Dell EMC PowerVault ME4 Series Storage System

Administrator's Guide

July 2020
Rev. A06

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

1

Getting started

PowerVault Manager is a web-based interface for configuring, monitoring, and managing the storage system.

Each controller module in the storage system contains a web server, which is accessed when you sign in to the PowerVault Manager. You can access all functions from either controller in a dual-controller system. If one controller becomes unavailable, you can continue to manage the storage system from the partner controller.

In addition to PowerVault Manager, each controller module in the storage system has SNMP, FTP, SFTP, SMI-S, SLP, and command-line interfaces. See this guide for information about all interfaces other than the command-line interface, For information about using the command-line interface (CLI), see the *Dell EMC PowerVault ME4 Series Storage System CLI Guide*.

Topics:

New user setup

ME4 Series storage systems that are running firmware version G280 or later do not contain default users.

The first time that you connect to a storage system that is not deployed, you are prompted to set up a new user.

NOTE: The PowerVault Manager and CLI are the only interfaces through which a storage system can be accessed until the new user is created.

Configure and provision a new storage system

The PowerVault Manager offers two ways for you to set up and provision your storage system:

- Guided setup and provisioning
- Manual setup and provisioning

The guided setup and provisioning process provides options for you to quickly set up your system by guiding you through the configuration and provisioning process. It provides you with limited, yet optimal storage configuration options to quickly enable I/O operations.

Manual setup and provisioning process provides more provisioning options and greater flexibility, but with the added complexity of selecting all settings and provisioning options. These include creating disk groups and pools, creating volumes, and mapping volumes to initiators.

NOTE: If you choose to use guided setup, you can still manually provision the system after the system is set up.

To access guided setup for the first time:

1. Configure your web browser to access the PowerVault Manager as described in Web browser requirements and setup on page 11.
2. Temporarily set the management host NIC to a 10.0.0.x address or to the same IPv6 subnet to enable communication with the storage system.
3. In a supported web browser:
   - For an IPv4 network, type `https://10.0.0.2` to access controller module A.
   - For an IPv6 network, type `https://fd6e:23ce:fed3:19d1::1` to access controller module A.
4. If the storage system is running G275 firmware, sign in to the PowerVault Manager using the user name **`manage`** and password **`!manage`**.

   For more information about signing in, see Signing in and signing out on page 13. For more information about using these options, see Guided setup on page 32.

   If the storage system is running G280 firmware:

a. Click **Get Started**.
b. Read the Commercial Terms of Sale and End User License Agreement (EULA), and click **Accept**.
c. Specify a new user name and password for the system, and click **Apply and Continue**.

The Welcome panel that is displayed provides options to set up and provision your system. For more information about using these options, see Guided setup on page 32.

NOTE: If you are unable to use the 10.0.0.x network to configure the system, see the Setting network port IP addresses using the CLI port and serial cable appendix in the *Dell EMC PowerVault ME4 Series Storage System Deployment Guide*.

To manually set up and provision a storage system for the first time:

1. Configure your web browser to access the PowerVault Manager as described in Web browser requirements and setup on page 11.
2. Temporarily set the management host NIC to a 10.0.0.x address or to the same IPv6 subnet to enable communication with the storage system.
3. In a supported web browser:
   - Type `https://10.0.0.2` to access controller module A on an IPv4 network.
   - Type `https://fd6e:23ce:fed3:19d1::1` to access controller module A on an IPv6 network.
4. If the storage system is running G275 firmware, sign in to the PowerVault Manager using the user name **manage** and password **!manage**.

   For more information about signing in, see Signing in and signing out on page 13. For more information about using these options, see Guided setup on page 32.

   If the storage system is running G280 firmware:

   a. Click **Get Started**.
   b. Read the Commercial Terms of Sale and End User License Agreement (EULA), and click **Accept**.
   c. Specify a new user name and password for the system, and click **Apply and Continue**.
5. Be sure that the controller modules and expansion modules have the latest firmware as described in Updating firmware on page 151.
6. Configure your system settings as described in Systems Settings panel on page 58.
7. Create disk groups and pools, and add dedicated spares to linear disk groups, as described in Adding a disk group on page 80 and Dedicated spares on page 86.
8. Create volumes and map them to initiators, as described in Create a volume on page 87.
9. From hosts, verify volume mappings by mounting the volumes and performing read/write tests to the volumes.
10. Optionally, for replication of virtual volumes and snapshots, create peer connections and replication sets as described in Creating a peer connection on page 119, Creating a replication set from the Replications topic on page 121, and Creating a replication set from the Volumes topic on page 101.

NOTE: If you are unable to use the 10.0.0.x network to configure the system, see the Setting network port IP addresses using the CLI port and serial cable appendix in the *Dell EMC PowerVault ME4 Series Storage System Deployment Guide*.

Using the PowerVault Manager interface

Web browser requirements and setup

- The Dell EMC PowerVault ME4 Series Series Storage System uses Mozilla Firefox 57 and newer, Google Chrome 57 and newer, Microsoft Internet Explorer 10 and 11, or Apple Safari 10.1 and newer.

  NOTE:

  The help content in PowerVault Manager is not viewable if you use the Microsoft Edge browser that shipped with Windows 10.
- To see the help window, you must enable pop-up windows.
- To optimize the display, use a color monitor and set its color quality to the highest setting.
- To navigate beyond the Sign In page (with a valid user account):
  - For Internet Explorer, set the local-intranet security option to medium or medium-low.
  - For Internet Explorer, add the network IP address of each controller as a trusted site.
  - Ensure that the browser is set to allow cookies, at least for the IP addresses of the storage system network ports.
  - If the PowerVault Manager is configured to use HTTPS, ensure that Internet Explorer is set to use TLS 1.2.

Tips for using PowerVault Manager

The following list contains tips for using PowerVault Manager:

- Do not use the Back, Forward, Reload, or Refresh buttons in the browser. PowerVault Manager has a single page on which content changes as you perform tasks and automatically updates to show current data.
- A red asterisk (*) identifies a required setting.
- As you set options in action panels, PowerVault Manager informs you whether a value is invalid or a required option is not set. If the **Apply** or **OK** button remains inactive after you set all required options, either press **Tab** or click in an empty area of the panel to activate the button.
- If an action panel has an Apply button and an **OK** button, click **Apply** to apply any changes and keep the panel open or click **OK** to apply any changes and close the panel. After clicking **Apply**, you can click **Close** to close the panel without losing changes already applied.
- You can move an action panel or a confirmation panel by dragging its top border.
- If you are signed in to PowerVault Manager and the controller you are accessing goes offline, the system informs you that the system is unavailable or that communication has been lost. After the controller comes back online, close and reopen the browser and start a new PowerVault Manager session.
- If your session is inactive for too long, you are signed out automatically. This timer resets after each action you perform. One minute before automatic sign-out you are prompted to continue using PowerVault Manager.
- If you start to perform an action in a panel (such as adding a new entry to a table) and then select an item or button that interrupts the action, a confirmation panel will ask if you want to navigate away and lose any changes made. If you want to continue performing the original action, click **No**. If you want to stop performing the original action, click **Yes**.
- In the banner or footer, or indicates that a panel has a menu. Click anywhere in the panel to display the menu.
- Right-click a row in a topic table to display the Action menu. This action provides a faster method for more experienced users to access the menu items. Hovering over a disabled menu item shows a tooltip indicating why the item is disabled.

Tips for using tables

Items such as initiators, hosts, volumes, and mappings are listed in tables. Use the following methods singly or together to quickly locate items that you want to work with.

Selecting items

- To select an item, click in its row.
- To select a range of adjacent items, click the first item in the range and **Shift+click** the last item in the range.
- To select or deselect one or more items, **Ctrl+click** each one.

Sorting items

To sort items by a specific column, click the column heading to reorder items from low to high ( ). Click again to reorder items from high to low ( ).

To sort items by multiple columns

1. In the first column to sort by, click its heading once or twice to reorder items.
2. In the second column to sort by, Shift+click its heading once or twice to reorder items. If you Shift+click a third time, the column is deselected.
3. Continue for each additional column to sort by.

Using filters to find items with specified text

To filter a multicolumn table, in the filter field above the table, enter the text to find. As you type, only items that contain the specified text remain shown. Filters are not case sensitive.

To use a column filter

1. In the column heading click the filter icon ( ). The filter menu appears.
2. Do one of the following:

- In the filter field, enter the text to find. As you type, only items that contain the specified text remain shown. Because a filter is active, the icon changes ( ). Previous search terms are listed below the field. Previous search terms that match displayed values are shown in bold.
- If the filter list has an entry for the text you want to find, select that entry.
- To show all items in the column, click the filter icon and select **All**.

To clear all filters and show all items, click **Clear Filters**.

Limiting the number of items shown

To show a specific number of items at a time in a multicolumn table, select a value from the Show menu. If more items exist, you can page through them by using the following buttons:

 Show next set of items.

 Reached end of list.

 Show previous set of items.

 Reached start of list.

Tips for using help

The following list contains tips for using help in PowerVault Manager:

- To display help for the content in the topic pane, click the help icon in the banner.

  NOTE:

  The help content in PowerVault Manager is not viewable if you use the Microsoft Edge browser that shipped with Windows 10.
- In the help window, click the table of contents icon to show or hide the Contents pane.
- As the context in the main panel is changed, the corresponding help topic is displayed in the help window. To prevent this automatic context-switching, click the pin icon . When a help window is pinned, you can still browse to other topics within the window and you can open a new window. You cannot unpin a help window. You can only close it.
- If you have viewed more than one help topic, you can click the arrow icons to display the previous or next topic.
- To close the help window, click the close icon .

Export data to a CSV file

You can export initiator, host, volume, mapping, and replication data that is displayed in tables to a downloadable Comma Separated Values (CSV) file that can be viewed in a spreadsheet for further analysis. Data can be exported for the entire table or for one or more selected rows, and it can be displayed in row format or column format. The exported CSV file contains all of the data in the table including information that is displayed in the hover panels.

1. Select one or more rows of data to export from a table that has an Export to CSV button.
2. Click **Export to CSV**. The Export Data to CSV panel opens.
3. Click **All** to export all of the data within the selected table, or click **Selected** to export only selected files.
4. Click **Rows** to export the data in row format, or **Columns** to export the data in column format.
5. Click **OK**. The data is exported to a CSV file.

Signing in and signing out

Multiple users can be sign in to each controller simultaneously.

For each active PowerVault Manager session, an identifier is stored in the browser. Depending on how your browser treats this session identifier, you might be able to run multiple independent sessions simultaneously. For example, each instance of Internet Explorer can run a separate PowerVault Manager session. However, all instances of Firefox, Chrome, and Safari share the same session.

NOTE: For best security, Sign out when you are ready to end your session. Do not close the browser window unless you are certain that it is the only browser instance.

Sign in

1. In the web browser address field, type `https://<IP address of a controller network port>` and press **Enter**.
   The Sign In page opens. If the Sign In page is not displayed, verify that you have typed the correct IP address.
   NOTE: HTTPS is enabled by default. To enable HTTP, see Enable or disable system-management settings.
2. Type the username of a PowerVault Manager user in the **User name** field.
3. Type the password of the PowerVault Manager user in the **Password** field.
4. To display the interface in a language different than the one configured for the user, select the language from the language drop-down menu.
   Language preferences can be configured for the system and for individual users. The default language is English.
5. Click **Sign In**.
   The Home page or the Welcome panel is displayed.

Sign out

1. Click **Sign Out**, located in the upper right of the PowerVault Manager window.
2. In the confirmation panel, click **Sign Out**.

System concepts

About virtual and linear storage

This product uses two different storage technologies that share a common user interface. One uses the virtual method while the other one uses the linear method.

Virtual storage is a method of mapping logical storage requests to physical storage (disks). It inserts a layer of virtualization such that logical host I/O requests are mapped onto pages of storage. Each page is then mapped onto physical storage. Within each page the mapping is linear, but there is no direct relationship between adjacent logical pages and their physical storage.

A page is a range of contiguous Logical Block Addresses (LBAs) in a disk group, which is one of up to 16 RAID sets that are grouped into a pool. Thus, a virtual volume as seen by a host represents a portion of storage in a pool. Multiple virtual volumes can be created in a pool, sharing its resources. This allows for a high level of flexibility, and the most efficient use of available physical resources.

Some advantages of using virtual storage are:

- It allows performance to scale as the number of disks in the pool increases.
- It virtualizes physical storage, allowing volumes to share available resources in a highly efficient way.
- It allows a volume to be comprised of more than 16 disks.

Virtual storage provides the foundation for data-management features such as thin provisioning, automated tiered storage, SSD read cache, and the quick rebuild feature.

The linear method maps logical host requests directly to physical storage. In some cases the mapping is one-to-one, while in most cases the mapping is across groups of physical storage devices, or slices of them. This linear method of mapping is highly efficient. The negative side of linear mapping is lack of flexibility. This makes it difficult to alter the physical layout after it is established.

About disk groups

A disk group is an aggregation of disks of the same type, using a specific RAID level that is incorporated as a component of a pool, for the purpose of storing volume data. Disk groups are used in both virtual and linear storage environments. You can add virtual, linear, or read-cache disk groups to a pool.

NOTE: After you create a disk group using one storage type, the system will use that storage type for additional disk groups. To switch to the other storage type, you must first remove all disk groups. For more information, see Removing disk groups on page 83.

All disks in a disk group must be the same type SSD: enterprise SAS, or midline SAS, For example, a disk group can contain different models of disks, and disks with different capacities and sector formats. If you mix disks with different capacities, the smallest disk determines the logical capacity of all other disks in the disk group, for all RAID levels except ADAPT. For example, the capacity of a disk group composed of one 500 GB disk and one 750 GB disk is equivalent to a disk group composed of two 500 GB disks. To maximize capacity, use disks of similar size.

Sector format

The system supports 512-byte native sector size disks, 512-byte emulated sector size disks, or a mix of these sector formats. The system identifies the sector format used by a disk, disk group, or pool as follows:

- 512n—All disks use the 512-byte native sector size. Each logical block and physical block is 512 bytes.
- 512e—All disks use 512-byte emulated sector size. Each logical block is 512 bytes and each physical block is 4096 bytes. Eight logical blocks will be stored sequentially in each physical block. Logical blocks may or may not be aligned with physical block boundaries.
- Mixed—The disk group contains a mix of 512n and 512e disks. For consistent and predictable performance, do not mix disks of different sector size types (512n, 512e).

You can provision storage by adding a disk group to a pool. Volumes then can be created in the pool.

Virtual disk groups

A virtual disk group requires the specification of a set of disks, RAID level, disk group type, pool target (A or B), and a name. If the virtual pool does not exist at the time of adding the disk group, the system will automatically create it. Multiple disk groups (up to 16) can be added to a single virtual pool.

NOTE: For optimal performance all virtual disk groups in the same tier should have the same RAID level, capacity disks, and physical number of disks.

When a virtual disk group is removed that contains active volume data, that volume data will drain or be moved to other disk group members within the pool, if they exist. Disk groups should only be removed when all volume data can cleanly be drained from the disk group. When the last disk group is removed, the pool ceases to exist and will be deleted from the system automatically.

NOTE: If the last disk group contains data, a warning appears prompting you to confirm removing the disk group.

The RAID level for a virtual disk group must be fault tolerant. The supported RAID levels for virtual disk groups are: RAID 1, RAID 5, RAID 6, RAID 10, and ADAPT. If RAID 10 is specified, the disk group must have at least two sub-groups.

Linear disk groups

A linear disk group requires the specification of a set of disks, RAID level, disk group type, and a name. Whenever the system creates a linear disk group, it also creates an identically named linear pool at the same time. No further disk groups can be added to a linear pool.

For maximum performance, all of the disks in a linear disk group must share the same classification, which is determined by disk type, size, and speed. This provides consistent performance for the data being accessed on that disk group. To dissolve a linear disk group, delete the disk group and the contained volumes are automatically deleted. The disks that compose that linear disk group are then available to be used for other purposes.

The RAID levels for linear disk groups created through the PowerVault Manager must be fault tolerant. The supported RAID levels for linear disk groups in the interface are: RAID 1, RAID 5, RAID 6, RAID 10, RAID 50 and ADAPT. RAID 10 and RAID 50 only appear in the interface if the system's disk configuration supports them. If RAID 10 is specified, the disk group has a minimum of two sub-groups. If RAID 50 is selected, depending on the number of selected disks, varying numbers of sub-groups can be created. Additionally, you can create fault-tolerant RAID-3 or non-fault-tolerant NRAID or RAID-0 disk groups through the CLI.

NOTE: Tiering, snapshots, and replications are not available for linear pools.

Read-cache disk groups

A read-cache disk group is a special type of a virtual disk group that is used to cache virtual pages to improve read performance. Read cache does not add to the overall capacity of the pool to which it has been added. You can add or remove it from the pool without any adverse effect on the volumes and their data for the pool, other than to impact the read-access performance.

If your system uses SSDs, you can create read-cache disk groups for virtual pools if you do not have any virtual disk groups for the pool that are comprised of SSDs. Virtual pools cannot contain both read-cache and a Performance tier.

Only a single read-cache disk group may exist within a pool. Increasing the size of read cache within a pool requires the user to remove the read-cache disk group, and then re-add a larger read-cache disk group. It is possible to have a read-cache disk group that consists of one or two disks with a non-fault tolerant RAID level. For more information on read cache, see About SSD read cache.

About RAID levels

The RAID controllers enable you to set up and manage disk groups, the storage for which may be spread across multiple disks. This is accomplished through firmware resident in the RAID controller. RAID refers to disk groups in which part of the storage capacity may be used to achieve fault tolerance by storing redundant data. The redundant data enables the system to reconstruct data if a disk in the disk group fails.

For a description of the ADAPT data protection level, see About ADAPT.

NOTE: Choosing the right RAID level for your application improves performance.

The following tables:

- Provide examples of appropriate RAID levels for different applications.
- Compare the features of different RAID levels.
- Describe the expansion capability for different RAID levels (linear disk groups).
- Suggest the number of disks to select for different RAID levels (virtual disk groups).
- Describe the expansion capability for different RAID levels.

NOTE: To create an NRAID, RAID-0, or RAID-3 (linear-only) disk group, you must use the CLI `add disk-group` command. For more information about this command, see the *Dell EMC PowerVault ME4 Series Storage System CLI Guide*.

NOTE: You can only create RAID-1, RAID-5, RAID-6, and RAID-10 and ADAPT virtual disk groups.

Table 1. Example applications and RAID levels

Application	RAID level
Testing multiple operating systems or software development (where redundancy is not an issue)	NRAID
Fast temporary storage or scratch disks for graphics, page layout, and image rendering	0
Workgroup servers	1 or 10
Video editing and production	3
Network operating system, databases, high availability applications, workgroup servers	5
Very large databases, web server, video on demand	50
Mission-critical environments that demand high availability and use large sequential workloads	6
Environments that need flexible storage and fast rebuilds	ADAPT

Table 2. RAID level comparison

RAID level	Min. disks	Description	Strengths	Weaknesses
NRAID	1	Non-RAID, nonstriped mapping to a single disk	Ability to use a single disk to store additional data	Not protected, lower performance (not striped)
0	2	Data striping without redundancy	Highest performance	No data protection: if one disk fails all data is lost
1	2	Disk mirroring	Very high performance and data protection; minimal penalty on write	High redundancy cost overhead: because all data is duplicated, twice

Table 2. RAID level comparison (continued)

RAID level	Min. disks	Description	Strengths	Weaknesses
			performance; protects against single disk failure	the storage capacity is required
3	3	Block-level data striping with dedicated parity disk	Excellent performance for large, sequential data requests (fast read); protects against single disk failure	Not well-suited for transaction-oriented network applications; write performance is lower on short writes (less than 1 stripe)
5	3	Block-level data striping with distributed parity	Best cost/performance for transaction-oriented networks; very high performance and data protection; supports multiple simultaneous reads and writes; can also be optimized for large, sequential requests; protects against single disk failure	Write performance is slower than RAID 0 or RAID 1
6	4	Block-level data striping with double distributed parity	Best suited for large sequential workloads; non-sequential read and sequential read/write performance is comparable to RAID 5; protects against dual disk failure	Higher redundancy cost than RAID 5 because the parity overhead is twice that of RAID 5; not well-suited for transaction-oriented network applications; non-sequential write performance is slower than RAID 5
10 (1+0)	4	Stripes data across multiple RAID-1 subgroups	Highest performance and data protection (protects against multiple disk failures)	High redundancy cost overhead: because all data is duplicated, twice the storage capacity is required; requires minimum of four disks
50 (5+0)	6	Stripes data across multiple RAID-5 sub-groups	Better random read and write performance and data protection than RAID 5; supports more disks than RAID 5; protects against multiple disk failures	Lower storage capacity than RAID 5
ADAPT	12	Distributed erasure coding with dual disk failure protection	Very fast rebuilds, no spare disks (built in spare capacity), large storage pools, simplified initial deployment and expansion	Requires minimum of 12 disks

Table 3. Number of disks per RAID level to optimize virtual disk group performance

RAID level	Number of disks (data and parity)
1	2 total (no parity)
5	3 total (2 data disks, 1 parity disk); 5 total (4 data disks, 1 parity disk); 9 total (8 data disks, 1 parity disk)

Table 3. Number of disks per RAID level to optimize virtual disk group performance (continued)

RAID level	Number of disks (data and parity)
6	4 total (2 data disks, 2 parity disks); 6 total (4 data disks, 2 parity disks); 10 total (8 data disks, 2 parity disks)
10	4–16 total
ADAPT	12–128 total

Table 4. Linear disk group expansion by RAID level

RAID level	Expansion capability	Maximum disks
NRAID	Cannot expand.	1
0, 3, 5, 6	You can add from 1 to 4 disks at a time.	16
1	Cannot expand.	2
10	You can add 2 or 4 disks at a time.	16
50	You can add one sub-group at a time. The added sub-group must contain the same number of disks as each of the existing sub-groups.	32
ADAPT	You can add up to 68 disks at a time.	128

About ADAPT

ADAPT is a RAID-based data protection level that maximizes flexibility, provides built in spare capacity, and allows for very fast rebuilds, large storage pools, and simplified expansion. All disks in the ADAPT disk group must be the same type (enterprise SAS, for example), and in the same tier, but can have different capacities. ADAPT is shown as a RAID level in the management interfaces.

ADAPT disk groups use all available space to maintain fault tolerance, and data is spread evenly across all of the disks. When new data is added, new disks are added, or the system recognizes that data is not distributed across disks in a balanced way, it moves the data to maintain balance across the disk group.

Reserving spare capacity for ADAPT disk groups is automatic since disk space dedicated to sparing is spread across all disks in the system. In the case of a disk failure, data will be moved to many disks in the disk group, allowing for quick rebuilds and minimal disruption to I/O.

The system will automatically default to a target spare capacity that is the sum of the largest two disks in the disk group, which is large enough to fully recover fault tolerance after loss of any two disks in the disk group. The actual spare capacity value can change depending on the current available spare capacity in the disk group. Spare capacity is determined by the system as disks are added to a disk group, or when disk groups are created, expanded, or rebalanced. For more information, see the topic about the `add disk-group` command in the *Dell EMC PowerVault ME4 Series Storage System CLI Guide*.

ADAPT disk groups can be expanded to either replenish current target spare capacity or to increase usable capacity. For more information, see Expanding a disk group on page 84.

A system using ADAPT disk groups cannot be downgraded to a system that does not support ADAPT.

About SSDs

The use of SSDs (solid-state drives) can greatly enhance the performance of a system. Since the SSDs do not have moving parts, data that is random in nature can be accessed much faster. You can use SSDs for virtual disk groups. When combined with virtual disk groups that consist of other classes of disks, improved read and write performance is possible through automated tiered storage. Alternatively, you can use one or two SSDs in read-cache disk groups to increase read performance for pools without a Performance tier. The application workload of a system determines the percentage of SSDs of the total disk capacity that is needed for best performance.

For more information about automated tiered storage, see About automated tiered storage on page 23. For more information on read-cache disk groups, see Read-cache disk groups on page 15. For information about using SSDs in all disk groups, see All-flash array on page 19.

Gauging the percentage of life remaining for SSDs

An SSD can be written and erased a limited number of times. Through the SSD Life Left disk property, you can gauge the percentage of disk life remaining. This value is polled every 5 minutes. When the value decreases to 20%, an event is logged with Informational severity. This event is logged again with Warning severity when the value decreases to 5%, 2% or 1%, and 0%. If a disk crosses more than one percentage threshold during a polling period, only the lowest percentage will be reported. When the value decreases to 0%, the integrity of the data is not guaranteed. To prevent data integrity issues, replace the SSD when the value decreases to 5% of life remaining.

You can view the value of the SSD Life Left property through the Disk Information panel. In the front view of the enclosure in the System topic, hover the cursor over any disk to view its properties. You can also view the Disk Information panel through the Pools topic. Select the pool for the disk group in the pools table, select the disk group in the Related Disk Groups table, and then hover the cursor over the disk in the Related Disks table.

All-flash array

The all-flash array feature, enabled by default, allows systems to run exclusively with disk groups that consist of SSDs, providing the ability to have a homogeneous SSD-only configuration. Systems using an all-flash array have one tier that consists solely of SSDs. If a system includes disk groups with spinning disks, the disk groups must be removed before the all-flash array feature can be used.

If you are using SSDs and spinning disks and the first disk group is provisioned with spinning disks, then the system can be provisioned to use spinning disks in virtual disk groups and use SSDs either in virtual disk groups or as read cache.

Internal disk management

SSDs use multiple algorithms to manage SSD endurance features. These include wear leveling, support for `Unmap` commands, and over-provisioning to minimize write amplification.

Wear leveling

Wear leveling is a technique for prolonging the service life of some kinds of erasable computer storage media, such as the flash memory used in SSDs. It attempts to ensure that all flash cells are written to or exercised as evenly as possible to avoid any hot spots where some cells are used up faster than other locations. There are several different wear leveling mechanisms used in flash memory systems, each with different levels of success.

Vendors have different algorithms to achieve optimum wear leveling. Wear leveling management occurs internal to the SSD. The SSD automatically manages wear leveling, which does not require any user interaction.

Overprovisioning

The write amplification factor of an SSD is defined as the ratio of the amount of data actually written by the SSD to the amount of host or user data requested to be written. This is used to account for the user data and activities like wear leveling. This affects wear leveling calculations and is influenced by the characteristics of data written to and read from SSDs. Data that is written in sequential LBAs that are aligned on 4KB boundaries results in the best write amplification factor. The worst write amplification factor typically occurs for randomly written LBAs of transfer sizes that are less than 4KB and that originate on LBAs that are not on 4KB boundaries. Try to align your data on 4KB boundaries.

TRIM and UNMAP commands

A command (known as `TRIM` in the ATA command set and `UNMAP` in the SCSI command set) allows an operating system to inform an SSD of the blocks of data that are no longer considered in use and can be wiped internally.

Data retention

Data retention is another major characteristic of SSDs that all SSD algorithms take into account while running. While powered up, the data retention of SSD cells are monitored and rewritten if the cell levels decay to an unexpected level. Data retention when the drive is powered off is affected by Program and Erase (PE) cycles and the temperature of the drive when stored.

Drive Writes per Day

DWD or DWPD refers to Drive Writes Per Day. Disk vendors rate SSD endurance by how many writes can occur over the lifetime of an SSD. As lower-cost SSDs that support fewer drive writes per day become available, the cost benefit analysis of which SSDs to use is highly dependent on your applications and I/O workload, as is the ratio of SSDs to conventional drives. In some environments, a ratio of 10% SSDs to 90% conventional drives, when combined with Dell EMC real-time tiering, can yield dramatic performance improvements.

Because data is characterized every five seconds and moved to the appropriate storage device, no fixed rule is used to determine which SSDs are used. For this reason, using SSDs with the same DWPD values is advised.

About SSD read cache

Unlike tiering, where a single copy of specific blocks of data resides in either spinning disks or SSDs, the Read Flash Cache (RFC) feature uses one SSD read-cache disk group per pool as a read cache for frequently accessed data only. Each read-cache disk group consists of one or two SSDs with a maximum usable capacity of 4TB. A separate copy of the data is also kept in spinning disks. Read-cache content is lost when a controller restart or failover occurs. Taken together, these attributes have several advantages:

- The performance cost of moving data to read-cache is lower than a full migration of data from a lower tier to a higher tier.
- Read-cache does not need to be fault tolerant, potentially lowering system cost.
- Controller read cache is effectively extended by two orders of magnitude, or more.

When a read-cache group consists of one SSD, it automatically uses NRAID. When a read-cache group consists of two SSDs, it automatically uses RAID 0.

For more information on SSDs, see About SSDs on page 18.

About spares

Spare disks are unused disks in your system that you designate to automatically replace a failed disk, restoring fault tolerance to disk groups in the system. Types of spares include:

- Dedicated spare. Reserved for use by a specific linear disk group to replace a failed disk. Most secure way to provide spares for disk groups, but expensive to reserve a spare for each disk group.
- Global spare. Reserved for use by any fault-tolerant disk group to replace a failed disk.
- Dynamic spare. Available compatible disk that is automatically assigned to replace a failed disk in a fault-tolerant disk group.

NOTE: You cannot designate spares for ADAPT disk groups. For information on how ADAPT disk groups manage sparing, see About RAID levels.

A controller automatically reconstructs a fault-tolerant disk group (RAID 1, 3, 5, 6, 10, 50) when one or more of its disks fails and a compatible spare disk is available. A disk is compatible if it has enough capacity to replace the failed disk and is the same speed and type (enterprise SAS, for example). It is not advisable to mix 10k and 15k disks in a single disk group. If the disks in the system are FDE-capable and the system is secure, spares must also be FDE-capable.

When a disk fails, the system looks for a dedicated spare first. If it does not find a dedicated spare, it looks for a global spare. If it does not find a compatible global spare and the dynamic spares option is enabled, it takes any available compatible disk. If no compatible disk is available, reconstruction cannot start.

NOTE: A best practice is to designate spares for use if disks fail. Dedicating spares to disk groups is the most secure method, but it is also expensive to reserve spares for each disk group. Alternatively, you can enable dynamic spares or assign global spares.

About pools

A *pool* is an aggregation of one or more disk groups that serves as a container for volumes. Virtual and linear storage systems both use pools. A disk group is a group of disks of the same type, using a specific RAID level that is incorporated as a component of a pool, that stores volume data. For virtual pools, when volumes are added to a pool the data is distributed across the pool's disk groups. For linear pools, which can only have one disk group per pool, volumes are also added to the pool, which contains the volume data.

