



## Hosts

### SANtricity 11.6

NetApp  
February 12, 2024

# Table of Contents

Hosts .....	1
Concepts .....	1
How tos .....	5
FAQs .....	23

# Hosts

## Concepts

### Host terminology

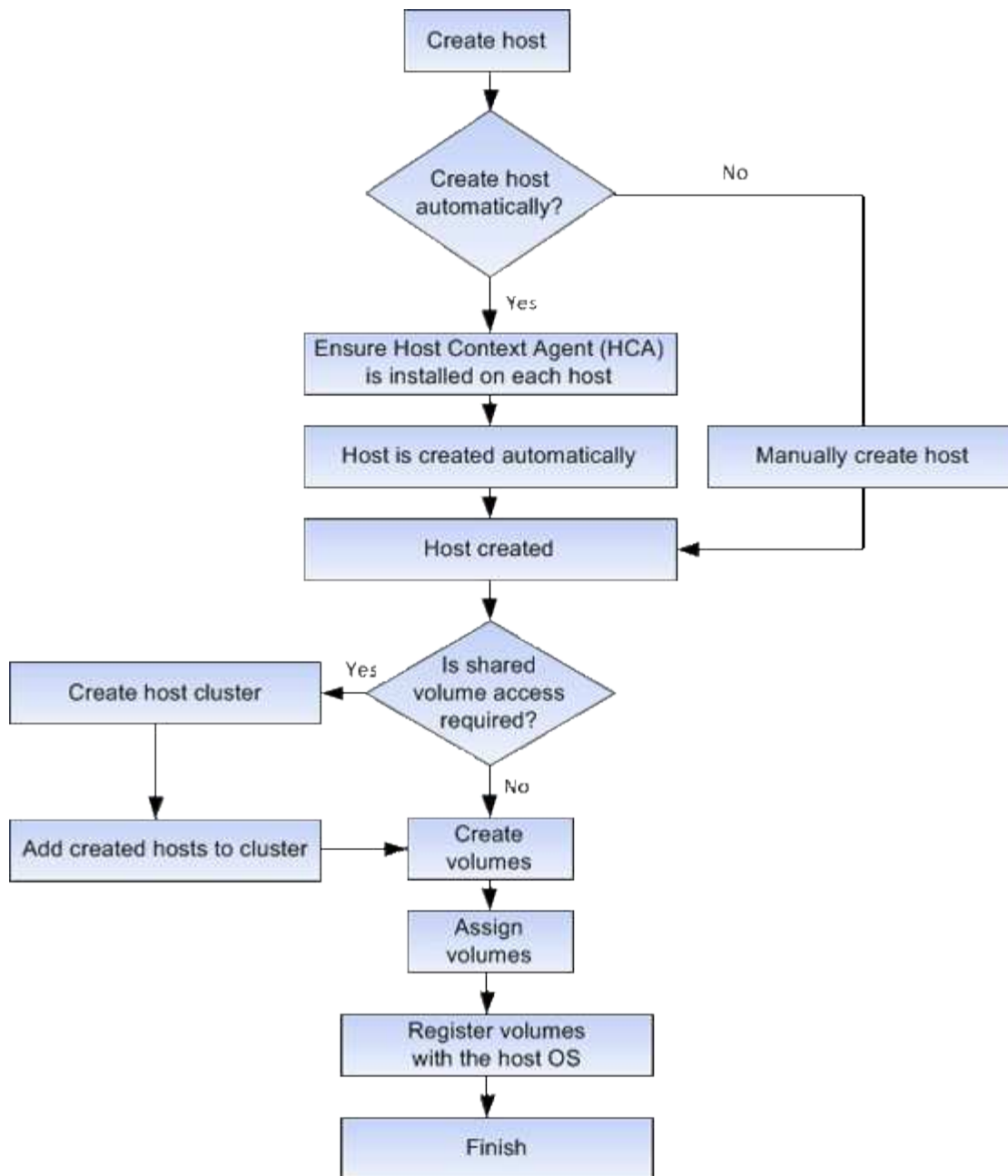
Learn how the host terms apply to your storage array.

