a workload to customize the storage array configuration for a specific application, such as VMware.

**About this task**

This task describes how to create volumes for a workload. Typically, a workload contains volumes with similar characteristics, which are optimized based on the type of application the workload supports. You can define a workload in this step or you can select existing workloads.

Keep these guidelines in mind:

- When using an application-specific workload, the system recommends an optimized volume configuration to minimize contention between application workload I/O and other traffic from your application instance. You can review the recommended volume configuration, and then edit, add, or delete the system-recommended volumes and characteristics using the Add/Edit Volumes dialog box (available in the next step).
- When using other application types, you manually specify the volume configuration using the Add/Edit Volumes dialog box (available in the next step).

**Steps**

1. 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:
     - 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.
     - Enter a name for the workload you want to create.
2. Click **Next**.
3. If your workload is associated with a supported application type, enter the information requested; otherwise, go to the next step.

#### Step 2c: Add or edit volumes

In the third step, you define the volume configuration.

**Before you begin**

- The pools or volume groups must have sufficient free capacity.
- The maximum number of volumes allowed in a volume group is 256.
- The maximum number of volumes allowed in a pool depends on the storage system model:
  - 2,048 volumes (EF600 and E5700 series)
  - 1,024 volumes (EF300)
  - 512 volumes (E2800 series)
- To create a Data Assurance (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.

- 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.
- To create a resource-provisioned volume, all drives must be NVMe drives with the Deallocated or Unwritten Logical Block Error (DULBE) option.

**About this task**

You create volumes from eligible pools or volume groups, which are shown in the Add/Edit Volumes dialog box. 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.

**Steps**

1. 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.

**Field Details**

| 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>Keep in mind that storage capacity is also required for copy services (snapshot images, snapshot volumes, volume copies, and remote mirrors); therefore, do not allocate all of the capacity to standard volumes.<br>Capacity in a pool is allocated in 4GiB increments. Any capacity that is not a multiple of 4GiB is allocated but not usable. To make sure that the entire capacity is usable, specify the capacity in 4GiB increments. If unusable capacity exists, the only way to regain it is to increase the capacity of the volume. |
| Volume Block Size (EF300 and EF600 only) | Shows the block sizes that can be created for the volume:<br>• 512 – 512 bytes<br>• 4K – 4,096 bytes |

| Field | Description |
| --- | --- |
| 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.<br>**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.<br>**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.<br>**Amount of time to change segment size** — The amount of time to change a volume's segment size depends on these variables:<br>• The I/O load from the host<br>• The modification priority of the volume<br>• The number of drives in the volume group<br>• The number of drive channels<br>• The processing power of the storage array controllers<br>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 secure-capable.<br>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.<br>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).<br>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. |

| Field | Description |
| --- | --- |
| 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. |

- **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.

**Field Details**

| 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>Keep in mind that storage capacity is also required for copy services (snapshot images, snapshot volumes, volume copies, and remote mirrors); therefore, do not allocate all of the capacity to standard volumes.<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 | Volume type 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:<br>• 512 — 512 bytes<br>• 4K — 4,096 bytes |

| Field | Description |
| --- | --- |
| 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.<br>**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.<br>**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.<br>**Amount of time to change segment size** — The amount of time to change a volume's segment size depends on these variables:<br>• The I/O load from the host<br>• The modification priority of the volume<br>• The number of drives in the volume group<br>• The number of drive channels<br>• The processing power of the storage array controllers<br>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 secure-capable.<br>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.<br>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).<br>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. |

| Field | Description |
| --- | --- |
| 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. |

2. To continue the volume creation sequence for the selected application, click **Next**.

#### Step 2d: Review volume configuration

In the last step, you review a summary of the volumes you intend to create and make any necessary changes.

#### Steps

1. Review the volumes you want to create. To make changes, click **Back**.
2. When you are satisfied with your volume configuration, click **Finish**.

#### After you finish

- In the vSphere Client, create datastores for the volumes.
- Perform any operating system modifications necessary on the application host so that the applications can use the volume.
- Run either the host-based `hot_add` utility or an operating system-specific utility (available from a third-party vendor), and then run the `SMdevices` utility to correlate volume names with host storage array names.

  The `hot_add` utility and the `SMdevices` utility are included as part of the `SMutils` package. The `SMutils` package is a collection of utilities to verify what the host sees from the storage array. It is included as part of the SANtricity software installation.

## Increase capacity of a volume

You can resize a volume to increase its reported capacity.

#### 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.)

#### About this task

This task describes how to 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. Be sure to consider any future capacity requirements that you might have for other volumes in this pool or volume group.

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 is unsupported, the expanded capacity is unusable, and you cannot restore the original volume capacity.

**Steps**

1. From the **Manage** page, select the storage array that contains the volumes you want to resize.
2. Select **Provisioning › Manage Volumes**.
3. Select the volume for which you want to increase capacity, and then select **Increase Capacity**.

   The Confirm Increase Capacity dialog box appears.

4. 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.

5. 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).
6. Click **Increase**.

   The volume's capacity is increased based on your selection. Be aware that this operation can be lengthy and could affect system performance.

**After you finish**

After you expand the volume capacity, you must manually increase the file system size to match. How you do this depends on the file system you are using. See your host operating system documentation for details.

## Change settings for a volume

You can change a volume's settings such as its name, host assignment, segment size, modification priority, caching, and so on.

**Before you begin**

Make sure that the volume you want to change is in Optimal status.

**Steps**

1. From the Manage page, select the storage array that contains the volumes you want to change.
2. Select **Provisioning › Manage Volumes**.
3. Select the volume that you want to change, and then select **View/Edit Settings**.

   The Volume Settings dialog box appears. The configuration settings for the volume you selected appear in this dialog box.

4. Select the **Basic** tab to change the volume's name and host assignment.

**Field Details**

| Setting | Description |
| --- | --- |
| Name | Displays the name of the volume. Change the name of a volume when the current name is no longer meaningful or applicable. |
| Capacities | Displays the reported and allocated capacity for the selected volume. |
| Pool / Volume group | Displays the name and RAID level of the pool or volume group. Indicates whether the pool or volume group is secure-capable and secure-enabled. |
| Host | Displays the volume assignment. You assign a volume to a host or host cluster so it can be accessed for I/O operations. This assignment grants a host or host cluster access to a particular volume or to a number of volumes in a storage array.<br>• **Assigned to** — Identifies the host or host cluster that has access to the selected volume.<br>• **LUN** — A logical unit number (LUN) is the number assigned to the address space that a host uses to access a volume. The volume is presented to the host as capacity in the form of a LUN. Each host has its own LUN address space. Therefore, the same LUN can be used by different hosts to access different volumes.<br>For NVMe interfaces, this column displays Namespace ID. A namespace is NVM storage that is formatted for block access. It is analogous to a logical unit in SCSI, which relates to a volume in the storage array. The namespace ID is the NVMe controller's unique identifier for the namespace, and can be set to a value between 1 and 255. It is analogous to a logical unit number (LUN) in SCSI. |
| Identifiers | Displays the identifiers for the selected volume.<br>• World-wide identifier (WWID). A unique hexadecimal identifier for the volume.<br>• Extended unique identifier (EUI). An EUI-64 identifier for the volume.<br>• Subsystem identifier (SSID). The storage array subsystem identifier of a volume. |

5. Select the **Advanced** tab to change additional configuration settings for a volume in a pool or in a volume group.

**Field Details**

| Setting | Description |
| --- | --- |
| Application & workload information | During volume creation, you can create application-specific workloads or other workloads. If applicable, the workload name, application type, and volume type appears for the selected volume.<br>You can change the workload name if desired. |
| Quality of Service settings | **Permanently disable data assurance** — This setting appears only if the volume is Data Assurance (DA)-enabled. DA checks for and corrects errors that might occur as data is transferred through the controllers down to the drives. Use this option to permanently disable DA on the selected volume. When disabled, DA cannot be re-enabled on this volume.<br>**Enable pre-read redundancy check** — This setting appears only if the volume is a thick volume. Pre-read redundancy checks determine whether the data on a volume is consistent any time a read is performed. A volume that has this feature enabled returns read errors if the data is determined to be inconsistent by the controller firmware. |
| Controller ownership | Defines the controller that is designated to be the owning, or primary, controller of the volume.<br>Controller ownership is very important and should be planned carefully. Controllers should be balanced as closely as possible for total I/Os. |
| Segment sizing | Shows the setting for segment sizing, which appears only for volumes in a volume group. You can change the segment size to optimize performance.<br>**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.<br>**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.<br>**Amount of time to change segment size.** The amount of time to change a volume's segment size depends on these variables:<br>• The I/O load from the host<br>• The modification priority of the volume<br>• The number of drives in the volume group<br>• The number of drive channels<br>• The processing power of the storage array controllers<br>When you change the segment size for a volume, I/O performance is affected, but your data remains available. |

| Setting | Description |
| --- | --- |
| Modification priority | Shows the setting for modification priority, which only appears for volumes in a volume group.<br>The modification priority defines how much processing time is allocated for volume modification operations relative to system performance. You can increase the volume modification priority, although this might affect system performance.<br>Move the slider bars to select a priority level.<br>**Modification priority rates** — The lowest priority rate benefits system performance, but the modification operation takes longer. The highest priority rate benefits the modification operation, but system performance might be compromised. |
| Caching | Shows the caching setting, which you can change to impact the overall I/O performance of a volume. |
| SSD Cache | (This feature is not available on the EF600 or EF300 storage system.)<br>Shows the SSD Cache setting, which you can enable on compatible volumes as a way to improve read-only performance. Volumes are compatible if they share the same drive security and data assurance capabilities.<br>The SSD Cache feature uses a single or multiple solid-state disks (SSDs) to implement a read cache. Application performance is improved because of the faster read times for SSDs. Because the read cache is in the storage array, caching is shared across all applications using the storage array. Simply select the volume that you want to cache, and then caching is automatic and dynamic. |

6. Click **Save**.

**Result**

The volume settings are changed based on your selections.

## Add volumes to workload

You can add unassigned volumes to an existing or new workload.

**About this task**

Volumes are not associated with a workload if they have been created using the command line interface (CLI) or if they have been migrated (imported/exported) from a different storage array.

**Steps**

1. From the Manage page, select the storage array that contains the volumes you want to add.
2. Select **Provisioning › Manage Volumes**.
3. Select the **Applications & Workloads** tab.

   The Applications & Workloads view appears.

4. Select **Add to Workload**.

   The Select Workload dialog box appears.

5. Do one of the following actions:
   - **Add volumes to an existing workload** — Select this option to add volumes to an existing workload. Use the drop-down list to select a workload. The workload's associated application type is assigned to the volumes you add to this workload.
   - **Add volumes to a new workload** — Select this option to define a new workload for an application type and add volumes to the new workload.
6. Select **Next** to continue with the add to workload sequence.

   The Select Volumes dialog box appears.

7. Select the volumes you want to add to the workload.
8. Review the volumes that you want to add to the selected workload.
9. When you are satisfied with your workload configuration, click **Finish**.

## Change workload settings

You can change the name for a workload and view its associated application type.

**Steps**

1. From the Manage page, select the storage array that contains the workload you want to change.
2. Select **Provisioning › Manage Volumes**.
3. Select the **Applications & Workloads** tab.

   The Applications & Workloads view appears.

4. Select the workload that you want to change, and then select **View/Edit Settings**.

   The Applications & Workloads Settings dialog box appears.

5. (Optional) Change the user-supplied name of the workload.
6. Click **Save**.

## Initialize volumes

A volume is automatically initialized when it is first created. However, the Recovery Guru might advise that you manually initialize a volume to recover from certain failure conditions.

Use this option only under the guidance of technical support. You can select one or more volumes to initialize.

**Before you begin**

- All I/O operations have been stopped.
- Any devices or file systems on the volumes you want to initialize must be unmounted.
- The volume is in Optimal status and no modification operations are in progress on the volume.*Attention:

*You cannot cancel the operation after it starts. All volume data is erased. Do not try this operation unless the Recovery Guru advises you to do so. Contact technical support before you begin this procedure.

**About this task**

When you initialize a volume, the volume keeps its WWN, host assignments, allocated capacity, and reserved capacity settings. It also keeps the same Data Assurance (DA) settings and security settings.

The following types of volumes cannot be initialized:

- Base volume of a snapshot volume
- Primary volume in a mirror relationship
- Secondary volume in a mirror relationship
- Source volume in a volume copy
- Target volume in a volume copy
- Volume that already has an initialization in progress

This procedure applies only to standard volumes created from pools or volume groups.

**Steps**

1. From the Manage page, select the storage array that contains the volumes you want to initialize.
2. Select **Provisioning › Manage Volumes**.
3. Select any volume, and then select **More › Initialize volumes**.

   The Initialize Volumes dialog box appears. All volumes on the storage array appear in this dialog box.
4. Select one or more volumes that you want to initialize and confirm that you want to perform the operation.

**Results**

The system performs the following actions:

- Erases all data from the volumes that were initialized.
- Clears the block indices, which causes unwritten blocks to be read as if they are zero-filled (the volume appears to be completely empty).

This operation can be lengthy and could affect system performance.

## Redistribute volumes

You redistribute volumes to move volumes back to their preferred controller owners. Typically, multipath drivers move volumes from their preferred controller owner when a problem occurs along the data path between the host and storage array.

**Before you begin**

- The volumes you want to redistribute are not in use, or I/O errors will occur.
- A multipath driver is installed on all hosts using the volumes you want to redistribute, or I/O errors will occur. If you want to redistribute volumes without a multipath driver on the hosts, all I/O activity to the volumes while the redistribution operation is in progress must be stopped to prevent application errors.