In both virtual and linear storage, if the owning controller fails, the partner controller assumes temporary ownership of the pool and resources owned by the failed controller. If a fault-tolerant cabling configuration, with appropriate mapping, is used to connect the controllers to hosts, LUNs for both controllers are accessible through the partner controller so I/O to volumes can continue without interruption.

You can provision disks into disk groups. For information about how provisioning disks works, see Adding a disk group.

Virtual pools and disk groups

The volumes within a virtual pool are allocated virtually (separated into fixed size pages, with each page allocated randomly from somewhere in the pool) and thinly (meaning that they initially exist as an entity but don't have any physical storage allocated to them). They are also allocated on-demand (as data is written to a page, it is allocated).

If you would like to create a virtual pool that is larger than 512 TiB on each controller, you can enable the large pools feature by using the `large-pools` parameter of the `set advanced-settings` CLI command. When the large pools feature is disabled, which is the default, the maximum size for a virtual pool is 512 TiB, and the maximum number of volumes per snapshot tree is 255 (base volume plus 254 snapshots). Enabling the large pools feature will increase the maximum size for a virtual pool to 1024 TiB (1 PiB) and decrease the maximum number of volumes per snapshot tree to 9 (base volume plus 8 snapshots). The maximum number of volumes per snapshot will decrease to fewer than 9 if more than 3 replication sets are defined for volumes in the snapshot tree. For more information about the `large-pools` parameter of the `set advanced-settings` CLI command, see the *Dell EMC PowerVault ME4 Series Storage System CLI Guide*.

NOTE: The physical capacity limit for a virtual pool is 512 TiB. When overcommit is enabled, the logical capacity limit is 1 PiB.

You can remove one or more disk groups, but not all, from a virtual pool without losing data if there is enough space available in the remaining disk groups to contain the data. When the last disk group is removed, the pool ceases to exist, and will be deleted from the system automatically. Alternatively, the entire pool can be deleted, which automatically deletes all volumes and disk groups residing on that pool.

If a system has at least one SSD, each virtual pool can also have a read-cache disk group. Unlike the other disk group types, read-cache disk groups are used internally by the system to improve read performance and do not increase the available capacity of the pool.

Linear pools and disk groups

Each time that the system adds a linear disk group, it also creates a corresponding pool for the disk group. Once a linear disk group and pool exists, volumes can be added to the pool. The volumes within a linear pool are allocated in a linear way, such that the disk blocks are sequentially stored on the disk group.

Linear storage maps logical host requests directly to physical storage. In some cases the mapping is one-to-one, while in most cases the mapping is across groups of physical storage devices, or slices of them.

About volumes and volume groups

A volume is a logical subdivision of a virtual or linear pool and can be mapped to host-based applications. A mapped volume provides addressable storage to a host (for example, a file system partition you create with your operating system or third-party tools). For more information about mapping, see About volume mapping.

Virtual volumes

Virtual volumes make use of a method of storing user data in virtualized pages. These pages may be spread throughout the underlying physical storage in a random fashion and allocated on demand. Virtualized storage therefore has a dynamic mapping between logical and physical blocks.

Because volumes and snapshots share the same underlying structure, it is possible to create snapshots of other snapshots, not just of volumes, creating a snapshot tree.

A maximum of 1024 virtual volumes can exist per system.

Volume groups

You can group a maximum of 1024 volumes (standard volumes, snapshots, or both) into a volume group. Doing so enables you to perform mapping operations for all volumes in a group at once, instead of for each volume individually.

A volume can be a member of only one group. All volumes in a group must be in the same virtual pool. A volume group cannot have the same name as another volume group, but can have the same name as any volume. A maximum of 256 volume groups can exist per system. If a volume group is being replicated, the maximum number of volumes that can exist in the group is 16.

NOTE: Volume groups apply only to virtual volumes. You cannot add linear volumes to a volume group.

Linear volumes

Linear volumes make use of a method of storing user data in sequential, fully allocated physical blocks. Mapping between the logical data presented to hosts and the physical location where it is stored is fixed, or static.

About volume cache options

You can set options that optimize reads and writes performed for each volume. It is recommended that you use the default settings.

Using write-back or write-through caching

CAUTION: Only disable write-back caching if you fully understand how the host operating system, application, and adapter move data. Used incorrectly, write-back caching can hinder system performance.

When modifying a volume you can change its write-back cache setting. Write-back is a cache-writing strategy in which the controller receives the data to be written to disks, stores it in the memory buffer, and immediately sends the host operating system a signal that the write operation is complete, without waiting until the data is actually written to the disk. Write-back cache mirrors all of the data from one controller module cache to the other. Write-back cache improves the performance of write operations and the throughput of the controller.

When write-back cache is disabled, write-through becomes the cache-writing strategy. Using write-through cache, the controller writes the data to the disks before signaling the host operating system that the process is complete. Write-through cache has lower write throughput performance than write-back, but it is the safer strategy, with minimum risk of data loss on power failure. However, write-through cache does not mirror the write data because the data is written to the disk before posting command completion and mirroring is not required. You can set conditions that cause the controller to change from write-back caching to write-through caching. For more information, see Changing system cache settings.

In both caching strategies, active-active failover of the controllers is enabled.

You can enable and disable the write-back cache for each volume. By default, volume write-back cache is enabled. Because controller cache is backed by supercapacitor technology, if the system loses power, data is not lost. For most applications, this is the preferred setting.

NOTE: The best practice for a fault-tolerant configuration is to use write-back caching.

Cache optimization mode

CAUTION: Changing the cache optimization setting while I/O is active can cause data corruption or loss. Before changing this setting, quiesce I/O from all initiators.

You can also change the optimization mode.

- Standard. This controller cache mode of operation is optimized for sequential and random I/O and is the optimization of choice for most workloads. In this mode, the cache is kept coherent with the partner controller. This mode gives you high performance and high redundancy. This is the default.
- No-mirror. In this mode of operation, the controller cache performs the same as the standard mode with the exception that the cache metadata is not mirrored to the partner. While this improves the response time of write I/O, it comes at the cost of redundancy. If this option is used, the user can expect higher write performance but is exposed to data loss if a controller fails.

Optimizing read-ahead caching

NOTE: Only change read-ahead cache settings if you fully understand how the host operating system, application, and adapter move data so that you can adjust the settings accordingly.

You can optimize a volume for sequential reads or streaming data by changing its read-ahead cache settings.

You can change the amount of data read in advance. Increasing the read-ahead cache size can greatly improve performance for multiple sequential read streams.

- The **Adaptive** option works well for most applications: it enables adaptive read-ahead, which allows the controller to dynamically calculate the optimum read-ahead size for the current workload.
- The **Stripe** option sets the read-ahead size to one stripe. The controllers treat NRAID and RAID-1 disk groups internally as if they have a stripe size of 512 KB, even though they are not striped.
- Specific size options let you select an amount of data for all accesses.

- The **Disabled** option turns off read-ahead cache. This is useful if the host is triggering read ahead for what are random accesses. This can happen if the host breaks up the random I/O into two smaller reads, triggering read ahead.

About thin provisioning

Thin provisioning is a virtual storage feature that allows a system administrator to overcommit physical storage resources. This allows the host system to operate as though it has more storage available than is actually allocated to it. When physical resources fill up, the administrator can add physical storage by adding additional disk groups on demand.

Paging is required to eliminate the lack of flexibility associated with linear mapping. Linear mapping limits the ability to easily expand the physical storage behind the thin-provisioned volume. Paged mapping allows physical resources to be disparate and noncontiguous, making it much easier to add storage on the fly.

For example, contrast the methods for creating a volume for Microsoft Exchange Server data:

- Typically, administrators create a storage-side volume for Exchange and map that volume with an assigned Logical Unit Number (LUN) to hosts, and then create a Microsoft Windows volume for that LUN. Each volume has a fixed size. There are ways to increase the size of a storage-side volume and its associated Windows volume, but they are often cumbersome. The administrator must make a trade-off between initial disk costs and a volume size that provides capacity for future growth.
- With thin provisioning, the administrator can create a very large volume, up to the maximum size allowed by Windows. The administrator can begin with only a small number of disks, and add more as physical storage needs grow. The process of expanding the Windows volume is eliminated.

NOTE: For a thin-provisioned volume mapped to a host, when data is deleted from the volume not all of the pages, or space associated with that data will be deallocated, or released. This is especially true for smaller files. To deallocate the pages in Windows, select the mapped volume and do either of the following:

- **Perform a quick format.**
- **View its properties, select the Tools tab, and under Defragmentation, click Optimize.**

About automated tiered storage

Automated Tiered Storage is a virtual storage feature that automatically moves data residing in one class of disks to a more appropriate class of disks based on data access patterns, with no manual configuration necessary.

- Frequently accessed data can move to disks with higher performance.
- Infrequently accessed data can move to disks with lower performance and lower costs.

Each virtual disk group, depending on the type of disks it uses, is automatically assigned to one of the following tiers:

- Performance – This highest tier uses SSDs, which provide the best performance but also the highest cost. For more information on SSDs, see About SSDs on page 18.
- Standard – This middle tier uses enterprise-class spinning SAS disks, which provide good performance with mid-level cost and capacity.
- Archive – This lowest tier uses midline spinning SAS disks, which provide the lowest performance with the lowest cost and highest capacity.

When the status of a disk group in the Performance Tier becomes critical (CRIT), the system will automatically drain data from that disk group to disk groups using spinning disks in other tiers providing that they can contain the data on the degraded disk group. This occurs because similar wear across the SSDs is likely, so more failures may be imminent.

If a system only has one class of disk, no tiering occurs. However, automated tiered storage rebalancing happens when adding or removing a disk group in a different tier.

NOTE: Tiers are automatically set up within a single virtual pool, but tiers do not span virtual pools.

Volume tier affinity

Volume tier affinity is a setting that enables a storage administrator to define QoS (Quality of Service) preferences for volumes in a storage environment.

The three volume tier affinity settings are:

- No Affinity – This setting uses the highest available performing tiers first and only uses the Archive tier when space is exhausted in the other tiers. Volume data moves into higher performing tiers based on the frequency of access and available space in the tiers.

- Performance – This setting prioritizes volume data to the higher tiers of service. If no space is available, lower performing tier space is used. Volume data moves into higher performing tiers based on the frequency of access and available space in the tiers.

  NOTE: The Performance affinity setting does not require an SSD tier and uses the highest performance tier available.
- Archive – This setting prioritizes the volume data to the lowest tier of service. Volume data can move to higher performing tiers based on the frequency of access and available space in the tiers.

NOTE: Volume tier affinity is not the same thing as pinning and it does not restrict data to a given tier and capacity. Data on a volume with Archive affinity can still be promoted to a performance tier when that data becomes in demand to the host application.

Volume tier affinity strategies

Volume tier affinity acts as a guide to the system on where to place data for a given volume in the available tiers.

The standard strategy is to prefer the highest spinning disk tiers for new sequential writes and the highest tier available (including SSD) for new random writes. As the host application accesses the data, it is moved to the most appropriate tier based on demand. Frequently accessed data is promoted up towards the highest performance tier and infrequently accessed data is demoted to the lower spinning disk-based tiers. The standard strategy is followed for data on volumes set to No Affinity.

For data on volumes set to the Performance affinity, the standard strategy is followed for all new writes. However, subsequent access to that data has a lower threshold for promotion upwards. The lower threshold makes it more likely for that data to be available on the higher performance tiers. Preferential treatment is provided to frequently accessed data that has performance affinity at the SSD tier. Archive or no affinity data is demoted out of the SSD tier to make room for data with an affinity of Performance. The Performance affinity is useful for volume data that you want to ensure has priority treatment for promotion to and retention in your highest performance tier.

For volumes that are set to the Archive affinity, all new writes are initially placed in the archive tier. If no space is available in the archive tier, new writes are placed on the next higher tier available. Subsequent access to that data enables for its promotion to the performance tiers as it is accessed more often. However, the data has a lower threshold for demotion. The data is moved out of the highest performance SSD tier when there is a need to promote frequently accessed data up from a lower tier.

About initiators, hosts, and host groups

An initiator represents an external port to which the storage system is connected. The external port may be a port in an I/O adapter such as an FC HBA in a server.

The controllers automatically discover initiators that have sent an `inquiry` command or a `report luns` command to the storage system, which typically happens when a host boots up or rescans for devices. When the command is received, the system saves the initiator ID. You can also manually create entries for initiators. For example, you might want to define an initiator before a controller port is physically connected through a switch to a host.

You can assign a nickname to an initiator to make it easy to recognize for volume mapping. For a named initiator, you can also select a profile specific to the operating system for that initiator. A maximum of 512 names can be assigned.

For ease of management, you can group 1 to 128 initiators that represent a server into a host. You can also group 1 to 256 hosts into a host group. This fact enables you to perform mapping operations for all initiators in a host, or all initiators and hosts in a group, instead of for each initiator or host individually. An initiator must have a nickname to be added to a host, and an initiator can be a member of only one host. A host can be a member of only one group. A host cannot have the same name as another host, but can have the same name as any initiator. A host group cannot have the same name as another host group, but can have the same name as any host. A maximum of 32 host groups can exist.

A storage system with iSCSI ports can be protected from unauthorized access via iSCSI by enabling Challenge Handshake Authentication Protocol (CHAP). CHAP authentication occurs during an attempt by a host to log in to the system. This authentication requires an identifier for the host and a shared secret between the host and the system. Optionally, the storage system can also be required to authenticate itself to the host. This is called mutual CHAP. Steps involved in enabling CHAP include:

- Decide on host node names (identifiers) and secrets. The host node name is its iSCS Qualified Name (IQN). A secret must have 12–16 characters.
- Define CHAP entries in the storage system.
- Enable CHAP on the storage system. Note that this applies to all iSCSI hosts, in order to avoid security exposures. Any current host connections will be terminated when CHAP is enabled and will need to be re-established using a CHAP login.
- Define CHAP secret in the host iSCSI initiator.
- Establish a new connection to the storage system using CHAP. The host should be displayable by the system, as well as the ports through which connections were made.

If it becomes necessary to add more hosts after CHAP is enabled, additional CHAP node names and secrets can be added. If a host attempts to log in to the storage system, it will become visible to the system, even if the full login is not successful due to incompatible

CHAP definitions. This information may be useful in configuring CHAP entries for new hosts. This information becomes visible when an iSCSI discovery session is established, because the storage system does not require discovery sessions to be authenticated. CHAP authentication must succeed for normal sessions to move to the full feature phase.

About volume mapping

Mappings between a volume and one or more initiators, hosts, or host groups hosts enable hosts to view and access the volume. There are two types of maps that can be created: default maps and explicit maps. Default maps enable all hosts to see the volume using a specified LUN and access permissions. Default mapping applies to any host that has not been explicitly mapped using different settings. Explicit maps override a volume's default map for specific hosts.

The advantage of a default mapping is that all connected hosts can discover the volume with no additional work by the administrator. The disadvantage is that all connected hosts can discover the volume with no restrictions. Therefore, this process is not recommended for specialized volumes that require restricted access.

If multiple hosts mount a volume without being cooperatively managed, volume data is at risk for corruption. To control access by specific hosts, you can create an explicit mapping. An explicit mapping can use a different access mode, LUN, and port settings to allow or prevent access by a host to a volume. If there is a default mapping, the explicit mapping overrides it.

When a volume is created, it is not mapped by default. You can create default or explicit mappings for it. You can change the default mapping of a volume, and create, modify, or delete explicit mappings. A mapping can specify read-write, read-only, or no access through one or more controller host ports to a volume. When a mapping specifies no access, the volume is masked.

For example, a payroll volume could be mapped with read-write access for the Human Resources host and be masked for all other hosts. An engineering volume could be mapped with read-write access for the Engineering host and read-only access for other departments' hosts.

A LUN identifies a mapped volume to a host. Both controllers share a set of LUNs, and any unused LUN can be assigned to a mapping. However, each LUN is generally only used once as a default LUN. For example, if LUN 5 is the default for Volume1, no other volume in the storage system can use LUN 5 on the same port as its default LUN. For explicit mappings, the rules differ: LUNs used in default mappings can be reused in explicit mappings for other volumes and other hosts.

NOTE: When an explicit mapping is deleted, the volume's default mapping takes effect. Though default mappings can be used for specific installations, using explicit mappings with hosts and host groups is recommended for most installations.

The storage system uses Unified LUN Presentation (ULP), which can expose all LUNs through all host ports on both controllers. The interconnect information is managed in the controller firmware. ULP appears to the host as an active-active storage system where the host can choose any available path to access a LUN regardless of disk group ownership. When ULP is in use, the controllers' operating redundancy mode is shown as Active-Active ULP. ULP uses the T10 Technical Committee of INCITS Asymmetric Logical Unit Access (ALUA) extensions, in SPC-3, to negotiate paths with aware host systems. Unaware host systems see all paths as being equal.

About operating with a single controller

If you purchased a 2U controller enclosure with a single controller module, note that it does not offer redundant configuration and, in the case of controller failure, leaves the system at risk for data unavailability. For more information, see About data protection with a single controller.

NOTE: If you are operating a system with a single controller, some functionality described in the documentation may be unavailable or not applicable to your system. For example, only one storage pool can exist and text about controller failover and recovery is not applicable.

About snapshots

The system can create snapshots of virtual volumes up to the maximum number supported by your system. Snapshots provide data protection by enabling you to create and save source volume data states at the point in time when the snapshot was created. Snapshots can be created manually or you can schedule snapshot creation. After a snapshot has been created, the source volume cannot be expanded.

When you reach the maximum number of snapshots for your system, before you can create a new snapshot, you must delete an existing snapshot. To view the maximum number of snapshots for your system, see the **System configuration limits** topic in the PowerVault Manager help.

The system treats a snapshot like any other volume. The snapshot can be mapped to hosts with read-only access, read-write access, or no access, depending on the purpose of the snapshot.

Snapshots use the rollback feature, which replaces the data of a source volume or snapshot with the data of a snapshot that was created from it.

Snapshots also use the reset snapshot feature, which enables you to replace the data in a snapshot with the current data in the source volume. When you reset a snapshot, the snapshot name and mappings are not changed.

The `set snapshot-space` CLI command enables you to set the percent of the pool that can be used for snapshots (the snapshot space). Optionally, you can specify a limit policy to enact when the snapshot space reaches the percentage. You can set the policy to either notify you via the event log that the percentage has been reached (in which case the system continues to take snapshots, using the general pool space), or to notify you and trigger automatic deletion of snapshots. If automatic deletion is triggered, snapshots are deleted according to their configured retention priority. For more information, see the *Dell EMC PowerVault ME4 Series Storage System CLI Guide*.

Snapshot creation and levels

Creating snapshots is a fast and efficient process that merely consists of pointing to the same data to which the source volume or snapshot points. Since snapshots reference volumes, they take up no space unless they or the source volume or source snapshot is modified.

Space does not have to be reserved for snapshots because all space in the pool is available for them. It is easy to take snapshots of snapshots and use them in the same way that you would use any volume. Since snapshots have the same structure as volumes, the system treats them the same way.

Because a snapshot can be the source of other snapshots, a single virtual volume can be the progenitor of many levels of snapshots. Originating from an original base volume, the levels of snapshots create a snapshot tree that can include up to 254 snapshots, each of which can also be thought of as a leaf of the tree. When snapshots in the tree are the source of additional snapshots, they create a new branch of the snapshot tree and are considered the parent snapshot of the child snapshots, which are the leaves of the branch.

The tree can contain snapshots that are identical to the volume or have content that has been later modified. Once the 254-snapshot limit has been reached, you cannot create additional snapshots of any item in the tree until you manually delete existing snapshots from the tree. You can only delete snapshots that do not have any child snapshots.

You cannot expand the base volume of a snapshot tree or any snapshots in the tree.

Rollback and reset snapshot features

With the rollback feature, if the contents of the selected snapshot have changed since it was created, the modified contents will overwrite those of the source volume or snapshot during a rollback. Since virtual snapshots are copies of a point in time, a modified snapshot cannot be reverted. If you want a virtual snapshot to provide the capability to revert the contents of the source volume or snapshot to when the snapshot was created, create a snapshot for this purpose and archive it so you do not change the contents.

For snapshots, the reset snapshot feature is supported for all snapshots in a tree hierarchy. However, a snapshot can only be reset to the immediate parent volume or snapshot from which it was created.

About copying volumes

For virtual storage, this feature enables you to copy a virtual base volume or snapshot to a new virtual volume.

The volume copy feature enables you to copy a base volume and snapshot to a new volume. This feature creates a complete “physical” copy of a base volume or virtual snapshot within a storage system. It is an exact copy of the source as it existed at the time the copy operation was initiated, consumes the same amount of space as the source, and is independent from an I/O perspective. In contrast, the snapshot feature creates a point-in-time logical copy of a volume, which remains dependent on the source volume.

The volume copy feature provides the following benefits:

- Additional data protection: An independent copy of a volume provides additional data protection against a complete source volume failure. If the source volume fails, the copy can be used to restore the volume to the point in time when the copy was created.
- Non-disruptive use of production data: With an independent copy of the volume, resource contention and the potential performance impact on production volumes is mitigated. Data blocks between the source and the copied volumes are independent, versus shared with snapshots, so that I/O is to each set of blocks respectively. Application I/O transactions are not competing with each other when accessing the same data blocks.

For more information about creating a copy of a virtual base volume or snapshot, see Copying a volume or snapshot.

About reconstruction

If one or more disks fail in a disk group and spares of the appropriate size (same or larger) and type (same as the failed disks) are available, the storage system automatically uses the spares to reconstruct the disk group. Disk group reconstruction does not require I/O to be stopped, so volumes can continue to be used while reconstruction is in progress.

If no spares are available, reconstruction does not start automatically. The copyback process starts when the failed disk is replaced. If you have configured the dynamic spares feature through the CLI, reconstruction will automatically start for disk groups. With dynamic spares enabled, if a disk fails and you replace it with a compatible disk, the storage system rescans the bus, finds the new disk, automatically designates it a spare, and starts reconstructing the disk group. See About spares.

For virtual storage, reconstruction of all disk groups uses a quick-rebuild feature. For more information on quick rebuild, see About quick rebuild.

When a disk fails, its fault LED illuminates amber. When a spare is used as a reconstruction target, its activity LED blinks green. During reconstruction, the fault LED and activity LEDs for all disks in the disk group blink. For descriptions of LED states, see the Deployment Guide.

NOTE: Reconstruction can take hours or days to complete, depending on the disk group RAID level and size, disk speed, utility priority, host I/O activity, and other processes running on the storage system.

At any time after disk failure, you can remove the failed disk and replace it with a new disk of the same type in the same slot.

The following steps describe the drive failure process that occurs when a drive fails in a disk group:

1. A drive fails.
2. An available compatible spare drive joins the disk group.
3. Reconstruction starts and the disk group status is `VRSC/RCON`.
4. The failed drive replaced by a new drive.
5. A copyback operation from the spare drive to the new drive begins. The status of the disk group is `CPYBK`.
6. When the copyback operation completes, the original spare drive exits the disk group and it becomes a spare drive again.

A drive may go missing from a slot because of accidental removal or bus/slot issues prevent it from being detected. The following steps describe the drive failure process that occurs when a drive goes missing from a slot:

1. A drive goes missing from a slot.
2. An available compatible spare drive joins the disk group.
3. Reconstruction starts and the disk group status is `VRSC/RCON`.
4. The missing drive is placed back in its slot or the missing drive is detected and shows up. The status of the drive is `LEFTOVER`.
5. Metadata of the `LEFTOVER` drive is cleared and the drive joins the disk group.

   NOTE: If more than one drive in the disk group has a status of `LEFTOVER`, please contact technical support before proceeding with any action.
6. A copyback operation from the spare drive to the drive that joined the disk group begins. The status of the disk group is `CPYBK`.
7. When the copyback operation completes, the original spare drive exits the disk group and it becomes a spare drive again.

About quick rebuild

Quick rebuild is a method for reconstructing a virtual disk group that is no longer fault-tolerant after a disk failure. This method takes advantage of virtual storage knowledge of where user data is written to rebuild only the data stripes that contain user data.

Typically, storage is only partially allocated to volumes so the quick-rebuild process completes significantly faster than a standard RAID rebuild. Data stripes that have not been allocated to user data are scrubbed in the background, using a lightweight process that allows future data allocations to be more efficient.

After a quick rebuild, scrub starts on the disk group within a few minutes.

About performance statistics

You can view current or historical performance statistics for components of the storage system.

Current performance statistics for disks, disk groups, pools, tiers, host ports, controllers, and volumes are displayed in tabular format. Current statistics show the current performance and are sampled immediately upon request.

Historical performance statistics for disks, pools, and tiers are displayed in graphs for ease of analysis. Historical statistics focus on disk workload. You can view historical statistics to determine whether I/O is balanced across pools and to identify disks that are experiencing errors or are performing poorly.

The system samples historical statistics for disks every quarter hour and retains these samples for 6 months. It samples statistics for pools and tiers every 5 minutes and retains this data for one week but does not persist it across failover or power cycling. By default, the graphs show the latest 100 data samples, but you can specify either a time range of samples to display or a count of samples to display. The graphs can show a maximum of 100 samples.

If you specify a time range of samples to display, the system determines whether the number of samples in the time range exceeds the number of samples that can be displayed (100), requiring aggregation. To determine this, the system divides the number of samples in the specified time range by 100, giving a quotient and a remainder. If the quotient is 1, the 100 newest samples will be displayed. If the quotient exceeds 1, each quotient number of newest samples will be aggregated into one sample for display. The remainder is the number of oldest samples that will be excluded from display.

- Example 1: A 1-hour range includes 4 samples. 4 is less than 100 so all 4 samples are displayed.
- Example 2: A 30-hour range includes 120 samples. 120 divided by 100 gives a quotient of 1 and a remainder of 20. Therefore, the newest 100 samples will be displayed and the oldest 20 samples will be excluded.
- Example 3: A 60-hour range includes 240 samples. 240 divided by 100 gives a quotient of 2 and a remainder of 40. Therefore, each two newest samples will be aggregated into one sample for display and the oldest 40 samples will be excluded.

If aggregation is required, the system calculates values for the aggregated samples. For a count statistic (total data transferred, data read, data written, total I/Os, number of reads, number of writes), the samples' values are added to produce the value of the aggregated sample. For a rate statistic - total data throughput, read throughput, write throughput, total IOPS, read IOPS, write IOPS - the samples' values are added and then are divided by their combined interval. The base unit for data throughput is bytes per second.

- Example 1: Two samples' number-of-reads values must be aggregated into one sample. If the value for sample 1 is 1060 and the value for sample 2 is 2000 then the value of the aggregated sample is 3060.
- Example 2: Continuing from example 1, each sample's interval is 900 seconds so their combined interval is 1800 seconds. Their aggregate read-IOPs value is their aggregate number of reads (3060) divided by their combined interval (1800 seconds), which is 1.7.

You can export historical performance statistics in CSV format to a file on the network for import into a spreadsheet or other application. You can also reset current or historical statistics, which clears the retained data and continues to gather new samples.

For more information about performance statistics, see Viewing performance statistics, Updating historical statistics, Exporting historical performance statistics, and Resetting performance statistics.

About firmware updates

Controller modules, expansion modules, and disk drives contain firmware that operate them. As newer firmware versions become available, they may be installed at the factory or at a customer maintenance depot or they may be installed by storage-system administrators at customer sites. For a dual-controller system, the following firmware-update scenarios are supported:

- The administrator installs a new firmware version in one controller and wants that version to be transferred to the partner controller.
- In a system that has been qualified with a specific firmware version, the administrator replaces one controller module and wants the firmware version in the remaining controller to be transferred to the new controller (which might contain older or newer firmware).

When a controller module is installed into an enclosure at the factory, the enclosure midplane serial number and firmware-update timestamp are recorded for each firmware component in controller flash memory, and will not be erased when the configuration is changed or is reset to defaults. These two pieces of data are not present in controller modules that are not factory-installed and are used as replacements.

Updating controller firmware with the Partner Firmware Update (PFU) option enabled will ensure that the same firmware version is installed in both controller modules. PFU uses the following algorithm to determine which controller module will update its partner:

- If both controllers are running the same firmware version, no change is made.
- If the firmware in only one controller has the proper midplane serial number then the firmware, midplane serial number, and attributes of that controller are transferred to the partner controller. Subsequently, the firmware update behavior for both controllers depends on the system settings.
- If the firmware in both controllers has the proper midplane serial number then the firmware having the latest firmware-update timestamp is transferred to the partner controller.
- If the firmware in neither controller has the proper midplane serial number, then the firmware version in controller A is transferred to controller B.

NOTE: Dell EMC recommends always updating controller firmware with the PFU option enabled unless otherwise directed by Tech Support.

For information about the procedures to update firmware in controller modules, expansion modules, and disk drives, see Updating firmware on page 59. That topic also describes how to use the activity progress interface to view detailed information about the progress of a firmware-update operation.

About managed logs

As the storage system operates, it records diagnostic data in several types of log files. The size of any log file is limited, so over time and during periods of high activity, these logs can fill up and begin overwriting their oldest data. The managed logs feature allows log data to be transferred to a log-collection system, and store it for later retrieval before any data is lost. The *log-collection system* is a host computer that is designated to receive the log data transferred from the storage system. The transfer does not remove any data from the logs in the storage system. This feature is disabled by default.

The managed logs feature can be configured to operate in *push mode* or *pull mode*:

- In push mode, when log data has accumulated to a significant size, the storage system sends notifications with attached log files via email to the log-collection system. The notification will specify the storage-system name, location, contact, and IP address, and will contain a single log segment in a compressed zip file. The log segment will be uniquely named to indicate the log-file type, the date and time of creation, and the storage system. This information will also be in the email subject line. The file name format is `logtype_yyyy_mm_dd__hh_mm_ss.zip`.
- In pull mode, when log data has accumulated to a significant size, the system sends notifications via email, SMI-S, or SNMP to the log-collection system, which can then use FTP or SFTP to transfer the appropriate logs from the storage system. The notification will specify the storage-system name, location, contact, and IP address and the log-file type or region that needs to be transferred.

The managed logs feature monitors the following controller-specific log files:

- Expander Controller (EC) log, which includes EC debug data, EC revisions, and PHY statistics
- Storage Controller (SC) debug log and controller event log
- SC crash logs, which include the SC boot log
- Management Controller (MC) log

Each log-file type also contains system-configuration information. The capacity status of each log file is maintained, as well as the status of what data has already been transferred. Three capacity-status levels are defined for each log file:

- Need to transfer—The log file has filled to the threshold at which content needs to be transferred. This threshold varies for different log files. When this level is reached:
  - In push mode, informational event 400 and all untransferred data is sent to the log-collection system.
  - In pull mode, informational event 400 is sent to the log-collection system, which can then request the untransferred log data. The log-collection system can pull log files individually, by controller.
- Warning—The log file is nearly full of untransferred data. When this level is reached, warning event 401 is sent to the log-collection system.
- Wrapped—The log file has filled with untransferred data and has started to overwrite its oldest data. When this level is reached, informational event 402 is sent to the log-collection system.