Component	Definition
Host	A host is a server that sends I/O to a volume on a storage array.
Host name	The host name should equate to the system name of the host.
Host cluster	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.
Host interface protocol	A host interface protocol is the connection (such as Fibre Channel, iSCSI, etc.) between the controllers and the hosts.
HBA or Network Interface Card (NIC)	A host bus adapter (HBA) is a board that resides in a host and contains one or more host ports.
Host port	A host port is a port on a host bus adapter (HBA) that provides the physical connection to a controller and is used for I/O operations.
Host port identifier	<p>A host port identifier is a unique world-wide name associated with each host port on a host bus adapter (HBA).</p> <ul style="list-style-type: none"><li>• Internet Small Computer System Interface (iSCSI) host port identifiers must have between 1 and 233 characters. iSCSI host port identifiers display in standard IQN format (e.g., <code>iqn.xxx.com.xxx:8b3ad</code>).</li><li>• Non-iSCSI host port identifiers such as Fibre Channel and Serial Attached SCSI (SAS) display as colon-delimited after every two characters (e.g., <code>xx:yy:zz</code>). Fibre Channel host port identifiers must have 16 characters.</li></ul>

Component	Definition
Host operating system type	The host operating system type is a configuration setting that defines how the controllers in the storage array react to I/O depending on the operating system (or variant) of the host. This is also sometimes called <i>host type</i> for short.
Controller host port	A controller host port is a port on the controller that provides the physical connection to a host and is used for I/O operations.
LUN	<p>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.</p> <p>Each host has its own LUN address space. Therefore, the same LUN can be used by different hosts to access different volumes.</p>

## Workflow for host creation and volume assignment

The following figure illustrates how to configure host access.



## Automatic versus 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. You can create a host automatically or manually.

### Automatic creation

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 using System Manager.

After the HCA performs its automatic detection, the host automatically appears in the Hosts page 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 creation

You might want to manually create a host for one of the following reasons:

1. You chose not to install the HCA utility on your hosts.
2. You want to ensure that the host port identifiers that were detected by the storage array controllers are associated correctly with the hosts.

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 to hosts and host clusters

For a host or host cluster to send I/O to a volume, you must assign the volume to the host or host cluster.

You can select 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.

## Access volumes

An access volume is a factory-configured volume on the storage array that is used for communication with the storage array and the host through the host I/O connection. The access volume requires a Logical Unit Number (LUN).

The access volume is used in two instances:

- **Automatic host creation** — The access volume is used by the Host Context Agent (HCA) utility to push host information (name, ports, host type) to System Manager for automatic host creation.
- **In-band management** — The access volume is used for an in-band connection to manage the storage array. This can only be done if you are managing the storage array with the command line interface (CLI).



In-band management is not available for EF600 storage systems.

An access volume is automatically created the first time you assign a volume to a host. For example, if you assign Volume\_1 and Volume\_2 to a host, when you view results of that assignment, you see three volumes (Volume\_1, Volume\_2, and Access).

If you are not automatically creating hosts or managing a storage array in-band with the CLI, you do not need the access volume, and you can free up the LUN by deleting the access volume. This action removes the volume-to-LUN assignment as well as any in-band management connections to the host.

## Maximum number of LUNs

The storage array has a maximum number of logical unit numbers (LUNs) that can be used for each host.

The maximum number depends on the operating system of the host. The storage array tracks the number of LUNs used. If you try to assign a volume to a host that exceeds the maximum number of LUNs, the host cannot access the volume.

## How to

### Configure host access

#### Create host automatically

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

#### Before you begin

The Host Context Agent (HCA) is installed and running on every host connected to the storage array. Hosts with the HCA installed and connected to the storage array are created automatically. To install the HCA, install SANtricity Storage Manager on the host and select the Host option. The HCA is not available on all supported operating systems. If it is not available, you must create the host manually.

#### Steps

1. Select **Storage > Hosts**.

The table lists the automatically-created hosts.

2. Verify that the information provided by the HCA is correct (name, host type, host port identifiers).

If you need to change any of the information, select the host, and then click **View/Edit Settings**.

3. **Optional:** If you want the automatically-created host to be in a cluster, create a host cluster and add the

host or hosts.

## Results

After a host is created automatically, the system displays the following items in the Hosts tile table:

- 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.

## Create host manually

For hosts that cannot be automatically discovered, you can manually create a host. 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.

### About this task

Keep these guidelines in mind when you create a host:

- 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. Select **Storage > Hosts**.
2. Click **Create > Host**.

The **Create Host** dialog box appears.

3. 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	<b>Optional:</b> If you have more than one type of host interface supported on your storage array, select the host interface type that you want to use.
Host ports	<p>Do one of the following:</p> <ul style="list-style-type: none"><li>• <b>Select I/O Interface</b></li></ul> <p>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.</p> <ul style="list-style-type: none"><li>• <b>Manual add</b></li></ul> <p>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.</p> <p>You can manually enter the host port identifiers or copy/paste them from the utility (one at a time) into the <b>Host ports</b> field.</p> <p>You must select one host port identifier at a time to associate it with the host, but you can continue to select as many identifiers that are associated with the host. Each identifier is displayed in the <b>Host ports</b> field. If necessary, you also can remove an identifier by selecting the <b>X</b> next to it.</p>

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

4. Click **Create**.

## Results

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.