**About this task**

Most host multipath drivers attempt to access each volume on a path to its preferred controller owner. However, if this preferred path becomes unavailable, the multipath driver on the host fails over to an alternate path. This failover might cause the volume ownership to change to the alternate controller. After you have resolved the condition that caused the failover, some hosts might automatically move the volume ownership back to the preferred controller owner, but in some cases, you might need to manually redistribute the volumes.

**Steps**

1. From the Manage page, select the storage array that contains the volumes you want to redistribute.
2. Select **Provisioning › Manage Volumes**.
3. Select **More › Redistribute volumes**.

   The Redistribute Volumes dialog box appears. All volumes on the storage array whose preferred controller owner does not match its current owner appear in this dialog box.

4. Select one or more volumes that you want to redistribute, and confirm that you want to perform the operation.

**Result**

The system moves the selected volumes to their preferred controller owners or you might see a Redistribute Volumes Unnecessary dialog box.

## Change controller ownership of a volume

You can change the preferred controller ownership of a volume, so that I/O for host applications is directed through the new path.

**Before you begin**

If you do not use a multipath driver, any host applications that are currently using the volume must be shut down. This action prevents application errors when the I/O path changes.

**About this task**

You can change controller ownership for one or more volumes in a pool or volume group.

**Steps**

1. From the Manage page, select the storage array that contains the volumes for which you want to change the controller ownership.
2. Select **Provisioning › Manage Volumes**.
3. Select any volume, and then select **More › Change ownership**.

   The Change Volume Ownership dialog box appears. All volumes on the storage array appear in this dialog box.

4. Use the **Preferred Owner** drop-down list to change the preferred controller for each volume that you want to change, and confirm that you want to perform the operation.

**Results**

- The system changes the controller ownership of the volume. I/O to the volume is now directed through this I/O path.
- The volume might not use the new I/O path until the multipath driver reconfigures to recognize the new

path.

This action usually takes less than five minutes.

## Change cache settings for a volume

You can change read cache and write cache settings to impact the overall I/O performance of a volume.

### About this task

Keep these guidelines in mind when you change cache settings for a volume:

- After opening the Change Cache Settings dialog box, you might see an icon shown next to the selected cache properties. This icon indicates that the controller has temporarily suspended caching operations. This action might occur when a new battery is charging, when a controller has been removed, or if a mismatch in cache sizes has been detected by the controller. After the condition has cleared, the cache properties selected in the dialog box become active. If the selected cache properties do not become active, contact technical support.
- You can change the cache settings for a single volume or for multiple volumes on a storage array. You can change the cache settings for all volumes at the same time.

### Steps

1. From the Manage page, select the storage array that contains the volumes for which you want to change cache settings.
2. Select **Provisioning › Manage Volumes**.
3. Select any volume, and then select **More › Change cache settings**.

   The Change Cache Settings dialog box appears. All volumes on the storage array appear in this dialog box.

4. Select the **Basic** tab to change the settings for read caching and write caching.

   **Field Details**

| Cache setting | Description |
| --- | --- |
| **Read Caching** | The read cache is a buffer that stores data that has been read from the drives. The data for a read operation might already be in the cache from a previous operation, which eliminates the need to access the drives. The data stays in the read cache until it is flushed. |
| **Write Caching** | The write cache is a buffer that stores data from the host that has not yet been written to the drives. The data stays in the write cache until it is written to the drives. Write caching can increase I/O performance.<br>Cache is automatically flushed after the Write caching is disabled for a volume. |

5. Select the **Advanced** tab to change the advanced settings for thick volumes. The advanced cache settings are available only for thick volumes.

**Field Details**

| Setting | Description |
| --- | --- |
| **Dynamic Read Cache Prefetch** | Dynamic Cache Read Prefetch allows the controller to copy additional sequential data blocks into the cache while it is reading data blocks from a drive to the cache. This caching increases the chance that future requests for data can be filled from the cache. Dynamic cache read prefetch is important for multimedia applications that use sequential I/O. The rate and amount of data that is prefetched into cache is self- adjusting based on the rate and request size of the host reads. Random access does not cause data to be prefetched into cache. This feature does not apply when read caching is disabled. |
| **Write Caching without Batteries** | The Write Caching without Batteries setting enables write caching to continue even when the batteries are missing, failed, discharged completely, or not fully charged. Choosing write caching without batteries is not typically recommended, because data might be lost if power is lost. Typically, write caching is turned off temporarily by the controller until the batteries are charged or a failed battery is replaced.<br><br>CAUTION: **Possible loss of data** — If you select this option and do not have a universal power supply for protection, you could lose data. In addition, you could lose data if you do not have controller batteries and you enable the Write caching without batteries option. |
| **Write Caching with Mirroring** | Write Caching with Mirroring occurs when the data written to the cache memory of one controller is also written to the cache memory of the other controller. Therefore, if one controller fails, the other can complete all outstanding write operations. Write cache mirroring is available only if write caching is enabled and two controllers are present. Write caching with mirroring is the default setting at volume creation. |

6. Click **Save** to change the cache settings.

## Change media scan settings for a volume

A media scan is a background operation that scans all data and redundancy information in the volume. Use this option to enable or disable the media scan settings for one or more volumes, or to change the scan duration.

**Before you begin**

Understand the following:

- Media scans run continuously at a constant rate based on the capacity to be scanned and the scan duration. Background scans may be temporarily suspended by a higher priority background task (e.g. reconstruction), but will resume at the same constant rate.
- A volume is scanned only when the media scan option is enabled for the storage array and for that volume. If redundancy check is also enabled for that volume, redundancy information in the volume will be checked for consistency with data, provided that the volume has redundancy. Media scan with redundancy check is enabled by default for each volume when it is created.
- If an unrecoverable medium error is encountered during the scan, data will be repaired using redundancy

information, if available.

For example, redundancy information is available in optimal RAID 5 volumes, or in RAID 6 volumes that are optimal or only have one drive failed. If the unrecoverable error cannot be repaired using redundancy information, the data block will be added to the unreadable sector log. Both correctable and uncorrectable medium errors are reported to the event log.

- If the redundancy check finds an inconsistency between data and the redundancy information, it is reported to the event log.

**About this task**

Media scans detect and repair media errors on disk blocks that are infrequently read by applications. This can prevent data loss in the event of a drive failure, as data for failed drives is reconstructed using redundancy information and data from other drives in the volume group or pool.

You can perform the following actions:

- Enable or disable background media scans for the entire storage array
- Change the scan duration for the entire storage array
- Enable or disable media scan for one or more volumes
- Enable or disable the redundancy check for one or more volumes

**Steps**

1. From the Manage page, select the storage array that contains the volumes for which you want to change media scan settings.
2. Select **Provisioning › Manage Volumes**.
3. Select any volume, and then select **More › Change media scan settings**.

   The Change Drive Media Scan Settings dialog box appears. All volumes on the storage array appear in this dialog box.

4. To enable the media scan, select the **Scan media over the course of…** check box. Disabling the media scan check box suspends all media scan settings.
5. Specify the number of days over which you want the media scan to run.
6. Select the **Media Scan** check box for each volume you want to perform a media scan on. The system enables the Redundancy Check option for each volume on which you choose to run a media scan. If there are individual volumes for which you do not want to perform a redundancy check, deselect the **Redundancy Check** check box.
7. Click **Save**.

**Result**

The system applies changes to background media scans based on your selection.

## Delete volume

You can delete one or more volumes to increase the free capacity of a pool or volume group.

**Before you begin**

On the volumes that you plan to delete, make sure that:

- All data is backed up.
- All Input/Output (I/O) is stopped.
- Any devices and file systems are unmounted.

**About this task**

Typically, you delete volumes if the volumes were created with the wrong parameters or capacity, or it no longer meets storage configuration needs. Deleting a volume increases the free capacity in the pool or volume group.

Deleting a volume causes loss of all data on those volumes.

Be aware that you **cannot** delete a volume that has one of these conditions:

- The volume is initializing.
- The volume is reconstructing.
- The volume is part of a volume group that contains a drive that is undergoing a copyback operation.
- The volume is undergoing a modification operation, such as a change of segment size, unless the volume is now in Failed status.
- The volume is holding any type of persistent reservation.
- The volume is a source volume or a target volume in a Copy Volume that has a status of Pending, In Progress, or Failed.

When a volume exceeds a given size (currently 128 TB), the delete operation is performed in the background and the freed space might not be immediately available.

**Steps**

1. From the **Manage** page, select the storage array that contains the volumes you want to delete.
2. Select **Provisioning › Manage Volumes**.
3. Click **Delete**.

   The Delete Volumes dialog box appears.
4. Select one or more volumes that you want to delete, and then confirm that you want to perform the operation.
5. Click **Delete**.

# Configure hosts

## Host creation overview

To manage storage with the Storage Plugin for vCenter, you must discover or define each host in the network. A host is a server that sends I/O to a volume on a storage array.

### Automatic vs manual host creation

Creating a host is one of the steps required to let the storage array know which hosts are attached to it and to allow I/O access to the 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.

  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.

#### How volumes are assigned

For a host to send I/O to a volume, you must assign the volume to it. You can select either a host or host cluster when you create a volume or you can assign a volume to a host or host cluster later. A host cluster is a group of hosts. You create a host cluster to make it easy to assign the same volumes to multiple hosts.

Assigning volumes to hosts is flexible, allowing you to meet your particular storage needs.

- **Stand-alone host, not part of a host cluster** — You can assign a volume to an individual host. The volume can be accessed only by the one host.
- **Host cluster** — You can assign a volume to a host cluster. The volume can be accessed by all the hosts in the host cluster.
- **Host within a host cluster** — You can assign a volume to an individual host that is part of a host cluster. Even though the host is part of a host cluster, the volume can be accessed only by the individual host and not by any other hosts in the host cluster.

When volumes are created, logical unit numbers (LUNs) are assigned automatically. The LUN serves as the address between the host and the controller during I/O operations. You can change LUNs after the volume is created.

## Create host access

To manage storage with the Storage Plugin for vCenter, you must discover or define each host in the network.

#### About this task

By creating a host, you define the host parameters to provide connection to the storage array and I/O access to the volumes.

You can allow the Host Context Agent (HCA) to automatically detect the hosts, and then verify that the information is correct by selecting **View/Edit Settings** from the Configure Hosts page. However, the HCA is not available on all supported operating systems and you must create the host manually.

When you create a host, keep these guidelines in mind:

- 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 Details**

| Setting | 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 | Do one of the following:<br>• **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.<br>• **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:<br>• 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.<br>• Leave the field blank if you do not require host authentication. Currently, the only iSCSI authentication method used is CHAP. |

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

**Result**

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`.

**After you finish**

You must assign a volume to a host so it can be used for I/O operations. Go to Assign volumes to hosts.

## Create host cluster

When two or more hosts require I/O access to the same volumes, you can create a host cluster.

**About this task**

Keep these guidelines in mind when you create a host cluster:

- This operation does not start unless there are two or more hosts available to create the cluster.
- Hosts in host clusters can have different operating systems (heterogeneous).
- NVMe hosts in host clusters cannot be mixed with non- NVMe hosts.
- To create a Data Assurance (DA)-enabled volume, the host connection you are planning to use must support DA.

  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.

- 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. Select **Create › Host cluster**.

   The Create Host Cluster dialog box appears.

4. Select the settings for the host cluster as appropriate.

| Setting | Description |
| --- | --- |
| Name | Type the name for the new host cluster. |
| Select hosts to share volume access | Select two or more hosts from the drop-down list. Only those hosts that are not already part of a host cluster appear in the list. |

5. Click **Create**.

   If the selected hosts are attached to interface types that have different Data Assurance (DA) capabilities, a dialog appears with the message that DA will be unavailable on the host cluster. This unavailability prevents DA-enabled volumes from being added to the host cluster. Select **Yes** to continue or **No** to cancel.

   DA increases data integrity across the entire storage system. DA enables the storage array to check for

errors that might occur when data is moved between the hosts and the drives. Using DA for the new volume ensures that any errors are detected.

**Result**

The new host cluster appears in the table with the assigned hosts in the rows beneath.

**After you finish**

You must assign a volume to a host cluster so it can be used for I/O operations. Go to Assign volumes to hosts.

## Assign volumes to hosts

You must assign a volume to a host or a host cluster so it can be used for I/O operations.

**Before you begin**

Keep these guidelines in mind when you assign volumes to hosts:

- You can assign a volume to only one host or host cluster at a time.
- Assigned volumes are shared between controllers in the storage array.
- The same logical unit number (LUN) cannot be used twice by a host or a host cluster to access a volume. You must use a unique LUN.
- For new volume groups, if you wait until all volumes are created and initialized before you assign them to a host, the volume initialization time is reduced. Keep in mind that once a volume associated with the volume group is mapped, all volumes will revert to the slower initialization.

**About this task**

A volume assignment grants a host or host cluster access to that volume in a storage array.

All unassigned volumes are displayed during this task, but functions for hosts with or without Data Assurance (DA) apply as follows:

- For a DA-capable host, you can select volumes that are either DA-enabled or not DA-enabled.
- For a host that is not DA-capable, if you select a volume that is DA-enabled, a warning states that the system must automatically turn off DA on the volume before assigning the volume to the host.

  Assigning a volume fails under these conditions:

- All volumes are assigned.
- The volume is already assigned to another host or host cluster. The ability to assign a volume is unavailable under these conditions:
- No valid hosts or host clusters exist.
- No host port identifiers have been defined for the host.
- All volume assignments have been defined.

**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 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.

4. 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.
5. Click **Assign** to complete the operation.