Following the transfer of a log's data in push or pull mode, the log's capacity status is reset to zero to indicate that there is no untransferred data.

NOTE: In push mode, if one controller is offline its partner will send the logs from both controllers.

Alternative methods for obtaining log data are to use the Save Logs action in the PowerVault Manager or the `get logs` command in the FTP or SFTP interface. These methods will transfer the entire contents of a log file without changing its capacity-status level. Use of Save Logs or `get logs` is expected as part of providing information for a technical support request. For information about using the Save Logs action, see Saving log data to a file. For information about using the FTP or SFTP interface, see Using FTP and SFTP.

About SupportAssist

SupportAssist provides an enhanced support experience for ME4 Series storage systems by sending configuration and diagnostic information to technical support at regular intervals.

Technical support analyzes this data and automatically performs health checks. If issues are detected that require attention, support cases are opened automatically, immediately starting the process to troubleshoot and resolve the issue. This process often occurs before storage administrators even notice that a problem exists.

If you need help with an issue and need to call technical support, they can access information about your storage system that was sent by SupportAssist. This feature enables technical support to help you right way, without having to wait for configuration and diagnostic data to be collected and sent to technical support.

SupportAssist data

The data that SupportAssist sends does not provide technical support with the information that is needed to connect to an ME4 Series array, because passwords are not transmitted.

The configuration and diagnostic information that is sent by SupportAssist includes the following:

- ME4 Series features
- ME4 Series logs
- Hardware inventory including model numbers and firmware versions
- Connectivity status of server, controller, and enclosure ports
- ME4 Series volume attributes like name, size, volume folder, storage profile, snapshot profile, and server mappings
- Controller network configuration
- I/O, storage, and replication usage information

Secure data transmission and storage

SupportAssist transmits data using a secure link. Data is sent using a 2048-bit RSA key over a Hypertext Transfer Protocol with Secure Socket Layer (HTTPS) session.

The data is stored securely in the SupportAssist database in accordance with the Dell EMC privacy policy. The Dell EMC privacy policy is available at http://www.dell.com/learn/us/en/uscorp1/policies-privacy?c=us&l=en&s=corp .

Enabling SupportAssist does not give technical support the ability to access the array to retrieve information. Data is always pushed to technical support, never pulled. SupportAssist can be disabled at any time, giving customers complete control over the transmission of SupportAssist data.

About CloudIQ

CloudIQ provides storage monitoring and proactive service, giving you information tailored to your needs, access to near real-time analytics, and the ability to monitor storage systems from anywhere at any time. CloudIQ simplifies storage monitoring and service by providing:

- Proactive serviceability that informs you about issues before they impact your environment.
- Centralized monitoring across your environment, using a dashboard that aggregates key information such as system health scores, performance metrics, and current capacity and trends.

CloudIQ requires the following:

- ME4 Series storage systems must be running firmware version G280 or later.
- SupportAssist must be enabled on ME4 Series storage systems.
- The **Enable CloudIQ** check box in the **SupportAssist** - **CloudIQ Settings** tab must be selected.

NOTE: For more information about CloudIQ, contact technical support or visit the CloudIQ product page.

About configuring DNS settings

You can set a domain host name for each controller module to identify it for management purposes by configuring settings in the Domain Name Service (DNS) tab. The DNS name server supports IPv4 and IPv6 formats, and the system supports a maximum of three DNS servers per controller. Configuring the storage system to communicate with a DNS server within your network will allow network changes, such as frequent IP address changes in a DHCP environment, to occur without interrupting notifications sent by the system to users.

The controller will advertise the domain host name to DNS servers, and the DNS servers will in turn create and advertise a fully qualified domain name (FQDN) for the controller by appending the domain host name to the DNS domain string that identifies the controller.

A host name must differ for each controller, is not case sensitive, and can have from 1 to 63 bytes. The name must start with a letter and end with a letter or digit, and can include letters, numbers, or hyphens, but no periods.

After a reachable DNS server is configured on the system, you can configure an SMTP server using a name such as `mysmtpserver.example.com`. Further, you could configure search domain `example.com` and SMTP server `mysmtpserver` and reach the same destination.

You must use this feature to configure DNS parameters before you configure email parameters in any environments where DNS i be required to resolve server names. The system does not support auto-configuration of DNS parameters if network parameters are set to DHCP mode, so DNS must be manually configured regardless of the DHCP setting. For more information about configuring DNS settings, see Configure DNS settings on page 43.

If DNS server functionality is operational and reachable by the controller's nslookup service, the FQDN for each controller is also shown. If nslookup output is not available, the domain name will show '-'.

NOTE: DNS settings are limited to SMTP server configuration for email notification only.

About replicating virtual volumes

Replication for virtual storage provides a remote copy of a volume, volume group, or snapshot on a remote system by periodically updating the remote copy to contain a point-in-time consistent image of a source volume.

For information about replication for virtual storage, see Working in the Replications topic.

About the Full Disk Encryption feature

Full Disk Encryption (FDE) is a method by which you can secure the data residing on the disks. It uses self-encrypting drives (SED), which are also referred to as FDE-capable disks. When secured and removed from a secured system, FDE-capable disks cannot be read by other systems.

The ability to secure a disk and system relies on passphrases and lock keys. A passphrase is a user-created password that allows users to manage lock keys. A lock key is generated by the system and manages the encryption and decryption of data on the disks. A lock key is persisted on the storage system and is not available outside the storage system.

A system and the FDE-capable disks in the system are initially unsecured but can be secured at any point. Until the system is secured, FDE-capable disks function exactly like disks that do not support FDE.

Enabling FDE protection involves setting a passphrase and securing the system. Data that was present on the system before it was secured is accessible in the same way it was when it was unsecured. However, if a disk is transferred to an unsecured system or a system with a different passphrase, the data is not accessible.

Secured disks and systems can be repurposed. Repurposing a disk changes the encryption key on the disk, effectively erasing all data on the disk and unsecuring the system and disks. Repurpose a disk only if you no longer need the data on the disk.

FDE operates on a per-system basis, not a per-disk group basis. To use FDE, all disks in the system must be FDE-capable. For information on setting up FDE and modifying FDE options, see Changing FDE settings.

NOTE: If you insert an FDE disk into a secured system and the disk does not come up in the expected state, perform a manual rescan. See Rescanning disk channels.

About data protection with a single controller

The system can operate with a single controller if its partner has gone offline or has been removed. Because single-controller operation is not a redundant configuration, this section presents some considerations concerning data protection.

The default caching mode for a volume is write back, as opposed to write through. In write-back mode, the host is notified that the controller has received the write when the data is present in the controller cache. In write-through mode, the host is notified that the controller has received the write when the data is written to disk. Therefore, in write-back mode, data is held in the controller cache until it is written to disk.

If the controller fails while in write-back mode, unwritten cache data likely exists. The same is true if the controller enclosure or the enclosure of the target volume is powered off without a proper shutdown. Data remains in the controller cache and associated volumes will be missing that data on the disk.

If the controller can be brought back online long enough to perform a proper shutdown and the disk group is online, the controller should be able to write its cache to disk without causing data loss.

If the controller cannot be brought back online long enough to write its cache data to disk, please contact technical support.

To help prevent data loss in case the controller fails, you can change the caching mode of a volume to write through. While this will cause significant performance degradation, this configuration guards against data loss. While write-back mode is much faster, this mode is not guaranteed against data loss in the case of a controller failure. If data protection is more important, use write-through caching. If performance is more important, use write-back caching.

For more information about volume cache options, see About volume cache options. For more information about changing cache settings for a volume, see Modifying a volume. For more information about changing system cache settings, see Changing system cache settings.

2

Working in the Home topic

The Home topic provides options to set up and configure your system and manage tasks, and displays an overview of the storage managed by the system. The content presented depends on the completion of all required actions in the Welcome panel. The standard Home topic is hidden by the Welcome panel until all required actions are complete.

Topics:

Guided setup

The Welcome panel provides options for you to quickly and easily set up your system by guiding you through the configuration and provisioning process.

With guided setup, you must first configure your system settings by accessing the System Settings panel and completing all required options. After these options are complete, you can then provision your system by accessing the Storage Setup panel and the Host Setup panel and completing the wizards.

NOTE: A user with the `manage` role must complete the guided setup process.

The Welcome panel also displays the health of the system. If the health of the system is degraded or faulty, you can click **System Information** to access the System topic. Here you can view information about each enclosure, including its physical components, in front, rear, and tabular views. For more information, see Working in the System topic. If the system detects that it has only one controller, its health shows as degraded. If you are operating the system with a single controller, acknowledge this in the panel. If the system has two controllers, click **System Information** to diagnose the problem.

If the system health is degraded, you may still be able to configure and provision the system. However, it is recommended that you resolve any health issues before continuing. If the system health is bad, you will be unable to configure and provision the system until you resolve the problem.

The Welcome panel appears when:

- You have a brand new system (storage is not provisioned, all disks are empty and available, and no settings have been selected).
- You have not entered all required system settings and/or the system has no pools.

NOTE: After you have entered all required systems settings, you can turn off access to the Welcome panel and configure and provision the system manually by clicking Skip the Welcome screen. A confirmation window appears, prompting you to confirm your selection. For information on manual configuration, see Configure and provision a new storage system on page 10.

To use guided setup:

1. From the Welcome panel, click **System Settings**.
2. Choose options to configure your system. For information about specific options, see Configuring system settings.

   NOTE: Tabs with a red asterisk next to them are required.

3. Save your settings and exit System Settings to return to the Welcome panel.
4. Click **Storage Setup** to access the Storage Setup wizard and follow the prompts to begin provisioning your system by creating disk groups and pools. For more information about using the Storage Setup wizard, see Provisioning disk groups and pools.
5. Save your settings and exit Storage Setup to return to the Welcome panel.
6. Click **Host Setup** to access the Host Setup wizard and follow the prompts to continue provisioning your system by attaching hosts. For more information see Attaching hosts and volumes.

Provisioning disk groups and pools

The Storage Setup wizard guides you through each step of the process, including creating disk groups and pools in preparation for attaching hosts and volumes.

NOTE: You can cancel the wizard at any time, but changes that are made in completed steps are saved.

Access the Storage Setup wizard from the Welcome panel or by choosing **Action** > **Storage Setup**. When you access the wizard, you must select the storage type for your environment. After selecting a storage type, you are guided through the steps to create disk groups and pools. The panels that appear and the options within them are dependent upon:

- Whether you select a virtual or linear storage type
- Whether the system is brand new (all disks are empty and available and no pools have been created)
- Whether the system has any pools
- Whether you are experienced with storage provisioning and want to set up your disk groups in a certain way

On-screen directions guide you through the provisioning process. If at any point you decide that you want to manually provision the system, cancel the wizard to do so. For more information about manual provisioning, see Configuring and provisioning a new storage system.

NOTE: You can use the Storage Setup wizard with manual provisioning. The Storage Setup wizard provides you with optimal storage configuration options to quickly enable I/O operations. Manual provisioning offers more options and greater flexibility, but with added complexity. If you choose to use the wizard, you can still manually provision the system at a later time.

Select the storage type

When you first access the wizard, you are prompted to select the type of storage to use for your environment. Read through the options and make your selection, then click **Next** to proceed.

NOTE: After you create a disk group using one storage type, the system will use that storage type for additional disk groups. To switch to the other storage type, you must first remove all disk groups. For more information, see Removing disk groups.

Create disk groups and pools

The panel that appears when creating disk groups and pools is dependent upon whether you are operating in a virtual storage environment or a linear storage environment.

Virtual storage environments

If you are operating in a virtual storage environment, the system scans all available disks, recommends one optimal storage configuration, and displays the suggested disk group layout within the panel. Disk groups are automatically grouped together by pool and tier and include a description of the total size and number of disks that will be provisioned (including the configuration of spares and unused disks).

If the system is unable to determine a valid storage configuration, the wizard lists the reasons why and provides directions on how to achieve a proper configuration. If the system is unhealthy, an error is displayed along with a description of how to fix it. Follow the recommendations in the wizard to correct the errors, then click **Rescan** to view the optimized configuration.

For a system with no pools provisioned, if you are satisfied with the recommended configuration, click **Create Pools** to provision the system as displayed in the panel and move on to attaching hosts. For a system that contains a pool, if you are satisfied with the recommended configuration, click **Expand Pools** to provision the system as displayed in the panel.

If your environment requires a unique setup, click **Go To Advanced Configuration** to access the Create Advanced Pools panel. Select Add Disk Group and follow the instructions to manually create disk groups one disk at a time. Select Manage Spares and follow the instructions to manually select global spares.

Linear storage environments

If you are operating in a linear storage environment, the Create Advanced Pools panel opens. Select **Add Disk Groups** and follow the instructions to manually create disk groups one at a time. Select **Manage Spares** and follow the instructions to manually select global spares. Click the icon for more information about options presented.

Open the guided disk group and pool creation wizard

1. Access Storage Setup by doing one of the following:
   - From the Welcome panel, click **Storage Setup**.
   - From the Home topic, click **Action > Storage Setup**.
2. Follow the on-screen directions to provision your system.

Attaching hosts and volumes in the Host Setup wizard

The Host Setup wizard guides you through each step in the process of selecting initiators and creating a host, grouping hosts, and attaching the host or host group to volumes within the system. As you complete each step, it is highlighted and marked with a check. If at any point you decide that you want to attach hosts at a later time, cancel the wizard.

Access the Host Setup wizard from the Welcome panel or by choosing **Action** > **Host Setup**. You are guided through the following sequential steps:

- Verify prerequisites in the Host Setup wizard
- Select a host in the Host Setup wizard
- Group hosts in the Host Setup wizard
- Add and manage volumes in the Host Setup wizard
- Configuration summary

You must navigate through the wizard each time you want to attach a host. At the end of each complete pass through the wizard, a single host or host group is configured to the system and you are prompted to configure another host. Choosing No exits the wizard and completes the system configuration.

NOTE: You can provision your system using the Storage Setup wizard in combination with manual provisioning. The Storage Setup wizard provides you with an optimal storage configuration based on the type of disks in the system. Manual provisioning offers more options and greater flexibility, but with added complexity. If you choose to use the wizard you can still manually provision the system at a later time.

Verify prerequisites in the Host Setup wizard

When you first access the wizard, introductory content is based on the host ports discovered on your system. Read the material and verify that all prerequisites have been satisfied to enable the wizard to successfully guide you through the process. When you are ready to attach hosts, click **Next**.

Select a host in the Host Setup wizard

The Select Host section of the wizard provides you with options to group initiators as a host and give that host a name. The system lists all initiators logged into the system that are not already mapped to volumes and assigns an editable nickname to each one that you select. When you are ready to move to the next step, click **Next**.

Group hosts in the Host Setup wizard

The Group Host section of the wizard lets you group hosts together with other hosts to facilitate clustering. You can select from a host group that has already been defined, or create a new host group starting with the current host. Follow the on-screen instructions for more information. Once you are ready to move to the next step, click **Next**.

Add and manage volumes in the Host Setup wizard

The Volumes section of the wizard provides options for you to add and manage volumes. By default, the system presents one volume on each pool, with each volume size defaulting to 100GB. The wizard lets you change the volume name and size and select the pool where

the volume will reside. Follow the instructions in the wizard to create the volumes shown in the table. Be sure to balance volume ownership between controllers. Once you are ready to move to the next step, click **Next**.

Configuration summary

The summary displays the host configuration you defined in the wizard. If you are happy with the setup, finish the process by selecting Configure Host. The volumes created are mapped to the host with read/write access and are visible on all four ports, and LUNs are automatically assigned.

Overall system status

The Home topic provides an overview of the storage managed by the system. This storage could be virtual or linear. Information is shown about hosts, host ports, storage capacity and usage, global spares, and logical storage components (like volumes, virtual snapshots, disk groups, and pools).

- Host information on page 35
- Port information
- Capacity information
- Storage information
- System health information
- Spares information

Host information

The Hosts block shows how many host groups, hosts, and initiators are defined in the system. An initiator identifies an external port to which the storage system is connected. The external port may be a port in an I/O adapter in a server, or a port in a network switch. A host is a user-defined set of initiators that represents a server. A host group is a user-defined set of hosts for ease of management.

NOTE: If the external port is a switch and there is no connection from the switch to an I/O adapter, then no host information will be shown.

Port information

The Ports A block shows the name and protocol type of each host port in controller A. The port icon indicates whether the port is active or inactive:

The Ports B block shows similar information for controller B.

Hover the cursor over a port to see the following information in the Port Information panel. If the health is not OK, the health reason and recommended action are shown to help you resolve problems.

Table 5. Port information

Port type	Information displayed for the port type
FC port	Name, type, ID (WWN), status, configured speed, actual speed, topology, primary loop ID, supported speeds, SFP status, part number, and health
iSCSI IPv4 port	Name, type, ID (IQN), status, configured speed, actual speed, IP version, MAC address, IP address, gateway, netmask, SFP status, part number, 10G compliance, cable length, cable technology, Ethernet compliance, and health
iSCSI IPv6 port	Name, type, ID (IQN), status, configured speed, actual speed, IP version, MAC address, IP address, SFP status, part number, 10G compliance, cable length, cable technology, Ethernet compliance, default router, link-local address, and health
SAS port	Name, type, ID (WWN), status, actual speed, topology, expected lanes, active lanes, disabled lanes, cable type, and health

The area between the blocks displays the following statistics that show the current performance from all hosts to the system:

- Current IOPS for all ports, calculated over the interval since these statistics were last requested - every 30 seconds unless more than one PowerVault Manager session is active or if the CLI command `show host-port-statistics` is issued - or reset.

- Current data throughput (MB/s) for all ports, calculated over the interval since these statistics were last requested or reset.

Capacity information

The Capacity block shows two color-coded bars. The lower bar represents the physical capacity of the system, showing the capacity of disk groups, spares, and unused disk space, if any. The upper bar identifies how the capacity is allocated and used.

The upper bar shows the reserved, allocated, and unallocated space for the system. Reserved space refers to space that is unavailable for host use. It consists of RAID parity and the metadata that is needed for internal management of data structures. The terms allocated space and unallocated space have the following meanings:

For virtual storage:

- Allocated space is the amount of space that the data written to the pools takes.
- Unallocated space is space that is designated for a pool but has not been allocated to a volume within that pool.
- Uncommitted space is the overall space minus the allocated and unallocated space.

For linear storage:

- Allocated space is the space that is designated for all volumes. When a linear volume is created, space equivalent to the volume size is reserved for it. This is not the case for virtual volumes.
- Unallocated space is the difference between the overall and allocated space.

If virtual storage is *overcommitted*, which means that the amount of storage capacity that is designated for use by volumes exceeds the physical capacity of the storage system, then the right upper bar is longer than the lower bar.

Hover the cursor over a segment of a bar to see the storage size of that segment. Point anywhere in this block to see the following information about capacity utilization in the Capacity Utilization panel:

- **Total Disk Capacity**: The total physical capacity of the system.
- **Unsued**: The total unused disk capacity of the system.
- **Total Spares**: The total spare capacity of the system
- **Virtual/Linear Disk Groups**: The capacity of disk groups, both total and by pool.
- **Reserved**: The reserved space for disk groups, both total and by pool.
- **Allocated**: The allocated space for disk groups, both total and by pool.
- **Unallocated**: The unallocated space for disk groups, both total and by pool.
- **Uncommitted**: The uncommitted space in each pool (total space minus the allocated and unallocated space) and total uncommitted space.

Storage information

The Storage A and Storage B blocks provide more detailed information about the logical storage of the system. The Storage A block shows information about virtual pool A, which is owned by controller A. For linear storage, it shows most of the same information for all of the linear pools owned by controller A. The Storage B block shows the same types of information about virtual pool B or the linear pools owned by controller B. In a single-controller system, only the storage block relevant to that controller will be shown (for example, only the Storage A block will be shown if controller A is the sole operating controller).

Each storage block contains color-coded graphs for virtual and linear storage.

For virtual storage, the block contains a pool capacity graph, a disk group utilization graph, and—if read cache is configured—a cache utilization graph. The pool capacity graph consists of two horizontal bars. The top bar represents the allocated and unallocated storage for the pool with the same information as the capacity top bar graph, but for the pool instead of the system. The bottom horizontal bar represents the size of the pool.

The disk group utilization graph consists of a graph with vertical measurements. The size of each disk group in the virtual pool is proportionally represented by a horizontal section of the graph. Vertical shading for each disk group section represents the relative space allocated in that disk group. A tool tip for each section shows the disk group name, size, and amount of unallocated space. The color for each disk group represents the tier to which it belongs.

The cache utilization graph also consists of a graph with vertical measurements. However, since read cache does not cache pool capacity, it is represented independently.

For linear storage, the pool capacity graph consists of a single horizontal bar that shows the overall storage for the pool(s) owned by the controller. Unlike with virtual storage, there is no bottom horizontal bar. The disk group utilization graph is similar to that shown for virtual storage. The size of each linear disk group in the storage block is proportionally represented by a horizontal section of the graph. Vertical shading for each disk group section represents the relative space allocated in that disk group. A tool tip for each section shows the disk group name, size, and amount of unallocated space. The sections are all the same color since linear disk groups are not tiered.

The number of volumes and virtual snapshots for the pool owned by the controller appears above the top horizontal bar for both virtual and linear storage.

Hover the cursor anywhere in a storage block to display the Storage Information panel. The Storage Information panel only contains information for the type of storage that you are using.

Table 6. Storage information

Storage type	Information displayed for the storage type
Virtual pool	• Owner, storage type, total size, allocated size, snapshot size, available size, allocation rate, and deallocation rate • For each tier: Pool percentage, number of disks, total size, allocated size, unallocated size, number of reclaimed pages, and health • If the pool health is not OK, an explanation and recommendations for resolving problems with unhealthy components is available. If the overall storage health is not OK, the health reason, recommended action, and unhealthy subcomponents are shown to help you resolve problems.
Linear pool	• Owner, storage type, total size, allocated size, and available size • If the pool health is not OK, an explanation and recommendations for resolving problems with unhealthy components is available. If the overall storage health is not OK, the health reason, recommended action, and unhealthy subcomponents are shown to help you resolve problems.

System health information

The health icon between the storage blocks indicates the health of the system. Hover the cursor over this icon to display the System Health panel, which shows more information about the health state. If the system health is not OK, the System Health panel also shows information about resolving problems with unhealthy components.

Spares information

The Spares block between the storage blocks and below the event icon shows the number of disks that are designated as global spares to automatically replace a failed disk in the system. Hover the cursor over the Spares block to see the disk types of the available global spares in the Global Spares Information panel.

Resolving a pool conflict caused by inserting a foreign disk group

If you insert a virtual disk group from an old system into a new system, the new system attempts to create a virtual pool for that disk group. If that system already has a virtual pool with the same name, the pool for the inserted disk group will be offline. For example, if the new system has a pool A and you insert a disk group that came from pool A on the old system, the imported pool A from old system will be offline.

This type of operation is not common, and you should consider your conflict resolution options carefully. To resolve this conflict, do either of the following:

- If the pool conflict was expected—for example, you want to access data on the disk group from pool A of the old system:
  1. Unmount and unmap the LUNs from any host accessing volumes on the new system.
  2. Stop I/O from hosts accessing any volumes on the new system and power down the new system.
  3. Physically remove all disks for the original pool A of the new system.
  4. Insert the disks from pool A of the old system.
  5. Restore power to the new system. The data on the disk group from pool A of the old system is now accessible.
  6. Copy that data to pool B on the new system.
  7. After you have copied the data to the new system, remove the disks from old system and reinsert the disks from the new system.
  8. Remap and remount the LUNs to any host that requires access to volumes on pool A of the new system.

CAUTION: This type of operation must be performed offline. Removing a virtual disk group or pool while the system is online may result in corruption and possible data loss. The system must be powered off before any disks are removed.

- If the pool conflict was unexpected—for example, you did not realize that there was a previous pool on the disks of the old system and data that is contained on the disks is no longer needed:
  1. Remove the disks that were from the old system out of the new system.
  2. Put the disks back into the old system.
  3. From the old system, delete the pool off the disks.

     CAUTION: Deleting a pool deletes all the data that it contains.
  4. Reinsert the disks into the new system.

     The disks from the old system now show as available and can be added to an existing pool on the new system.

If you are unable to find a pool with a duplicate name, or are unsure of how to safely proceed, download logs from the system, and contact technical support for assistance.

Configuring system settings

Access the System Settings panel by doing one of the following:

- In the Home topic, select **Action > System Settings**.
- In the System topic, select **Action > System Settings**.
- In the Welcome panel, select **System Settings**.

The System Settings panel provides options for you to quickly and easily configure your system, including:

- Set the system date and time
- Manage users
- Configure controller network ports
- Enable or disable management interface services
- Change system information settings
- Set system notification settings
- Enable SupportAssist on page 49
- Change host port settings (if applicable)

Navigate the options by clicking the tabs located on the left side of the panel. Tabs with a red asterisk next to them are required. To apply and save changes, click **Apply**, To apply changes and close the panel, click **Apply and Close**.

Set the system date and time

Use the Date and Time panel to change the storage system date and time that appears in the banner. It is important to set the date and time so that entries in system logs and notifications have correct time stamps.

You can set the date and time manually or configure the system to use NTP to obtain them from an available network-attached server. Using NTP allows multiple storage devices, hosts, log files, and so forth to be synchronized. The NTP value can be an IPv4 address, IPv6 address, or FQDN. If NTP is enabled but no NTP server is present, the date and time are maintained as if NTP was not enabled.

NTP server time is provided in the UTC time scale, which provides several options:

- To synchronize the times and logs between storage devices installed in multiple time zones, set all the storage devices to use UTC.
- To use the local time for a storage device, set its time zone offset.
- If a time server can provide local time rather than UTC, configure the storage devices to use that time server, with no further time adjustment.

Whether NTP is enabled or disabled, the storage system does not automatically make time adjustments for Daylight Saving Time. You must make such adjustments manually.

Enter date and time settings manually

1. `Perform one of the following to access the Date and Time options:`
   - In the Home topic, select **Action > System Settings**.
   - In the System topic, select **Action > System Settings**.

- In the banner, click the **System Date/Time Bar** panel and select **Set Date and Time**.
- In the Welcome panel, select **System Settings > Date and Time**.

2. If checked, clear the **Network Time Protocol (NTP)** check box.
3. To set the Date value, enter the current date in the format YYYY-MM-DD.
4. To set the Time value, enter two-digit values for the hour and minutes and select either AM, PM, or 24H (24-hour clock).
5. `Perform one of the following:`
   - To save your settings and continue configuring your system, click **Apply**.
   - To save your settings and close the panel, click **Apply and Close**.

   A confirmation panel appears.
6. Click **OK** to save your changes. Otherwise, click **Cancel**.

Obtain the date and time from an NTP server

1. `Perform one of the following to access the Date and Time options:`
   - In the Home topic, select **Action > System Settings**.
   - In the System topic, select **Action > System Settings**.
   - In the banner, click the **System Date/Time Bar** panel and select **Set Date and Time**.
   - In the Welcome panel, select **System Settings > Date and Time**.
2. Select the **Network Time Protocol (NTP)** check box.
3. `Perform one of the following:`
   - To have the system retrieve time values from a specific NTP server, enter its IP address in the NTP Server Address field.
   - To have the system listen for time messages sent by an NTP server in broadcast mode, clear the NTP Server Address field.
4. In the NTP Time Zone Offset field, enter the time zone as an offset in hours, and optionally minutes, from UTC. For example: the Pacific Time Zone offset is -8 during Pacific Standard Time or -7 during Pacific Daylight Time and the offset for Bangalore, India is +5:30.
5. `Perform one of the following:`
   - To save your settings and continue configuring your system, click **Apply**.
   - To save your settings and close the panel, click **Apply and Close**.

   A confirmation panel appears.
6. Click **OK** to save your changes. Otherwise, click **Cancel**.

Managing users

The system provides three default users. Nine more users can be created.

The default users are “standard users,” which can access one or more of the following management interfaces: PowerVault Manager, CLI, SMI-S, or FTP and SFTP. You can also create SNMPv3 users, which can either access the Management Information Base (MIB) or receive trap notifications. SNMPv3 users support SNMPv3 security features, such as authentication and encryption. For information about configuring trap notifications, see Setting system notification settings. For information about the MIB, see SNMP reference.

As a user with the `manage` role, you can modify or delete any user other than your current user. Users with the `monitor` role can change all settings for their own user except for user type and role. However, users with the `monitor` role can only view the settings for other users.

User options

The following options apply to standard and SNMPv3 users:

- User Name. A user name is case sensitive and can have a maximum of 29 bytes. It cannot already exist in the system or include the following: a space or " , < \
- Password. A password is case sensitive and can have 8–32 characters. If the password contains only printable ASCII characters, then it must contain at least one uppercase character, one lowercase character, one numeric character, and one non-alphanumeric character. A password can include printable UTF-8 characters except for the following: a space or " ' , < > \
- Confirm Password. Re-enter the new password.
- User Type. When creating a new user, select **Standard** to show options for a standard user, or **SNMPv3** to show options for an SNMPv3 user.

The following options apply only to a standard user:

- Roles. Select one or more of the following roles:
  - **Monitor.** Enables the user to view but not change system status and settings. This is enabled by default and cannot be disabled.
  - **Manage.** Enables the user to change system settings.
- Interfaces. Select one or more of the following interfaces:
  - **WBI.** Enables access to the PowerVault Manager.
  - **CLI.** Enables access to the command-line interface.
  - **SMI-S.** Enables access to the SMI-S interface, which is used for remote management of the system through your network.
  - **FTP.** Enables access to the FTP interface or the SFTP interface, which can be used instead of the PowerVault Manager to install firmware updates and to download logs.
- Base Preference. Select the base for entry and display of storage-space sizes:
  - **Base 2.** Sizes are shown as powers of 2, using 1024 as a divisor for each magnitude.
  - **Base 10.** Sizes are shown as powers of 10, using 1000 as a divisor for each magnitude.
- Precision Preference. Select the number of decimal places, 1 through 10, for display of storage-space sizes.
- Unit Preference. Select one of the following options for display of storage-space sizes:
  - **Auto.** Enables the system to determine the proper unit for a size. Based on the precision setting, if the selected unit is too large to meaningfully display a size, the system uses a smaller unit for that size. For example, if the unit is set to TB and the precision is set to 1, the size 0.11709 TB is shown as 117.1 GB.
  - **TB.** Display all sizes in terabytes.
  - **GB.** Display all sizes in gigabytes.
  - **MB.** Display all sizes in megabytes.
- Temperature Preference. Select whether to use the Celsius or Fahrenheit scale for display of temperatures.
- Timeout. Select the amount of time that the user's session can be idle before the user is automatically signed out (2– 720 minutes).
- Locale. Select a display language for the user. Installed language sets include Chinese-Simplified, English, French, German, Japanese, Korean, and Spanish. The locale determines the character used for the decimal (radix) point.

