NetApp

Create storage

SANtricity 11.5

NetApp
February 12, 2024

Table of Contents

Create storage

Create workloads

You can create workloads for any type of application.

About this task

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

System Manager 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)

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.

- *When using other application types*, you manually specify the volume configuration using the Add/Edit Volumes dialog box.

Steps

1. Select **Storage › Volumes**.

2. Select **Create › Workload**.

   The **Create Application Workload** dialog box appears.

3. 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.

4. Click **Create**.

After you finish

You are ready to add storage capacity to the workload you created. Use the **Create Volume** option to create one or more volumes for an application, and to allocate specific amounts of capacity to each volume.

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.

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

- Step 1: Select host
- Step 2: Select workload
- Step 3: Add or edit volumes
- Step 4: Review configuration

> (i) 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.

Step 1: Select host

You select a specific host or host cluster to assign it to a volume. This assignment grants a host or a host cluster access to one or more volumes for I/O operations. You can choose to assign a host later, if needed.

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.

> (i) 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 .

    The Select Workload dialog box appears.

Step 2: Select workload

You 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

System Manager may suggest a volume configuration based on the application or workload you selected. This volume configuration is optimized based on the type of application the workload supports. You can accept the recommended volume configuration or you can edit it as needed. If you selected one of the "Other" applications, you must manually specify the volumes and characteristics you want to create.

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 communicated between a host and a storage array. 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	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.

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.

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. |

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. **Allowed segment size transitions** — 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. **SSD Cache-enabled volumes** — You can specify a 4-KiB segment size for SSD Cache-enabled volumes. Make sure you select the 4-KiB segment size only for SSD Cache-enabled volumes that handle small-block I/O operations (for example, 16 KiB I/O block sizes or smaller). Performance might be impacted if you select 4 KiB as the segment size for SSD Cache-enabled volumes that handle large block sequential operations. **Amount of time to change segment size** — The amount of time to change a volume's segment size depends on these variables: • The I/O load from the host • The modification priority of the volume • The number of drives in the volume group • The number of drive channels • The processing power of the storage array controllers When you change the segment size for a volume, I/O performance is affected, but your data remains available.

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

◦ **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	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. 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. 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.

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. **Allowed segment size transitions** — 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. **SSD Cache-enabled volumes** — You can specify a 4-KiB segment size for SSD Cache-enabled volumes. Make sure you select the 4-KiB segment size only for SSD Cache-enabled volumes that handle small-block I/O operations (for example, 16 KiB I/O block sizes or smaller). Performance might be impacted if you select 4 KiB as the segment size for SSD Cache-enabled volumes that handle large block sequential operations. **Amount of time to change segment size** — The amount of time to change a volume's segment size depends on these variables: • The I/O load from the host • The modification priority of the volume • The number of drives in the volume group • The number of drive channels • The processing power of the storage array controllers When you change the segment size for a volume, I/O performance is affected, but your data remains available.

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

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

Step 4: Review configuration

You can 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.