**Results**

After successfully assigning a volume or volumes to a host or a host cluster, 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.

## Unassign volumes

If you no longer need I/O access to a volume, you can unassign it from the host or host cluster.

**About this task**

Keep these guidelines in mind when you unassign a volume:

- If you are removing the last assigned volume from a host cluster, and the host cluster also has hosts with specific assigned volumes, make sure that you remove or move those assignments before removing the last assignment for the host cluster.
- If a host cluster, a host, or a host port is assigned to a volume that is registered to the operating system, you must clear this registration before you can remove these nodes.

**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 the host or host cluster that you want to edit, and then click **Unassign Volumes**.

   A dialog box appears that shows all the volumes that are currently assigned.

4. Select the check box next to each volume that you want to unassign or select the check box in the table header to select all volumes.
5. Click **Unassign**.

**Results**

- The volumes that were unassigned are available for a new assignment.
- Until the changes are configured on the host, the volume is still recognized by the host operating system.

## Change the settings for a host

You can change the name, host operating system type, and associated host clusters for a host or host cluster.

**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 the host that you want to edit, and then click **View/Edit Settings**.

   A dialog box appears that shows the current host settings.

4. To change host properties, make sure the **Properties** tab is selected and then change the settings as appropriate.

   **Field Details**

| Setting | Description |
| --- | --- |
| Name | You can change the user-supplied name of the host. Specifying a name for the host is required. |
| Associated host cluster | You can choose one of the following options:<br>• **None** — The host remains a standalone host. If the host was associated to a host cluster, the system removes the host from the cluster.<br>• **<Host Cluster>** — The system associates the host to the selected cluster. |
| Host operating system type | You can change the type of operating system running on the host you defined. |

5. To change port settings, click the **Host Ports** tab and then change the settings as appropriate.

**Field Details**

| Setting | Description |
| --- | --- |
| Host Port | You can choose one of the following options:<br>• **Add** — Use Add to associate a new host port identifier to the host. The length of the host port identifier name is determined by the host interface technology. Fibre Channel and Infiniband host port identifier names must have 16 characters. iSCSI host port identifier names have a maximum of 223 characters. The port must be unique. A port number that has already been configured is not allowed.<br>• **Delete** — Use Delete to remove (unassociate) a host port identifier. The Delete option does not physically remove the host port. This option removes the association between the host port and the host. Unless you remove the host bus adapter or the iSCSI initiator, the host port is still recognized by the controller.<br>If you delete a host port identifier, it is no longer associated with this host. Also, the host loses access to any of its assigned volumes through this host port identifier. |
| Label | To change the port label name, click the **Edit** icon (pencil). The port label name must be unique. A label name that has already been configured is not allowed. |
| CHAP Secret | Appears only for iSCSI hosts. You can set or change the CHAP secret for the initiators (iSCSI hosts).<br>The system uses the Challenge Handshake Authentication Protocol (CHAP) method, which validates the identity of targets and initiators during the initial link. Authentication is based on a shared security key called a CHAP secret. |

6. Click **Save**.

## Delete host or host cluster

You can remove a host or host cluster so that volumes are no longer associated with that host.

**About this task**

Keep these guidelines in mind when you delete a host or a host cluster:

- Any specific volume assignments are deleted, and the associated volumes are available for a new assignment.
- If the host is part of a host cluster that has its own specific assignments, the host cluster is unaffected. However, if the host is part of a host cluster that does not have any other assignments, the host cluster and any other associated hosts or host port identifiers inherit any default assignments.
- Any host port identifiers that were associated with the host become undefined.

**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 the host or host cluster that you want to delete, and then click **Delete**.

   The confirmation dialog box appears.

4. Confirm that you want to perform the operation, and then click **Delete**.

**Results**

If you deleted a host, the system performs the following actions:

- Deletes the host and, if applicable, removes it from the host cluster.
- Removes access to any assigned volumes.
- Returns the associated volumes to an unassigned state.
- Returns any host port identifiers associated with the host to an unassociated state. If you deleted a host cluster, the system performs the following actions:
  - Deletes the host cluster and its associated hosts (if any).
  - Removes access to any assigned volumes.
  - Returns the associated volumes to an unassigned state.
  - Returns any host port identifiers associated with the hosts to an unassociated state.

# Configure pools and volume groups

## Pools and volume group overview

To provision storage in the Storage Plugin for vCenter, you create either a pool or volume group that will contain the Hard Disk Drives (HDD) or Solid State Disk (SSD) drives that you want to use in your storage array.

**Provisioning**

Physical hardware is provisioned into logical components so that data can be organized and easily retrieved. There are two types of groupings supported:

- Pools
- Volume groups

The pools and volume groups are the top-level units of storage in a storage array: they divide the capacity of drives into manageable divisions. Within these logical divisions are the individual volumes or LUNs where data is stored.

When a storage system is deployed, the first step is to present the available drive capacity to the various hosts by:

- Creating pools or volume groups with sufficient capacity
- Adding the number of drives required to meet performance requirements to the pool or volume group
- Selecting the desired level of RAID protection (if using volume groups) to meet specific business requirements

You can have pools or volume groups on the same storage system, but a drive cannot be part of more than one pool or volume group. Volumes that are presented to hosts for I/O are then created, using the space on the pool or volume group.

## Pools

Pools are designed to aggregate physical hard disk drives into a large storage space and to provide enhanced RAID protection for it. A pool creates many virtual RAID sets from the total number of drives assigned to the pool, and it spreads the data out evenly among all participating drives. If a drive is lost or added, the system dynamically re-balances the data across all the active drives.

Pools function as another RAID level, virtualizing the underlying RAID architecture to optimize performance and flexibility when performing tasks such as rebuilding, drive expansion, and handling drive loss. The system automatically sets the RAID level at 6 in an 8+2 configuration (eight data disks plus two parity disks).

#### Drive matching

You can choose from either HDD or SSDs for use in pools; however, as with volume groups, all drives in the pool must use the same technology. The controllers automatically select which drives to include, so you must make sure that you have a sufficient number of drives for the technology you choose.

#### Managing failed drives

Pools have a minimum capacity of 11 drives; however, one drive’s worth of capacity is reserved for spare capacity in the event of a drive failure. This spare capacity is called “preservation capacity.”

When pools are created, a certain amount of capacity is preserved for emergency use. This capacity is expressed in terms of a number of drives, but the actual implementation is spread across the entire pool of drives. The default amount of capacity that is preserved is based on the number of drives in the pool.

After the pool is created, you can change the preservation capacity value to more or less capacity, or even set it to no preservation capacity (0 drive’s worth). The maximum amount of capacity that can be preserved (expressed as a number of drives) is 10, but the capacity that is available might be less, based on the total number of drives in the pool.

## Volume groups

Volume groups define how capacity is allotted in the storage system to volumes. Disk drives are organized into RAID groups and volumes reside across the drives in a RAID group. Therefore, volume group configuration settings identify which drives are part of the group and what RAID level is used.

When you create a volume group, controllers automatically select the drives to include in the group. You must manually choose the RAID level for the group. The capacity of the volume group is the total of the number of drives that you select, multiplied by their capacity.

#### Drive matching

You must match the drives in the volume group for size and performance. If there are smaller and larger drives in the volume group, all drives are recognized as the smallest capacity size. If there are slower and faster

drives in the volume group, all drives are recognized at the slowest speed. These factors affect the performance and overall capacity of the storage system.

You cannot mix different drive technologies (HDD and SSD drives). RAID 3, 5, and 6 are limited to a maximum of 30 drives. RAID 1 and RAID 10 uses mirroring, so these volume groups must have an even number of disks.

#### Managing failed drives

Volume groups use hot spare drives as a standby in case a drive fails in RAID 1/10, RAID 3, RAID 5, or RAID 6 volumes contained in a volume group. A hot spare drive contains no data and adds another level of redundancy to your storage array.

If a drive fails in the storage array, the hot spare drive is automatically substituted for the failed drive without requiring a physical swap. If the hot spare drive is available when a drive fails, the controller uses redundancy data to reconstruct the data from the failed drive to the hot spare drive.

### Decide whether to use pools or volume groups

#### Choose a pool

- If you need faster drive rebuilds and simplified storage administration, and/or have a highly random workload.
- If you want to distribute the data for each volume randomly across a set of drives that comprise the pool.You cannot set or change the RAID level of pools or the volumes in the pools. Pools use RAID level 6.

#### Choose a volume group

- If you need maximum system bandwidth, the ability to tune storage settings, and a highly sequential workload.
- If you want to distribute the data across the drives based on a RAID level. You can specify the RAID level when you create the volume group.
- If you want to write the data for each volume sequentially across the set of drives that comprise the volume group.

Because pools can co-exist with volume groups, a storage array can contain both pools and volume groups.

### Automatic versus manual pool creation

Depending on your storage configuration, you can allow the system to create pools automatically or you can manually create them yourself. A pool is a set of logically grouped drives.

Before you create and manage pools, review the following sections for how pools are automatically created and when you might need to manually create them.

#### Automatic creation

When the system detects unassigned capacity in the storage array, it initiates automatic pool creation is initiated when the system detects unassigned capacity in a storage array. It automatically prompts you to create one or more pools, or add the unassigned capacity to an existing pool, or both.

Automatic pool creation occurs when one of these conditions is true:

- Pools do not exist in the storage array, and there are enough similar drives to create a new pool.
- New drives are added to a storage array that has at least one pool.Each drive in a pool must be of the same drive type (HDD or SSD) and have similar capacity. The system will prompt you to complete the following tasks:
- Create a single pool if there are a sufficient number of drives of those types.
- Create multiple pools if the unassigned capacity consists of different drive types.
- Add the drives to the existing pool if a pool is already defined in the storage array, and add new drives of the same drive type to the pool.
- Add the drives of the same drive type to the existing pool, and use the other drive types to create different pools if the new drives are of different drive types.

#### Manual creation

You might want to create a pool manually when automatic creation cannot determine the best configuration. This situation can occur for one of the following reasons:

- The new drives could potentially be added to more than one pool.
- One or more of the new pool candidates can use shelf loss protection or drawer loss protection.
- One or more of the current pool candidates cannot maintain their shelf loss protection or drawer loss protection status.You might also want to create a pool manually if you have multiple applications on your storage array and do not want them competing for the same drive resources. In this case, you might consider manually creating a smaller pool for one or more of the applications. You can assign just one or two volumes instead of assigning the workload to a large pool that has many volumes across which to distribute the data. Manually creating a separate pool that is dedicated to the workload of a specific application can allow storage array operations to perform more rapidly, with less contention.

## Create pool automatically

You can create pools automatically when the system detects at least 11 unassigned drives or it detects one unassigned drive that is eligible for an existing pool. A pool is a set of logically grouped drives.

#### Before you begin

You can launch the Pool Auto-Configuration dialog box when one of these conditions are true:

- At least one unassigned drive has been detected that can be added to an existing pool with similar drive types.
- Eleven (11) or more unassigned drives have been detected that can be used to create a new pool (if they cannot be added to an existing pool due to dissimilar drive types).

#### About this task

You can use automatic pool creation to easily configure all unassigned drives in the storage array into one pool and to add drives into existing pools.

Keep in mind the following:

- When you add drives to a storage array, the system automatically detects the drives and prompts you to create a single pool or multiple pools based on the drive type and the current configuration.
- If pools were previously defined, the system automatically prompts you with the option of adding the

compatible drives to an existing pool. When new drives are added to an existing pool, the system automatically redistributes the data across the new capacity, which now includes the new drives that you added.

- When configuring an EF600 or EF300 storage array, make sure each controller has access to an equal number of drives in the first 12 slots and an equal number of drives in the last 12 slots. This configuration helps the controllers use both drive-side PCIe buses more effectively. For pool creation, you should use all drives in the storage array.

**Steps**

1. From the Manage page, select the storage array for the pool.
2. Select **Provisioning › Configure Pools and Volume Groups**.
3. Select **More › Launch pool auto-configuration**.

   The results table lists new pools, existing pools with drives added, or both. A new pool is named with a sequential number by default.

   Notice that the system does the following:

   - Creates a single pool if there are a sufficient number of drives with the same drive type (HDD or SSD) and have similar capacity.
   - Creates multiple pools if the unassigned capacity consists of different drive types.
   - Adds the drives to an existing pool if a pool is already defined in the storage array, and you add new drives of the same drive type to the pool.
   - Adds the drives of the same drive type to the existing pool, and use the other drive types to create different pools if the new drives are of different drive types.
4. To change the name of a new pool, click the **Edit** icon (the pencil).
5. To view additional characteristics of the pool, position the cursor over or touch the Details icon (the page).

   Information about the drive type, security capability, data assurance (DA) capability, shelf loss protection, and drawer loss protection appears.

   For EF600 and EF300 storage arrays, settings are also displayed for resource provisioning and volume block sizes.
6. Click **Accept**.

## Create pool manually

You can create a pool manually if your setup does not meet the requirements for automatic pool configuration. A pool is a set of logically grouped drives.

**Before you begin**

- You must have a minimum of 11 drives with the same drive type (HDD or SSD).
- Shelf loss protection requires that the drives comprising the pool are located in at least six different drive shelves and there are no more than two drives in a single drive shelf.
- Drawer loss protection requires that the drives comprising the pool are located in at least five different drawers and the pool includes an equal number of drive shelves from each drawer.
- When configuring an EF600 or EF300 storage array, make sure each controller has access to an equal number of drives in the first 12 slots and an equal number of drives in the last 12 slots. This configuration

helps the controllers use both drive-side PCIe buses more effectively. For pool creation, you should use all drives in the storage array.