The following options apply only to an SNMPv3 user:

- SNMPv3 Account Type. Select one of the following types:
  - **User Access.** Enables the user to view the SNMP MIB.
  - **Trap Target.** Enables the user to receive SNMP trap notifications.
- SNMPv3 Authentication Type. Select whether to use MD5 or SHA (SHA-1) authentication, or no authentication. If authentication is enabled, the password set in the Password and Confirm Password fields must include a minimum of 8 characters and follow the other SNMPv3 privacy password rules.
- SNMPv3 Privacy Type. Select whether to use DES or AES encryption, or no encryption. To use encryption you must also set a privacy password and enable authentication.
- SNMPv3 Privacy Password. If the privacy type is set to use encryption, specify an encryption password. This password is case sensitive and can have 8–32 characters. If the password contains only printable ASCII characters, then it must contain at least one uppercase character, one lowercase character, and one non-alphabetic character. A password can include printable UTF-8 characters except for the following: a space or " , < > \
- Trap Host Address. If the account type is **Trap Target**, specify the network address of the host system that will receive SNMP traps. The value can be an IPv4 address, IPv6 address, or FQDN.

Adding, modifying, and deleting users

Add a user

1. `Log in as a user with the manage role and perform one of the following:`
   - In the Home topic, select **Action > System Settings**, then click the **Managing Users** tab.
   - In the System topic, select **Action > System Settings**, then click the **Manage Users** tab.
   - In the banner, click the user panel and select **Manage Users**.
   - In the Welcome panel, select **System Settings > Manage Users**.The Manage Users tab displays a table of existing users and options to set.
2. Below the table, click **New**.
3. Set the options.
4. `Perform one of the following:`

- To save your settings and continue configuring your system, click **Apply**.
- To save your settings and close the panel, click **Apply and Close**.

  A confirmation panel appears.

5. Click **OK** to save your changes. Otherwise, click **Cancel**.

Create a user from an existing user

1. `Log in as a user with the manage role and perform one of the following:`
   - In the Home topic, select **Action > System Settings**, then click the **Managing Users** tab.
   - In the System topic, select **Action > System Settings**., then click the **Manage Users** tab.
   - In the banner, click the user panel and select **Manage Users**.
   - In the Welcome panel, select **System Settings > Manage Users**The Manage Users tab displays a table of existing users and options to set.
2. Select the user to copy.
3. Click **Copy**. A user named `copy_of_selected-user` appears in the table.
4. Set a new user name and password and optionally change other settings.
5. `Perform one of the following:`
   - To save your settings and continue configuring your system, click **Apply**.
   - To save your settings and close the panel, click **Apply and Close**.

   A confirmation panel appear.
6. Click **OK** to save your changes. Otherwise, click **Cancel**.

Modify a user

1. `Log in as a user with the manage role and perform one of the following:`
   - In the Home topic, select **Action > System Settings**, then click the **Managing Users** tab.
   - In the System topic, select **Action > System Settings**, then click the **Manage Users** tab.
   - In the banner, click the user panel and select **Manage Users**.
   - In the Welcome panel, select **System Settings > Manage Users**.The Manage Users tab displays a table of existing users and options to set.
2. Select the user to modify.
3. Change the settings. You cannot change the user name. Users with the `monitor` role can change their own settings except for their role and interface settings.
4. `Perform one of the following:`
   - To save your settings and continue configuring your system, click **Apply**.
   - To save your settings and close the panel, click **Apply and Close**.

   A confirmation panel appears.
5. Click **OK** to save your changes. Otherwise, click **Cancel**.

Delete a user other than your current user

1. `Log in as a user with the manage role and perform one of the following:`
   - In the Home topic, select **Action > System Settings**, then click the **Managing Users** tab.
   - In the System topic, select **Action > System Settings**, then click the **Manage Users** tab.
   - In the banner, click the user panel and select **Manage Users**.
   - In the Welcome panel, select **System Settings > Manage Users**.The Manage Users tab displays a table of existing users and options to set.
2. Select the user to delete.
3. Click **Delete**. A confirmation panel appears.
4. `Perform one of the following:`
   - To save your settings and continue configuring your system, click **Apply**.
   - To save your settings and close the panel, click **Apply and Close**.

   A confirmation panel appears.

5. Click **OK** to save your changes. Otherwise, click **Cancel**. If you clicked OK, the user is removed, the table is updated, and any sessions associated with that user name are terminated.

NOTE: The system requires that at least one user with the manage role to exist.

Configuring network ports on controller modules

If you used the default 10.0.0.2/10.0.0.3 IPv4 addresses to access the guided setup, Dell EMC recommends changing the IPv4 addresses to avoid an IP conflict if you have more than ME4 Series storage system on you network.

You can manually set static IP addresses for network ports on controller modules. Alternatively, the IP addresses can be set automatically using DHCP for IPv4 or Auto for IPv6, which uses DHCPv6 and/or SLAAC. When setting IP values, you can choose either IPv4 or IPv6 formatting for each controller. You can also set the addressing mode and IP version differently for each controller module and use them concurrently. For example, you could set IPv4 on controller module A to Manual and set IPv6 on controller module B to Auto.

When using DHCP mode, the system obtains values for the network port IP address, subnet mask, and gateway from a DHCP server if it is available. If a DHCP server is unavailable, current addressing is unchanged. You must have some means of determining what addresses have been assigned, such as the list of bindings on the DHCP server. When using Auto mode, addresses are retrieved from both DHCP and Stateless address auto-configuration (SLAAC). DNS settings are also automatically retrieved from the network.

Each controller has the following factory-default IP settings:

- IP address source: Manual
- Controller A IP address: 10.0.0.2
- Controller B IP address: 10.0.0.3
- IP subnet mask: 255.255.255.0
- Gateway IP address: 10.0.0.1

When DHCP is enabled, the following initial values are set and remain set until the system can contact a DHCP server for new addresses:

- Controller IP addresses: 169.254.x.x (where the value of x.x is the lowest 16 bits of the controller serial number)
- IP subnet mask: 255.255.0.0
- Gateway IP address: 10.0.0.0

169.254.x.x addresses (including gateway 169.254.0.1) are on a private subnet that is reserved for unconfigured systems and the addresses are not routable. Using these addresses prevents the DHCP server from reassigning the addresses and possibly causing a conflict where two controllers have the same IP address. As soon as possible, change these IP values to proper values for your network.

For IPv6, when Manual mode is enabled you can enter up to four static IP addresses for each controller. When Auto is enabled, the following initial values are set and remain set until the system can contact a DHCPv6 and/or SLAAC server for new addresses:

- Controller A IP address: fd6e:23ce:fed3:19d1::1
- Controller B IP address: fd6e:23ce:fed3:19d1::2
- Gateway IP address: fd6e:23ce:fed3:19d1::3

CAUTION: Changing IP settings can cause management hosts to lose access to the storage system after the changes are applied in the confirmation step.

After you set the type of controller network ports to use, you can configure domain names using the Domain Name Service (DNS). DNS accepts IPv4 and IPv6 address formats. For more information about the DNS feature, see About configuring DNS settings.

NOTE: DNS settings are automatically applied when using DHCP for IPv4 and Auto for IPv6.

Set IPv4 addresses for network ports

Perform the following steps to set IPv4 addresses for the network ports:

1. Perform one of the following to access Network options:
   - In the Home topic, select **Action > System Settings**, and then click the **Network** tab.
   - In the System topic, select **Action > System Settings**, and then click the **Network** tab.
2. Select the **IPv4** tab.

   IPv4 uses 32-bit address.
3. Select the type of IP address settings to use for each controller from the **Source** drop-down menu:
   - Select **Manual** to specify static IP addresses.
   - Select **DHCP** to allow the system to automatically obtain IP addresses from a DHCP server.

4. If you selected **Manual**, perform the following steps: , and then
   a. Type the IP address, IP mask, and Gateway addresses for each controller.
   b. Record the IP addresses.

   NOTE: The following IP addresses are reserved for internal use by the storage system: 169.254.255.1, 169.254.255.2, 169.254.255.3, 169.254.255.4, and 127.0.0.1. Because these addresses are routable, do not use them anywhere in your network.
5. If you selected **DHCP**, complete the remaining steps to allow the controller to obtain IP addresses from a DHCP server.
6. Click **Apply**.

   A confirmation panel appears.
7. Click **OK**.
   If you selected **DHCP** and the controllers successfully obtained IP addresses from the DHCP server, the new IP addresses are displayed. Record the new addresses and sign out to use the new IP address to access PowerVault Manager.

Set IPv6 values for network ports

Perform the following steps to set IPv6 addresses for the network ports:

1. Perform one of the following to access network options:
   - In the Home topic, select **Action > System Settings**, and then click the **Network** tab.
   - In the System topic, select **Action > System Settings**, and then click the **Network** tab.
2. Select the IPv6 tab.

   IPv6 uses 128-bit addresses.
3. Select the type of IP address settings to use for each controller from the **Source** drop-down menu:
   - Select **Manual** to specify up to four static IP addresses for each controller.
   - Select **Auto** to allow the system to automatically obtain IP addresses.
4. If you chose **Manual**, perform the following steps for each controller:
   a. Click **Add Address**.
   b. Type the IPv6 addresses in the **IP Address** field.
   c. Type a label for the IP address in the **Address Label** field.
   d. Click **Add**.
   e. Record the IPv6 address.

   NOTE: The following IP addresses are reserved for internal use by the storage system: 169.254.255.1, 169.254.255.2, 169.254.255.3, 169.254.255.4, and 127.0.0.1. Because these addresses are routable, do not use them anywhere in your network.
5. If you selected **Auto**, complete the remaining steps to allow the controllers to obtain IP addresses.
6. Click **Apply**.

   A confirmation panel appears.
7. Click **OK**.
8. Sign out and use the new IP address to access PowerVault Manager.

Configure DNS settings

Perform the following steps to configure DNS settings:

1. Perform one of the following to access Network options:
   - In the Home topic, select **Action > System Settings**, and then click the **Network** tab.
   - In the System topic, select **Action > System Settings**, and then click the **Network** tab.
2. Select the **DNS** tab.
3. Enter a hostname in the **Hostname** text box to set a domain hostname for each controller module. Use the following naming conventions:
   - The name must differ for each controller.
   - The name can have from 1 byte to 63 bytes.

- The name is not case-sensitive.
- The name must start with a letter and end with a letter or digit.
- The name can include letters, numbers, or hyphens; no periods.

4. Enter up to three network addresses for each controller in the DNS Servers fields.
   The resolver queries the network in the order that is listed until reaching a valid destination address. Any valid setting is treated as enabling DNS resolution for the system.
5. Specify up to three domain names for each controller in the **Search Domains** fields to search when resolving host names that are configured in the storage system.
   The resolver queries the network in the order that is listed until finding a match.
   NOTE: To reset Hostname to its default setting, select the Reset button for each controller. To clear the configured DNS Servers and Search Domains, select the Clear DNS Settings button for each controller.
6. Perform one of the following:
   - To save your settings and continue configuring your system, click **Apply**.
   - To save your settings and close the panel, click **Apply and Close**.

   A confirmation panel appears.
7. Click **Yes** to save your changes. Otherwise, click **No**.

Enable or disable system-management settings

You can enable or disable management services to limit the ways in which users and host-based management applications can access the storage system. Network management services operate outside the data path and do not affect host I/O to the system. In-band services operate through the data path and can slightly reduce I/O performance.

To allow specific users to access the PowerVault Manager, CLI, or other interfaces, see Adding, modifying, and deleting users.

1. Perform one of the following to access the Services options:
   - In the Home topic, select **Action > System Settings**, then click the **Services** tab.
   - In the System topic, select **Action > System Settings**, then click the **Services** tab.
   - In the banner, click the user panel and select **Set Up System Services**.
   - In the Welcome panel, select **System Settings**, and then click the **Services** tab.
2. Enable the services that you want to use to manage the storage system, and disable the others.
   - Web Browser Interface (WBI). The web application that is the primary interface for managing the system. You can enable use of HTTP and/or HTTPS for increased security, or of both. If you disable both, you lose access to this interface.
   - Command Line Interface (CLI). An advanced-user interface that is used to manage the system and can be used to write scripts. SSH (secure shell) is enabled by default. The default port number for SSH is 22. Telnet is disabled by default, but you can enable it in the CLI.
   - Storage Management Initiative Specification (SMI-S). Used for remote management of the system through your network. You can enable use of secure (encrypted) or unsecure (unencrypted) SMI-S:
     - **Enable.** Select this check box to enable unencrypted communication between SMI-S clients and the embedded SMI-S provider in each controller module using HTTP port 5988. Clear this check box to disable the active port and use of SMI-S.
     - **Encrypted.** Select this check box to enable encrypted communication, which disables HTTP port 5988 and enables HTTPS port 5989 instead. Clear this check box to disable port 5989 and enable port 5988. This is the default.

       NOTE: SMI-S is not supported for a system with 5U84 enclosures.
   - Service Location Protocol (SLP). Enables or disables the Service Location Protocol (SLP) interface. SLP is a discovery protocol that enables computers and other devices to find services in a LAN without prior configuration. This system uses SLP v2.
   - File Transfer Protocol (FTP). A secondary interface for installing firmware updates and downloading logs.
   - SSH File Transfer Protocol (SFTP). A secure secondary interface for installing firmware updates, downloading logs, and installing security certificates and keys. All data that is sent between the client and server is encrypted. SFTP is enabled by default. If selected, specify the port number to use. The default is 1022.
   - Simple Network Management Protocol (SNMP). Used for remote monitoring of the system through your network.
   - Service Debug. Used for technical support only. Enables or disables debug capabilities, including Telnet debug ports and privileged diagnostic user IDs.

     NOTE: Properly shut down the debug console by using the CLI command set protocols debug disable. Do not just close the console directly or by using the CLI command `exit`.

- Activity Progress Reporting. Provides access to the activity progress interface using HTTP port 8081. This mechanism reports whether a firmware update or partner firmware update operation is active and shows the progress through each step of the operation. When the update operation completes, status is presented indicating either the successful completion, or an error indication if the operation failed.
- In-band SES Capability. Used for in-band monitoring of system status based on SCSI Enclosure Services (SES) data. This service operates through the data path and can slightly reduce I/O performance. SES is disabled by default.

3. Perform one of the following:
   - To save your settings and continue configuring your system, click **Apply**.
   - To save your settings and close the panel, click **Apply and Close**.

   A confirmation panel appears.
4. Click **OK**.

Change system information settings

Perform the following steps to changed system information settings:

1. Perform one of the following to access the Services options:
   - In the Home topic, select **Action > System Settings**, then click the **System information** tab.
   - In the System topic, select **Action > System Settings**, then click the **System information** tab.
   - In the banner, click the user panel and select **Set System Information**.
   - In the Welcome panel, select **System Settings**, and then click the **System information** tab.
2. Set the system name, contact, location, and information or description values. The name is shown in the browser title bar or tab. The name, location, and contact are included in event notifications. All four values are recorded in system debug logs for reference by service personnel. Each value can include a maximum of 79 bytes, using all characters except the following: `" < > \`
3. Perform one of the following:
   - To save your settings and continue configuring your system, click **Apply**.
   - To save your settings and close the panel, click **Apply and Close**.

   A confirmation panel appears.
4. Click **OK**.

Setting system notification settings

The Notifications tab provides options for you to set up and test several types of system notifications.

- Configuring SMTP settings.
- Sending notifications to email addresses when events occur in the system.
- Sending notifications to SNMP trap hosts.
- Enabling managed logs settings, which transfers log data to a log-collection system. For more information about the managed logs feature, see About managed logs.
- Setting remote syslog notifications to allow the logging of events by the syslog of a specified host computer. Syslog is a protocol for sending event messages across an IP network to a logging server. This feature supports User Datagram Protocol (UDP) but not Transmission Control Protocol (TCP).
- Testing notifications.

NOTE: Enable at least one notification service to monitor the system.

Configure SMTP settings

Perform the following steps to configure SMTP settings:

1. Perform one of the following to access the options in the Notifications tab:
   - In the Home topic, select **Action > System Settings**, then click **Notifications**.
   - In the System topic, select **Action > System Settings**, then click **Notifications**.
   - In the footer, click the events panel and select **Set Up Notifications**.
   - In the Welcome panel, select **System Settings**, and then click the **Notifications** tab.
2. If the mail server is not on the local network, ensure that the gateway IP address was set in Configuring controller network ports.

3. Select the **Email** tab.
4. In the **SMTP Server address** field, enter the network address of the SMTP mail server to use for the email messages.
5. In the **Sender Domain** field, enter a domain name, which is joined with an @ symbol to the sender name to form the "from" address for remote notification. The domain name can have a maximum of 255 bytes. Because this name is used as part of an email address, do not include spaces or the following: \ " : ; < > ( )
   If the domain name is not valid, some email servers fail to process the email.
6. In the **Sender Name** field, enter a sender name, which is joined with an @ symbol to the domain name to form the *from* address for remote notification. This name provides a way to identify the system that is sending the notification. The sender name can have a maximum of 64 bytes. Because this name is used as part of an email address, do not include spaces or the following: \ " : ; < > ( ) [ ] Storage-1.
7. In the **Port** text box, enter the port to use when communicating with the SMTP server.

   Leaving the port set to `Default` tells the system to use the default port that is associated with the security protocol.
8. Set the security protocol to use when communicating with the SMTP server:
   - **None.** Does not use a security protocol. The standard SMTP port is 25, and is the system default.
   - **TLS.** Enables Transport Layer Security (TLS) authentication. The standard ports are 25 or 587. The system default is 587.
   - **SSL.** Enables Secure Sockets Layer (SSL) authentication. The standard port is 465, the system default.
9. If you selected TLS or SSL, type the password of the sender in the **Sender Password** and **Confirm Password** fields.
10. Perform one of the following:
    - To save your settings and continue configuring your system, click **Apply**.
    - To save your settings and close the panel, click **Apply and Close**.

    A confirmation panel appears.
11. Click **OK**.

Send email notifications

Perform the following steps to send email notifications:

1. Perform one of the following to access the options in the Notifications tab:
   - In the Home topic, select **Action > System Settings**, then click **Notifications**.
   - In the System topic, select **Action > System Settings**, then click **Notifications**.
   - In the footer, click the events panel and select **Set Up Notifications**.
   - In the Welcome panel, select **System Settings**, and then click the **Notifications** tab.
2. Select the **Email** tab and ensure that the SMTP Server and SMTP Domain options are set, as described in Configure SMTP settings on page 45.
3. Set the email notification:
   - To enable email notifications, select the **Enable Email Notifications** check box. This action enables the notification level and email address fields.
   - To disable email notifications, clear the **Enable Email Notifications** check box. This action disables the notification level and email address fields.
4. If email notification is enabled, select the minimum severity for which the system should send email notifications:
   - **Critical**
   - **Critical, Error**
   - **Critical, Error, Warning**
   - **Critical, Error, Warning, Resolved**
   - **Critical, Error, Warning, Resolved, Informational**
5. If email notification is enabled, in one or more of the Email Address fields enter an email address to which the system should send notifications. Each email address must use the format `user-name@domain-name`. Each email address can have a maximum of 320 bytes. For example: **Admin@mydomain.com** or **IT-team@mydomain.com.**
6. Perform one of the following:
   - To save your settings and continue configuring your system, click **Apply**.
   - To save your settings and close the panel, click **Apply and Close**.

   A confirmation panel appears.
7. Click **OK**.

Test email notifications settings

Perform the following steps to test email notifications settings:

1. Configure your system to send email notifications.
2. Click **Test Email**. A test notification is sent to the notification email addresses.
3. Verify that the test notification reached the intended recipient.
4. Click **OK**.

   If there was an error in sending a test notification, event 611 is displayed in the confirmation.

Send notifications to SNMP trap hosts

Perform the following steps to send notifications to SNMP trap hosts:

1. Perform one of the following to access the options in the Notifications tab:
   - In the Home topic, select **Action > System Settings**, then click **Notifications**.
   - In the System topic, select **Action > System Settings**, then click **Notifications**.
   - In the footer, click the events panel and select **Set Up Notifications**.
   - In the Welcome panel, select **System Settings**, and then click the **Notifications** tab.
2. Select the **SNMP** tab. If a message near the top of the panel informs you that the SNMP service is disabled, enable the service.
3. Select the minimum Notification Level severity for which the system should send email notifications: **Critical** (only); **Error** (and Critical); **Warning** (and Error and Critical); **Informational/Resolved** (all); or **none**.
4. In the **Read community** field, enter the SNMP read password for your network. This password is included in traps that are sent. This string must differ from the write-community string. The value is case-sensitive and can have a maximum of 31 bytes. It can include any character except for the following: `" < >`

   The default is public.
5. In the **Write community** field, enter the SNMP write password for your network. This string must differ from the read-community string. The value is case-sensitive and can have a maximum of 31 bytes. It can include any character except for the following: `" < >`

   The default is private.
6. In the **Trap Host Address** fields, enter the network addresses of hosts that are configured to receive SNMP traps. The values can be IPv4 addresses, IPv6 addresses, or FQDNs.
7. Perform one of the following:
   - To save your settings and continue configuring your system, click **Apply**.
   - To save your settings and close the panel, click **Apply and Close**.

   A confirmation panel appears.
8. Click **OK**.

Test SNMP notification settings

Perform the following steps to test SNMP notification settings:

1. Configure three SNMP trap hosts to receive notifications of system events.
2. Click **Test SNMP**. A test notification is sent to each configured trap host.
3. Verify that the test notification reached the intended location.
4. Click **OK**.

   If there was an error in sending a test notification, event 611 is displayed in the confirmation.

Configure managed logs settings

Perform the following steps to configure managed logs settings:

1. Perform one of the following to access the options in the Notifications tab:
   - In the Home topic, select **Action > System Settings**, then click **Notifications**.
   - In the System topic, select **Action > System Settings**, then click **Notifications**.
   - In the footer, click the events panel and select **Set Up Notifications**.
   - In the Welcome panel, select **System Settings**, and then click the **Notifications** tab.
2. Select the **Email** tab and ensure that the SMTP Server and SMTP Domain options are set. See Configure SMTP settings on page 45.
3. Select the **Managed Logs** tab.

4. Set the managed log option:
   - To enable managed logs, select the **Enable Managed Logs** check box.
   - To disable managed logs, clear the **Enable Managed Logs** check box.
5. If the managed logs option is enabled, type the email address of the log-collection system in the **Email destination address** field.
   The email address must use the format `user-name@domain-name` and can have a maximum of 320 bytes. For example: **LogCollector@mydomain.com**.
6. Select one of the following options:
   - To use push mode, which automatically attaches system log files to managed-logs email notifications that are sent to the log-collection system, select the **Include logs as an email attachment** check box.
   - To use pull mode, clear the **Include logs as an email attachment** check box.
7. Perform one of the following:
   - To save your settings and continue configuring your system, click **Apply**.
   - To save your settings and close the panel, click **Apply and Close**.

   A confirmation panel appears.
8. Click **OK**.

Test managed logs notification settings

Perform the following steps to test managed logs notification settings:

1. Configure your system to send a notification when managed logs are sent to the log collection system.
2. Click **Test Managed Logs**. A test event is sent to the log collection system.
3. Verify that the test notification reached the intended location.
4. Click **OK**.
   If there was an error in sending a test notification, event 611 is displayed in the confirmation.

Configure remote syslog notifications

Perform the following steps to configure remote syslog notifications:

1. Perform one of the following to access the options in the Notifications tab:
   - In the Home topic, select **Action > System Settings**, then click **Notifications**.
   - In the System topic, select **Action > System Settings**, then click **Notifications**.
   - In the footer, click the events panel and select **Set Up Notifications**.
   - In the Welcome panel, select **System Settings**, and then click the **Notifications** tab.
2. Select the **Syslog** tab.
3. Configure the Syslog options:
   - **Notification Level**: Select the minimum severity for which the system should send notifications: **Critical** (only); **Error** (and Critical); **Warning** (and Error and Critical); **Resolved** (and Error, Critical, and Warning); **Informational** (all); or **none** (Disabled), which disables syslog notification.
   - **Syslog Server**: Network address of the syslog host system. The value can be an IPv4 address, IPv6 address, or FQDN. If the **Notification Level** is other than **none** (Disabled), you must specify the **Syslog Server IP Address**.
   - **Syslog Server Port Number**: Port number of the syslog host system.
4. Perform one of the following:
   - To save your settings and continue configuring your system, click **Apply**.
   - To save your settings and close the panel, click **Apply and Close**.

   A confirmation panel appears.
5. Click **OK**.

Test remote syslog notification settings

Perform the following steps to test remote syslog notification settings:

1. Configure your system to send a notification when an event is sent to the remote syslog server.
2. Click **Test Syslog**. A test event is sent to the syslog server.

3. Verify that the test notification reached the intended location.
4. Click **OK**.

   If there was an error in sending a test notification, event 611 is displayed in the confirmation.

Configuring SupportAssist

SupportAssist sends configuration and diagnostic information from an ME4 Series storage system to technical support.

When enabled, you agree to allow the feature to remotely monitor the storage system, collect diagnostic information, and transmit the data to a remote support server. Each time SupportAssist runs, a service tag is sent that includes a unique identifier for your system. This identifier can be used to contact you if your system needs repair.

Event information sent to the remote server includes error and critical event messages, event IDs, event codes, timestamps, and component identifiers. Log data information includes:

- Current configuration state of the storage system
- XML API dump of the storage system
- Event log
- Full debug log

In a dual-controller system, controller A is responsible for sending data to the SupportAssist server. If controller A is down, controller B sends data to the support server.

Enable SupportAssist

Perform the following steps to enable SupportAssist on an ME4 Series storage system:

If the ME4 Series storage system does not have direct access to the Internet, configure a web proxy. See Configure SupportAssist to use a web proxy on page 50.

1. Perform one of the following actions to access the SupportAssist options:
   - In the Home topic, select **Action > System Settings**, then click the **SupportAssist** tab.
   - In the System topic, select **Action > System Settings**, then click the **SupportAssist** tab.
2. Select the **SupportAssist** checkbox.
   The SupportAssist agreement is displayed.
3. Read through the agreement, then acknowledge it by clicking **Accept**.
   The system attempts to establish connectivity with the remote support server. Once connectivity is established, the system collects an initial full debug log dump and sends it to the SupportAssist server.

   NOTE: If the system cannot contact the remote support server, an error message is displayed that contains details about the connection failure and provides recommended actions.
4. In the **Contact Information** tab, type the primary contact information and select the preferred contact settings.

   To receive email messages when a storage system issue occurs, select the **Yes, I would like to receive emails from SupportAssist when issues arise, including hardware failure notifications** checkbox.
5. Click **Apply** or **Apply and Close**, and click **OK** on the confirmation panel.

   To disable SupportAssist:

   a. Clear the **SupportAssist** check box.
      The SupportAssist opt out confirmation panel is displayed.
   b. Click **Yes**.
   c. Click **Apply** or **Apply and Close**.
      The SupportAssist changes confirmation panel is displayed.
   d. Click **OK**.

Control SupportAssist

Perform the following steps to view and control SupportAssist settings on an ME4 Series storage system:

1. Perform one of the following actions to access the SupportAssist options:
   - In the Home topic, select **Action > System Settings**, then click the **SupportAssist** tab.
   - In the System topic, select **Action > System Settings**, then click the **SupportAssist** tab.
   - In the Welcome panel, select **System Settings**, then click the **SupportAssist** tab.

   The SupportAssist tab displays the following information:

- **State** – Operational status of SupportAssist on the ME4 Series storage system.
- **Operation Mode** – Operational mode of SupportAssist on the ME4 Series storage system.
- **Last Logs Send Status** – Status of the last attempt to send ME4 Series storage system logs to SupportAssist.
- **Last Logs Send Time** – Date and time of the last attempt to send ME4 Series storage system logs to SupportAssist.
- **Last Event Send Status** – Status of the last attempt to send ME4 Series storage system events to SupportAssist.
- **Last Event Send Time** – Date and time of the last attempt to send ME4 Series storage system events to SupportAssist.

2. The SupportAssist feature can be disabled or enabled by performing the following actions:
   - To disable SupportAssist, clear the **SupportAsist** check box, click **Yes** on the confirmation panel, click **Apply** or **Apply and Close**, and click **OK** on the confirmation panel.
   - To enable SupportAssist, select the **SupportAsist** check box, click **Accept** on the confirmation panel, click **Apply** or **Apply and Close**, and click **OK** on the confirmation panel.
3. The following actions can be performed on the SupportAssist tab:
   - To pause sending storage system information to SupportAssist, click **Pause**, and click **Yes** on the confirmation panel.
   - To resume sending storage system information installation to SupportAssist, click **Resume**, and click **Yes** on the confirmation panel.
   - To manually place the system into maintenance mode, click **Enable Maintenance**. Placing the system into maintenance mode notifies SupportAssist not to create support tickets during planned system downtime.
   - To manually remove the system from maintenance mode, click **Disable Maintenance**.
   - To manually send storage system logs to SupportAssist, click **Send Logs**, and click **Yes** on the confirmation panel.
   - To check the network connection to the SupportAssist infrastructure, click **Check Connection**, and click **Yes** on the confirmation panel.
   - To clear the SupportAssist proxy settings, click **Clear Web Proxy**, and click **Yes** on the confirmation panel.

Configure SupportAssist to use a web proxy

If the storage array does not have direct access to the Internet, SupportAssist can use a web proxy to send data to technical support .

NOTE: DNS must be configured on each controller to allow SupportAssist to work with a web proxy. To configure DNS, see Configure DNS settings on page 43.