## Create host cluster

You create a host cluster when two or more hosts require I/O access to the same volumes.

## 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).
- 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.

DA is **not** supported by iSCSI over TCP/IP, or by the SRP over InfiniBand.

- 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. Select **Storage > Hosts**.
2. Select **Create > Host Cluster**.

The **Create Host Cluster** dialog box appears.

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

### Field details

Setting	Description
Name	Type the name for the new host cluster.
Hosts	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.

4. Click **Create**.

If the selected hosts are attached to interface types that have different Data Assurance (DA) capabilities, a dialog box 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.

### Results

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

### 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. In addition, the volume creation sequence provides options to allocate specific amounts of capacity to each volume you want to create.

### About this task

Most application types default to a user-defined volume configuration. Some application types have a smart configuration applied at volume creation. For example, if you are creating volumes for 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. System Manager uses this information to create an optimal volume configuration for you, which can be edited as needed.



If you want to mirror a volume, first create the volumes that you want to mirror, and then use the **Storage › Volumes › Copy Services › Mirror a volume asynchronously** option.

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

### Step 1: Select host for a volume

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. In addition, the volume creation sequence provides options to allocate specific amounts of capacity to each volume you want to create.

#### Before you begin

- Valid hosts or host clusters exist under the **Hosts** tile.
- Host port identifiers have been defined for the host.
- Before creating a 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.

#### 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.



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. Select **Storage › Volumes**.
2. Select **Create › Volume**.

The **Create Volumes** dialog box appears.

3. 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.
4. To continue the volume creation sequence for the selected host or host cluster, click **Next**, and go to [Step 2: Select a workload for a volume](#).

The **Select Workload** dialog box appears.

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

Select a workload to customize the storage array configuration for a specific application, such as Microsoft SQL Server, Microsoft Exchange, Video Surveillance applications, or VMware. You can select "Other application" if the application you intend to use on this storage array is not listed.

## About this task

This task describes how to create volumes for an existing workload.

- *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. 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.
- *When you are creating volumes using "Other" applications* (or applications without specific volume creation support), you manually specify the volume configuration using the **Add/Edit Volumes** dialog box.

## Steps

1. Do one of the following:
  - Select the **Create volumes for an existing workload** option to create volumes for an existing workload.
  - Select the **Create a new workload** option to define a new workload for a supported application or for "Other" applications.
    - 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 [Step 3: Add or edit volumes](#).

## Step 3: Add or edit volumes

### Before you begin

- The pools or volume groups must have sufficient free capacity.
- To create a Data Assurance (DA)-enabled volume, the host connection you are planning to use must support DA.

### Selecting a DA capable pool or volume group

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 in System Manager. 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.



DA is not supported by iSCSI over TCP/IP, or by the SRP over InfiniBand.

- To create a secure-enabled volume, a security key must be created for the storage array.

### Selecting a secure-capable pool or volume group

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 in System Manager. 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.

### About this task

You create volumes from pools or volume groups. The **Add/Edit Volumes** dialog box shows all eligible pools and volume groups on the storage array. 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:
  - **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 by System Manager during the volume creation sequence. You can either accept the default name or provide a more descriptive one indicating the type of data stored in the volume.
Reported Capacity	<p>Define the capacity of the new volume and the capacity units to use (MiB, GiB, or TiB). For <b>Thick volumes</b>, the minimum capacity is 1 MiB, and the maximum capacity is determined by the number and capacity of the drives in the pool or volume group.</p> <p>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.</p> <p>Capacity in a pool is allocated in 4-GiB increments. Any capacity that is not a multiple of 4 GiB is allocated but not usable. To make sure that the entire capacity is usable, specify the capacity in 4-GiB increments. If unusable capacity exists, the only way to regain it is to increase the capacity of the volume.</p>

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



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

- **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 by System Manager during the volume creation sequence. You can either accept the default name or provide a more descriptive one indicating the type of data stored in the volume.
Reported Capacity	<p>Define the capacity of the new volume and the capacity units to use (MiB, GiB, or TiB). For <b>Thick volumes</b>, the minimum capacity is 1 MiB, and the maximum capacity is determined by the number and capacity of the drives in the pool or volume group.</p> <p>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.</p> <p>Capacity in a pool is allocated in 4-GiB increments. Any capacity that is not a multiple of 4 GiB is allocated but not usable. To make sure that the entire capacity is usable, specify the capacity in 4-GiB increments. If unusable capacity exists, the only way to regain it is to increase the capacity of the volume.</p>
Volume Type	Volume type indicates the type of volume that was created for an application-specific workload.