**About this task**

During pool creation you determine its characteristics, such as drive type, security capability, data assurance (DA) capability, shelf loss protection, and drawer loss protection.

For EF600 and EF300 storage arrays, settings also include resource provisioning and volume block sizes.

**Steps**

1. From the Manage page, select the storage array for the pool.
2. Select **Provisioning › Configure Pools and Volume Groups**.
3. Click **Create › Pool**.

   The Create Pool dialog box appears.

4. Type a name for the pool.
5. (Optional) If you have more than one type of drive in your storage array, select the drive type that you want to use.

   The results table lists all the possible pools that you can create.

6. Select the pool candidate that you want to use based on the following characteristics, and then click **Create**.

**Field Details**

| Characteristic | Use |
| --- | --- |
| Free Capacity | Shows the free capacity of the pool candidate in GiB. Select a pool candidate with the capacity for your application's storage needs. Preservation (spare) capacity is also distributed throughout the pool and is not part of the free capacity amount. |
| Total Drives | Shows the number of drives available in the pool candidate.<br>The system automatically reserves as many drives as possible for preservation capacity (for every six drives in a pool, the system reserves one drive for preservation capacity).<br>When a drive failure occurs, the preservation capacity is used to hold the reconstructed data. |
| Drive Block Size (EF300 and EF600 only) | Shows the block size (sector size) that the drives in the pool can write. Values may include:<br>• 512 — 512-byte sector size.<br>• 4K — 4,096-byte sector size. |
| Secure-Capable | Indicates whether this pool candidate is comprised entirely of secure-capable drives, which can be either Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives.<br>• You can protect your pool with Drive Security, but all drives must be secure- capable to use this feature.<br>• If you want to create an FDE-only pool, look for **Yes - FDE** in the Secure-Capable column. If you want to create a FIPS-only pool, look for **Yes - FIPS** or **Yes - FIPS (Mixed)**. "Mixed" indicates a mixture of 140-2 and 140-3 level drives. If you use a mixture of these levels, be aware that the pool will then operate at the lower level of security (140-2).<br>• You can create a pool comprised of drives that may or may not be secure- capable or are a mix of security levels. If the drives in the pool include drives that are not secure-capable, you cannot make the pool secure. |
| Enable Security? | Provides the option for enabling the Drive Security feature with secure-capable drives. If the pool is secure-capable and you have created a security key, you can enable security by selecting the check box.<br>ⓘ The only way to remove Drive Security after it is enabled is to delete the pool and erase the drives. |

| Characteristic | Use |
| --- | --- |
| DA Capable | Indicates if Data Assurance (DA) is available for this pool candidate. DA checks for and corrects errors that might occur as data is transferred through the controllers down to the drives.<br>If you want to use DA, select a pool that is DA capable. This option is available only when the DA feature has been enabled.<br>A pool can contain drives that are DA-capable or not DA-capable, but all drives must be DA capable for you to use this feature. |
| Resource Provisioning Capable (EF300 and EF600 only) | Shows if Resource Provisioning is available for this pool candidate. 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. |
| Shelf Loss Protection | Shows if shelf loss protection is available.<br>Shelf loss protection guarantees accessibility to the data on the volumes in a pool if a total loss of communication occurs with a single drive shelf. |
| Drawer Loss Protection | Shows if drawer loss protection is available, which is provided only if you are using a drive shelf that contains drawers.<br>Drawer loss protection guarantees accessibility to the data on the volumes in a pool if a total loss of communication occurs with a single drawer in a drive shelf. |
| Volume Block Sizes Supported (EF300 and EF600 only) | Shows the block sizes that can be created for the volumes in the pool:<br>• 512n — 512 bytes native.<br>• 512e — 512 bytes emulated.<br>• 4K — 4,096 bytes. |

## Create a volume group

You can create a volume group for one or more volumes that are accessible to the host. A volume group is a container for volumes with shared characteristics such as RAID level and capacity.

**Before you begin**

Review the following guidelines:

- You need at least one unassigned drive.
- Limits exist as to how much drive capacity you can have in a single volume group. These limits vary according to your host type.
- To enable shelf/drawer loss protection, you must create a volume group that uses drives located in at least three shelves or drawers, unless you are using RAID 1, where two shelves/drawers is the minimum.
- When configuring an EF600 or EF300 storage array, make sure each controller has access to an equal number of drives in the first 12 slots and an equal number of drives in the last 12 slots. This configuration

helps the controllers use both drive-side PCIe buses more effectively. The system currently allows for drive selection under the Advanced feature when creating a volume group.

Review how your choice of RAID level affects the resulting capacity of the volume group.

- If you select RAID 1, you must add two drives at a time to make sure that a mirrored pair is selected. Mirroring and striping (known as RAID 10 or RAID 1+0) is achieved when four or more drives are selected.
- If you select RAID 5, you must add a minimum of three drives to create the volume group.
- If you select RAID 6, you must add a minimum of five drives to create the volume group.

**About this task**

During volume group creation you determine the group characteristics, such as the number of drives, security capability, data assurance (DA) capability, shelf loss protection, and drawer loss protection.

For EF600 and EF300 storage arrays, settings also include resource provisioning, drive block sizes, and volume block sizes.

With larger capacity drives and the ability to distribute volumes across controllers, creating more than one volume per volume group is a good way to make use of your storage capacity and to protect your data.

**Steps**

1. From the Manage page, select the storage array for the volume group.
2. Select **Provisioning › Configure Pools and Volume Groups**.
3. Click **Create › Volume group**.

   The Create Volume Group dialog box appears.

4. Type a name for the volume group.
5. Select the RAID level that best meets your requirements for data storage and protection. The volume group candidate table appears and displays only the candidates that support the selected RAID level.
6. (Optional) If you have more than one type of drive in your storage array, select the drive type that you want to use.

   The volume group candidate table appears and displays only the candidates that support the selected drive type and RAID level.

7. (Optional) You can select either the automatic method or manual method to define which drives to use in the volume group. The Automatic method is the default selection.

   Do not use the Manual method unless you are an expert who understands drive redundancy and optimal drive configurations.

   To select drives manually, click the **Manually select drives (advanced)** link. When clicked, it changes to **Automatically select drives (advanced)**.

   The Manual method lets you select which specific drives comprise the volume group. You can select specific unassigned drives to obtain the capacity that you require. If the storage array contains drives with different media types or different interface types, you can choose only the unconfigured capacity for a single drive type to create the new volume group.

8. Based on the displayed drive characteristics, select the drives you want to use in the volume group, and then click **Create**.

The drive characteristics displayed depend on whether you selected the automatic method or manual method. For more information, see the SANtricity System Manager documentation, Create a volume group.

## Add capacity to a pool or volume group

You can add drives to expand the free capacity in an existing pool or volume group.

### Before you begin

- Drives must be in an Optimal status.
- Drives must have the same drive type (HDD or SSD).
- The pool or volume group must be in an Optimal status.
- If the pool or volume group contains all secure-capable drives, add only drives that are secure-capable to continue to use the encryption abilities of the secure-capable drives.

Secure-capable drives can be either Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives.

### About this task

In this task, you can add free capacity to be included in the pool or volume group. You can use this free capacity to create additional volumes. The data in the volumes remains accessible during this operation.

For pools, you can add a maximum of 60 drives at a time. For volume groups, you can add a maximum of two drives at a time. If you need to add more than the maximum number of drives, repeat the procedure. (A pool cannot contain more drives than the maximum limit for a storage array.)

With the addition of drives, your preservation capacity may need to be increased. You should consider increasing your reserved capacity after an expansion operation.

Avoid using drives that are Data Assurance (DA) capable to add capacity to a pool or volume group that is not DA capable. The pool or volume group cannot take advantage of the capabilities of the DA-capable drive. Consider using drives that are not DA capable in this situation.

### Steps

1. From the Manage page, select the storage array with the pool or volume group.
2. Select **Provisioning › Configure Pools and Volume Groups**.
3. Select the pool or volume group to which you want to add drives, and then click **Add Capacity**.

   The Add Capacity dialog box appears. Only the unassigned drives that are compatible with the pool or volume group appear.

4. Under **Select drives to add capacity…**, select one or more drives that you want to add to the existing pool or volume group.

   The controller firmware arranges the unassigned drives with the best options listed at the top. The total free capacity that is added to the pool or volume group appears below the list in **Total capacity selected**.

**Field Details**

| Field | Description |
| --- | --- |
| Shelf | Indicates the shelf location of the drive. |
| Bay | Indicates the bay location of the drive |
| Capacity (GiB) | Indicates the drive capacity.<br>• Whenever possible, select drives that have a capacity equal to the capacities of the current drives in the pool or volume group.<br>• If you must add unassigned drives with a smaller capacity, be aware that the usable capacity of each drive currently in the pool or volume group is reduced. Therefore, the drive capacity is the same across the pool or volume group.<br>• If you must add unassigned drives with a larger capacity, be aware that the usable capacity of the unassigned drives that you add is reduced so that they match the current capacities of the drives in the pool or volume group. |
| Secure-Capable | Indicates whether the drive is secure-capable.<br>• You can protect your pool or volume group with the Drive Security feature, but all drives must be secure-capable to use this feature.<br>• It is possible to create a pool or volume group with a mix of secure-capable and non-secure-capable drives, but the Drive Security feature cannot be enabled.<br>• A pool or volume group with all secure-capable drives cannot accept a non-secure-capable drive for sparing or expansion, even if the encryption capability is not in use.<br>• Secure-capable drives can be either Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives. A FIPS drive can be level 140-2 or 140-3, with level 140-3 as the higher level of security. If you select a mixture of 140-2 and 140-3 level drives, the pool or volume group will then operate at the lower level of security (140-2). |

| Field | Description |
| --- | --- |
| DA Capable | Indicates whether the drive is Data Assurance (DA) capable.<br>• Using drives that are not Data Assurance (DA) capable to add capacity to a DA-capable pool or volume group is not recommended. The pool or volume group no longer has DA capabilities, and you no longer have the option to enable DA on newly created volumes within the pool or volume group.<br>• Using drives that are Data Assurance (DA) capable to add capacity to a pool or volume group that is non DA-capable is not recommended, because that pool or volume group cannot take advantage of the capabilities of the DA-capable drive (the drive attributes do not match). Consider using drives that are not DA-capable in this situation. |
| DULBE Capable | Indicates whether the drive has the option for Deallocated or Unwritten Logical Block Error (DULBE). DULBE is an option on NVMe drives that allows the EF300 or EF600 storage array to support resource-provisioned volumes. |

5. Click **Add**.

   If you are adding drives to a pool or volume group, a confirmation dialog box appears if you selected a drive that causes the pool or volume group to no longer have one or more of the following attributes:

   ◦ Shelf loss protection
   ◦ Drawer loss protection
   ◦ Full Disk Encryption capability
   ◦ Data Assurance capability
   ◦ DULBE capability

6. To continue, click **Yes**; otherwise click **Cancel**.

**Result**

After you add the unassigned drives to a pool or volume group, the data in each volume of the pool or volume group is redistributed to include the additional drives.

## Create SSD Cache

To dynamically accelerate system performance, you can use the SSD Cache feature to cache the most frequently accessed data ("hot" data) onto lower latency Solid State Drives (SSDs). SSD Cache is used exclusively for host reads.

**Before you begin**

Your storage array must contain some SSD drives.

SSD Cache is not available on the EF600 or EF300 storage system.

**About this task**

When you create SSD Cache, you can use a single drive or multiple drives. Because the read cache is in the storage array, caching is shared across all applications using the storage array. You select the volumes that you want to cache, and then caching is automatic and dynamic.

Follow these guidelines when you create SSD Cache.

- You can enable security on the SSD Cache only when you are creating it, not later.
- Only one SSD Cache is supported per storage array.
- The maximum usable SSD Cache capacity on a storage array is dependent on the controller's primary cache capacity.
- SSD Cache is not supported on snapshot images.
- If you import or export volumes that are SSD Cache enabled or disabled, the cached data is not imported or exported.
- Any volume assigned to use a controller's SSD Cache is not eligible for an automatic load balance transfer.
- If the associated volumes are secure-enabled, create a secure-enabled SSD Cache.

**Steps**

1. From the Manage page, select the storage array for the cache.
2. Select **Provisioning › Configure Pools and Volume Groups**.
3. Click **Create › SSD Cache**.

   The Create SSD Cache dialog box appears.

4. Type a name for the SSD Cache.
5. Select the SSD Cache candidate that you want to use based on the following characteristics.

**Field Details**

| Characteristic | Use |
| --- | --- |
| **Capacity** | Shows the available capacity in GiB. Select the capacity for your application's storage needs.<br>The maximum capacity for SSD Cache depends on the controller's primary cache capacity. If you allocate more than the maximum amount to SSD Cache, then any extra capacity is unusable.<br>SSD Cache capacity counts towards your overall allocated capacity. |
| **Total drives** | Shows the number of drives available for this SSD cache. Select the SSD candidate with the number of drives that you want |
| **Secure-capable** | Indicates whether the SSD Cache candidate is comprised entirely of secure-capable drives, which can be either Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives.<br>If you want to create a secure-enabled SSD Cache, look for "Yes - FDE" or "Yes - FIPS" in the Secure-capable column. |
| **Enable security?** | Provides the option for enabling the Drive Security feature with secure-capable drives. If you want to create a secure-enabled SSD Cache, select the **Enable Security** check box.<br><br>NOTE: Once enabled, security cannot be disabled. You can enable security on the SSD Cache only when you are creating it, not later. |
| **DA capable** | Indicates if Data Assurance (DA) is available for this SSD Cache candidate. Data Assurance (DA) checks for and corrects errors that might occur as data is transferred through the controllers down to the drives.<br>If you want to use DA, select an SSD Cache candidate that is DA capable. This option is available only when the DA feature has been enabled.<br>SSD Cache can contain both DA-capable and non-DA-capable drives, but all drives must be DA-capable for you to use DA. |

6. Associate the SSD Cache with the volumes for which you want to implement SSD read caching. To enable SSD Cache on compatible volumes immediately, select the **Enable SSD Cache on existing compatible volumes that are mapped to hosts** check box.