1. Perform one of the following actions to access the SupportAssist options:
   - In the Home topic, select **Action > System Settings**, then click the **SupportAssist** tab.
   - In the System topic, select **Action > System Settings**, then click the **SupportAssist** tab.
   - In the Welcome panel, select **System Settings**, then click the **SupportAssist** tab.
2. On the **Web Proxy Settings** tab:
   a. Select the **Web Proxy** checkbox.
   b. Type the hostname IP address of the proxy server in the **Host** field.
   c. Type the port number of the proxy server in the **Port** field.
   d. If the proxy server requires authentication, type the credentials in the **User Name** and **Password** fields.
3. Click **Apply** or **Apply and Close**, and click **OK** on the confirmation panel.

Enable or disable CloudIQ

The CloudIQ feature is enabled by default on ME4 Series storage systems. To send data to CloudIQ, the ME4 Series storage system must be onboarded to CloudIQ and SupportAssist must be enabled on the storage system.

To stop sending data to CloudIQ, without removing the storage system from CloudIQ, clear the **Enable CloudIQ** checkbox.

1. Perform one of the following actions to access the SupportAssist options:
   - In the Home topic, select **Action > System Settings**, then click the **SupportAssist** tab.
   - In the System topic, select **Action > System Settings**, then click the **SupportAssist** tab.
   - In the Welcome panel, select **System Settings**, then click the **SupportAssist** tab.
2. On the **CloudIQ Settings** tab, select or clear the **Enable CloudIQ** checkbox.
3. Click **Apply** or **Apply and Close**, and click **OK** on the confirmation panel.

   NOTE: It may take several hours for changes to the CloudIQ setting to take effect.

Changing host port settings

You can configure controller host-interface settings for ports except for systems with a 4-port SAS controller module. To enable the system to communicate with hosts, you must configure the host-interface options of the system.

NOTE: If the current settings are correct, port configuration is optional.

For a system with a 2-port SAS controller module, host ports can be configured to use standard cables. A standard cable can connect one port on a SAS host to one controller port, using four PHY lanes per port. Use of fan-out cables is enabled by default. When configuring the host-interface settings for a 2-port SAS controller module, the Host Ports Settings panel displays the following:

- Current link speed
- Cable type
- Number of PHY lanes expected for the SAS port
- Number of PHY lanes active for each SAS port

The number of ports that are displayed depends on the configuration of the system.

CNC host ports can be configured as all FC or all iSCSI ports, or a combination of both. FC ports support use of qualified 8 Gb/s or 16 Gb/s SFPs. You can set FC ports to auto-negotiate the link speed or to use a specific link speed. iSCSI ports support use of qualified 1 Gb/s, 10 Gb/s SFPs. or qualified 10 Gb/s Direct Attach Copper (DAC) cables. iSCSI port speeds are auto-negotiated.

NOTE: For information about setting host parameters such as FC port topology, and the host-port mode, see the *Dell EMC PowerVault ME4 Series Storage System CLI Guide*.

Configure FC ports

Perform the following steps to configure FC ports:

1. Perform one of the following to access the options in the Ports tab:
   - In the Home topic, select **Action > System Settings**, then click **Ports**.
   - In the System topic, select **Action > System Settings**, then click **Ports**.
2. From the Port Settings tab, set the port-specific options:
   - Set the **Speed** option to the proper value to communicate with the host, or to auto, which auto-negotiates the proper link speed. Because a speed mismatch prevents communication between the port and host, set a speed only if you need to force the port to use a known speed.
   - Set the **Connection Mode** to either point-to-point or auto:
     - **point-to-point**: Fibre Channel point-to-point.
     - **auto**: Automatically sets the mode based on the detected connection type.
3. Perform one of the following:
   - To save your settings and continue configuring your system, click **Apply**.
   - To save your settings and close the panel, click **Apply and Close**.

   A confirmation panel appears.
4. Click **OK**.

Configure iSCSI ports

Perform the following steps to configure iSCSI ports:

1. Perform one of the following to access the options in the Ports tab:
   - In the Home topic, select **Action > System Settings**, then click **Ports**.
   - In the System topic, select **Action > System Settings**, then click **Ports**.
2. From the **Port Settings** tab, Set the parameters for the iSCSI ports:
   - **IP Address**: For IPv4 or IPv6, the port IP address. For corresponding ports in each controller, assign one port to one subnet and the other port to a second subnet. Ensure that each iSCSI host port in the storage system is assigned a different IP address. For example, in a system using IPv4:
     - Controller A port 2: 10.10.10.100
     - Controller A port 3: 10.11.10.120
     - Controller B port 2: 10.10.10.110
     - Controller B port 3: 10.11.10.130
   - **Netmask**: For IPv4, subnet mask for assigned port IP address.

- **Gateway**: For IPv4, gateway IP address for assigned port IP address.
- **Default Router**: For IPv6, default router for assigned port IP address.

3. In the Advanced Settings section of the panel, set the options that apply to all iSCSI ports:
   - **Enable Authentication (CHAP)**: Enables or disables the use of the Challenge Handshake Authentication Protocol (CHAP). Enabling or disabling CHAP in this panel updates its setting in the Configure CHAP panel (available in the Hosts topic by selecting **Action > Configure CHAP**. CHAP is disabled by default.
     NOTE: CHAP records for iSCSI login authentication must be defined if CHAP is enabled. To create CHAP records, see Configuring CHAP.
   - **Link Speed**:
     - Auto – Auto-negotiates the proper speed.
     - 1 Gbit/s – Forces the speed to 1 Gbit/sec, overriding a downshift that can occur during auto-negotiation with 1-Gbit/sec HBAs. This setting does not apply to 10 Gbit/sec HBAs.
   - **Enable Jumbo Frames**: Enables or disables support for jumbo frames. Allowing for 100 bytes of overhead, a normal frame can contain a 1400-byte payload whereas a jumbo frame can contain a maximum 8900-byte payload for larger data transfers.
     NOTE: Use of jumbo frames can succeed only if jumbo-frame support is enabled on all network components in the data path.
   - **iSCSI IP Version**: Specifies whether IP values use Internet Protocol version 4 (IPv4) or version 6 (IPv6) format. IPv4 uses 32-bit addresses. IPv6 uses 128-bit addresses.
   - **Enable iSNS**: Enables or disables registration with a specified Internet Storage Name Service server, which provides name-to-IP-address mapping.
   - **iSNS Address**: Specifies the IP address of an iSNS server.
   - **Alternate iSNS Address**: Specifies the IP address of an alternate iSNS server, which can be on a different subnet.
     CAUTION: Changing IP settings can cause data hosts to lose access to the storage system.
4. Perform one of the following:
   - To save your settings and continue configuring your system, click **Apply**.
   - To save your settings and close the panel, click **Apply and Close**.

   A confirmation panel appears.
5. Click **OK**.

Configure two ports as FC and two ports as iSCSI per controller

Perform the following steps to configure two ports as FC and two ports as iSCSI:

1. Perform one of the following to access the options in the Ports tab:
   - In the Home topic, select **Action > System Settings**, then click the **Ports** tab.
   - In the System topic, select **Action > System Settings**, then click the **Ports** tab.
2. From the **Host Post Mode** drop-down menu, select **FC-and-iSCSI**.
   NOTE: Ports 0 and 1 are FC ports. Ports 2 and 3 are iSCSI ports.
3. Click **Apply and Close**.
   A confirmation panel appears.
4. Click **OK**.
   The controller modules restart.
5. Perform one of the following to access the options in the Ports tab:
   - In the Home topic, select **Action > System Settings**, then click the **Ports** tab.
   - In the System topic, select **Action > System Settings**, then click the **Ports** tab.
6. In the Ports Settings tab, set the FC port-specific options:
   - Set the **Speed** option to the proper value to communicate with the host, or to auto, which auto-negotiates the proper link speed. Because a speed mismatch prevents communication between the port and host, set a speed only if you need to force the port to use a known speed.
   - Set the **Connection Mode** to either point-to-point or auto:
     - **point-to-point**: Fibre Channel point-to-point.
     - **auto**: Automatically sets the mode based on the detected connection type.
7. Set the parameters for the iSCSI ports:

- **IP Address**: For IPv4 or IPv6, the port IP address. For corresponding ports in each controller, assign one port to one subnet and the other port to a second subnet. Ensure that each iSCSI host port in the storage system is assigned a different IP address. For example, in a system using IPv4:
  - Controller A port 2: 10.10.10.100
  - Controller A port 3: 10.11.10.120
  - Controller B port 2: 10.10.10.110
  - Controller B port 3: 10.11.10.130
- **Netmask**: For IPv4, subnet mask for assigned port IP address.
- **Gateway**: For IPv4, gateway IP address for assigned port IP address.
- **Default Router**: For IPv6, default router for assigned port IP address.

8. In the Advanced Settings tab of the panel, set the options that apply to all iSCSI ports:
   - **Enable Authentication (CHAP)**: Enables or disables the use of the Challenge Handshake Authentication Protocol (CHAP). Enabling or disabling CHAP in this panel updates its setting in the Configure CHAP panel (available in the Hosts topic by selecting **Action > Configure CHAP**. CHAP is disabled by default.
     NOTE: CHAP records for iSCSI login authentication must be defined if CHAP is enabled. To create CHAP records, see Configuring CHAP.
   - **Link Speed**:
     - Auto – Auto-negotiates the proper speed.
     - 1 Gb/s – Forces the speed to 1 Gbit/sec, overriding a downshift that can occur during auto-negotiation with 1-Gbit/sec HBAs. This setting does not apply to 10 Gbit/sec HBAs.
   - **Enable Jumbo Frames**: Enables or disables support for jumbo frames. Allowing for 100 bytes of overhead, a normal frame can contain a 1400-byte payload whereas a jumbo frame can contain a maximum 8900-byte payload for larger data transfers.
     NOTE: Use of jumbo frames can succeed only if jumbo-frame support is enabled on all network components in the data path.
   - **iSCSI IP Version**: Specifies whether IP values use Internet Protocol version 4 (IPv4) or version 6 (IPv6) format. IPv4 uses 32-bit addresses. IPv6 uses 128-bit addresses.
   - **Enable iSNS**: Enables or disables registration with a specified Internet Storage Name Service server, which provides name-to-IP-address mapping.
   - **iSNS Address**: Specifies the IP address of an iSNS server.
   - **Alternate iSNS Address**: Specifies the IP address of an alternate iSNS server, which can be on a different subnet.
     CAUTION: Changing IP settings can cause data hosts to lose access to the storage system.
9. Perform one of the following:
   - To save your settings and continue configuring your system, click **Apply**.
   - To save your settings and close the panel, click **Apply and Close**.

   A confirmation panel appears.
10. Click **OK**.

Managing scheduled tasks

The Manage Schedules action is enabled when at least one scheduled task exists.

When accessed, you can modify or delete scheduled tasks to:

- Create virtual snapshots
- Reset virtual snapshots
- Enable or disable drive spin down (DSD) for non-ADAPT linear disk groups
- Run virtual replications

NOTE: You can only create a task and schedule to enable or disable DSD through the CLI, though you can modify the schedule through the PowerVault Manager. For more information, see the *Dell EMC PowerVault ME4 Series Storage System CLI Guide*.

Modify a schedule from the Home topic

Perform the following steps to modify a schedule:

1. In the Home topic, select **Action > Manage Schedules**.

2. Select the schedule to modify. The schedule settings appear at the bottom of the panel.
3. If you want to replicate the last snapshot in the primary volume, select the **Last Snapshot** check box.

   The snapshot must exist at the time of the replication. This snapshot may have been created either manually or by scheduling the snapshot.

   NOTE: This option is unavailable when replicating volume groups.

4. Specify a date and a time in the future to specify when to run the scheduled task. This date and time is also the starting point for any specified recurrence.
   - To set the **Date** value, enter the current date in the format *YYYY-MM-DD*.
   - To set the Time value, enter two-digit values for the hour and minutes and select either **AM, PM**, or **24H** (24-hour clock).
5. If you want the task to run more than once, select the Repeat check box.
   - Specify how often the task should repeat. Enter a number, and select the appropriate time unit. Replications can recur no less than 30 minutes apart.
   - To allow the schedule to run without an end date, clear the **End** check box. To specify when the schedule should stop running, select the **End** check box
   - To allow the schedule to run at any time, clear the **Time Constraint** check box. To specify a time range within which the schedule can run, select the **Time Constraint** check box.
   - To allow the schedule to run on any day, clear the **Date Constraint** check box. To specify the days when the schedule can run, select the **Date Constraint** check box.
6. Click **OK**.
   The schedule is modified.
7. Click **OK**.

Delete a schedule from the Home topic

1. In the Home topic, select **Action > Manage Schedules**. The Manage Schedules panel opens.
2. Select the schedule to delete.
3. Click **Delete Schedule**. A confirmation panel appears.
4. Click **OK** to continue. Otherwise, click **Cancel**. If you clicked OK, the schedule was deleted.
5. Click **OK**

3

Working in the System topic

Topics:

Viewing system components

The System topic enables you to see information about each enclosure and its physical components in front, rear, and tabular views. Components vary by enclosure model.

NOTE: If an attached enclosure or component is unsupported, the system health shows as Degraded and the unsupported component's health shows as Fault. Hover the cursor over the faulty component to see why it is unsupported and the recommended action to take. For more information, review the event log.

Front view

The Front tab shows the front of all enclosures in a graphical view.

For each enclosure, the front view shows the enclosure ID and other information. For each drawer, the front view shows the drawer ID and other information. To see more information about an enclosure, drawer, or disks, hover the cursor over an enclosure ear, drawer, or a disk. To illuminate a locator LED for an enclosure or disk, select one or more components and click **Turn On LEDs**. To turn off individual locator LEDs, select the components and click **Turn Off LEDs**. To turn off all locator LEDs, ensure that no components are selected and click **Turn Off LEDs**.

Table 7. Enclosure Information and Disk Information panels

Panel	Information displayed
Enclosure Information	ID, status, vendor model, disk count, WWN, midplane serial number, revision, part number, manufacturing date, manufacturing location, EMP A revision, EMP B revision, EMP A bus ID, EMP B bus ID, EMP A target ID, EMP B target ID, midplane type, enclosure power (watts), PCIe 2-capable, health
Disk Information	Location, serial number, usage, description, size, status, RPM (spinning disk only), SSD life left, manufacturer, model, revision, power on hours, FDE state, FDE lock key, job running, sector format, transfer rate, SMART, drive spin down count, health
Drawer Information	General: Name, drawer position, number of disks, ID, status, WWN, health Left sideplane: Name, status, path ID, expanders, name and status of each expander Right sideplane: Name, status, path ID, expanders, name and status of each expander

If the health of a component is not good, the health reason, recommended action, and unhealthy subcomponents are shown to help you resolve problems.

The following are descriptions of some Disk Information panel items:

- **Power On Hours** – Total number of hours that the disk has been powered on since it was manufactured. This value is updated in 30-minute increments.
- **FDE State** – FDE state of the disk. For more information about FDE states, see the *Dell EMC PowerVault ME4 Series Storage System CLI Guide*.
- **FDE lock keys** – FDE lock keys are generated from the FDE passphrase and manage locking and unlocking the FDE-capable disks in the system. Clearing the lock keys and power cycling the system denies access to data on the disks.

Rear view

The Rear tab shows the rear of all enclosures in a graphical view.

The rear view shows enclosure IDs and the presence or absence of power supplies, controller modules, and expansion modules. It also shows controller module IDs, host port types and names, network port IP addresses, and expansion port names.

To see more information, hover the cursor over an enclosure ear or a component. To illuminate a locator LED for any of the components, select one or more components and click **Turn On LEDs**. To turn off individual locator LEDs, select the components and click **Turn Off LEDs**. To turn off all locator LEDs, ensure that no components are selected and click **Turn Off LEDs**. For a 5U84 enclosure, only enclosures, I/O modules, and disks are selectable.

NOTE: Protocol-specific properties are displayed only for host ports that use those protocols.

Table 8. Additional information panels for the rear view of the enclosure

Panel	Information displayed
Enclosure Information	ID, status, vendor, model, disk count, WWN, midplane serial number, revision, part number, manufacturing date, manufacturing location, EMP A revision, EMP B revision, EMP A bus ID, EMP B bus ID, EMP A target ID, EMP B target ID, midplane type, enclosure power (watts), PCIe 2-capable, health
Power Supply Information	Status, vendor, model, serial number, revision, location, part number, manufacturing date, manufacturing location, health
Controller Information	ID, IP address, description, status, model, serial number, hardware version, system cache memory (MB), revision, CPLD version, Storage Controller code version, Storage Controller CPU type, part number, position, hardware version, manufacturing date, manufacturing location, health
Port Information (FC)	Name, type, ID (WWN), status, configured speed, actual speed, topology, primary loop ID, supported speeds, SFP status, part number, health
Port Information (iSCSI)	Name, type, ID (IQN), status, configured speed, actual speed, IP version, MAC address, address, gateway, netmask, SFP status, part number, 10G compliance, cable length, cable technology, Ethernet compliance, health
Port Information (SAS)	Name, type, ID (WWN), status, actual speed, topology, expected lanes, active lanes, disabled lanes, health
Network Information	Name, mode, IP address, network mask, gateway, MAC address, health
Expansion Port Information	Enclosure ID, controller ID, name, status, health
Expansion Module Information (IOM)	ID, description, serial number, revision, health

If the health of a component is not OK, the health reason, recommended action, and unhealthy subcomponents are shown to help you resolve problems.

Table view

The Table tab shows a tabular view of information about physical components in the system. By default, the table shows 20 entries at a time.

For each component, the table shows the following information:

Table 9. Table view information

Field	Description
Health	Shows the health of the component: OK, Degraded, Fault, N/A, or Unknown.

Table 9. Table view information (continued)

Field	Description
Type	Shows the component type: enclosure, disk, power supply, controller module, network port, host port, expansion port, CompactFlash card, or I/O module (expansion module).
Enclosure	Shows the enclosure ID.
Location	Shows the location of the component. · For an enclosure, the location is shown in the format *Rack rack-ID.shelf-ID*. You can set the location through the CLI `set enclosure` command. · For a disk, the location is shown in the format *enclosure-ID.disk-slot*. · For a power supply or I/O module, the locations Left, Left-Middle, Middle, Right-Middle, and Right are as viewed from the rear of the enclosure. · For a host port, the location is shown as controller ID and port number.
Information	Shows additional, component-specific information: · For an enclosure, its FRU description and current disk count. · For a disk, its description, capacity, and usage. · Type is shown as either: ○ **SAS** – Enterprise SAS spinning disk. ○ **SAS MDL** – Midline SAS spinning disk. ○ **SSD SAS** – SAS solid-state disk. · Usage is shown as either: ○ **AVAIL** – The disk is available. ○ **GLOBAL SP** – The disk is configured as a spare. ○ **DEDICATED SP** – The disk is configured as a dedicated spare. ○ **pool-ID:tier name** for disk groups that are part of a virtual pool or `pool-ID: Linear` for disk groups that are part of linear pools. The disk is part of a disk group. ○ **FAILED** – The disk is unusable and must be replaced. Reasons for this status include: excessive media errors, SMART error, disk hardware failure, or unsupported disk. ○ **LEFTOVR** – The disk is part of a disk group that is not found in the system. ○ **UNUSABLE** – The disk cannot be used in a disk group. Possible reasons include: ▪ The system is secured, and the disk is data locked with a different passphrase. ▪ The system is secured/locked (no passphrase available) and the disk is data/locked. ▪ The system is secured and the disk is not FDE capable. · For a power supply: its FRU description. · For a fan: its rotational speed in r/min (revolutions per minute). · For a controller module: its ID. · For a network port: its IP address. · For a host port:, one of the following values: ○ **FC(L)** – Fibre Channel-Arbitrated Loop (public or private) ○ **FC(P)** – Fibre Channel Point-to-Point ○ **FC(-)** – Fibre Channel disconnected ○ **SAS** – Serial Attached SCSI ○ **iSCSI** – Internet SCSI · For an expansion port, either **Out Port** or **In Port**. · For an I/O module, its ID.
Status	Shows the component status: · For an enclosure: **Up**. · For a disk: ○ **Up** The disk is present and is properly communicating with the expander. ○ **Spun Down** The disk is present and has been spun down by the DSD feature.

Table 9. Table view information (continued)

Field	Description
	○ **Warning** The disk is present but the system is having communication problems with the disk LED processor. For disk and midplane types where this processor also controls power to the disk, power-on failure will result in the Error status. ○ **Error** The disk is present but not detected by the expander. ○ **Unknown** Initial status when the disk is first detected or powered on. ○ **Not Present** The disk slot indicates that no disk is present. ○ **Unrecoverable** The disk is present but has unrecoverable errors. ○ **Unavailable** The disk is present but cannot communicate with the expander. ○ **Unsupported** The disk is present but is an unsupported type. · For a power supply: **Up**, **Warning**, **Error**, **Not Present**, or **Unknown**. · For a fan: **Up**, **Error,**, **Off**, or **Missing**. · For a controller module or I/O module: **Operational**, **Down**, **Not Installed**, or **Unknown**. · For a network port: **N/A**. · For a host port: ○ **Up** – The port is cabled and has an I/O link. ○ **Warning** – Not all of the port PHYs are up. ○ **Error** – The port is reporting an error condition. ○ **Not Present** – The controller module is not installed or is down. ○ **Disconnected** – Either no I/O link is detected or the port is not cabled. · For an expansion port: **Up**, **Disconnected**or **Unknown**. · For a CompactFlash card: **Installed**, **Not Installed**, or **Unknown**.

Systems Settings panel

The System Settings panel provides options for you to quickly and easily configure your system. Access the panel by doing one of the following:

- In the Home topic, select **Action > System Settings**.
- In the System topic, select **Action > System Settings**.
- In the Welcome panel, select **System Settings**.

For more information on configuring system setting options, see Configuring system settings.

Resetting host ports

Making a configuration or cabling change on a host might cause the storage system to stop accepting I/O requests from that host. For example, this problem can occur after moving host cables from one HBA to another on the host. To fix such a problem you might need to reset controller host ports, or channels.

For FC, you can reset a single port. For an FC host port configured to use FC-AL, or loop topology, a reset issues a loop initialization primitive (LIP).

For iSCSI, you can reset a port pair, either the first and second ports or the third and fourth ports.

For SAS, you can reset a port pair. Resetting a SAS host port issues a `COMINT/COMRESET` sequence and might reset other ports.

Rescanning disk channels

A rescan forces a rediscovery of disks and enclosures in the storage system. If both storage controllers are online and can communicate with both expansion modules in each connected enclosure, a rescan also reassigns enclosure IDs to follow the enclosure cabling order of controller A. For further cabling information, refer to your product's deployment guide.

You might need to rescan disk channels after system power-up to display enclosures in the proper order. The rescan temporarily pauses all I/O processes, then resumes normal operation. It can take up to two minutes for enclosure IDs to be corrected.

You do not have to perform a manual rescan after inserting or removing non-FDE disks. The controllers automatically detect these changes. When disks are inserted, they are detected after a short delay, which allows the disks to spin up.

Clearing disk metadata

You can clear metadata from a leftover disk to make it available for use.

CAUTION: Only use this command when all disk groups are online and leftover disks exist. Improper use of this command may result in data loss. Do not use this command when a disk group is offline and one or more leftover disks exist. If you are uncertain whether to use this command, contact technical support for assistance.

Each disk in a disk group has metadata that identifies the owning disk group, the other disks in the disk group, and the last time data was written to the virtual pool or linear disk group. The following situations cause a disk to become a *leftover*:

- The disks' timestamps do not match so the system designates members having an older timestamp as leftovers.
- A disk is not detected during a rescan, then is subsequently detected.
- A disk that is a member of a disk group in another system is moved into this system without the other members of its group.

When a disk becomes a leftover, the following changes occur:

- The disk's health becomes Degraded and its usage value becomes LEFTOVR.
- The disk is automatically excluded from the disk group, causing the disk group's health to become Degraded or Fault, depending on the RAID level.
- The disk's fault LED is illuminated amber.

If a spare is available, and the health of the disk group is Degraded or Critical, the disk group will use them to start reconstruction. When reconstruction is complete, you can clear the leftover disk's metadata. Clearing the metadata will change the disk's health to OK and its usage value to AVAIL. The disk may become available for use in a new disk group.

NOTE: If a spare is not available to begin reconstruction, or reconstruction has not completed, keep the leftover disk so that you will have an opportunity to recover its data.

This command clears metadata from leftover disks only. If you specify disks that are not leftovers, the disks are not changed.

Clear metadata from leftover disks

1. In the System topic, select **Action > Clear Metadata**. The Clear Metadata panel opens.
2. Select the leftover disks from which to clear metadata.
3. Click **OK**.
4. Click **Yes** to continue. Otherwise, click **No**. If you clicked Yes, the metadata is cleared.
5. Click **OK**.

Updating firmware

The **Update Firmware** dialog box displays the current versions of firmware on the controller modules, expansion modules, and disk drives.

If SupportAssist is enabled on an ME4 Series storage system, the storage system periodically checks if a firmware update is available. If a firmware update is available, a message about the firmware update is added to the storage system event log.

For information about supported releases for firmware update, see the *Dell EMC PowerVault ME4 Series Storage System Release Notes.*. For information about which controller module updates the other controller module when one is replaced, see About firmware update.

To monitor the progress of a firmware update using the activity progress interface, see Using the activity progress interface.

Best practices for firmware update

- In the health panel in the footer, verify that the system health status is OK. If the system health status is not OK, view the Health Reason value in the health panel in the footer and resolve all problems before you update the firmware. For information about the health panel, see Viewing health information.
- Run the `check firmware-upgrade-health` CLI command before updating the firmware. This command performs a series of health checks to determine whether any conditions exist that need to be resolved before the firmware can be updated. Any conditions that are detected are listed with their potential risks. For information about this command, see the *Dell EMC PowerVault ME4 Series Storage System CLI Guide*.

- If any unwritten cache data is present, the firmware update will not proceed. Before you can update the firmware, unwritten data must be removed from cache. For more information about the `clear cache` command, see the *Dell EMC PowerVault ME4 Series Storage System CLI Guide*.
- If a disk group is quarantined, contact technical support for help resolving the problem that is causing the component to be quarantined before updating the firmware.
- To ensure success of an online update, select a period of low I/O activity. This helps the update complete as quickly as possible and avoids disruption to host and applications due to timeouts. Attempting to update a storage system that is processing a large, I/O-intensive batch job may cause hosts to lose connectivity with the storage system.

Updating controller module firmware

In a dual-controller system, both controller modules should run the same firmware version. Storage systems in a replication set should run the same or compatible firmware versions. You can update the firmware in each controller module by loading a firmware file obtained from the enclosure vendor.

Prepare to update controller module firmware

Perform the following steps to prepare to update the firmware on a controller module:

1. Follow the best practices described in Best practices for firmware update.
2. Download the appropriate firmware `.zip` file to your computer or network.
3. Extract the firmware `.bin` file from the `.zip` file.

   NOTE: Some extraction tools automatically extract the contents of `.bin` file. However, the contents of the `.bin` file cannot be used to perform the firmware update.

4. If the storage system has a single controller, stop I/O to the storage system before you start the firmware update.

Update controller module firmware

Perform the following steps to update the firmware on a controller module:

1. Perform one of the following as a user with the `manage` role:
   - In the banner, click the system panel and select **Update Firmware**.
   - In the System topic, select **Action > Update Firmware**.

   The **Update Firmware** panel opens. The **Update Controller Modules** tab displays versions of firmware that are currently installed for the components in each controller.
2. Click **Browse** and select the firmware file to install.
3. Optionally, select or clear the Partner Firmware Update (PFU) check box to enable or disable PFU, and confirm the action.

   NOTE: For information about which controller module updates the other when a controller module is replaced, see About firmware update.

4. Click **OK**.
   A **Progress of Firmware Update** panel displays the firmware-update progress.

   The process starts by validating the firmware file:
   - If the file is invalid, verify that you specified the correct firmware file. If you did, try downloading it again from the source location.
   - If the file is valid, the process continues.

     CAUTION: Do not perform a power cycle or controller restart during a firmware update. If the update is interrupted or there is a power failure, the module might become inoperative. If this issue occurs, contact technical support. The module might need to be returned to the factory for reprogramming.

     Firmware update typically takes 10 minutes for a controller with current CPLD firmware, or 20 minutes for a controller with downlevel CPLD firmware. If the controller enclosure has connected enclosures, allow additional time for each expansion module enclosure management processor (EMP) to be updated. This task typically takes 2.5 minutes for each EMP in a drive enclosure.

     If the Storage Controller cannot be updated, the update operation is canceled. Verify that you specified the correct firmware file and repeat the update. If this problem persists, contact technical support.

     When firmware update on the local controller is complete, users are automatically signed out and the MC restarts. Until the restart is complete, sign-in pages say that the system is currently unavailable. When this message is cleared, you may sign in again.

If PFU is enabled, allow as additional 10 minutes to 20 minutes for the partner controller to be updated.

5. Clear your web browser cache, then sign in to the PowerVault Manager. If PFU is still running on the controller you sign in to, a panel shows PFU progress and prevents you from performing other tasks until PFU is complete.

   NOTE: If PFU is enabled for the system, after firmware update has completed on both controllers, check the system health. If the system health is Degraded and the health reason indicates that the firmware version is incorrect, verify that you specified the correct firmware file and repeat the update. If this problem persists, contact technical support.

Updating expansion module firmware

An expansion enclosure can contain one or two expansion modules. Each expansion module contains an enclosure management processor (EMP). When you update controller-module firmware, all expansion modules are automatically updated to a compatible firmware version.

Prepare to update expansion module firmware

1. Follow the best practices in Best practices for firmware update.
2. Obtain the appropriate firmware file and download it to your computer or network.
3. If the storage system has a single controller, stop I/O to the storage system before starting the firmware update.

Update expansion module firmware

1. Perform one of the following:
   - In the banner, click the system panel and select **Update Firmware**.
   - In the System topic, select **Action > Update Firmware**.

   The Update Firmware panel opens.
2. Select the Update Expansion Modules tab. This tab shows information about each expansion module in the system.
3. Select the expansion modules to update.
4. Click **File** and select the firmware file to install.
5. Click **OK**. Messages show firmware update progress.

   CAUTION: Do not perform a power cycle or controller restart during the firmware update. If the update is interrupted or there is a power failure, the module might become inoperative. If this occurs, contact technical support. The module might need to be returned to the factory for reprogramming.

   It typically takes 3 minutes to update each EMP in an expansion enclosure. Wait for a message that the code load has completed.
6. Verify that each updated expansion module has the new firmware version.

Updating disk-drive firmware

You can update disk-drive firmware by loading a firmware file obtained from your reseller.

A dual-ported disk drive can be updated from either controller.