Field	Description
Segment Size	<p>Shows the setting for segment sizing, which only appears for volumes in a volume group. You can change the segment size to optimize performance.</p> <p><b>Allowed segment size transitions</b> — System Manager determines the segment size transitions that are allowed. Segment sizes that are inappropriate transitions from the current segment size are unavailable on the drop-down list. Allowed transitions usually are double or half of the current segment size. For example, if the current volume segment size is 32 KiB, a new volume segment size of either 16 KiB or 64 KiB is allowed.</p> <p><b>SSD Cache-enabled volumes</b> — You can specify a 4-KiB segment size for SSD Cache-enabled volumes. Make sure you select the 4-KiB segment size only for SSD Cache-enabled volumes that handle small-block I/O operations (for example, 16 KiB I/O block sizes or smaller). Performance might be impacted if you select 4 KiB as the segment size for SSD Cache-enabled volumes that handle large block sequential operations.</p> <p><b>Amount of time to change segment size</b> — The amount of time to change a volume's segment size depends on these variables:</p> <ul style="list-style-type: none"> <li>• The I/O load from the host</li> <li>• The modification priority of the volume</li> <li>• The number of drives in the volume group</li> <li>• The number of drive channels</li> <li>• The processing power of the storage array controllers</li> </ul> <p>When you change the segment size for a volume, I/O performance is affected, but your data remains available.</p>
Secure-capable	<p><b>Yes</b> appears next to "Secure-capable" only if the drives in the pool or volume group are secure-capable.</p> <p>Drive security prevents unauthorized access to the data on a drive that is physically removed from the storage array. This option is available only when the drive security feature has been enabled, and a security key is set up for the storage array.</p> <p>A pool or volume group can contain both secure-capable and non-secure-capable drives, but all drives must be secure-capable to use their encryption capabilities.</p>

Field	Description
DA	<p><b>Yes</b> appears next to "DA" only if the drives in the pool or volume group support Data Assurance (DA).</p> <p>DA increases data integrity across the entire storage system. DA enables the storage array to check for errors that might occur as data is transferred through the controllers down to the drives. Using DA for the new volume ensures that any errors are detected.</p>

2. To continue the volume creation sequence for the selected application, click **Next**, and go to [Step 4: Review volume configuration](#).

#### Step 4: Review volume configuration

Review a summary of the volumes you intend to create and make any necessary changes.

#### Steps

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

#### Results

System Manager creates the new volumes in the selected pools and volume groups, and then displays the new volumes in the All Volumes table.

#### After you finish

- 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.

#### Assign volumes

You must assign a volume to a host or a host cluster so it can be used for I/O operations. This assignment grants a host or host cluster access to one or more volumes in a storage array.

#### Before you begin

Keep these guidelines in mind when you assign volumes:

- 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.

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.

### About this task

All unassigned volumes are displayed, 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.

### Steps

1. Select **Storage > Hosts**.
2. 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.

3. 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.
4. 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.

## Manage hosts and host clusters

### Change the settings for a host

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

### Steps

1. Select **Storage > Hosts**.
2. Select the host that you want to edit, and then click **View/Edit Settings**.

A dialog box appears that shows the current host settings.

3. If it is not already selected, click the **Properties** tab.
4. 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	<p>You can choose one of the following options:</p> <ul style="list-style-type: none"><li>• <b>None</b> — The host remains a standalone host. If the host was associated to a host cluster, the system removes the host from the cluster.</li><li>• <b>&lt;Host Cluster&gt;</b> — The system associates the host to the selected cluster.</li></ul>
Host operating system type	You can change the type of operating system running on the host you defined.

5. Click **Save**.

### Change the settings for a host cluster

You can change the host cluster name, or add or remove hosts in a host cluster.

#### Steps

1. Select **Storage > Hosts**.
2. Select the host cluster you want to edit, and then click **View/Edit Settings**.

A dialog box appears that shows the current host cluster settings.

3. Change the settings for the host cluster as appropriate.

#### Field Details

Setting	Description
Name	You can specify the user-supplied name of the host cluster. Specifying a name for a cluster is required.
Associated Hosts	<p>To add a host, click the <b>Associated Hosts</b> box, and then select a host name from the drop-down list. You cannot manually enter a host name.</p> <p>To delete a host, click the <b>X</b> next to the host name.</p>

4. Click **Save**.

## Unassign volumes

Unassign volumes from hosts or host clusters if you no longer need I/O access to that volume 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. Select **Storage > Hosts**.
2. 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.