   Volumes are compatible if they share the same Drive Security and DA capabilities.

7. Click **Create**.

## Change configuration settings for a pool

You can edit the settings for a pool, including its name, capacity alerts settings, modification priorities, and preservation capacity.

**About this task**

This task describes how to change configuration settings for a pool.

> You cannot change the RAID level of a pool using the plugin interface. The plugin automatically configures pools as RAID 6.

**Steps**

1. From the Manage page, select the storage array with the pool.
2. Select **Provisioning › Configure Pools and Volume Groups**.
3. Select the pool that you want to edit, and then click **View/Edit Settings**.

   The Pool Settings dialog box appears.
4. Select the **Settings** tab, and then edit the pool settings as appropriate.

**Field Details**

| Setting | Description |
| --- | --- |
| Name | You can change the user-supplied name of the pool. Specifying a name for a pool is required. |
| Capacity alerts | You can send alert notifications when the free capacity in a pool reaches or exceeds a specified threshold. When the data stored in the pool exceeds the specified threshold, the plugin sends a message, allowing you time to add more storage space or to delete unnecessary objects.<br>Alerts are shown in the Notifications area on the Dashboard and can be sent from the server to administrators by email and SNMP trap messages.<br>You can define the following capacity alerts:<br>• **Critical alert** — This critical alert notifies you when the free capacity in the pool reaches or exceeds the specified threshold. Use the spinner controls to adjust the threshold percentage. Select the check box to disable this notification.<br>• **Early alert** — This early alert notifies you when the free capacity in a pool is reaching a specified threshold. Use the spinner controls to adjust the threshold percentage. Select the check box to disable this notification. |
| Modification priorities | You can specify the priority levels for modification operations in a pool relative to system performance. A higher priority for modification operations in a pool causes an operation to complete faster, but can slow the host I/O performance. A lower priority causes operations to take longer, but host I/O performance is less affected.<br>You can choose from five priority levels: lowest, low, medium, high, and highest. The higher the priority level, the larger is the impact on host I/O and system performance.<br>• **Critical reconstruction priority** — This slider bar determines the priority of a data reconstruction operation when multiple drive failures result in a condition where some data has no redundancy and an additional drive failure might result in loss of data.<br>• **Degraded reconstruction priority** — This slider bar determines the priority of the data reconstruction operation when a drive failure has occurred, but the data still has redundancy and an additional drive failure does not result in loss of data.<br>• **Background operation priority** — This slider bar determines the priority of the pool background operations that occur while the pool is in an optimal state. These operations include Dynamic Volume Expansion (DVE), Instant Availability Format (IAF), and migrating data to a replaced or added drive. |

| Setting | Description |
| --- | --- |
| Preservation capacity ("Optimization capacity" for the EF600 or EF300) | **Preservation capacity** — You can define the number of drives to determine the capacity that is reserved on the pool to support potential drive failures. When a drive failure occurs, the preservation capacity is used to hold the reconstructed data. Pools use preservation capacity during the data reconstruction process instead of hot spare drives, which are used in volume groups.<br>Use the spinner controls to adjust the number of drives. Based on the number of drives, the preservation capacity in the pool appears next to the spinner box.<br>Keep the following information in mind about preservation capacity.<br>• Because preservation capacity is subtracted from the total free capacity of a pool, the amount of capacity that you reserve affects how much free capacity is available to create volumes. If you specify 0 for the preservation capacity, all of the free capacity on the pool is used for volume creation.<br>• If you decrease the preservation capacity, you increase the capacity that can be used for pool volumes.<br>**Additional optimization capacity (EF600 and EF300 arrays only)** — When a pool is created, a recommended optimization capacity is generated that provides a balance of available capacity versus performance and drive wear life. You can adjust this balance by moving the slider to the right for better performance and drive wear life at the expense of increased available capacity, or by moving it to the left for increased available capacity at the expense of better performance and drive wear life. SSD drives will have longer life and better maximum write performance when a portion of their capacity is unallocated. For drives associated with a pool, unallocated capacity is comprised of a pool's preservation capacity, the free capacity (capacity not used by volumes), and a portion of the usable capacity set aside as additional optimization capacity. The additional optimization capacity ensures a minimum level of optimization capacity by reducing the usable capacity, and as such, is not available for volume creation. |

5. Click **Save**.

## Change configuration settings for a volume group

You can edit the settings for a volume group, including its name and RAID level.

### Before you begin

If you are changing the RAID level to accommodate the performance needs of the applications that are accessing the volume group, be sure to meet the following prerequisites:

- The volume group must be in Optimal status.
- You must have enough capacity in the volume group to convert to the new RAID level.

### Steps

1. From the Manage page, select the storage array with the volume group.
2. Select **Provisioning › Configure Pools and Volume Groups**.
3. Select the volume group that you want to edit, and then click **View/Edit Settings**.

   The Volume Group Settings dialog box appears.
4. Select the **Settings** tab, and then edit the volume group settings as appropriate.

**Field Details**

| Setting | Description |
| --- | --- |
| Name | You can change the user-supplied name of the volume group. Specifying a name for a volume group is required. |
| RAID level | Select the new RAID level from the drop-down menu.<br>• **RAID 0 striping** — Offers high performance but does not provide any data redundancy. If a single drive fails in the volume group, all the associated volumes fail, and all data is lost. A striping RAID group combines two or more drives into one large, logical drive.<br>• **RAID 1 mirroring** — Offers high performance and the best data availability and is suitable for storing sensitive data on a corporate or personal level. Protects your data by automatically mirroring the contents of one drive to the second drive in the mirrored pair. It provides protection in the event of a single drive failure.<br>• **RAID 10 striping/mirroring** — Provides a combination of RAID 0 (striping) and RAID 1 (mirroring) and is achieved when four or more drives are selected. RAID 10 is suitable for high volume transaction applications, such as a database, that require high performance and fault tolerance.<br>• **RAID 5** — Optimal for multi-user environments (such as database or file system storage) where typical I/O size is small and there is a high proportion of read activity.<br>• **RAID 6** — Optimal for environments requiring redundancy protection beyond RAID 5, but not requiring high write performance.<br>RAID 3 can be assigned only to volume groups using the command line interface (CLI).<br>When you change the RAID level, you cannot cancel this operation after it begins. During the change, your data remains available. |
| Optimization capacity (EF600 arrays only) | When a volume group is created, a recommended optimization capacity is generated that provides a balance of available capacity versus performance and drive wear life. You can adjust this balance by moving the slider to the right for better performance and drive wear life at the expense of increased available capacity, or by moving it to the left for increased available capacity at the expense of better performance and drive wear life. SSD drives will have longer life and better maximum write performance when a portion of their capacity is unallocated. For drives associated with a volume group, unallocated capacity is comprised of a group's free capacity (capacity not used by volumes) and a portion of the usable capacity set aside as additional optimization capacity. The additional optimization capacity ensures a minimum level of optimization capacity by reducing the usable capacity, and as such, is not available for volume creation. |

5. Click **Save**.

A confirmation dialog box appears if capacity is reduced, volume redundancy is lost, or shelf/ drawer loss

protection is lost as a result of the RAID level change. Select **Yes** to continue; otherwise click **No**.

**Result**

If you change the RAID level for a volume group, the plugin changes the RAID levels of every volume that comprises the volume group. Performance might be slightly affected during the operation.

## Change SSD Cache settings

You can edit the name of the SSD Cache and view its status, maximum and current capacity, Drive Security and Data Assurance status, and its associated volumes and drives.

This feature is not available on the EF600 or EF300 storage system.

**Steps**

1. From the Manage page, select the storage array with the SSD Cache.
2. Select **Provisioning › Configure Pools and Volume Groups**.
3. Select the SSD Cache that you want to edit, and then click **View/Edit Settings**.

   The SSD Cache Settings dialog box appears.
4. Review or edit the SSD Cache settings as appropriate.

**Field Details**

| Setting | Description |
| --- | --- |
| Name | Displays the name of the SSD Cache, which you can change. A name for the SSD Cache is required. |
| Characteristics | Shows the status for the SSD Cache. Possible statuses include:<br>• Optimal<br>• Unknown<br>• Degraded<br>• Failed (A failed state results in a critical MEL event.)<br>• Suspended |
| Capacities | Shows the current capacity and maximum capacity allowed for the SSD Cache.<br>The maximum capacity allowed for the SSD Cache depends on the controller's primary cache size:<br>• Up to 1 GiB<br>• 1 GiB to 2 GiB<br>• 2 GiB to 4 GiB<br>• More than 4 GiB |
| Security and DA | Shows the Drive Security and Data Assurance status for the SSD Cache.<br>• **Secure-capable** --Indicates whether the SSD Cache is comprised entirely of secure-capable drives. A secure-capable drive is a self-encrypting drive that can protect its data from unauthorized access.<br>• **Secure-enabled** — Indicates whether security is enabled on the SSD Cache.<br>• **DA capable** — Indicates whether the SSD Cache is comprised entirely of DA-capable drives. A DA-capable drive can check for and correct errors that might occur as data is communicated between the host and storage array. |
| Associated objects | Shows the volumes and drives associated with the SSD Cache. |

5. Click **Save**.

## View SSD Cache statistics

You can view statistics for the SSD Cache, such as reads, writes, cache hits, cache allocation percentage, and cache utilization percentage.

This feature is not available on the EF600 or EF300 storage system.

**About this task**

The nominal statistics, which are a subset of the detailed statistics, are shown on the View SSD Cache Statistics dialog box. You can view detailed statistics for the SSD Cache only when you export all SSD statistics to a .csv file.

As you review and interpret the statistics, keep in mind that some interpretations are derived by looking at a combination of statistics.

**Steps**

1. From the Manage page, select the storage array with the SSD Cache.
2. Select **Provisioning › Configure Pools and Volume Groups**.
3. Select the SSD Cache for which you want to view statistics, and then click **More › View SSD Cache** statistics.

   The View SSD Cache Statistics dialog box appears and displays the nominal statistics for the selected SSD cache.

   **Field Details**

| Setting | Description |
|---|---|
| **Reads** | Shows the total number of host reads from the SSD Cache-enabled volumes.<br>The greater the ratio of Reads to Writes, the better is the operation of the cache. |
| **Writes** | The total number of host writes to the SSD Cache-enabled volumes.<br>The greater the ratio of Reads to Writes, the better is the operation of the cache. |
| **Cache hits** | Shows the number of cache hits. |
| **Cache hits %** | Shows the percentage of cache hits. This number is derived from Cache Hits / (reads + writes). The cache hit percentage should be greater than 50 percent for effective SSD Cache operation. |
| **Cache allocation %** | Shows the percentage of SSD Cache storage that is allocated, expressed as a percentage of the SSD Cache storage that is available to this controller and is derived from allocated bytes / available bytes. |
| **Cache utilization %** | Shows the percentage of SSD Cache storage that contains data from enabled volumes, expressed as a percentage of SSD Cache storage that is allocated. This amount represents the utilization or density of the SSD Cache. Derived from allocated bytes / available bytes. |
| **Export All** | Exports all SSD Cache statistics to a CSV format. The exported file contains all available statistics for the SSD Cache (both nominal and detailed). |

4. Click **Cancel** to close the dialog box.

## Check volume redundancy

Under the guidance of technical support or as instructed by the Recovery Guru, you can check the redundancy on a volume in a pool or volume group to determine whether the data on that volume is consistent.

Redundancy data is used to quickly reconstruct information on a replacement drive if one of the drives in the pool or volume group fails.

### Before you begin

- The status of the pool or volume group must be Optimal.
- The pool or volume group must have no volume modification operations in progress.
- You can check redundancy on any RAID level except on RAID 0, because RAID 0 has no data redundancy. (Pools are configured only as RAID 6.)

> Check volume redundancy only when instructed to do so by the Recovery Guru and under the guidance of technical support.

### About this task

You can perform this check only on one pool or volume group at a time. A volume redundancy check performs the following actions:

- Scans the data blocks in a RAID 3 volume, a RAID 5 volume, or a RAID 6 volume, and checks the redundancy information for each block. (RAID 3 can only be assigned to volume groups using the command line interface.)
- Compares the data blocks on RAID 1 mirrored drives.
- Returns redundancy errors if the controller firmware determines that the data is inconsistent.

> Immediately running a redundancy check on the same pool or volume group might cause an error. To avoid this problem, wait one to two minutes before running another redundancy check on the same pool or volume group.

### Steps

1. From the Manage page, select the storage array with the pool or volume group.
2. Select **Provisioning › Configure Pools and Volume Groups**.
3. Select **Uncommon Tasks › Check volume redundancy**.

   The Check Redundancy dialog box appears.
4. Select the volumes you want to check, and then type check to confirm you want to perform this operation.
5. Click **Check**.

   The check volume redundancy operation starts. The volumes in the pool or volume group are sequentially scanned, starting from the top of the table in the dialog box. These actions occur as each volume is scanned:

   - The volume is selected in the volume table.
   - The status of the redundancy check is shown in the Status column.