Prepare to update disk-drive firmware

1. Follow the best practices in Best practices for firmware update.
2. Obtain the appropriate firmware file and download it to your computer or network.
3. Stop I/O to the storage system. During the update all volumes will be temporarily inaccessible to hosts. If I/O is not stopped, mapped hosts will report I/O errors. Volume access is restored after the update completes.

Update disk-drive firmware

1. Perform one of the following:
   - In the banner, click the system panel and select **Update Firmware**.
   - In the System topic, select **Action > Update Firmware**.

   The Update Firmware panel opens.

2. Select the Update Disk Drives tab. This tab shows information about each disk drive in the system.
3. Select the disk drives to update.
4. Click **File** and select the firmware file to install.
5. Click **OK**.

   CAUTION: Do not power cycle enclosures or restart a controller during the firmware update. If the update is interrupted or there is a power failure, the disk drive might become inoperative. If this occurs, contact technical support.

   It typically takes several minutes for the firmware to load. Wait for a message that the update has completed.

6. Verify that each disk drive has the new firmware revision.

Using the activity progress interface

The activity progress interface reports whether a firmware update or partner firmware update operation is active and shows the progress through each step of the operation. In addition, when the update operation completes, status is presented indicating either the successful completion, or an error indication if the operation failed.

Use the activity progress interface

1. Enable the Activity Progress Monitor service. See Enable or disable system-management settings.
2. In a new tab in your web browser, enter the URL for the form: `http://controller-address:8081/cgi-bin/content.cgi?mc=MC-identifier&refresh=true` where:
   - ***controller-address*** – Required parameter that specifies the IP address of a controller network port.
   - **mc=*MC-identifier*** – Optional parameter that specifies the controller for which to report progress/status:
     - **mc=A** – Shows output for controller A only.
     - **mc=B** – Shows output for controller B only.
     - **mc=both** – Shows output for both controllers.
     - **mc=self** – Shows output for the controller whose IP address is specified.
   - **refresh=true** – Optional parameter that causes automatic refresh of the displayed output every second. This will continue until either:
     - The parameter is removed.
     - The controller whose IP address is specified is restarted and communication is lost.

     When activity is in progress, the interface will display an MC-specific Activity Progress table with the following properties and values.

Table 10. Activity progress properties and values

Property	Value
Time	The date and time of the latest status update.
Seconds	The number of seconds this component has been active.
Component	The name of the object being processed.
Status	The status of the component representing its progress/completion state. ○ **ACTIVE** – The operation for this component is currently active and in progress. ○ **OK** – The operation for this component completed successfully and is now inactive. ○ **N/A** – The operation for this component was not completed because it was not applicable. ○ **ERROR** – The operation for this component failed with an error (see code and message).
Code	A numeric code indicating the status. ○ **0** – The operation for this component completed with a “completed successfully” status. ○ **1** – The operation for this component was not attempted because it is not applicable (the component doesn’t exist or doesn’t need updating).

Table 10. Activity progress properties and values (continued)

Property	Value
	○ **2** – The operation is in progress. The other properties will indicate the progress item (message, current, total, percent). ○ **10 or higher** – The operation for this component completed with a failure. The code and message indicate the reason for the error.
Message	A textual message indicating the progress status or error condition.

Changing FDE settings

In the Full Disk Encryption panel, you can change settings for these options:

- FDE general configuration
  - Set the passphrase
  - Clear lock keys
  - Secure the system
  - Repurpose the system
- Repurpose disks
- Set import lock key IDs

Changing FDE general configuration

CAUTION: Do not change FDE configuration settings while running I/O. Temporary data unavailability may result. Also, the intended configuration change might not take effect.

Setting the passphrase

You can set the FDE passphrase the system uses to write to and read from FDE-capable disks. From the passphrase, the system generates the lock key ID that is used to secure the FDE-capable disks. If the passphrase for a system is different from the passphrase associated with a disk, the system cannot access data on the disks.

NOTE: Be sure to record the passphrase as it cannot be recovered if lost.

Set or change the passphrase

Perform the following steps to set the passphrase:

1. In the System topic, select **Action > Full Disk Encryption**.
   The Full Disk Encryption panel opens with the **FDE General Configuration** tab selected.
2. Type a passphrase in the **Passphrase** field of the Set/Create Passphrase section. A passphrase is case-sensitive and can include 8–32 printable UTF-8 characters except for the following: `, < > \`
3. Retype the passphrase in the **Re-enter Passphrase** field.
4. Perform one of the following:
   - To secure the system now, click **Secure**, and then click **Set**. A dialog box confirms that the passphrase was changed successfully.
   - To save the passphrase without securing the system, click **Set**. A dialog box confirms that the passphrase was changed successfully. To secure the system later, see Securing the system.

Clearing lock keys

Lock keys are generated from the passphrase and manage locking and unlocking the FDE-capable disks in the system. Clearing the lock keys and power cycling the system denies access to data on the disks. Use this procedure when the system is not under your physical control.

If the lock keys are cleared while the system is secured, the system enters the FDE lock-ready state, in preparation for the system being powered down and transported.

After the system has been transported and powered up, the system and disks enter the Secured, Locked state, and volumes become inaccessible. To restore access to data, re-type the original passphrase using the CLI command `set fde-lock-key`.

NOTE: The FDE tabs are dynamic, and the Clear All FDE Keys option is not available on a secured system until the current passphrase is entered in the Current Passphrase field. (If you do not have a passphrase, the Clear All FDE Keys option is not displayed. If you have a passphrase but have not entered it, you can view but not access this option.) If there is no passphrase, set one using the procedure in Setting the passphrase.

Clear lock keys

Performing the steps to clear the lock keys:

1. In the System topic, select **Action > Full Disk Encryption**.
   The Full Disk Encryption panel opens with the FDE General Configuration tab selected.
2. Enter the passphrase in the **Current Passphrase** field.
3. In the Secure System section, click the **Secure** button.
4. Click **Clear**.
   A dialog box appears.
5. Perform one of the following:
   - To clear the lock keys for the system, click **OK**.
   - To cancel the request, click **Cancel**.

Securing the system

An FDE-capable system must be secured to enable FDE protection.

The FDE tabs are dynamic, and the Secure option is not available until the current passphrase is entered in the Current Passphrase field. (If you do not have a passphrase, the Secure option is not displayed. If you have a passphrase but have not entered it, you can view but not access this option.) If there is no passphrase, set one using the procedure in Setting the passphrase.

Perform the following steps to secure the system:

1. In the System topic, select **Action > Full Disk Encryption**.
   The Full Disk Encryption panel opens with the **FDE General Configuration** tab selected.
2. Type the passphrase in the **Current Passphrase** field.
3. Click **Secure**.
   A message displays confirming that the system is in a secure state.

Repurposing the system

You can repurpose a system to erase all data on the system and return its FDE state to unsecure.

CAUTION: Repurposing a system erases all disks in the system and restores the FDE state to unsecure.

Repurposing disks

You can repurpose a disk that is no longer part of a disk group.

Repurposing a disk resets the encryption key on the disk, deleting all data on the disk. After a disk is repurposed in a secured system, the disk is secured using the system lock key ID and the new encryption key on the disk, making the disk usable to the system.

Repurposing a disk in an unsecured system removes all associated lock keys and makes that disk available to any system.

CAUTION: Repurposing a disk changes the encryption key on the disk and deletes all data on the disk. Repurpose a disk only if you no longer need the data on the disk.

Setting import lock key IDs

You can set the passphrase associated with an import lock key to unlock FDE-secured disks that are inserted into the system from a different secure system. If the correct passphrase is not entered, the system cannot access data on the disk.

After importing disks into the system, the disks will now be associated with the system lock key ID and data will no longer be accessible using the import lock key. This effectively transfers security to the local system passphrase.

Set or change the import passphrase

1. In the System topic, select **Action > Full Disk Encryption**.
   The Full Disk Encryption panel opens with the FDE General Configuration tab selected.
2. Select the Set Import Lock Key ID tab.
3. In the **Passphrase** field, enter the passphrase associated with the displayed lock key.
4. Re-enter the passphrase.
5. Click **Set. A** dialog box will confirm the passphrase was changed successfully.

Configuring advanced settings

Use the Advanced Settings panel to change disk settings, cache settings, partner firmware update settings, and system utility settings.

Changing disk settings

The Disk tab provides options to change disk settings, including SMART configuration, EMP polling rate, dynamic spares, and drive spin down options.

Configuring SMART

Self-Monitoring Analysis and Reporting Technology (SMART) provides data that enables you to monitor disks and analyze why a disk failed. When SMART is enabled, the system checks for SMART events one minute after a restart and every five minutes thereafter. SMART events are recorded in the event log.

Change the SMART setting

1. In the System topic, select **Action > Advanced Settings > Disk**.
2. Set the SMART Configuration option to one of the following:
   - **Don't Modify**. Allows current disks to retain their individual SMART settings and does not change the setting for new disks added to the system.
   - **Enabled**. Enables SMART for all current disks after the next rescan and automatically enables SMART for new disks added to the system. This option is the default.
   - **Disabled**. Disables SMART for all current disks after the next rescan and automatically disables SMART for new disks added to the system.
3. Click **Apply**. If you chose to disable SMART, a confirmation panel appears. Click **Apply** to accept the changes or click **Cancel**.

Configuring the EMP polling rate

You can change the frequency interval that the storage system polls each attached enclosure's management processor (EMP) for changes to temperature, power supply and fan status, and the presence or absence of disks. Typically you can use the default setting.

- Increasing the interval might slightly improve processing efficiency, but changes in device status are communicated less frequently. For example, this increases the amount of time before LEDs are updated to reflect status changes.
- Decreasing the interval slightly decreases processing efficiency, but changes in device status are communicated more frequently. For example, this decreases the amount of time before LEDs are updated to reflect status changes.

Change the EMP polling rate

1. In the System topic, select **Action > Advanced Settings > Disk**.
2. Set the EMP Polling Rate interval. The options are 5, 10, or 30 seconds; or 1, 5, 10, 15, 20, 25, 30, 45, or 60 minutes. The default is 5 seconds.
3. Click **Apply**.

Configuring dynamic spares

The dynamic spares feature lets you use all of your disks in fault-tolerant disk groups without designating a disk as a spare. With dynamic spares enabled, if a disk fails and you replace it with a compatible disk, the storage system rescans the bus, finds the new disk, automatically designates it a spare, and starts reconstructing the disk group. A compatible disk has enough capacity to replace the failed

disk and is the same type: SATA SSD, SAS SSD, enterprise SAS, or midline SAS. If a spare or available compatible disk is already present, the dynamic spares feature uses that disk to start the reconstruction and the replacement disk can be used for another purpose.

Change the dynamic spares setting

1. In the System topic, select **Action > Advanced Settings > Disk**.
2. Either select enable, or clear to disable the **Dynamic Spare Capability** option. The dynamic spares setting is enabled by default.
3. Click **Apply**. If you chose to disable dynamic spares, a confirmation panel appears. Click **Apply** to accept the changes or click **Cancel**.

Configuring drive spin down for available disks and global spares

For spinning disks, the drive spin down (DSD) feature monitors disk activity within system enclosures and spins down inactive disks to conserve energy. You can enable or disable DSD for available spinning disks that are in non-ADAPT linear disk groups, for spinning disks that are not in a virtual pool, and for global spares. You can also set the period of inactivity after which available disks and global spares automatically spin down.

To configure a time period to suspend and resume DSD for all disks, see Scheduling drive spin down for available disks and global spares.

DSD affects disk operations as follows:

- Spun-down disks are not polled for SMART events.
- Operations requiring access to disks may be delayed while the disks are spinning back up.

Configure DSD for available disks and global spares

1. In the System topic, select **Action > Advanced Settings > Disk**.
2. Set the options:
   - Either select to enable, or clear to disable the **Available and Spare Drive Spin Down Capability** option. If you are enabling DSD, a warning prompt appears. To use DSD, click **Yes**. To leave DSD disabled, click **No**.
   - Set the **Drive Spin Down Delay (minutes)** option, which is the period of inactivity after which available disks and global spares automatically spin down, from 1 through 360 minutes. The default is 15 minutes.
3. Click **Apply**. When processing is complete a success dialog appears.
4. Click **OK**.

Scheduling drive spin down for available disks and global spares

For all spinning disks that are configured to use drive spin down (DSD), you can configure a time period to suspend and resume DSD so that disks remain spun-up during hours of frequent activity.

To configure DSD for available disks and global spares, see Configuring drive spin down for available disks and global spares.

DSD affects disk operations as follows:

- Spun-down disks are not polled for SMART events.
- Operations requiring access to disks may be delayed while the disks are spinning back up.
- If a suspend period is configured and it starts while a disk has started spinning down, the disk spins up again.

Schedule DSD for all spinning disks

1. In the System topic, select **Action > Advanced Settings > Disk**.
2. Set the options:
   - Select the Drive Spin Down Suspend Period option.
   - Set the Time to Suspend and Time to Resume options. For each, enter hour and minutes values and select either AM, PM, or 24H (24-hour clock).
   - If you want the schedule to apply only Monday through Friday, select the Exclude Weekend Days from Suspend Period option.
3. Click **Apply**. When processing is complete a success dialog appears.
4. Click **OK**.

Changing system cache settings

The Cache tab provides options to change the synchronize-cache mode, missing LUN response, host control of the write-back cache setting, cache redundancy mode, and auto-write-through cache triggers and behaviors.

Changing the synchronize-cache mode

You can control how the storage system handles the `SCSI SYNCHRONIZE CACHE` command. Typically you can use the default setting. However, if the system has performance problems or problems writing to databases or other applications, contact technical support to determine if you should change this option.

Change the synchronize-cache mode

1. In the System topic, select **Action > Advanced Settings > Cache**.
2. Set the Sync Cache Mode option to either:
   - **Immediate.** Good status is returned immediately and cache content is unchanged. This is the default.
   - **Flush to Disk.** Good status is returned only after all write-back data for the specified volume is flushed to disk.
3. Click **Apply**.

Changing the missing LUN response

Some operating systems do not look beyond LUN 0 if they do not find a LUN 0 or cannot handle noncontiguous LUNs. The Missing LUN Response option handles these situations by enabling the host drivers to continue probing for LUNs until they reach the LUN to which they have access.

This option controls the SCSI sense data returned for volumes that are not accessible because they don't exist or have been hidden through volume mapping (this does not apply to volumes of offline disk groups).

Change the missing LUN response

1. In the System topic, select **Action > Advanced Settings > Cache**.
2. Set the Missing LUN Response option to either:
   - Not Ready. Sends a reply that there is a LUN where a gap has been created but that it's "not ready." Sense data returned is a Sense Key of `2h` and an ASC/ASCQ of `04/03`.
   - Illegal Request. Sends a reply that there is a LUN but that the request is "illegal." Sense data returned is a Sense Key of `5h` and an ASC/ASCQ of `25/00`. If the system is used in a VMware environment, use this option. This is the default.
3. Click **Apply**.

Controlling host access to the write-back cache setting

You can prevent hosts from using `SCSI MODE SELECT` commands to change the write-back cache setting of the system.

Some operating systems disable write cache. Host control of write-back cache is disabled by default, which prevents the host from modifying the cache setting.

Enabling the host control of write-back cache option is useful in some environments where the host disables the write-back cache. However, enabling this option might result in degraded performance.

Change host access to the write-back cache setting

1. In the System topic, select **Action > Advanced Settings > Cache**.
2. Either select to enable or clear to disable the **Host Control of Write-Back Cache** option.
3. Click **Apply**.

Changing auto-write-through cache triggers and behaviors

You can set conditions that trigger a controller to change the cache mode from write-back to write-through, as described in About volume cache options. You can also specify actions for the system to take when write-through caching is triggered.

Change auto-write-through cache triggers and behaviors

1. In the System topic, select **Action > Advanced Settings > Cache**.
2. In the Auto-Write Through Cache Trigger Conditions section, either select to enable or clear to disable the options:

Controller Failure	Changes to write-through if a controller fails. In a dual-controller system this option is disabledby default. In Single Controller mode this option is grayed out.
Cache Power	Changes to write-through if cache backup power is not fully charged or fails. Enabled by default.
CompactFlash	Changes to write-through if CompactFlash memory is not detected during POST, fails during POST, or fails while the controller is under operation. Enabled by default.
Power Supply Failure	Changes to write-through if a power supply unit fails. Disabled by default.
Fan Failure	Changes to write-through if a cooling fan fails. Disabled by default.
Over-temperature Failure	Forces a controller shutdown if a temperature is detected that exceeds system threshold limits. Disabled by default.

3. In the Auto-Write Through Cache Behaviors section, either select to enable or clear to disable the options:

Revert when Trigger Condition Clears	When enabled, the cache policy changes back to write-back caching after the trigger condition is cleared. When disabled, the cache policy remains write-through caching after the trigger condition is cleared. Enabled by default.
Notify Other Controller	Notifies the partner controller that a trigger condition occurred. Enable this option to have the partner also change to write-through mode for better data protection. Disable this option to allow the partner to continue using its current caching mode for better performance. In a dual-controller system this option is disabled by default. In Single Controller mode this option is grayed out.

4. Click **Apply**. If you disabled Cache Power or CompactFlash, a confirmation prompt appears. Choose **Apply** to accept the changes, or Cancel to discard the changes.

Configuring partner firmware update

In a dual-controller system in which partner firmware update is enabled (the default), when you update firmware on one controller, the system automatically updates the partner controller. Disable partner firmware update only if requested by a service technician.

Change the partner firmware update setting

1. In the System topic, select **Action > Advanced Settings > Firmware**.
2. Either select (enable) or clear (disable) the **Partner Firmware Update** option.
3. Click **Apply**.

Configuring system utilities

The System Utilities tab lets you configure background scrub for disk groups and individual disks, set utility priority, and enable or disable managed logs.

Configuring background scrub for disk groups

You can enable or disable whether the system continuously analyzes disks in disk groups to find and fix disk errors. This command will fix parity mismatches for RAID 5 and 6; find but not fix mirror mismatches for RAID 1 and 10. It will not fix media errors.

You can use a disk group while it is being scrubbed. Background disk group scrub runs at background utility priority, which reduces to no activity if processor usage is above a certain percentage or if I/O is occurring on the disk group being scrubbed. A disk group scrub may be in process on multiple disk groups at once. A new disk group will first be scrubbed 20 minutes after creation. After a disk group is scrubbed, scrub will start again after the interval specified by the **Disk Group Scrub Interval hours** option.

When a scrub is complete, event 207 is logged and specifies whether errors were found and whether user action is required. Enabling background disk group scrub is recommended.

NOTE: If you choose to disable background disk group scrub, you can still scrub a selected disk group by using Action > Disk Group Utilities.

Configure background scrub for disk groups

1. In the System topic, choose **Action > Advanced Settings > System Utilities**.
2. Set the options:
   - Either select to enable, or clear to disable the **Disk Group Scrub** option. This option is enabled by default.
   - Set the **Disk Group Scrub Interval (hours)** option, which is the interval between background disk group scrub finishing and starting again, from 0 through 360 hours. The default is 24 hours.
3. Click **Apply**.

Configuring background scrub for disks not in disk groups

You can enable or disable whether the system continuously analyzes disks that are not in disk groups to find and fix disk errors. The interval between background disk scrub finishing and starting again is 72 hours. The first time you enable this option, background disk scrub will start with minimal delay. If you disable and then re-enable this option, background disk scrub will start 72 hours after the last background disk scrub completed.

Enabling background disk scrub is recommended for SAS disks.

Configure background scrub for disks not in disk groups

1. In the System topic, choose **Action > Advanced Settings > System Utilities**.
2. Either select to enable, or clear to disable the **Disk Scrub** option. This option is disabled by default.
3. Click **Apply**.

Configuring utility priority

You can change the priority at which the Verify, Reconstruct, Expand, and Initialize utilities run when there are active I/O operations competing for the system's controllers.

Change the utility priority

1. In the System panel, choose **Action > Advanced Settings > System Utilities**.
2. Set the Utility Priority option to either:
   - **High**. Use when your highest priority is to get the system back to a fully fault-tolerant state. This causes heavy I/O with the host to be slower than normal. This value is the default.
   - **Medium**. Use when you want to balance data streaming with data redundancy.
   - **Low**. Use when streaming data without interruption, such as for a web server, is more important than data redundancy. This enables a utility such as Reconstruct to run at a slower rate with minimal effect on host I/O.
3. Click **Apply**.

Enabling or disabling managed logs

You can enable or disable the managed logs feature, which allows log files to be transferred from the storage system to a log-collection system to avoid losing diagnostic data. For an overview of the managed logs feature, including how to configure and test it, see About managed logs.

Using maintenance mode

Enabling maintenance mode prevents SupportAssist from creating support tickets during planned system downtime.

An ME4 Series storage system automatically enters maintenance mode during a user-initiated restart of a controller or during a firmware update. When the controller restart or firmware update is complete, the ME4 Series storage system automatically exits maintenance mode.

NOTE: Maintenance mode can also be manually enabled or disabled on an ME4 Series storage system.

Enable maintenance mode

Perform the following steps manually enable maintenance mode on the ME4 Series storage system:

1. Perform one of the following actions to access the SupportAssist options:
   - In the Home topic, select **Action > System Settings**, then click the **SupportAssist** tab.
   - In the System topic, select **Action > System Settings**, then click the **SupportAssist** tab.
   - In the Welcome panel, select **System Settings**, then click the **SupportAssist** tab.
2. Click **Enable Maintenance** and click **Yes** on the confirmation panel.
   The ME4 Series storage system enters maintenance mode.

Disable maintenance mode

Perform the following steps to manually disable maintenance mode on the ME4 Series storage system:

1. Perform one of the following actions to access the SupportAssist options:
   - In the Home topic, select **Action > System Settings**, then click the **SupportAssist** tab.
   - In the System topic, select **Action > System Settings**, then click the **SupportAssist** tab.
   - In the Welcome panel, select **System Settings**, then click the **SupportAssist** tab.
2. Click **Disable Maintenance** and click **Yes** on the confirmation panel.
   The ME4 Series storage system exits maintenance mode.

Restarting or shutting down controllers

Each controller module contains a Management Controller processor and a Storage Controller processor. When necessary, you can restart or shut down these processors for one controller or both controllers.

Restarting controllers

Perform a restart when the PowerVault Manager informs you that you have changed a configuration setting that requires a restart or when the controller is not working properly.

When you restart a management controller, communication with it is lost until it successfully restarts. If the restart fails, the management controller in the partner controller module in a dual-controller system remains active with full ownership of operations and configuration information.

When you restart a storage controller, it attempts to shut down with a proper failover sequence. This sequence includes stopping all I/O operations and flushing the write cache to disk. At the end, the controller restarts. Restarting a storage controller restarts the corresponding management controller.

CAUTION: If you restart both controller modules in a dual-controller system, all users will lose access to the system and its data until the restart is complete.

NOTE: When a storage controller is restarted, current performance statistics that it recorded are reset to zero, but historical performance statistics are not affected. In a dual-controller system, disk statistics may be reduced but are not reset to zero, because disk statistics are shared between the two controllers. For more information, see Viewing performance statistics.

Perform a restart

Perform the following steps to restart a controller:

1. Perform one of the following:
   - In the banner, click the system panel and select **Restart System**.
   - In the System topic, select **Action > Restart System**.

   The Controller Restart and Shut Down panel opens.

2. Select the **Restart** operation.
3. Select the controller type to restart: **Management or Storage**.
4. Select the controller module to restart: **Controller A, Controller B**, or both.
5. Click **OK**.
   A confirmation panel appears
6. Click **OK**.
   A message is displayed that describes restart activity.

Shutting down controllers

Perform a shut down before you remove a controller module from an enclosure, or before you power off its enclosure for maintenance, repair, or a move. Shutting down the storage controller in a controller module ensures that a proper failover sequence is used, which includes stopping all I/O operations and writing any data in write cache to disk. If you shut down the storage controller in both controller modules, hosts cannot access system data.

CAUTION: You can continue to use the CLI when either or both storage controllers are shut down, but some information might not be available.

Perform a shutdown

Perform the following steps to shut down a controller:

1. Perform one of the following:
   - In the banner, click the system panel and select **Restart System**.
   - In the System topic, select **Action > Restart System**.

   The Controller Restart and Shut Down panel opens.
2. Select the **Shut Down** operation, which automatically selects the Storage controller type.
3. Select the controller module to shut down: **Controller A, Controller B,** or both.
4. Click **OK**.
   A confirmation panel appears.
5. Click **OK**.
   A message is displayed that describes shutdown activity.

4

Working in the Hosts topic

Topics:

Viewing hosts

The Hosts topic shows a tabular view of information about initiators, hosts, and host groups that are defined in the system. For more information about hosts, see About initiators, hosts, and host groups. The Hosts topic also enables users to map initiators and view map details.

Hosts table

The hosts table shows the following information:

NOTE: The table shows 10 entries at a time by default.

- Group. Shows the group name if the initiator is grouped into a host group; otherwise, --.
- Host. Shows the hostname if the initiator is grouped into a host; otherwise, --.
- Nickname. Shows the nickname that is assigned to the initiator.
- ID. Shows the initiator ID, which is the WWN of an FC or SAS initiator or the IQN of an iSCSI initiator.
- Profile. Shows `Standard`, which is the default profile setting.
- Discovered. Shows `Yes` for a discovered initiator. Shows `Yes` for an initiator that is currently not logged into the system.
- Mapped. Shows `Yes` for an initiator that is mapped to volumes, or `No` for an initiator that is not mapped.
- Host Type. Shows the host interface protocol.

Related Maps table

For selected initiators, the Related Maps table shows the following information. By default, the table shows 20 entries at a time.

- Group.Host.Nickname. Identifies the initiators to which the mapping applies:
  - `initiator-name`—The mapping applies to this initiator only.
  - `initiator-ID`—The mapping applies to this initiator only, and the initiator has no nickname.
  - `host-name.*`—The mapping applies to all initiators in this host.
  - `host-group-name.*.*`—The mapping applies to all hosts in this group.
- Volume. Identifies the volumes to which the mapping applies:
  - **volume-name**—The mapping applies to this volume only.
  - **volume-group-name**.*—The mapping applies to all volumes in this volume group.

- Access. Shows the type of access assigned to the mapping:
  - `read-write`—The mapping permits read and write access.
  - `read-only`—The mapping permits read access.
  - `no-access`—The mapping prevents access.
- LUN. Shows whether the mapping uses a single LUN or a range of LUNs (indicated by *).
- Ports. Lists the controller host ports to which the mapping applies. Each number represents corresponding ports on both controllers.

To display more information about a mapping, see Viewing map details.

Create an initiator

You can manually create initiators. For example, you might want to define an initiator before a controller port is physically connected through a switch to a host.

1. Determine the FC or SAS WWN or iSCSI IQN to use for the initiator.
2. In the Hosts topic, select **Action > Create Initiator**. The Create Initiator panel opens.
3. In the Initiator **ID** field, enter the WWN or IQN. A WWN value can include a colon between each pair of digits but the colons will be discarded.
4. In the **Initiator Name** field, enter a nickname that helps you easily identify the initiator. For example, you could use `MailServer_FCp1`. An initiator name is case sensitive and can have a maximum of 32 bytes. It cannot already exist in the system or include the following: " , . < \
   If the name is used by another initiator, you are prompted to enter a different name.
5. In the Profile list, select **Standard**.
6. Click **OK**. The initiator is created and the hosts table is updated.

Modify an initiator

1. In the Hosts topic, select one initiator to modify.
2. Select **Action > Modify Initiator**. The Modify Initiator panel opens.
3. In the **Initiator Name** field, enter a new nickname to help you identify the initiator. For example, you could use `MailServer_FCp2`. An initiator name is case sensitive and can have a maximum of 32 bytes. It cannot already exist in the system or include the following: " , . < \
   If the name is used by another initiator, you are prompted to enter a different name.
4. In the Profile list, select **Standard**.
5. Click **OK**. The hosts table is updated.

Delete initiators

You can delete manually created initiators that are not grouped or are not mapped. You cannot delete manually created initiators that are mapped. You also cannot delete a discovered initiator but you can remove its nickname through the delete operation.

1. In the Hosts topic, select a number, from 1 through 1024, of ungrouped, undiscovered initiators to delete.
2. Select **Action > Delete Initiators**. The Delete Initiators panel opens and lists the initiators to be deleted.
3. Click **OK**.
   - If the initiator you are trying to delete is currently undiscovered, the changes are processed and the hosts table is updated.
   - If the initiator you are trying to delete is currently discovered then a confirmation panel appears. Click **Yes** to save your changes. The changes are processed and the hosts table is updated.

Add initiators to a host

You can add existing named initiators to an existing host or to a new host. To add an initiator to a host, the initiator must be mapped with the same access, port, and LUN settings to the same volumes or volume groups as every other initiator in the host.

1. In the Hosts topic, select 1 through 128 named initiators to add to a host.
2. Select **Action > Add to Host**. The Add to Host panel opens.
3. Perform one of the following:

- To use an existing host, select its name in the Host Select list.
- To create a host, enter a name for the host in the Host Select field. A host name is case sensitive and can have a maximum of 32 bytes. It cannot already exist in the system or include the following: " , . < \

4. Click **OK**. For the selected initiators, the Host value changes from -- to the specified host name.

Remove initiators from hosts

You can remove all except the last initiator from a host. Removing an initiator from a host will ungroup the initiator but will not delete it. To remove all initiators, remove the host.

1. In the Hosts topic, select 1 through 1024 initiators to remove from their hosts.
2. Select **Action > Remove from Host**. The Remove from Host panel opens and lists the initiators to be removed.
3. Click **OK**. For the selected initiators, the Host value changes to --.

Remove hosts

You can remove hosts that are not grouped. Removing a host will ungroup its initiators but will not delete them.

1. In the Hosts topic, select 1 through 512 ungrouped hosts to remove.
2. Select **Action > Remove Host**. The Remove Host panel opens and lists the hosts to be removed.
3. Click **OK**. For initiators that were in the selected hosts, the Host value changes to --.

Rename a host

You can rename a host.

1. In the Hosts topic, select an initiator that belongs to the host that you want to rename.
2. Select **Action > Rename Host**. The Rename Host panel opens.
3. In the **New Host Name** field, enter a new name for the host. A host name is case sensitive and can have a maximum of 32 bytes. It cannot already exist in the system or include the following: " , . < \
   If the name is used by another host, you are prompted to enter a different name.
4. Click **OK**. The hosts table is updated.

Add hosts to a host group

You can add existing hosts to an existing host group or new host group.

The host must be mapped with the same access, port, and LUN settings to the same volumes or volume groups as every other initiator in the host group.