3. 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.
4. 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 host port identifiers for a host

Change the host port identifiers when you want to change the user label on a host port identifier, add a new host port identifier to the host, or delete a host port identifier from the host.

### About this task

When changing host port identifiers, keep the following guidelines in mind:

- **Add** — When you add a host port, you are associating the host port identifier to the host you created to connect to your storage array. You can manually enter port information using a host bus adapter (HBA) utility.
- **Edit** — You can edit the host ports to move (associate) a host port to a different host. You might have moved the host bus adapter or iSCSI initiator to a different host, so you must move (associate) the host port to the new host.
- **Delete** — You can delete host ports to remove (unassociate) host ports from a host.

### Steps

1. Select **Storage > Hosts**.

2. Select the host to which the ports will be associated, and then click **View/Edit Settings**.


If you want to add ports to a host in a host cluster, expand the host cluster and select the desired host. You cannot add ports at the host cluster level.

A dialog box appears that shows the current host settings.

3. Click the **Host Ports** tab.

The dialog box shows the current host port identifiers.

4. Change the host port identifier settings as appropriate.

Setting	Description
Host Port	<p>You can choose one of the following options:</p> <ul style="list-style-type: none"><li>• <b>Add</b> — 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.<ul style="list-style-type: none"><li>◦ Fibre Channel host port identifier names must have 16 characters.</li><li>◦ Infiniband host port identifier names must have 16 characters.</li><li>◦ iSCSI host port identifier names have a maximum of 223 characters.</li><li>◦ The port must be unique.</li><li>◦ A port number that has already been configured is not allowed.</li></ul></li><li>• <b>Delete</b> — Use Delete to remove (unassociate) a host port identifier. The <b>Delete</b> 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.</li></ul> <div> 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.</div>
Label	To change the port label name, click the <b>Edit</b> icon (pencil). The port label name must be unique. A label name that has already been configured is not allowed.
CHAP Secret	<p>Appears only for iSCSI hosts. You can set or change the CHAP secret for the initiators (iSCSI hosts).</p> <p>System Manager 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.</p>

5. Click **Save**.



## Delete host or host cluster

You can delete a host or host cluster.

### 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. Select **Storage › Hosts**.
2. Select the host or host cluster that you want to delete, and then click **Delete**.

The **confirmation** dialog box appears.

3. 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.

## FAQs

### What are hosts and host clusters?

A host is a server that sends I/O to a volume on a storage array. 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.

You define a host separately. It can either be an independent entity or be added to a host cluster. You can assign volumes to an individual host, or a host can be part of a host cluster that shares access to one or more volumes with other hosts in the host cluster.

The host cluster is a logical entity that you create in SANtricity System Manager. You must add hosts to the host cluster before you can assign volumes.

## 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 (ATTO)	Supports Mac OS versions using an ATTO Technology, Inc., multipathing driver.

Host Operating System type	Operating System (OS) and multipath driver
Windows (ATTO)	Supports Windows operating systems using an ATTO Technology, Inc., multipathing 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 (Kernel 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 in System Manager.

## What are HBAs and adapter ports?

A host bus adapter (HBA) is a board that resides in a host and contains one or more host ports. A host port is a port on a host bus adapter (HBA) that provides the physical connection to a controller and is used for I/O operations.

The adapter ports on the HBA are called host ports. Most HBAs have either one or two host ports. The HBA has a unique World Wide Identifier (WWID), and each HBA host port has a unique WWID. The host port identifiers are used to associate the appropriate HBA with the physical host when you are either manually creating the host through SANtricity System Manager or automatically creating the host using the host context agent.

## 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 of System Manager.



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.

## How do I create CHAP secrets?

If you set up Challenge Handshake Authentication Protocol (CHAP) authentication on any iSCSI host connected to the storage array, you must re-enter that initiator CHAP secret for each iSCSI host. To do this, you can use System Manager either as part of the Create Host operation or through the View/Edit Settings option.

If you are using CHAP mutual authentication, you also must define a target CHAP secret for the storage array in the Settings page and re-enter that target CHAP secret on each iSCSI host.

## What is the default cluster?

The default cluster is a system-defined entity that allows any unassociated host bus adapter (HBA) host port identifier that has logged into the storage array to gain access to any volumes assigned to the default cluster. An unassociated host port identifier is a host port that while physically installed in a host and logged into the storage array is not logically associated with a particular host.



If you want your 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 can be done either manually using System Manager 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 System Manager.

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 System Manager, and you can then use System Manager to manage this entity.

## Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

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

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

## Trademark information

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