- The check stops on any media or parity error encountered, and then reports the error. The following table provide more information about the status of the redundancy check:

**Field Details**

| Status | Description |
|---|---|
| **Pending** | This is the first volume to be scanned, and you have not clicked Start to start the redundancy check.<br>-or-<br>The redundancy check operation is being performed on other volumes in the pool or volume group. |
| **Checking** | The volume is undergoing the redundancy check. |
| **Passed** | The volume passed the redundancy check. No inconsistencies were detected in the redundancy information. |
| **Failed** | The volume failed the redundancy check. Inconsistencies were detected in the redundancy information. |
| **Media error** | The drive media is defective and is unreadable. Follow the instructions displayed in the Recovery Guru. |
| **Parity error** | The parity is not what it should be for a given portion of the data. A parity error is potentially serious and could cause a permanent loss of data. |

6. Click **Done** after the last volume in the pool or volume group has been checked.

## Delete pool or volume group

You can delete a pool or volume group to create more unassigned capacity, which you can reconfigure to meet your application storage needs.

**Before you begin**

- You must have backed up the data on all of the volumes in the pool or volume group.
- You must have stopped all input/output (I/O).
- You must unmount any file systems on the volumes.
- You must have deleted any mirror relationships in the pool or volume group.
- You must have stopped any volume copy operation in progress for the pool or volume group.
- The pool or volume group must not be participating in an asynchronous mirroring operation.
- The drives in the volume group must not have a persistent reservation.

**Steps**

1. From the Manage page, select the storage array with the pool or volume group.
2. Select **Provisioning › Configure Pools and Volume Groups**.
3. Select one pool or volume group from the list.

   You can select only one pool or volume group at a time. Scroll down the list to see additional pools or volume groups.

4. Select **Uncommon Tasks › Delete** and confirm.

**Results**

The system performs the following actions:

- Deletes all of the data in the pool or volume group.
- Deletes all the drives associated with the pool or volume group.
- Unassigns the associated drives, which allows you to reuse them in new or existing pools or volume groups.

## Consolidate free capacity for a volume group

Use the Consolidate Free Capacity option to consolidate existing free extents on a selected volume group. By performing this action, you can create additional volumes from the maximum amount of free capacity in a volume group.

**Before you begin**

- The volume group must contain at least one free capacity area.
- All of the volumes in the volume group must be online and in Optimal status.
- Volume modification operations must not be in progress, such as changing the segment size of a volume.

**About this task**

You cannot cancel the operation after it begins. Your data remains accessible during the consolidation operation.

You can launch the Consolidate Free Capacity dialog box using any of the following methods:

- When at least one free capacity area is detected for a volume group, the Consolidate free capacity recommendation appears on the Home page in the Notification area. Click the **Consolidate free capacity** link to launch the dialog box.
- You can also launch the Consolidate Free Capacity dialog box from the Pools & Volume Groups page as described in the following task.

**More about free capacity areas**

A free capacity area is the free capacity that can result from deleting a volume or from not using all available free capacity during volume creation. When you create a volume in a volume group that has one or more free capacity areas, the volume's capacity is limited to the largest free capacity area in that volume group. For example, if a volume group has a total of 15 GiB free capacity, and the largest free capacity area is 10 GiB, the largest volume you can create is 10 GiB.

You consolidate free capacity on a volume group to improve write performance. Your volume group's free capacity will become fragmented over time as the host writes, modifies, and deletes files. Eventually, the available capacity will not be located in a single contiguous block, but will be scattered in small fragments across the volume group. This causes further file fragmentation, since the host must write new files as fragments to fit them into the available ranges of free clusters.

By consolidating free capacity on a selected volume group, you will notice improved file system performance whenever the host writes new files. The consolidation process will also help prevent new files from being fragmented in the future.

**Steps**

1. From the Manage page, select the storage array with the volume group.
2. Select **Provisioning › Configure Pools and Volume Groups**.
3. Select the volume group with free capacity that you want to consolidate, and then select **Uncommon Tasks › Consolidate volume group free capacity**.

   The Consolidate Free Capacity dialog box appears.
4. Type `consolidate` to confirm you want to perform this operation.
5. Click **Consolidate**.

**Result**

The system begins consolidating (defragmenting) the volume group's free capacity areas into one contiguous amount for subsequent storage configuration tasks.

**After you finish**

From the navigation sidebar, select **Operations** to view the progress of the Consolidate Free Capacity operation. This operation can be lengthy and could affect system performance.

## Turn on locator lights

You can locate drives to physically identify all of the drives that comprise a selected pool, volume group, or SSD Cache. An LED indicator lights up on each drive in the selected pool, volume group, or SSD Cache.

**Steps**

1. From the Manage page, select the storage array.
2. Select **Provisioning › Configure Pools and Volume Groups**.
3. Select the pool, volume group, or SSD Cache you want to locate, and then click **More › Turn on locator lights**.

   A dialog box appears that indicates the lights on the drives comprising the selected pool, volume group, or SSD Cache are turned on.
4. After you successfully locate the drives, click **Turn Off**.

## Remove capacity

You can remove drives to decrease the capacity of an existing pool or SSD Cache.

After you remove drives, the data in each volume of the pool or SSD Cache is redistributed to the remaining drives. The removed drives become unassigned, and their capacity becomes part of the total free capacity of the storage array.

**About this task**

Follow these guidelines when you remove capacity:

- You cannot remove the last drive in an SSD Cache without first deleting the SSD Cache.
- You cannot reduce the number of drives in a pool to be less than 11 drives.

- You can remove a maximum of 12 drives at a time. If you need to remove more than 12 drives, repeat the procedure.
- You cannot remove drives if there is not enough free capacity in the pool or SSD Cache to contain the data, when that data is redistributed to the remaining drives in the pool or SSD Cache.

The following are potential performance impacts:

- Removing drives from a pool or SSD Cache might result in reduced volume performance.
- The preservation capacity is not consumed when you remove capacity from a pool or SSD Cache. However, the preservation capacity might decrease based on the number of drives remaining in the pool or SSD Cache.

The following are impacts to secure-capable drives:

- If you remove the last drive that is not secure-capable, the pool is left with all secure-capable drives. In this situation, you are given the option to enable security for the pool.
- If you remove the last drive that is not Data Assurance (DA) capable, the pool is left with all DA-capable drives.
- Any new volumes that you create on the pool will be DA-capable. If you want existing volumes to be DA-capable, you need to delete and then re-create the volume.

**Steps**

1. From the Manage page, select the storage array.

   Select **Provisioning › Configure Pools and Volume Groups**.

2. Select the pool or SSD Cache, and then click **More › Remove capacity**.

   The Remove Capacity dialog box appears.

3. Select one or more drives in the list.

   As you select or de-select drives in the list, the Total capacity selected field updates. This field shows the total capacity of the pool or SSD Cache that results after you remove the selected drives.

4. Click **Remove**, and then confirm you want to remove the drives.

**Result**

The newly reduced capacity of the pool or SSD Cache is reflected in the Pools and Volume Groups view.

## Enable security for a pool or volume group

You can enable Drive Security for a pool or volume group to prevent unauthorized access to the data on the drives contained in the pool or volume group.

Read and write access for the drives is only available through a controller that is configured with a security key.

**Before you begin**

- The Drive Security feature must be enabled.
- A security key must be created.
- The pool or volume group must be in an Optimal state.

- All of the drives in the pool or volume group must be secure-capable drives.

**About this task**

If you want to use Drive Security, select a pool or volume group that is secure-capable. 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.

After enabling security, you can only remove it by deleting the pool or volume group, and then erasing the drives.

**Steps**

1. From the Manage page, select the storage array with the pool or volume group.
2. Select **Provisioning › Configure Pools and Volume Groups**.
3. Select the pool or volume group on which you want to enable security, and then click **More › Enable security**.

   The Confirm Enable Security dialog box appears.
4. Confirm that you want to enable security for the selected pool or volume group, and then click **Enable**.

# 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: Execute the registration script
- Method 2: Use the vCenter Server Mob pages

**Method 1: Execute 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: Use 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**.

# FAQs

### What settings are imported?

The Import Settings feature is a batch operation that loads configurations from one storage array to multiple storage arrays.

The settings that are imported during this operation depend on how the source storage array is configured in System Manager. The following settings can be imported to multiple storage arrays:

- **Email alerts** — Settings include a mail server address and the email addresses of the alert recipients.
- **Syslog alerts** — Settings include a syslog server address and a UDP port.
- **SNMP alerts** — Settings include a community name and IP address for the SNMP server.
- **AutoSupport** — Settings include the separate features (Basic AutoSupport, AutoSupport OnDemand, and Remote Diagnostics), the maintenance window, delivery method, and dispatch schedule.
- **Directory services** — Configuration includes the domain name and URL of an LDAP (Lightweight Directory Access Protocol) server, along with the mappings for the LDAP server's user groups to the storage array's predefined roles.
- **Storage configuration** — Configurations include volumes (only thick and only non-repository volumes), volume groups, pools, and hot spare drive assignments.
- **System settings** — Configurations include media scan settings for a volume, SSD cache for controllers, and automatic load balancing (does not include host connectivity reporting).

## Why do I not see all of my storage arrays?

During the Import Settings operation, some of your storage arrays might not be available in the target selection dialog box.

Storage arrays might not appear for the following reasons:

- The firmware version is below 8.50.
- The storage array is offline.
- The system cannot communicate with that array (for example, the array has certificate, password, or networking problems).

## Why are these volumes not associated with a workload?

Volumes are not associated with a workload if they have been created using the command line interface (CLI) or if they have been migrated (imported/exported) from a different storage array.

## How does my selected workload impact volume creation?

During volume creation, you are prompted for information about a workload's use. The system uses this information to create an optimal volume configuration for you, which can be edited as needed. Optionally, you can skip this step in the volume creation sequence.

A workload is a storage object that supports an application. You can define one or more workloads, or instances, per application. For some applications, the system configures the workload to contain volumes with similar underlying volume characteristics. These volume characteristics are optimized based on the type of application the workload supports. For example, if you create a workload that supports a Microsoft SQL Server application and then subsequently create volumes for that workload, the underlying volume characteristics are optimized to support Microsoft SQL Server.

- **Application-specific** — When you are creating volumes using an application-specific workload, the

system may recommend an optimized volume configuration to minimize contention between application workload I/O and other traffic from your application instance. Volume characteristics like I/O type, segment size, controller ownership, and read and write cache are automatically recommended and optimized for workloads that are created for the following application types.

  - Microsoft SQL Server
  - Microsoft Exchange Server
  - Video surveillance applications
  - VMware ESXi (for volumes to be used with Virtual Machine File System)

    You can review the recommended volume configuration and edit, add, or delete the system-recommended volumes and characteristics using the Add/Edit Volumes dialog box.

- **Other (or applications without specific volume creation support)** — Other workloads use a volume configuration that you must manually specify when you want to create a workload that is not associated with a specific application, or if there is no built-in optimization for the application you intend to use on the storage array. You must manually specify the volume configuration using the Add/Edit Volumes dialog box.

## Why do I not see all my volumes, hosts, or host clusters?

Snapshot volumes with a DA-enabled base volume are not eligible to be assigned to a host that is not Data Assurance (DA) capable. You must disable DA on the base volume before a snapshot volume can be assigned to a host that is not DA capable.

Consider the following guidelines for the host to which you are assigning the snapshot volume:

- A host is not DA capable if it is connected to the storage array through an I/O interface that is not DA capable.
- A host cluster is not DA capable if it has at least one host member that is not DA capable.

> ⓘ You cannot disable DA on a volume that is associated with snapshots (consistency groups, snapshot groups, snapshot images, and snapshot volumes), volume copies, and mirrors. All associated reserved capacity and snapshot objects must be deleted before DA can be disabled on the base volume.

## Why can I not delete the selected workload?

This workload consists of a group of volumes that were created using the command line interface (CLI) or migrated (imported/exported) from a different storage array. As a result, the volumes in this workload are not associated with an application-specific workload, so the workload cannot be deleted.

## How do application-specific workloads help me manage my storage array?

The volume characteristics of your application-specific workload dictate how the workload interacts with the components of your storage array and helps determine the performance of your environment under a given configuration.

An application is software such as SQL Server or Exchange. You define one or more workloads to support each application. For some applications, the system automatically recommends a volume configuration that

optimizes storage. Characteristics such as I/O type, segment size, controller ownership, and read and write cache are included in the volume configuration.

## What do I need to do to recognize the expanded capacity?

If you increase the capacity for a volume, the host might not immediately recognize the increase in volume capacity.

Most operating systems recognize the expanded volume capacity and automatically expand after the volume expansion is initiated. However, some might not. If your OS does not automatically recognize the expanded volume capacity, you might need to perform a disk rescan or reboot.

After you have expanded the volume capacity, you must manually increase the file system size to match. How you do this depends on the file system you are using.

Refer to your host operating system documentation for additional details.

## When would I want to use the assign host later selection?

If you want to speed the process for creating volumes, you can skip the host assignment step so that newly created volumes are initialized offline.

Newly created volumes must be initialized. The system can initialize them using one of two modes – either an Immediate Available Format (IAF) background initialization process or an offline process.

When you map a volume to a host, it forces any initializing volumes in that group to transition to background initialization. This background initialization process allows for concurrent host I/O, which can sometimes be time-consuming.

When none of the volumes in a volume group are mapped, offline initialization is performed. The offline process is much faster than the background process.

## What do I need to know about host block size requirements?

For EF300 and EF600 systems, a volume can be set to support a 512-byte or a 4KiB block size (also called "sector size"). You must set the correct value during volume creation. If possible, the system suggests the appropriate default value.

Before setting the volume block size, read the following limitations and guidelines.