1. In the Hosts topic, select 1 through 256 initiators that belong to a host that you want to add to a host group.
2. Select **Action > Add to Host Group**. The Add to Host Group panel opens.
3. Perform one of the following:
   - To use an existing host group, select its name in the Host Group Select list.
   - To create a host group, enter a name for the host group in the Host Group Select field. A host group name is case-sensitive and can have a maximum of 32 bytes. It cannot exist in the system or include the following: " , . < \
4. Click **OK**.

Remove hosts from a host group

You can remove all except the last host from a host group. Removing a host from a host group will ungroup the host but will not delete it.

1. In the Hosts topic, select 1 through 256 hosts to remove from their host group.
2. Select **Action > Remove from Host Group**. The Remove from Host Group panel opens and lists the hosts to be removed.
3. Click **OK**. For the selected hosts, the Group value changes to --.

Rename a host group

You can rename a host group.

1. In the Hosts topic, select a host group to rename.
2. Select **Action > Rename Host Group**. The Rename Host Group panel opens.
3. In the **New Host Group Name** field, enter a new name for the host group. A host group name is case sensitive and can have a maximum of 32 bytes. It cannot already exist in the system or include the following: " , . < \
   If the name is used by another host group, you are prompted to enter a different name.
4. Click **OK**. The hosts table is updated.

Remove host groups

You can remove host groups. Removing a host group will ungroup its hosts but will not delete them.

1. In the Hosts topic, select 1 through 32 host groups to remove.
2. Select **Action > Remove Host Group**. The Remove Host Group panel opens and lists the host groups to be removed.
3. Click **OK**. For hosts that were in the selected host groups, the Group value changes to --.

Configuring CHAP

For iSCSI, you can use Challenge-Handshake Authentication Protocol (CHAP) to perform authentication between the initiator and target of a login request. To perform this identification, a database of CHAP records must exist on the initiator and target. Each CHAP record can specify one name-secret pair to authenticate the initiator only (one-way CHAP) or two pairs to authenticate both the initiator and the target (mutual CHAP). For a login request from an iSCSI host to a controller iSCSI port, the host is the initiator and the controller port is the target.

When CHAP is enabled and the storage system is the recipient of a login request from a known originator (initiator), the system will request a known secret. If the originator supplies the secret, the connection will be allowed.

To enable or disable CHAP for all iSCSI nodes, see Changing host port settings on page 51.

Special considerations apply when CHAP is used in a system with a peer connection, which is used in replication. In a peer connection, a storage system can act as the originator or recipient of a login request. As the originator, with a valid CHAP record it can authenticate CHAP even if CHAP is disabled. This is possible because the system will supply the CHAP secret requested by its peer and the connection will be allowed. For information about setting up CHAP for use in a peer connection and how CHAP interacts with replication, see Creating a peer connection on page 119.

Add or modify a CHAP record

1. If you intend to use mutual CHAP and need to determine the IQN of a controller iSCSI port, perform the following:
   - Select the **System** topic.
   - Select the **Rear** view.
   - Hover the cursor over the iSCSI host port that you intend to use. In the Port Information panel that appears, note the IQN in the ID field value.
2. In the Hosts topic, select **Action > Configure CHAP**. The Configure CHAP panel opens with existing CHAP records listed.
3. Select the Enable Authentication (CHAP) checkbox to enable use of CHAP for all iSCSI nodes, then confirm the operation.

   NOTE: Enabling or disabling CHAP here will update its setting in the Advanced Settings tab in the Host Ports Settings panel.

4. Perform one of the following:
   - To modify an existing record, select it. The record values appear in the fields below the CHAP records list for editing. You cannot edit the IQN.
   - To add a new record, click **New**.
5. For a new record, in the Node Name (IQN) field, enter the IQN of the initiator. The value is case sensitive and can include a maximum of 223 bytes, including 0–9, lowercase a–z, hyphen, colon, and period.
6. In the **Secret** field, enter a secret for the target to use to authenticate the initiator. The secret is case sensitive and can include 12–16 bytes. The value can include spaces and printable UTF-8 characters except for the following: " <

7. To use mutual CHAP:
   - Select the **Mutual CHAP** check box.
   - In the **Mutual CHAP Name** field, enter the IQN obtained in step 1. The value is case sensitive and can include a maximum of 223 bytes and the following: 0–9, lowercase a–z, hyphen, colon, and period.
   - In the **Mutual CHAP Secret** field, enter a secret for the initiator to use to authenticate the target. The secret is case sensitive, can include 12–16 bytes, and must differ from the initiator secret. The value can include spaces and printable UTF-8 characters except for the following: " <

   A storage system secret is shared by both controllers.
8. Click **Apply** or **OK**. The CHAP records table is updated.

Delete a CHAP record

1. **NOTE: Deleting CHAP records may make volumes inaccessible and the data in those volumes unavailable.**

   In the Hosts topic, select **Action > Configure CHAP**. The Configure CHAP panel opens with existing CHAP records listed.
2. Select the record to delete.
3. Click **Delete** A confirmation panel appears.
4. **NOTE:**

   Click **Remove** to continue. Otherwise, click **Cancel**. If you clicked Remove, the CHAP record is deleted.

5

Working in the Pools topic

Topics:

Viewing pools

The Pools topic shows a tabular view of information about the pools and disk groups that are defined in the system, as well as information for the disks that each disk group contains. Corresponding to the two storage methods, there are both virtual and linear pools and disk groups. There is another type of disk group, the read-cache disk group, which is also related to virtual storage. Read-cache disk groups consist of SSDs. If your system does not use SSDs, you will not be able to create read-cache disk groups.

For more information about pools, see About pools on page 20. For more information about disk groups, see About disk groups on page 14.

Pools table

The pools table shows the following information. The system is limited to two virtual pools, which are named A and B. When you create a linear disk group, the system automatically creates a linear pool with the same name that you designated for the disk group. The system supports up to 64 linear pools and disk groups.

- **Name** – Shows the name of the pool.
- **Health** – Shows the health of the pool: OK, Degraded, Fault, N/A, or Unknown.
- **Size** – Shows the storage capacity defined for the pool when it was created.
- **Class** – Shows the storage type for the pool: virtual or linear.
- **Avail** – Shows the storage capacity presently available for the pool.
- **Volumes** – Shows the number of volumes defined for the disk groups of the pool.
- **Disk Groups** – Shows the number of disk groups in the pool.

To see more information about a pool, hover the cursor over the pool in the table. The Pool Information panel that appears contains the following information:

Table 11. Pool Information panel

Panel	Information displayed
Pool Information	Virtual: Name, serial number, size, available, overcommit, pool overcommitted, low threshold, mid threshold, high threshold, allocated pages, snapshot pages, available pages, sector format, health Linear: Name, serial number, size, available, owner, sector format, health

For more information about and to manage the above overcommit, low threshold, mid threshold, and high threshold settings, see Changing pool settings.

Related Disk Groups table

When you select a pool in the pools table, the disk groups for it appear in the Related Disk Groups table.

For selected pools, the Related Disk Groups table shows the following information:

Table 12. Disk Groups table

Field	Description
Name	Shows the name of the disk group.
Health	Shows the health of the disk group: OK, Degraded, Fault, N/A, or Unknown.
Pool	Shows the name of the pool to which the disk group belongs.
RAID	Shows the RAID level for the disk group.
Class	Shows the storage type for the disk group: · **Virtual** (includes read-cache disk groups) · **Linear**
Disk Description	Shows the disk type. For virtual disk groups, the disk group's tier appears in parentheses after its disk type. For read-cache disk groups, `Read Cache` appears in parentheses after the disk type.
Size	Shows the storage capacity defined for the disk group when it was created.
Free	Shows the available storage capacity for the disk group.
Current Job	Shows the following current system operations for the disk group, if any are occurring: · **DRSC** – A disk is being scrubbed. · **EXPD** – The linear disk group is being expanded. · **INIT** – The disk group is being initialized. · **RBAL** – The ADAPT disk group is being rebalanced. · **RCON** – At least one disk in the disk group is being reconstructed. · **VDRAIN** – The disk group is being removed and its data is being drained to another disk group. · **VPREP** – The virtual disk group is being prepared for use in a virtual pool. · **VRECV** – The virtual disk group is being recovered to restore its membership in the virtual pool. · **VREMV** – The virtual disk group and its data are being removed. · **VRFY** – The disk group is being verified. · **VRSC** – The disk group is being scrubbed.
Status	Shows the status for the disk group: · **CRIT** – Critical. The disk group is online but isn't fault tolerant because some of its disks are down. · **DMGD** – Damaged. The disk group is online and fault tolerant, but some of its disks are damaged. · **FTDN** – Fault tolerant with a down disk. The disk group is online and fault tolerant, but some of its disks are down. · **FTOL** – Fault tolerant and online. The disk group is online and fault tolerant. · **MSNG** – Missing. The disk group is online and fault tolerant, but some of its disks are missing. · **OFFL** – Offline. Either the disk group is using offline initialization, or its disks are down and data may be lost. · **QTCR** – Quarantined critical. The disk group is critical with at least one inaccessible disk. For example, two disks are inaccessible in a RAID-6 disk group or one disk is inaccessible for other fault-tolerant RAID levels. If the inaccessible disks come online or if after 60 seconds from being quarantined the disk group is QTCR or QTDN, the disk group is automatically dequarantined. · **QTDN** – Quarantined with a down disk. For example, the RAID-6 disk group has one inaccessible disk. The disk group is fault tolerant but degraded. If the inaccessible disks come online or if after 60 seconds from being quarantined the disk group is QTCR or QTDN, the disk group is automatically dequarantined. · **QTOF** – Quarantined offline. The disk group is offline with multiple inaccessible disks causing user data to be incomplete, or is an NRAID or RAID-0 disk group. · **STOP** – The disk group is stopped. · **UNKN** – Unknown. · **UP** – Up. The disk group is online and does not have fault-tolerant attributes.

Table 12. Disk Groups table (continued)

Field	Description
Disks	Shows the number of disks in the disk group.

To see more information about a disk group, select the pool for the disk group in the pools table, then hover the cursor over the disk group in the Related Disk Groups table. The Disk Group Information panel opens and displays detailed information about the disk group.

Table 13. Disk Group Information panel

Panel	Information displayed
Disk Group Information	Virtual: Name, serial number, pool, tier, % of pool, allocated pages, available pages, ADAPT target spare capacity, ADAPT actual spare capacity, chunk size, sector format, creation date, minimum disk size, active drive spin down enable, size, free, RAID, disks, status, current job, health Linear: Name, serial number, pool, owner, chunk size, spares, sector format, creation date, minimum disk size, active drive spin down enable, size, free, RAID, disks, status, current job, health Read cache: Name, serial number, pool, tier, allocated pages, available pages, sector format, health

Related Disks table

When you select a disk group in the Related Disk Groups table, the disks for it appear in the Related Disks table.

For selected disks, the Related Disks table shows the following information:

Table 14. Related Disks table

Field	Description
Location	Shows the location of the disk.
Health	Shows the health of the disk: OK, Degraded, Fault, N/A, or Unknown.
Description	Shows the disk type: · **SAS** – Enterprise SAS spinning disk. · **SAS MDL** – Midline SAS spinning disk. · **SSD SAS** – SAS solid-state disk.
Size	Shows the storage capacity of the disk.
Usage	Shows how the disk is being used: · **LINEAR POOL** – The disk is part of a linear pool. · **DEDICATED SP** – The disk is a dedicated spare for a linear disk group. · **VIRTUAL POOL** – The disk is part of a virtual pool. · **LEFTOVR** – The disk is leftover. · **FAILED** – The disk is unusable and must be replaced. Reasons for this status include: excessive media errors, SMART error, disk hardware failure, or unsupported disk.
Disk Group	Shows the disk group that contains the disk.
Status	Shows the status of the disk: · **Up** – The disk is present and is properly communicating with the expander. · **Spun Down** – The disk is present and has been spun down by the DSD feature. · **Warning** – The disk is present but the system is having communication problems with the disk LED processor. For disk and midplane types where this processor also controls power to the disk, power-on failure will result in Error status. · **Unrecoverable** – The disk is present but has unrecoverable errors.

To see more information about a disk in a disk group, select the pool for the disk group in the pools table, select the disk group in the Related Disk Groups table, and then hover the cursor over the disk in the Related Disks table. The Disk Information panel opens and displays detailed information about the disk.

Table 15. Disk Information panel

Panel	Information displayed
Disk Information	Location, serial number, usage, description, size, status, revolutions per minute (spinning disk only), SSD life left, manufacturer, model, firmware revision, power on hours, job status, FDE state, FDE lock key, job running, sector format, transfer rate, SMART, drive spin down count, health

The following are descriptions of some Disk Information panel items:

- **Power On Hours** – Total number of hours that the disk has been powered on since it was manufactured. This value is updated in 30-minute increments.
- **FDE State** – FDE state of the disk. For more information about FDE states, see the *Dell EMC PowerVault ME4 Series Storage System CLI Guide*.
- **FDE lock keys** – FDE lock keys are generated from the FDE passphrase and manage locking and unlocking the FDE-capable disks in the system. Clearing the lock keys and power cycling the system denies access to data on the disks.

Adding a disk group

You can create virtual or linear disk groups using specified disks through the Add Disk Group panel. You can also create read-cache disk groups through this panel. When creating a disk group, you explicitly select the RAID level and individual disks and incorporate them into a pool. All disks in a disk group must be the same type (enterprise SAS, for example). Disk groups support a mix of 512n and 512e disks. However, for consistent and predictable performance, do not mix disks of different rotational speed or sector size types (512n, 512e). For more information about disk groups, see About disk groups.

NOTE: After you create a disk group using one storage type, the system uses that storage type for additional disk groups. To switch to the other storage type, you must first remove all disk groups. For more information, see Removing disk groups.

Add Disk Group panel overview

The Add Disk Group panel displays different options based on the type of disk group you want to create and the data protection level selected. There are three sections in the panel.

The top section provides options to name and define the disk group type, select the pool that it resides on, and choose its data protection (RAID) level.

The middle section contains the Disk Selection Sets summary, which presents cumulative data for the disks that are selected for the disk group. The section displays information about the data protection and disk type that is selected for the disk group, as well as the total number of disks selected, the minimum and maximum number of disks allowed for the specified data protection level, the size of the disk group (total capacity of all selected drives), and the **Complete** check box. The **Complete** check box indicates if the minimum number of disks that are needed to configure the disk group have been selected, and automatically changes from ☒ to a ☑. For dedicated spares, it is always ☑, since selecting additional spares is optional.

As you select drives to add to the disk group, a color-coded bar graph displays the following:

- Disk group available capacity
- Dedicated overhead capacity (for data protection and array metadata)
- Wasted capacity

The bottom section lists the disks that are located within each enclosure in your system, along with their details. Add disks to the disk group by doing one of the following:

- Select a range of disks within an enclosure by entering a comma-separated list that contains the enclosure number and disk range in the **Enter Range of Disks** text box. Use the format `enclosure-number.disk-range,enclosure-number.disk-range`.

  For example, to select disk 3-12 in enclosure 1 and disk 5-23 in enclosure 2, enter **`1.3-12,2.5-23`**.
- Select all disks by selecting the **Select All** checkbox.
- Filter the disks in the list per disk type, enclosure ID, slot location, disk size, or health by entering applicable search criteria in the text box. Clear the filter by clicking the **Clear Filters** button.
- Click individual disks within the table to select them and add them to the disk group.

Adding virtual disk groups

The system supports a maximum of two pools, one per controller module: A and B. You can add up to 16 virtual disk groups for each virtual pool. If a virtual pool does not exist, the system will automatically add it when creating the disk group. Once a virtual pool and disk group exist, volumes can be added to the pool. Once you add a virtual disk group, you cannot modify it. If your organization's needs change, you can modify your storage amount by adding new virtual disk groups or deleting existing ones.

Depending on the type of disks selected, virtual disk groups belong to one of the following tiers:

- Enterprise SAS disks: Standard tier.
- Midline SAS disks: Archive tier.
- SSDs: Performance tier.

NOTE: All virtual groups in the same tier within a virtual pool should have the same data protection level to provide consistent performance across the tier.

NOTE: If a virtual pool contains a single virtual disk group, and it has been quarantined, you cannot add a new virtual disk group to the pool until you have removed the existing disk group from quarantine. For information about removing a disk group from quarantine, see the *Dell EMC PowerVault ME4 Series Storage System CLI Guide*.

Adding linear disk groups

The system supports a maximum of 64 pools and disk groups. Whenever you add a linear disk group, you also automatically add a new linear pool. You cannot add further disk groups to a linear pool. However, you can expand storage by adding disks and dedicated spares to existing linear disk groups.

All of the disks in a linear disk group must share the same classification, which is determined by disk type, size, and speed. This provides consistent performance for the data being accessed on that disk group. When you delete a linear disk group, the contained volumes are automatically deleted. The disks that compose that linear disk group are then available to be used for other purposes.

Read-cache disk groups

If your system has SSDs, you can also add read-cache disk groups. Read cache is a special type of virtual disk group that can be added only to a virtual pool. It is used for the purpose of caching virtual pages for improving read performance. A virtual pool can contain only one read-cache disk group. A virtual pool cannot contain both read cache and a Performance tier. At least one virtual disk group must exist before a read-cache disk group can be added. NRAID is automatically used for a read-cache disk group with a single disk. RAID-0 is automatically used for a read-cache disk group with the maximum of two disks. When you create a read-cache disk group, the system automatically creates a read-cache tier, if one does not already exist. Unlike the other tiers, it is not used in tiered migration of data.

Disk group options

The following options appear in the top section of the Add Disk Group panel:

Table 16. Disk group options

Option	Description
Name	A disk group name is case-sensitive and can have a maximum of 32 bytes. The name cannot already exist in the system or include the following: `" , < \`
Type	When creating a disk group, select one following: • **Virtual**: Shows options for a virtual disk group • **Linear**: Shows options for a linear disk group • **Read Cache**: Shows options for a read cache disk group
Pool (only appears for virtual and read-cache disk groups)	Select the name of the virtual pool (A or B) to contain the group.
Assign to (optional, only appears for linear disk groups)	For a system operating in Active-Active ULP mode, this option specifies the controller module to own the group. To let the system automatically load-balance groups between controller modules, select the Auto setting instead of Controller A or Controller B.

Table 16. Disk group options (continued)

Option	Description
RAID Level	Select one of the following RAID levels when creating a virtual or linear disk group: • **RAID 1** – Requires 2 disks. • **RAID 5** – Requires 3-16 disks. • **RAID 6** – Requires 4-16 disks. • **RAID 10** – Requires 4-16 disks, with a minimum of two RAID-1 subgroups, each having two disks. • **RAID 50** – (only appears for linear disk groups). Requires 6-32 disks, with a minimum of two RAID-5 subgroups, each having three disks. • **ADAPT** – Requires 12-128 disks. To create an NRAID, RAID-0, or RAID-3 (linear-only) disk group, you must use the CLI `add disk-group` command. For more information on this command, see the *Dell EMC PowerVault ME4 Series Storage System CLI Guide*.
Number of Sub-groups (options only appear when RAID-10 or RAID-50 is selected)	Changes the number of sub-groups that the disk group should contain.
Chunk size (optional, only for linear non-ADAPT disk groups)	Specifies the amount of contiguous data, in KB, that is written to a group member before moving to the next member of the group. For NRAID and RAID 1, chunk-size has no meaning and is therefore not applicable. For RAID 50, this option sets the chunk size of each RAID-5 subgroup. The following chunk size options are available when creating a linear disk group: • 64k • 128k • 256k • 512k For a virtual group, the system uses one of the following chunk sizes, which cannot be changed: ○ RAID 1: Not applicable ○ RAID 5 and RAID 6: ▪ With 2, 4, or 8 non-parity disks: 512k. For example, a RAID-5 group with 3, 5, or 9 total disks or a RAID-6 group with 4, 6, or 10 total disks. ▪ Other configurations: 64k ○ RAID 10: 512k
Online Initialization (only appears for linear disk groups)	Specifies whether the group is initialized online or offline. • Online. When the Online Initialization check box is selected, you can use the group immediately after creating it while it is initializing. Because online uses the verify method to create the group, it takes longer to complete initializing than offline. Online initialization is fault-tolerant. • Offline. When the Online Initialization check box is cleared, you must wait for the group initialization process to finish before using the group. However, offline takes less time to complete initializing than online.

Add a disk group

Perform the following steps to add a disk group:

1. In the Pools topic, select **Action > Add Disk Group**. The Add Disk Group panel opens.
2. Set the options. See Disk group options for more information.
3. If you are creating a linear disk group, select the **RAID *number*** or **SPARE** option to determine if you are selecting disks for the RAID configuration or as dedicated spares for the disk group.

   NOTE: The ADAPT RAID level does not have a dedicated spare option.

4. Select the disks that you want to add to the disk group from the table.

NOTE: Disks that are already used or are not available for use are not populated in the table.

5. Click **Add**.

   If your disk group contains both 512n and 512e disks, a dialog box appears. Perform one of the following:

   - To create the disk group, click **Yes**.
   - To cancel the request, click **No**.

   If the task succeeds, the new disk group appears in the Related Disk Groups table in the Pools topic.

Modifying a disk group

You can rename any virtual and read-cache disk group. For linear disk groups, you can also assign a different controller to, expand the capacity of, enable the drive spin down (DSD) feature, and set a DSD delay for non-ADAPT linear disk groups.

Renaming virtual disk groups

When you rename a virtual disk group, the Modify Disk Group panel is a simplified version of the one that appears when modifying linear disk groups.

Modify the drive spin down feature

The DSD feature monitors disk activity within system enclosures and spins down inactive spinning disks to conserve energy. You can enable or disable DSD for non-ADAPT linear disk group, and set a period of inactivity after which the disk group disks and dedicated spares automatically spin down.

1. In the Pools topic, select the pool in the pools table for the disk group that you are modifying.

   NOTE: To see more information about a pool, hover the cursor over the pool in the table. See Viewing pools for more details about the Pool Information panel that appears.

2. Select the disk group in the Related Disk Groups table.
3. Select **Action > Modify Disk Group.**
   The Modify Disk Group panel opens.
4. To change the disk group name, type a new name in the **New Name** field.

   A disk group name is case-sensitive and can have a maximum of 32 bytes. It cannot already exist in the system or include the following characters: `" , < \`
5. To assign a controller to the disk group in a dual-controller system, select the controller from the Owner list.

   NOTE: If you only want to modify the name and/or controller for the disk group, you can click OK and not go to the next step.

6. To enable drive spin down for the disk group, select the **Enable Drive Spin Down** check box.
7. To set a period of inactivity after which available disks and global spares are automatically spun down for the disk group, type the number of minutes in the **Drive Spin Down Delay** field.

   The maximum value is 360 minutes. The default is 15 minutes.
8. Click **Modify**.
   The disk group modification begins.
9. Click **OK** when the disk group modification is complete.

Removing disk groups

You can delete a single disk group or select multiple disk groups and delete them in a single operation. By removing disk groups, you can also remove pools. Removing all disk groups within a pool will also trigger the automatic removal of the associated pool.

If all disk groups for a pool have volumes assigned and are selected for removal, a confirmation panel will warn the user that the pool and all its volumes will be removed. For linear disk groups, this is always the case since linear pools can only have one disk group per pool.

Unless a virtual pool consists exclusively of SSDs, if a virtual pool has more than one disk group and at least one volume that contains data, the system attempts to drain the disk group to be deleted by moving the volume data that it contains to other disk groups in the pool. When removing one or more, but not all, disk groups from a virtual pool, the following possible results can occur:

- If the other disk groups do not have room for the data of the selected disk group, the delete operation will fail immediately and a message will be displayed.
- If there is room to drain the volume data to other disk groups, a message will appear that draining has commenced and an event will be generated upon completion (progress will also be shown in the Current Job column of the Related Disk Groups table).
    - When the disk group draining completes, an event will be generated, the disk group disappears, and the drives for it becomes available.
    - If a host writes during the disk group draining, which results in there not being enough room to finish the draining, an event will be generated, the draining terminates, and the disk group will remain in the pool.

NOTE: Disk group removal (draining) can take a very long time depending on a number of factors in the system, including but not limited to: large pool configuration; the amount of I/O traffic to the system (e.g., active I/O pages to the draining disk group); the type of the disk group page migration (enterprise SAS, midline SAS, SSD); the size of the draining disk group(s) in the system; and the number of disk groups draining at the same time.

If you remove the last disk group in a virtual pool, the system will prompt you to confirm removing the pool, too. If you choose yes, the pool will be removed. If you choose no, the disk group and the pool will remain.

NOTE: If the disk group is the last disk group for a pool that is used in a peer connection or it contains a volume that is used in a replication set, the Remove Disk Groups menu option will be unavailable.

Remove a disk group

1. In the Pools topic, select the pool for the disk groups that you are deleting in the pools table. Then, select the disk groups in the Related Disk Groups table.

   NOTE: To see more information about a pool, hover the cursor over the pool in the table. Viewing pools contains more details about the Pool Information panel that appears.

2. Select **Action > Remove Disk Groups**. The Remove Disk Groups panel opens.
3. Click **OK**.
4. Click **Yes** to continue. Otherwise, click **No**. If you clicked Yes, the disk groups and their volumes are deleted, the pool for the disk groups might be deleted, the disks for the disk groups become available, and the Related Disk Groups table is updated.

Expanding a disk group

You can expand the capacity of a linear disk group, or a virtual disk group with a RAID level set to ADAPT up to the maximum number of disks that the storage system supports. Host I/O to the disk group can continue while the expansion proceeds. You can then create or expand a volume to use the new free space that becomes available when the expansion is complete. As described in About RAID levels, the RAID level determines whether the disk group can be expanded and the maximum number of disks the disk group can have. This task cannot be performed on an NRAID or RAID-1 disk group.

The following table summarizes disk group types that can be expanded.

Table 17. Disk group expansion

Disk Group Type	Expand Available	Notes
Linear	Yes	Excludes NRAD and RAID 1.
Virtual	No	Add a new disk group to a virtual pool.
ADAPT Virtual or Linear	Yes	

When expanding a disk group, all disks in the disk group must be the same type (enterprise SAS, for example). Disk groups support a mix of 512n and 512e disks. However, for best performance, all disks should use the same sector format. For more information about disk groups, see About disk groups.

Before expanding non-ADAPT disk groups, back up the disk group's data so that if you need to stop expansion and delete the disk group, you can move the data into a new, larger disk group.

Adding single-ported disks to a disk group that contains dual-ported disks is supported. However, because single-ported disks are not fault-tolerant, a confirmation prompt will appear.

NOTE: Expansion can take hours or days to complete, depending on the disk group's RAID level and size, disk speed, utility priority, and other processes running on the storage system. You can stop expansion only by deleting the disk group. For ADAPT disk groups, expansion is very fast and extra capacity is immediately available when rebalancing is not needed. If rebalancing is needed, extra capacity may not be available until rebalancing is complete.

When disks are added to an ADAPT disk group, the system will first replenish any spare capacity needed to be fully fault-tolerant, then use the remainder for expansion of user data capacity. When set to the default spare capacity, the system will try to replenish spare capacity to be the sum of the largest two disks in the group.

- When default spare capacity has been overridden the system will try to replenish spare capacity to meet the configured target GiB. For more information, see the topic about the `add disk-group` command in the *Dell EMC PowerVault ME4 Series Storage System CLI Guide*.
- If the actual spare capacity meets the target spare capacity, the new disk capacity will be allocated to user data. For information on how ADAPT disk groups manage sparing, see About RAID levels.

There are three sections that comprise the Expand Disk Group panel. The top section displays information about the disk group, including its name, type, owner (controller), and data protection (RAID) level. The information that is based on the type of disk group being expanded.

The middle section contains the disk selection sets summary and Disks table which presents cumulative data for existing disks and dedicated spares in the disk group as well as for selected disks. The amount of disk space is color-coded to show total, available, dedicated spares, and overhead disk space amounts.

The Disks table lists information about the disks and dedicated spares in the disk group, updating as you select disks to expand the disk group to show the total number of disks selected and the total size of the disk group.

The bottom section lists the disks in each enclosure in your system, along with their details. Select the disks that you want to add to the current disk group by doing one of the following:

- Select a range of disks within an enclosure by entering a comma-separated list that contains the enclosure number and disk range in the **Enter Range of Disks** text box. Use the format `enclosure-number.disk-range,enclosure-number.disk-range`. For example, to select disks 3-12 in enclosure 1 and 5-23 in enclosure 2, enter **`1.3-12,2.5-23`**.
- Select all disks by checking the **Select All** checkbox.
- Filter the disks in the list per disk description, enclosure ID, slot location, or disk size by entering applicable search criteria in the text box. Clear the filter by clicking the **Clear Filters** button.
- Click on individual disks within the table to select them and add them to the disk group.

Selected disks are highlighted in blue. To remove disks from the group, click on them the disks to deselect them.

Expand a disk group

1. In the Pools topic, select the pool for the disk group that you are expanding. Then select the disk group in the Expand Disk Group table.

   NOTE: To see more information about a pool, hover the cursor over the pool in the table. Viewing pools contains more details about the Pool Information panel that appears.

2. Select **Action > Expand Disk Group**. The Expand Disk Group panel opens displaying disk group information and disk tables.
3. For disk groups with RAID-10 or RAID-50 configurations, choose the number of new sub-groups in the Additional Sub-groups list.
4. Select additional disks that you want to add to the disk group from the table in the bottom section.
5. Click **Modify**. A confirmation panel appears.
6. Click **Yes** to continue. Otherwise click **No**. If you clicked Yes, the disk group expansion starts.
7. To close the confirmation panel, click **OK**.

Managing spares

The Manage Spares panel displays a list of current spares and lets you add and remove global spares for virtual and linear disk groups, and dedicated spares for linear disk groups. The options in the panel are dependent on the type of disk group selected.

Global spares

In the PowerVault Manager, you can designate a maximum of 64 global spares for disk groups that do not use the ADAPT RAID level. If a disk in any fault-tolerant virtual or linear disk group fails, a global spare—which must be the same size or larger and the same type as the failed disk—is automatically used to reconstruct the disk group. This is true of RAID 1, 5, 6, 10 for virtual disk groups and RAID 1, 3, 5, 6, 10, 50 for linear ones. At least one disk group must exist before you can add a global spare. A spare must have sufficient capacity to replace the smallest disk in an existing disk group.

The disk group will remain in critical status until the parity or mirror data is completely written to the spare, at which time the disk group will return to fault-tolerant status. For RAID-50 linear disk groups, if more than one subgroup becomes critical, reconstruction and use of spares occur in the order subgroups are numbered.