- Some operating systems and virtual machines (notably VMware, at this time) require a 512-byte block size and do not support 4KiB, so make sure you know the host requirements before creating a volume. Typically, you can achieve the best performance by setting a volume to present a 4KiB block size; however, ensure that your host allows for 4KiB (or “4Kn”) blocks.
- The type of drives you select for your pool or volume group also determines what volume block sizes are supported, as follows:
  - If you create a volume group using drives that write to 512-byte blocks, then you can only create volumes with 512-byte blocks.
  - If you create a volume group using drives that write to 4KiB blocks, then you can create volumes with either 512-byte or 4KiB blocks.
- If the array has an iSCSI host interface card, all volumes are limited to 512-byte blocks (regardless of

volume group block size). This is due to a specific hardware implementation.

- You cannot change a block size once it is set. If you need to change a block size, you must delete the volume and re-create it.

## Why would I need to create a host cluster?

You need to create a host cluster if you want to have two or more hosts share access to the same set of volumes. Normally, the individual hosts have clustering software installed on them to coordinate volume access.

## How do I know which host operating system type is correct?

The Host Operating System Type field contains the operating system of the host. You can select the recommended host type from the drop-down list or allow the Host Context Agent (HCA) to configure the host and appropriate host operating system type.

The host types that appear in the drop-down list depend on the storage array model and the firmware version. The most recent versions display the most common options first, which are the most likely to be appropriate. Appearance on this list does not imply the option is fully supported.

For more information about host support, refer to the NetApp Interoperability Matrix Tool.

Some of the following host types might appear in the list:

| Host Operating System type | Operating System (OS) and multipath driver |
|---|---|
| Linux DM-MP (Kernel 3.10 or later) | Supports Linux operating systems using a Device Mapper multipath failover solution with a 3.10 or later Kernel. |
| VMware ESXi | Supports VMware ESXi operating systems running the Native Multipathing Plug-in (NMP) architecture using the VMware built-in Storage Array Type Policy module SATP_ALUA. |
| Windows (clustered or non-clustered) | Supports Windows clustered or non-clustered configurations that are not running the ATTO multipathing driver. |
| ATTO Cluster (all operating systems) | Supports all cluster configurations using the ATTO Technology, Inc., multipathing driver. |
| Linux (Veritas DMP) | Supports Linux operating systems using a Veritas DMP multipathing solution. |
| Linux (ATTO) | Supports Linux operating systems using an ATTO Technology, Inc., multipathing driver. |
| Mac OS | Supports Mac OS versions using an ATTO Technology, Inc., multipathing driver. |
| Windows (ATTO) | Supports Windows operating systems using an ATTO Technology, Inc., multipathing driver. |

| Host Operating System type | Operating System (OS) and multipath driver |
|---|---|
| FlexArray (ALUA) | Supports a NetApp FlexArray system using ALUA for multipathing. |
| IBM SVC | Supports an IBM SAN Volume Controller configuration. |
| Factory Default | Reserved for the initial start-up of the storage array. If your host operating system type is set to Factory Default, change it to match the host operating system and multipath driver running on the connected host. |
| Linux DM-MP (Kernal 3.9 or earlier) | Supports Linux operating systems using a Device Mapper multipath failover solution with a 3.9 or earlier Kernel. |
| Window Clustered (deprecated) | If your host operating system type is set to this value, use the Windows (clustered or non-clustered) setting instead. |

After the HCA is installed and the storage is attached to the host, the HCA sends the host topology to the storage controllers through the I/O path. Based on the host topology, the storage controllers automatically define the host and the associated host ports, and then set the host type.

If the HCA does not select the recommended host type, you must manually set the host type.

## How do I match the host ports to a host?

If you are manually creating a host, you first must use the appropriate host bus adapter (HBA) utility available on the host to determine the host port identifiers associated with each HBA installed in the host.

When you have this information, select the host port identifiers that have logged into the storage array from the list provided in the Create Host dialog.

Make sure you select the appropriate host port identifiers for the host you are creating. If you associate the wrong host port identifiers, you might cause unintended access from another host to this data.

If you are automatically creating hosts using the host context agent (HCA) installed on each host, the HCA should automatically associate the host port identifiers with each host and configure them appropriately.

## What is the default cluster?

The default cluster is a system-defined entity that allows any unassociated host port identifier that has logged into the storage array to gain access to volumes assigned to the default cluster.

An unassociated host port identifier is a host port that is not logically associated with a particular host but is physically installed in a host and logged into the storage array.

If you want hosts to have specific access to certain volumes in the storage array, you must not use the default cluster. Instead, you must associate the host port identifiers with their corresponding hosts. This task can be done either manually during the Create Host operation or automatically using the host context agent (HCA) installed on each host. Then, you assign volumes either to an individual host or to a host cluster.

You should only use the default cluster in special situations where your external storage environment is conducive to allowing all the hosts and all the logged-in host port identifiers connected to the storage array have access to all of the volumes (all-access mode) without specifically making the hosts known to the storage array or the user interface.

Initially, you can assign volumes only to the default cluster through the command line interface (CLI). However, after you assign at least one volume to the default cluster, this entity (called Default Cluster) is displayed in the user interface where you can then manage this entity.

## What is redundancy check?

A redundancy check determines whether the data on a volume in a pool or volume group is consistent. Redundancy data is used to quickly reconstruct information on a replacement drive if one of the drives in the pool or volume group fails.

You can perform this check only on one pool or volume group at a time. A volume redundancy check performs the following actions:

- Scans the data blocks in a RAID 3 volume, a RAID 5 volume, or a RAID 6 volume, and then checks the redundancy information for each block. (RAID 3 can only be assigned to volume groups using the command line interface.)
- Compares the data blocks on RAID 1 mirrored drives.
- Returns redundancy errors if the data is determined to be inconsistent by the controller firmware.

Immediately running a redundancy check on the same pool or volume group might cause an error. To avoid this problem, wait one to two minutes before running another redundancy check on the same pool or volume group.

## What is preservation capacity?

Preservation capacity is the amount of capacity (number of drives) that is reserved in a pool to support potential drive failures.

When a pool is created, the system automatically reserves a default amount of preservation capacity depending on the number of drives in the pool.

Pools use preservation capacity during reconstruction, whereas volume groups use hot spare drives for the same purpose. The preservation capacity method is an improvement over hot spare drives because it allows reconstruction to happen faster. Preservation capacity is spread over a number of drives in the pool instead of on one drive in the case of a hot spare drive, so you are not limited by the speed or availability of one drive.

## What RAID level is best for my application?

To maximize the performance of a volume group, you must select the appropriate RAID

level.

You can determine the appropriate RAID level by knowing the read and write percentages for the applications that are accessing the volume group. Use the Performance page to obtain these percentages.

### RAID levels and application performance

RAID relies on a series of configurations, called levels, to determine how user and redundancy data is written and retrieved from the drives. Each RAID level provides different performance features. Applications with a high read percentage will perform well using RAID 5 volumes or RAID 6 volumes because of the outstanding read performance of the RAID 5 and RAID 6 configurations.

Applications with a low read percentage (write-intensive) do not perform as well on RAID 5 volumes or RAID 6 volumes. The degraded performance is the result of the way that a controller writes data and redundancy data to the drives in a RAID 5 volume group or a RAID 6 volume group.

Select a RAID level based on the following information.

#### RAID 0

**Description:**

- Non-redundant, striping mode.
- RAID 0 stripes data across all of the drives in the volume group.

**Data protection features:**

- RAID 0 is not recommended for high availability needs. RAID 0 is better for non-critical data.
- If a single drive fails in the volume group, all of the associated volumes fail, and all data is lost.

**Drive number requirements:**

- A minimum of one drive is required for RAID Level 0.
- RAID 0 volume groups can have more than 30 drives.
- You can create a volume group that includes all of the drives in the storage array.

#### RAID 1 or RAID 10

**Description:**

- Striping/mirror mode.

**How it works:**

- RAID 1 uses disk mirroring to write data to two duplicate disks simultaneously.
- RAID 10 uses drive striping to stripe data across a set of mirrored drive pairs.

**Data protection features:**

- RAID 1 and RAID 10 offer high performance and the best data availability.
- RAID 1 and RAID 10 use drive mirroring to make an exact copy from one drive to another drive.
- If one of the drives in a drive pair fails, the storage array can instantly switch to the other drive without any

loss of data or service.

- A single drive failure causes associated volumes to become degraded. The mirror drive allows access to the data.
- A drive-pair failure in a volume group causes all of the associated volumes to fail, and data loss could occur.

**Drive number requirements:**

- A minimum of two drives is required for RAID 1: one drive for the user data, and one drive for the mirrored data.
- If you select four or more drives, RAID 10 is automatically configured across the volume group: two drives for user data, and two drives for the mirrored data.
- You must have an even number of drives in the volume group. If you do not have an even number of drives and you have some remaining unassigned drives, go to **Pools & Volume Groups** to add additional drives to the volume group, and retry the operation.
- RAID 1 and RAID 10 volume groups can have more than 30 drives. A volume group can be created that includes all of the drives in the storage array.

#### RAID 5

**Description:**

- High I/O mode.

**How it works:**

- User data and redundant information (parity) are striped across the drives.
- The equivalent capacity of one drive is used for redundant information.

**Data protection features**

- If a single drive fails in a RAID 5 volume group, all of the associated volumes become degraded. The redundant information allows the data to still be accessed.
- If two or more drives fail in a RAID 5 volume group, all of the associated volumes fail, and all data is lost.

**Drive number requirements:**

- You must have a minimum of three drives in the volume group.
- Typically, you are limited to a maximum of 30 drives in the volume group.

#### RAID 6

**Description:**

- High I/O mode.

**How it works:**

- User data and redundant information (dual parity) are striped across the drives.
- The equivalent capacity of two drives is used for redundant information.

**Data protection features:**

- If one or two drives fail in a RAID 6 volume group, all of the associated volumes become degraded, but the redundant information allows the data to still be accessed.
- If three or more drives fail in a RAID 6 volume group, all of the associated volumes fail, and all data is lost.

**Drive number requirements:**

- You must have a minimum of five drives in the volume group.
- Typically, you are limited to a maximum of 30 drives in the volume group.

You cannot change the RAID level of a pool. The user interface automatically configures pools as RAID 6.

**RAID levels and data protection**

RAID 1, RAID 5, and RAID 6 write redundancy data to the drive media for fault tolerance. The redundancy data might be a copy of the data (mirrored) or an error-correcting code derived from the data. You can use the redundancy data to quickly reconstruct information on a replacement drive if a drive fails.

You configure a single RAID level across a single volume group. All redundancy data for that volume group is stored within the volume group. The capacity of the volume group is the aggregate capacity of the member drives minus the capacity reserved for redundancy data. The amount of capacity needed for redundancy depends on the RAID level used.

## Why are some drives not showing up?

In the Add Capacity dialog, not all drives are available for adding capacity to an existing pool or volume group.

Drives are not eligible for any of the following reasons:

- A drive must be unassigned and not secure-enabled. Drives already part of another pool, another volume group, or configured as a hot spare are not eligible. If a drive is unassigned but is secure-enabled, you must manually erase that drive for it to become eligible.
- A drive that is in a non-optimal state is not eligible.
- If the capacity of a drive is too small, it is not eligible.
- The drive media type must match within a pool or volume group. You cannot mix the following:
  - Hard Disk Drives (HDDs) with Solid State Disks (SSDs)
  - NVMe with SAS drives
  - Drives with 512-byte and 4KiB volume block sizes
- If a pool or volume group contains all secure-capable drives, non-secure-capable drives are not listed.
- If a pool or volume group contains all Federal Information Processing Standards (FIPS) drives, non-FIPS drives are not listed.
- If a pool or volume group contains all Data Assurance (DA)-capable drives and there is at least one DA-enabled volume in the pool or volume group, a drive that is not DA capable is not eligible, so it cannot be added to that pool or volume group. However, if there is no DA- enabled volume in the pool or volume group, a drive that is not DA capable can be added to that pool or volume group. If you decide to mix these drives, keep in mind that you cannot create any DA-enabled volumes.

Capacity can be increased in your storage array by adding new drives or by deleting pools or volume groups.

## Why can I not increase my preservation capacity?

If you have created volumes on all available usable capacity, you might not be able to increase preservation capacity.

Preservation capacity is the amount of capacity (number of drives) that is reserved on a pool to support potential drive failures. When a pool is created, the system automatically reserves a default amount of preservation capacity depending on the number of drives in the pool. If you have created volumes on all available usable capacity, you cannot increase preservation capacity without adding capacity to the pool by either adding drives or deleting volumes.

You can change the preservation capacity from Pools & Volume Groups. Select the pool that you want to edit. Click **View/Edit Settings**, and then select the **Settings** tab.

Preservation capacity is specified as a number of drives, even though the actual preservation capacity is distributed across the drives in the pool.

## What is Data Assurance?

Data Assurance (DA) implements the T10 Protection Information (PI) standard, which increases data integrity by checking for and correcting errors that might occur as data is transferred along the I/O path.

The typical use of the Data Assurance feature will check the portion of the I/O path between the controllers and drives. DA capabilities are presented at the pool and volume group level.

When this feature is enabled, the storage array appends error-checking codes (also known as cyclic redundancy checks or CRCs) to each block of data in the volume. After a data block is moved, the storage array uses these CRC codes to determine if any errors occurred during transmission. Potentially corrupted data is neither written to disk nor returned to the host. If you want to use the DA feature, select a pool or volume group that is DA capable when you create a new volume (look for **Yes** next to **DA** in the pool and volume group candidates table).

Make sure you assign these DA-enabled volumes to a host using an I/O interface that is capable of DA. I/O interfaces that are capable of DA include Fibre Channel, SAS, iSCSI over TCP/IP, NVMe/FC, NVMe/IB, NVME/RoCE and iSER over InfiniBand (iSCSI Extensions for RDMA/ IB). DA is not supported by SRP over InfiniBand.

## What is FDE/FIPS security?

FDE/FIPS security refers to secure-capable drives that encrypt data during writes and decrypt data during reads using a unique encryption key.

These secure-capable drives prevent unauthorized access to the data on a drive that is physically removed from the storage array. Secure-capable drives can be either Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives. FIPS drives have undergone certification testing.

For volumes that require FIPS support, use only FIPS drives. Mixing FIPS and FDE drives in a volume group or pool will result in all drives being treated as FDE drives. Also, an FDE drive cannot be added to or used as a spare in an all-FIPS volume group or pool.

## What is secure-capable (Drive Security)?

Drive Security is a feature that prevents unauthorized access to data on secure-enabled drives when removed from the storage array.

These drives can be either Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives.

## How do I view and interpret all SSD Cache statistics?

You can view nominal statistics and detailed statistics for SSD Cache.

Nominal statistics are a subset of the detailed statistics. The detailed statistics can be viewed only when you export all SSD statistics to a .csv file. As you review and interpret the statistics, keep in mind that some interpretations are derived by looking at a combination of statistics.

#### Nominal statistics

To view SSD Cache statistics, go to the **Manage** page. Select **Provisioning › Configure Pools & Volume Groups**. Select the SSD Cache that you want to view statistics for, and then select **More › View Statistics**. The nominal statistics are shown on the View SSD Cache Statistics dialog.

This feature is not available on the EF600 or EF300 storage system.

The list includes nominal statistics, which are a subset of the detailed statistics.

#### Detailed statistics

The detailed statistics consist of the nominal statistics, plus additional statistics. These additional statistics are saved along with the nominal statistics, but unlike the nominal statistics, they do not display in the View SSD Cache Statistics dialog. You can view the detailed statistics only after exporting the statistics to a .csv file.

The detailed statistics are listed after the nominal statistics.

## What is shelf loss protection and drawer loss protection?

Shelf loss protection and drawer loss protection are attributes of pools and volume groups that allow you to maintain data access in the event of a single shelf or drawer failure.

#### Shelf loss protection

A shelf is the enclosure that contains either the drives or the drives and the controller. Shelf loss protection guarantees accessibility to the data on the volumes in a pool or volume group if a total loss of communication occurs with a single drive shelf. An example of total loss of communication might be loss of power to the drive shelf or failure of both I/O modules (IOMs).

Shelf loss protection is not guaranteed if a drive has already failed in the pool or volume group. In this situation, losing access to a drive shelf and consequently another drive in the pool or volume group causes loss of data.

The criteria for shelf loss protection depends on the protection method, as described in the following table.

| Level | Criteria for shelf loss protection | Minimum number of shelves required |
|---|---|---|
| Pool | The pool must include drives from at least five shelves and there must be an equal number of drives in each shelf. Shelf loss protection is not applicable to high-capacity shelves; if your system contains high-capacity shelves, refer to Drawer Loss Protection. | 5 |
| RAID 6 | The volume group contains no more than two drives in a single drawer. | 3 |
| RAID 3 or RAID 5 | Each drive in the volume group is located in a separate shelf. | 3 |
| RAID 1 | Each drive in a RAID 1 pair must be located in a separate shelf. | 2 |
| RAID 0 | Cannot achieve Shelf Loss Protection. | Not applicable |

#### Drawer loss protection

A drawer is one of the compartments of a shelf that you pull out to access the drives. Only the high-capacity shelves have drawers. Drawer loss protection guarantees accessibility to the data on the volumes in a pool or volume group if a total loss of communication occurs with a single drawer. An example of total loss of communication might be loss of power to the drawer or failure of an internal component within the drawer.

Drawer loss protection is not guaranteed if a drive has already failed in the pool or volume group. In this situation, losing access to a drawer (and consequently another drive in the pool or volume group) causes loss of data.

The criteria for drawer loss protection depends on the protection method, as described in the following table:

| Level | Criteria for drawer loss protection | Minimum number of drawers required |
|---|---|---|
| Pool | Pool candidates must include drives from all drawers, and there must be an equal number of drives in each drawer.<br>The pool must include drives from at least five drawers and there must be an equal number of drives in each drawer.<br>A 60-drive shelf can achieve Drawer Loss Protection when the pool contains 15, 20, 25, 30, 35, 40, 45, 50, 55, or 60 drives. Increments in multiples of 5 can be added to the pool after initial creation. | 5 |
| RAID 6 | The volume group contains no more than two drives in a single drawer. | 3 |
| RAID 3 or 5 | Each drive in the volume group is located in a separate drawer | 3 |
| RAID 1 | Each drive in a mirrored pair must be located in a separate drawer. | 2 |
| RAID 0 | Cannot achieve Drawer Loss Protection. | Not applicable |

## How do I maintain shelf and drawer loss protection?

To maintain shelf and drawer loss protection for a pool or volume group, use the criteria specified in the following table.

| Level | Criteria for shelf/drawer loss protection | Minimum number of shelves/ drawers required |
|---|---|---|
| Pool | For shelves, the pool must contain no more than two drives in a single shelf.<br>For drawers, the pool must include an equal number of drives from each drawer. | 6 for shelves<br>5 for drawers |
| RAID 6 | The volume group contains no more than two drives in a single shelf or drawer. | 3 |
| RAID 3 or RAID 5 | Each drive in the volume group is located in a separate shelf or drawer. | 3 |

| Level | Criteria for shelf/drawer loss protection | Minimum number of shelves/ drawers required |
|---|---|---|
| RAID 1 | Each drive in a mirrored pair must be located in a separate shelf or drawer. | 2 |
| RAID 0 | Cannot achieve shelf/drawer loss protection. | Not applicable |

Shelf/drawer loss protection is not maintained if a drive has already failed in the pool or volume group. In this situation, losing access to a drive shelf or drawer, and consequently another drive in the pool or volume group, causes loss of data.

## What is optimization capacity for pools?

SSD drives will have longer life and better maximum write performance when a portion of their capacity is unallocated.

For drives associated with a pool, unallocated capacity is comprised of a pool's preservation capacity, the free capacity (capacity not used by volumes), and a portion of the usable capacity set aside as additional optimization capacity. The additional optimization capacity ensures a minimum level of optimization capacity by reducing the usable capacity, and as such, is not available for volume creation.

When a pool is created, a recommended optimization capacity is generated that provides a balance of performance, drive wear life, and available capacity. The Additional Optimization Capacity slider located in the Pool Settings dialog allows adjustments to the pool's optimization capacity. Adjusting the slider provides for better performance and drive wear life at the expense of available capacity, or additional available capacity at the expense of performance and drive wear life.

The Additional Optimization Capacity slider is only available for EF600 and EF300 storage systems.

## What is optimization capacity for volume groups?

SSD drives will have longer life and better maximum write performance when a portion of their capacity is unallocated.

For drives associated with a volume group, unallocated capacity is comprised of a volume group's free capacity (capacity not used by volumes), and a portion of the usable capacity set aside as optimization capacity. The additional optimization capacity ensures a minimum level of optimization capacity by reducing the usable capacity, and as such, is not available for volume creation.

When a volume group is created, a recommended optimization capacity is generated that provides a balance of performance, drive wear life, and available capacity. The Additional Optimization Capacity slider in the Volume Group Settings dialog allows adjustments to a volume group's optimization capacity. Adjusting the slider provides for better performance and drive wear life at the expense of available capacity, or additional available capacity at the expense of performance and drive wear life.

Additional Optimization Capacity slider is only available for EF600 and EF300 storage systems.

## What is resource provisioning capable?

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.

A resource-provisioned volume is a thick volume in an SSD volume group or pool, where drive capacity is allocated (assigned to the volume) when the volume is created, but the drive blocks are deallocated (unmapped). By comparison, in a traditional thick volume, all drive blocks are mapped or allocated during a background volume initialization operation in order to initialize the Data Assurance protection information fields and to make data and RAID parity consistent in each RAID stripe. With a resource provisioned volume, there is no time-bound background initialization. Instead, each RAID stripe is initialized upon the first write to a volume block in the stripe.

Resource-provisioned volumes are supported only on SSD volume groups and pools, where all drives in the group or pool support the NVMe Deallocated or Unwritten Logical Block Error Enable (DULBE) error recovery capability. When a resource-provisioned volume is created, all drive blocks assigned to the volume are deallocated (unmapped). In addition, hosts can deallocate logical blocks in the volume using the NVMe Dataset Management command. Deallocating blocks can improve SSD wear life and increase maximum write performance. The improvement varies with each drive model and capacity.

## What do I need to know about the resource-provisioned volumes feature?

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.

The Resource Provisioning capability is not available at this time. In some views, components might be reported as resource-provisioning capable, but the ability to create resource-provisioned volumes has been disabled until it can be re-enabled in a future update.

### Resource-provisioned volumes

A resource-provisioned volume is a thick volume in an SSD volume group or pool, where drive capacity is allocated (assigned to the volume) when the volume is created, but the drive blocks are deallocated (unmapped). By comparison, in a traditional thick volume, all drive blocks are mapped or allocated during a background volume initialization operation in order to initialize the Data Assurance protection information fields and to make data and RAID parity consistent in each RAID stripe. With a resource provisioned volume, there is no time-bound background initialization. Instead, each RAID stripe is initialized upon the first write to a volume block in the stripe.

Resource-provisioned volumes are supported only on SSD volume groups and pools, where all drives in the group or pool support the NVMe Deallocated or Unwritten Logical Block Error Enable (DULBE) error recovery capability. When a resource-provisioned volume is created, all drive blocks assigned to the volume are deallocated (unmapped). In addition, hosts can deallocate logical blocks in the volume using the NVMe Dataset Management command. Deallocating blocks can improve SSD wear life and increase maximum write performance. The improvement varies with each drive model and capacity.

### Enabling and disabling the feature

Resource provisioning is enabled by default on systems where the drives support DULBE. You can disable that default setting from Pools & Volume Groups. Disabling resource provisioning is a permanent action for existing

volumes and cannot be reversed (i.e., you cannot re-enable resource provisioning for these volume groups and pools).

However, if you want to re-enable resource provisioning again for any new volumes you create, you can do so from **Settings › System**. Be aware that when you re-enable resource provisioning, only newly created volume groups and pools are affected. Any existing volume groups and pools will remain unchanged. If desired, you can also disable resource provisioning again from **Settings › System**.

## What is the difference between internal security key and external security key management?

When you implement the Drive Security feature, you can use an internal security key or an external security key to lock down data when a secure-enabled drive is removed from the storage array.

A security key is a string of characters, which is shared between the secure-enabled drives and controllers in a storage array. Internal keys are maintained on the controller's persistent memory. External keys are maintained on a separate key management server, using a Key Management Interoperability Protocol (KMIP).

## What do I need to know before creating a security key?

A security key is shared by controllers and secure-enabled drives within a storage array. If a secure-enabled drive is removed from the storage array, the security key protects the data from unauthorized access.

You can create and manage security keys using one of the following methods:

- Internal key management on the controller's persistent memory.
- External key management on an external key management server.

### Internal key management

Internal keys are maintained and "hidden" in a non-accessible location on the controller's persistent memory. Before creating an internal security key, you must do the following:

1. Install secure-capable drives in the storage array. These drives can be Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives.
2. Make sure the Drive Security feature is enabled. If necessary, contact your storage vendor for instructions on enabling the Drive Security feature.

You can then create an internal security key, which involves defining an identifier and a pass phrase. The identifier is a string that is associated with the security key, and is stored on the controller and on all drives associated with the key. The pass phrase is used to encrypt the security key for backup purposes. When you are finished, the security key is stored on the controller in a non-accessible location. You can then create secure-enabled volume groups or pools, or you can enable security on existing volume groups and pools.

### External key management

External keys are maintained on a separate key management server, using a Key Management Interoperability Protocol (KMIP). Before creating an external security key, you must do the following:

1. Install secure-capable drives in the storage array. These drives can be Full Disk Encryption (FDE) drives or

Federal Information Processing Standard (FIPS) drives.

2. Make sure the Drive Security feature is enabled. If necessary, contact your storage vendor for instructions on enabling the Drive Security feature
3. Obtain a signed, client certificate file. A client certificate validates the storage array's controllers, so the key management server can trust their KMIP requests.
   a. First, you complete and download a client Certificate Signing Request (CSR). Go to **Settings › Certificates › Key Management › Complete CSR**.
   b. Next, you request a signed client certificate from a CA that is trusted by the key management server. (You can also create and download a client certificate from the key management server using the downloaded CSR file.)
   c. Once you have a client certificate file, copy that file to the host where you are accessing System Manager.
4. Retrieve a certificate file from the key management server, and then copy that file to the host where you are accessing System Manager. A key management server certificate validates the key management server, so the storage array can trust its IP address. You can use a root, intermediate, or server certificate for the key management server.

You can then create an external key, which involves defining the IP address of the key management server and the port number used for KMIP communications. During this process, you also load certificate files. When you are finished, the system connects to the key management server with the credentials you entered. You can then create secure-enabled volume groups or pools, or you can enable security on existing volume groups and pools.

## Why do I need to define a pass phrase?

The pass phrase is used to encrypt and decrypt the security key file stored on the local management client. Without the pass phrase, the security key cannot be decrypted and used to unlock data from a secure-enabled drive if it is re-installed in another storage array.