The Change Global Spares panel consists of two sections. The top section contains the disk sets summary and Disks table which presents cumulative data for existing global spares for the disk group as well as for selected disks. The Disks table lists information about the global spares in the disk group, updating as you select disks to add to show the total number of disks selected as global spares and the total size of the global spares.

The bottom section lists the disks located within each enclosure in your system that can be designated as global spares along with their details. Disks that are designated as global spares, as well as disks you select to designate as global spares, are highlighted in blue. Select disks by doing one of the following:

- Select a range of disks within an enclosure by entering a comma-separated list that contains the enclosure number and disk range in the **Enter Range of Disks** text box. Use the format `enclosure-number.disk-range,enclosure-number.disk-range`. For example, to select disks 3-12 in enclosure 1 and 5-23 in enclosure 2, enter 1.3-**`12,2.5-23`**.
- Select all disks by checking the **Select All** checkbox.
- Filter the disks in the list per disk type, enclosure ID, slot location, or disk size by entering applicable search criteria in the text box. Clear the filter by selecting the **Clear Filters** button.
- Click on individual disks within the table to select them and add them to the disk group.

Remove global spares by clicking on current global spares to deselect them. Viewing pools contains more details about the Disk Information panel.

NOTE: Disk groups support a mix of 512n and 512e disks. For consistent and predictable performance, do not mix disks of different rotational speed or sector size types (512n, 512e). If a global spare has a different sector format than the disks in a disk group, an event will appear when the system chooses the spare after a disk in the disk group fails. For more information about disk groups, see About disk groups.

Add global spares

1. In the Pools topic, select **Action > Manage Spare**. The Manage Spare panel opens.
2. To add global spares, click on the available disks to highlight them.
3. Click **Add Spares**. The system updates the global spares and a confirmation panel opens.
4. To close the confirmation panel, click **OK**.

Remove global spares

1. In the Pools topic, select **Action > Manage Spare**. The Manage Spare panel opens.
2. To remove global spares, click on current spares to deselect them.
3. Click **Remove**. The system updates the global spares and a confirmation panel opens.
4. To close the confirmation panel, click **OK**.

Dedicated spares

The Manage Spares panel consists of two sections. The top section lists the current spares in the system and includes information about each. The bottom section lists all the available disks that can be designated as spares and includes details about each disk. If you selected a linear disk group, this section displays disks that can be used as dedicated spares for the selected disk group.

Click individual disks within the table to select them. Filter the disks in the list per disk description, location, or disk size by entering applicable search criteria in the text box. Clear the filter by clicking the Clear Filters button.

Disk groups support both 512n and 512e disks. However, for consistent and predictable performance, do not mix disks of different rotational speed or sector size types (512n, 512e). For more information about disk groups, see About disk groups.

Add dedicated spares

1. In the Pools topic, select the linear pool for the disk group that you are modifying in the pools table. Then, select the disk group in the Related Disk Groups table.
2. Select **Action > Manage Spares**. The Manage Spares panel opens.
3. Check the **Assign dedicated spares to the disk group** box, then select the disk group in which you want the dedicated spare to reside.
4. In the Add New Spares section, click on available disks to select them.
5. Click **Add Spares**. The system updates the dedicated spares and a confirmation panel appears.
6. To close the confirmation panel, click **OK**.

Create a volume

You can add volumes to virtual pools and linear disk groups. Use the Create Virtual Volumes panel or the Create Linear Volumes panel to create volumes. You can access the panels from either the Pools and Volumes topics.

1. In the Pools topic, select a pool in the pools table.

   NOTE: To see more information about a pool, hover the cursor over the pool in the table. See Viewing pools for more details about the Pool Information panel that appears.

2. Select a disk group in the Related Disk Groups table.
3. Select **Action** > **Create Volumes**.
   The Create Virtual Volumes or Create Linear Volumes panel opens, depending on the type of disk group that you selected.

   For more information about creating virtual volumes, see Create a virtual volume. For more information about creating linear volumes, see Create a linear volume.

Changing pool settings

Each virtual pool has three thresholds for page allocation as a percentage of pool capacity. You can set the low and middle thresholds. The high threshold is automatically calculated based on the available capacity of the pool minus 200 GB of reserved space.

NOTE: If the pool size is 500 GB or smaller, or the middle threshold is relatively high or both, the high threshold may not guarantee 200 GB of reserved space in the pool. The controller cannot automatically adjust the low and middle thresholds in such cases.

You can view and change settings that govern the operation of each virtual pool:

- **Low Threshold**: When this percentage of virtual pool capacity has been used, informational event 462 is generated to notify the administrator. This value must be less than the Mid Threshold value. The default is 50 percent.
- **Mid Threshold**: When this percentage of virtual pool capacity has been used, event 462 is generated to notify the administrator to add capacity to the pool. This value must be between the Low Threshold and High Threshold values. The default is 75 percent. If the pool is not overcommitted, the event has an Informational severity. If the pool is overcommitted, the event has a Warning severity.
- **High Threshold**: When this percentage of virtual pool capacity has been used, event 462 is generated to alert the administrator to add capacity to the pool. This value is automatically calculated based on the available capacity of the pool minus 200 GB of reserved space. If the pool is not overcommitted, the event has an Informational severity. If the pool is overcommitted, the event has Warning severity and the system uses write-through cache mode until virtual pool usage drops back below this threshold.
- **Enable overcommitment of pools?**: This check box controls whether the allocated size of the volumes can exceed the physical capacity of the pool.

  NOTE: The above pool settings apply only to virtual pools. They do not affect linear pools.

NOTE: If your system has a replication set, the pool might be unexpectedly overcommitted because of the size of the internal snapshots of the replication set. If the pool is overcommitted and has exceeded its high threshold, its health shows as degraded in the Pools topic. If the pool is overcommitted and has exceeded its high threshold, its health shows as degraded in the Pools topic. If you try to disable overcommitment and the total space that is allocated to thin-provisioned volumes exceeds the physical capacity of their pool, an error states that there is insufficient free disk space to complete the operation and overcommitment remains enabled.

To check if the pool is overcommitted, hover the cursor over the pool in the pools table to display the Pool Information panel . If the Pool Overcommitted value is True, the pool is overcommitted. If the Pool Overcommitted value is False, the pool is not overcommitted.

Verifying and scrubbing disk groups

Verify a disk group

If you suspect that a fault-tolerant, mirror or parity, disk group has a problem, run the Verify utility to check the disk group's integrity. For example, if you haven't checked the system for parity inconsistencies recently and are concerned about the disk health, verify its disk groups. The Verify utility analyzes the selected disk group to find and fix inconsistencies between its redundancy data and its user data. This utility fixes parity mismatches for RAID 3, 5, 6, and 50, and finds but not fixes mirror mismatches for RAID 1 and 10. This task can be performed only on a disk group whose status is fault tolerant and online (FTOL). It cannot be performed for NRAID or RAID 0 read cache disk groups.

Verification can last over an hour, depending on the size of the disk group, the utility priority, and the amount of I/O activity. You can use a disk group while it is being verified. When verification is complete, event 21 is logged and specifies the number of inconsistencies found. Such inconsistencies can indicate that a disk in the disk group is going bad. For information about identifying a failing disk, use the SMART option. For more information, see Configuring SMART.

If too many utilities are running for verification to start, either wait until those utilities have completed and try again, or abort a utility to free system resources. If you abort verification, you cannot resume it. You must start the process again from the beginning.

Verify a disk group

1. In the Pools topic, select the pool for the disk group that you plan to verify in the pools table.

   NOTE: To see more information about a pool, hover the cursor over the pool in the table. See Viewing pools for more details about the Pool Information panel that appears.

2. Select the disk group in the Related Disk Groups table.
3. Select **Action > Disk Group Utilities**.
   The Disk Group Utilities panel opens, showing the current job status.
4. Click **Verify Disk Group**.
   A message confirms that verification has started.
5. Click **OK**.
   The panel shows the progress of the disk group verification.

Abort a disk group verification

Perform the following steps to abort a disk group verification:

1. In the Pools topic, select the pool for the disk group that you are verifying in the pools table.
2. Select the disk group in the Related Disk Groups table.
3. Select **Action** > **Disk Group Utilities**.
   The Disk Group Utilities panel opens, showing the current job status.
4. Click **Abort Verify**.
   A message confirms that verification has been aborted.
5. Click **OK**.

Scrubbing a disk group

The system-level Disk Group Scrub option automatically checks all disk groups for disk defects. If this option is disabled, you can still perform a scrub on a selected disk group. A scrub analyzes the selected disk group to find and fix disk errors. A scrub also fixes parity mismatches for RAID 3, 5 and 6 and ADAPT and mirror mismatches for RAID 1 and 10.

A scrub can last over an hour, depending on the size of the disk group, the utility priority, and the amount of I/O activity. However, a manual scrub is typically faster than a background scrub. You can use a disk group while it is being scrubbed. When a scrub is complete, event 207 is logged and specifies whether errors were found and whether user action is required.

Scrub a disk group

1. In the Pools topic, select the pool for the disk group that you plan to scrub in the pools table.
2. Select the disk group in the Related Disk Groups table.

3. Select **Action > Disk Group Utilities**. The Disk Group Utilities panel opens, showing the current job status.
4. Click **Scrub Disk Group**. A message confirms that the scrub has started.
5. Click **OK**. The panel shows the scrub's progress.

Abort a disk group scrub

1. In the Pools topic, select the pool for the disk group that you are verifying in the pools table. Then, select the disk group in the Related Disk Groups table.

   NOTE: If the disk group is being scrubbed but the Abort Scrub button is grayed out, a background scrub is in progress. To stop the background scrub, disable the Disk Group Scrub option as described in Configuring system utilities.

2. Select **Action > Disk Group Utilities**. The Disk Group Utilities panel opens, showing the current job status.
3. Click **Abort Scrub**. A message confirms that the scrub has been aborted.
4. Click **OK**.

Abort a disk group scrub

Perform the following steps to abort a disk group scrub:

1. In the Pools topic, select the pool for the disk group that you are scrubbing in the pools table.
2. Select the disk group in the Related Disk Groups table.
3. Select **Action** > **Disk Group Utilities**.
   The Disk Group Utilities panel opens, showing the current job status.

   NOTE: If the disk group is being scrubbed, but the Abort Scrub button is unavailable, a background scrub is in progress. To stop the background scrub, disable the Disk Group Scrub option as described in Configuring system utilities on page 68.

4. Click **Abort Scrub**.
   A message confirms that scrub has been aborted.
5. Click **OK**.

Removing a disk group from quarantine

Contact technical support for assistance in determining if the recovery procedure that makes use of the Dequarantine Disk Group panel and the trust command is applicable to your situation and for assistance in performing it.

CAUTION: Carefully read this topic to determine whether to use the Dequarantine Disk Group panel to manually remove a disk group from quarantine.

NOTE: For status descriptions, see Related Disk Groups table.

- The Dequarantine Disk Group panel should only be used as part of the emergency procedure to attempt to recover data and is normally followed by use of the CLI trust command. If a disk group is manually dequarantined and does not have enough disks to continue operation, its status will change to offline (OFFL) and its data may or may not be recoverable through use of the trust command.
- See the help for the trust command.
- To continue operation—that is, not go to quarantined status—a RAID-3 or RAID-5 disk group can have only one inaccessible disk; a RAID-6 disk group can have only one or two inaccessible disks; a RAID-10 or RAID-50 disk group can have only one inaccessible disk per sub-disk group. For example, a 16-disk RAID-10 disk group can remain online (critical) with 8 inaccessible disks if one disk per mirror is inaccessible.
- The system will automatically quarantine a disk group having a fault-tolerant RAID level if one or more of its disks becomes inaccessible, or to prevent invalid, or stale data that may exist in the controller from being written to the disk group. Quarantine will not occur if a known-failed disk becomes inaccessible or if a disk becomes inaccessible after failover or recovery. The system will automatically quarantine an NRAID or RAID-0 disk group to prevent invalid data from being written to the disk group. If quarantine occurs because of an inaccessible disk, event 172 is logged. If quarantine occurs to prevent writing invalid data, event 485 is logged.

Examples of when quarantine can occur are:

- At system power-up, a disk group has fewer disks online than at the previous power-up. This may happen because a disk is slow to spin up or because an enclosure is not powered up. The disk group will be automatically dequarantined if the inaccessible disks come online and the disk group status becomes FTOL, or if after 60 seconds the disk group status is QTCR or QTDN.

- During system operation, a disk group loses redundancy plus one more disk. For example, three disks are inaccessible in a RAID-6 disk group or two disks are inaccessible for other fault-tolerant RAID levels. The disk group will be automatically dequarantined if after 60 seconds the disk group status is FTOL, FTDN, or CRIT.

Quarantine isolates the disk group from host access and prevents the system from changing the disk group status to OFFL. The number of inaccessible disks determines the quarantine status, from least to most severe:

- QTDN (quarantined with a down disk): The RAID-6 disk group has one inaccessible disk. The disk group is fault tolerant but degraded. If the inaccessible disks come online or if after 60 seconds from being quarantined the disk group is QTCR or QTDN, the disk group is automatically dequarantined.
- QTCR (quarantined critical): The disk group is critical with at least one inaccessible disk. For example, two disks are inaccessible in a RAID-6 disk group or one disk is inaccessible for other fault-tolerant RAID levels. If the inaccessible disks come online or if after 60 seconds from being quarantined the disk group is QTCR or QTDN, the disk group is automatically dequarantined.
- QTOF (quarantined offline): The disk group is offline with multiple inaccessible disks causing user data to be incomplete, or is an NRAID or RAID-0 disk group.

When a disk group is quarantined, its disks become write-locked, its volumes become inaccessible, and it is not available to hosts until it is dequarantined. If there are interdependencies between the quarantined disk group's volumes and volumes in other disk groups, quarantine may temporarily impact operation of those other volumes. Depending on the operation, the length of the outage, and the settings associated with the operation, the operation may automatically resume when the disk group is dequarantined or may require manual intervention. A disk group can remain quarantined indefinitely without risk of data loss.

A disk group is dequarantined when it is brought back online, which can occur in three ways:

- If the inaccessible disks come online, making the disk group FTOL, the disk group is automatically dequarantined.
- If after 60 seconds from being quarantined the disk group is QTCR or QTDN, the disk group is automatically dequarantined. The inaccessible disks are marked as failed and the disk group status changes to critical (CRIT) or fault tolerant with a down disk (FTDN). If the inaccessible disks later come online, they are marked as leftover (LEFTOVR).
- The `dequarantine` command is used to manually remove a disk group from quarantine. If the inaccessible disks later come online, they are marked as leftover (LEFTOVR). If event 485 was logged, use the `dequarantine` command only as specified by the recommended-action text to help prevent data corruption or loss.

A quarantined disk group can be fully recovered if the inaccessible disks are restored. Make sure that all disks are properly seated, that no disks have been inadvertently removed, and that no cables have been unplugged. Sometimes not all disks in the disk group power up. Check that all enclosures have restarted after a power failure. If these problems are found and then fixed, the disk group recovers and no data is lost.

If the inaccessible disks cannot be restored (for example, they failed), and the disk group's status is FTDN or CRIT, and compatible spares are available, reconstruction will automatically begin.

If a replacement disk (reconstruct target) is inaccessible at power up, the disk group becomes quarantined. When the disk is found, the disk group is dequarantined and reconstruction starts. If reconstruction was in process, it continues where it left off.

NOTE: The only tasks allowed for a quarantined disk group are Dequarantine Disk Group and Remove Disk Groups. If you delete a quarantined disk group and its inaccessible disks later come online, the disk group will reappear as quarantined or offline and you must delete it again to clear those disks.

Remove a disk group from quarantine

If specified by the recommended action for event 172 or 485, you can remove a disk group from quarantine.

CAUTION: To help prevent the loss of data, contact technical support before removing a disk group from quarantine.

1. In the Pools topic, select the quarantined disk group.
2. Select **Action > Dequarantine Disk Group**.

   The Dequarantine Disk Group panel opens.
3. Click **OK**.

   Depending on the number of disks that remain active in the disk group, its health might change to Degraded (RAID 6 only) and its status changes to FTOL, CRIT, or FTDN. For status descriptions, see Related Disk Groups table.

6

Working in the Volumes topic

Topics:

Viewing volumes

The Volumes topic shows a tabular view of information about volumes, replication sets, and virtual snapshots that are defined in the system. For more information about volumes, see About volumes and volume groups. For more information about replication, see About replicating virtual volumes. For more information about snapshots, see About snapshots.

Volumes table in the Volumes topic

The volumes table shows the following information. By default, the table shows 10 entries at a time.

- **Group** – Shows the group name if the volume is grouped into a volume group; otherwise, --.
- **Name** – Shows the name of the volume.
- **Pool** – Shows whether the volume is in pool A or B for virtual pools or pool-name for linear pools.
- **Type** – Shows whether the volume is a base volume (virtual), standard volume (linear), or a snapshot (virtual).
- **Size** – Shows the storage capacity defined for the volume when it was created, minus 60 KB for internal use.
- **Allocated** – Shows the storage capacity allocated to the volume for written data.

NOTE: When selecting one or more volumes or snapshots in the volumes table, the Snapshots, Maps, Replication Sets, and Schedules tabs are enabled if they have associated information for the selected items.

To see more information about a volume or snapshot, hover the cursor over the volume in the table. The Volume Information panel opens and displays detailed information about the volume or snapshot.

Table 18. Volume Information panel

Panel	Information displayed
Volume Information	Name, type, pool, group, class, size, allocated size, owner, serial number, volume copy job, write policy, optimization, read-ahead size, tier affinity, health

NOTE: For more information about write policy and read-ahead size, see Modifying a volume.

Snapshots table in the Volumes topic

To see more information about a snapshot and any child snapshots taken of it, select the snapshot or volume that is associated with it in the volumes table. If it is not already selected, click the **Snapshots** tab. The snapshots and all related snapshots appear in the Snapshots table.

The Snapshots table shows the following snapshot information. By default, the table shows 10 entries at a time.

- **Name** – Shows the name of the snapshot.
- **Base Volume** – Shows the name of the virtual volume from which the snapshot was created. All virtual volumes are base volumes when created and are volumes from which virtual snapshots can be created.
- **Parent Volume** – Shows the name of the volume from which the snapshot was created.
- **Creation Date/Time** – Shows the date and time when the snapshot was created.
- **Status** – Shows whether the snapshot is available or unavailable. A snapshot can be unavailable for one of the following reasons:
  - The source volume is not accessible or is not found.
  - The snapshot is pending.
  - A rollback with modified data is in progress.
- **Snapshot Data** – Shows the total amount of data associated with the specific snapshot (data copied from a source volume to a snapshot and data written directly to a snapshot).

To see more information about a snapshot, hover the cursor over the snapshot in the table. The Snapshot Information panel opens and displays detailed information about the snapshot.

Table 19. Snapshots Information panel

Panel	Information displayed
Snapshot Information	Name, serial number, status, status reason, retention priority, snapshot data, unique data, shared data, pool, class, number of snaps, number of snapshots in tree, source volume, total size, creation date/time, type, parent volume, base volume, health

NOTE: Class refers to the storage type: virtual or linear.

Maps table in the Volumes topic

To see information about the maps for a snapshot or volume, select the snapshot or volume in the volumes table. Then, select the Map tab. The maps appear in the Maps table.

The Maps table shows the following mapping information. By default, the table shows 10 entries at a time.

- Group.Host.Nickname. Identifies the initiators to which the mapping applies:
  - `initiator-name`—The mapping applies to this initiator only.
  - `initiator-ID`—The mapping applies to this initiator only, and the initiator has no nickname.
  - `host-name.*`—The mapping applies to all initiators in this host.
  - `host-group-name.*.*`—The mapping applies to all hosts in this group.
- Volume. Identifies the volumes to which the mapping applies:
  - `volume-name`—The mapping applies to this volume only.
  - `volume-group-name.*`—The mapping applies to all volumes in this volume group.
- Access. Shows the type of access assigned to the mapping:
  - `read-write`—The mapping permits read and write access.
  - `read-only`—The mapping permits read access.
  - `no-access`—The mapping prevents access.
- LUN. Shows the LUN number or '*' if the map is to a volume group.
- Ports. Lists the controller host ports to which the mapping applies. Each number represents corresponding ports on both controllers.

To display more information about a mapping, see Viewing map details.

Replication Sets table in the Volumes topic

To see information about the replication set for a volume or volume group, select a volume in the volumes table. If it is not already selected, select the Replication Sets tab. The replication appears in the Replication Sets table.

The Replication Sets table shows the following information. By default, the table shows 10 entries at a time.

- **Name** – Shows the replication set name.
- **Primary Volume** – Shows the primary volume name. For replication sets that use volume groups, the primary volume name is `volume-group-name.*` , where .* signifies that the replication set contains more than one volume. If the volume is on the local system, the icon appears.
- **Secondary Volume** – Shows the secondary volume name. For replication sets that use volume groups, the secondary volume name is `volume-group-name.*` , where .* signifies that the replication set contains more than one volume. If the volume is on the local system, the icon appears.
- **Status** – Shows the status of the replication set:
  - `Not Ready` – The replication set is not ready for replications because the system is still preparing the replication set.
  - `Unsynchronized` – The primary and secondary volumes are unsynchronized because the system has prepared the replication set, but the initial replication has not run.
  - `Running` – A replication is in progress.
  - `Ready` – The replication set is ready for a replication.
  - `Suspended` – Replications have been suspended.
  - `Unknown` – This system cannot communicate with the primary system and thus cannot be sure of the current state of the replication set. Check the state of the primary system.
- **Last Successful Run** – Shows the date and time of the last successful replication.
- **Estimated Completion Time** – Shows the estimated date and time for the replication in progress to complete.

NOTE: If you change the time zone of the secondary system in a replication set whose primary and secondary systems are in different time zones, you must restart the system to enable management interfaces to show proper time values for replication operations.

To see more information about a replication set, hover the cursor over the replication set in the table. The Replication Set Information panel opens and displays detailed information about the replication set.

Table 20. Replication Sets panel

Panel	Information displayed
Replication Set Information	Name, serial number, status, primary volume group, primary volume group serial, secondary volume group, secondary volume group serial, peer connection, queue policy, queue count, secondary volume snapshot history, primary volume snapshot history, retention count, retention priority, snapshot basename, associated schedule name, current run progress, current run start time, current run estimated time to completion, current run transferred date, last successful run, last run start time, last run end time, last run transferred date, last run status, last run error status

Schedules table in the Volumes topic

For information about the schedules for a snapshot, select the snapshot in the volumes table. For information about the schedules for copy operations for a volume, select the volume in the volumes table. For information about the schedules for a replication set, select a volume for the replication set in the volumes table. If it is not already selected, select the Schedules tab. The schedules appear in the Schedules table.

The Schedules table shows the following schedule information. By default, the table shows 10 entries at a time.

- **Schedule Name** – Shows the name of the schedule.
- **Schedule Specification** – Shows the schedule settings for running the associated task.
- **Status** – Shows the status for the schedule:
  - `Uninitialized` – The schedule is not yet ready to run.
  - `Ready` – The schedule is ready to run at the next scheduled time.
  - `Suspended` – The schedule had an error and is holding in its current state.
  - `Expired` – The schedule exceeded a constraint and will not run again.
  - `Invalid` – The schedule is invalid.

- `Deleted` – The schedule has been deleted.

- **Task Type** – Shows the type of schedule:
  - `TakeSnapshot` – The schedule creates a snapshot of a source volume.
  - `ResetSnapshot` – The schedule deletes the data in the snapshot and resets it to the current data in the volume from which the snapshot was created. The snapshot's name and other volume characteristics are not changed.
  - `VolumeCopy` – The schedule copies a source volume to a new volume. It creates the destination volume you specify, which must be in a disk group owned by the same controller as the source volume. The source volume can be a base volume, standard volume, or a snapshot.
  - `Replicate` – The schedule replicates a virtual replication set to a remote system.

To see more information about a schedule, hover the cursor over the schedule in the table. The Schedule Information panel opens and displays detailed information about the schedule.

Table 21. Schedule Information panel

Panel	Information displayed
Schedule Information	Name, schedule specification, schedule status, next time, task name, task type, task status, task state, error message. Additional schedule information per task type: • Replication set - source volume, source volume serial • Reset snapshot - snapshot name, snapshot serial • Take snapshot - source volume, source volume serial, prefix, count, last created

Creating a virtual volume

You can add volumes to a virtual pool. You can create an individual virtual volume, multiple virtual volumes with different settings, or multiple virtual volumes with the same settings. In the latter case, the volumes will have the same base name with a numeric suffix (starting at 0000) to make each name unique and they will be placed in the same pool. You can also select a volume tier affinity setting to specify a tier for the volume data.

The Create Virtual Volumes panel contains a graphical representation of storage capacity for pools A and B. Each graph provides the number of existing volumes, free space, allocated and unallocated space, and committed and overcommitted space for pool A or B. The graph for the specified pool of the prospective new virtual volume also shows the impact of storage space and the prospective new volume on the pool.

The volumes table in the Volumes topic lists all volumes, volume groups, and snapshots. To see more information about a virtual volume, hover the cursor over the volume in the table. Viewing volumes contains more details about the Volume Information panel that appears.

Create virtual volumes

Perform the following steps to create virtual volumes:

1. Perform one of the following:
   - In the Pools topic, select a virtual pool in the pools table and select **Action > Create Volumes**.
   - In the Volumes topic, select **Action > Create Virtual Volumes**.

   The Create Virtual Volumes panel opens and shows the current capacity usage of each pool.

   NOTE: If a virtual pool does not exist, the option to create virtual volumes will be unavailable.

2. Optional: Change the volume name. The default is `Voln`, where n starts at 0001 and increments by one for each volume that has a default name. A volume name is case-sensitive and can have a maximum of 32 bytes. It cannot already exist in the system or include the following: `" , < \`

   If the name is used by another volume, the name is automatically changed to be unique. For example, `MyVolume` would change to `MyVolume0001`, or `Volume2` would change to Volume3.

3. Optional: Change the volume size, including unit of measurement. You can use any of the following units: MiB, GiB, TiB, MB, GB, TB. The default size is 100 GB. See the *System configuration limits* topic in the PowerVault Manager help for the maximum volume size that the system supports.

   Volume sizes are aligned to 4.2 MB (4 MiB) boundaries. When a volume is created or expanded, if the resulting size is less than 4.2 MB it will be increased to 4.2 MB. A value greater than 4.2 MB will be decreased to the nearest 4.2 MB boundary.

4. Optional: Change the number of volumes to create. See the *System configuration limits* topic in the PowerVault Manager help for the maximum number of volumes supported per pool.
5. Optional: Specify a volume tier affinity setting to automatically associate the volume data with a specific tier, moving all volume data to that tier whenever possible. The default is **No Affinity**. For more information about the volume tier affinity feature, see About automated tiered storage.
6. Optional: Select the pool in which to create the volume. The system load-balances volumes between the pools so the default may be A or B, whichever contains fewer volumes.
7. Optional: To create another volume with different settings, click **Add Row** and then change the settings. To remove the row that the cursor is in, click **Remove Row**.
8. Click **OK**.

   If creating the volume will overcommit the pool capacity, the system prompts you to configure event notification to be warned before the pool runs out of physical storage.
9. If the virtual volume exceeds the capacity:
   a. Click **OK** to continue. Otherwise, click **Cancel**. If you clicked **OK**, the volumes are created and the volumes table is updated.
   b. To close the confirmation panel, click **OK**.

Creating a linear volume

You can add volumes to a linear pool through the Pools and Volumes topics. You can create an individual linear volume or multiple copies of a linear volume with the same settings. In the latter case, the copies will have the same base name with a numeric suffix (starting at 0001) to make each name unique.

To see more information about a volume, hover the cursor over the volume in the volumes table. Viewing volumes contains more details about the Volume Information panel that appears.

Create linear volumes

Perform the following steps to create linear volumes:

1. Perform one of the following:
   - In the Pools topic, select a linear pool in the pools table and **Action > Create Volumes**.
   - In the Volumes topic, select **Action > Create Linear Volumes**.

   The Create Linear Volumes panel opens.
2. Optional: If you started creating the volume through the Volumes topic, you can change the linear pool for the volume.
3. Optional: Change the number of copies to create by modifying the default of 1. See the *System configuration limits* topic in the PowerVault Manager help for the maximum number of volumes per controller.

   NOTE: After selecting more than one copy, the next time that you place your cursor in another field, the Create Linear Volumes panel will collapse, so that the snapshot options no longer appear.
4. Optional: Change the volume name. The default is `pool-name_vn`, where n starts at 0001. A volume name is case-sensitive and can have a maximum of 32 bytes. It cannot already exist in the system or include the following: `" * , . < > \`

   If the name is used by another volume, the name is automatically changed to be unique. For example, `MyVolume` would change to `MyVolume0001`, or `Volume2` would change to `Volume3`.
5. Change the volume size, including unit of measurement. You can use any of the following units: MiB, GiB, TiB, MB, GB, TB. The maximum size depends on the unused capacity of the volume pool. See *System configuration limits* topic in the PowerVault Manager help for the maximum volume size that the system supports.

   Volume sizes are aligned to 4.2 MB (4 MiB) boundaries. When a volume is created or expanded, if the resulting size is less than 4.2 MB, it will be increased to 4.2 MB. A value greater than 4.2 MB, it will be decreased to the nearest 4.2 MB boundary.

   NOTE: Disk group space is allocated in 8 GiB memory chunks. There must be a minimum of 8 GiB remaining in the disk group and you should expect disk group space to be consumed by multiples of 8 GiB regardless of the volume size requested.
6. Click **OK**. The volumes are created, and the volumes table is updated.

Modifying a volume

You can change the name and cache settings for a volume. You can also expand a volume. If a virtual volume is not a secondary volume involved in replication, you can expand the size of the volume but not make it smaller. If a linear volume is neither the parent of a snapshot nor a primary or secondary volume, you can expand the size of the volume but not make it smaller. Because volume expansion does not require I/O to be stopped, the volume can continue to be used during expansion.

The volume cache settings consist of the write policy, cache optimization mode, and read-ahead size. For more information on volume cache settings, see About volume cache options.

CAUTION: Only change the volume cache settings if you fully understand how the host operating system, application, and adapter move data so that you can adjust the settings accordingly.

The volume tier affinity settings are No Affinity, Archive, and Performance. For more information about these settings, see Volume tier affinity features.

To see more information about a volume, hover the cursor over the volume in the table. Viewing volumes contains more details about the Volume Information panel that appears.

Modify a volume

Perform the following steps to modify a volume:

1. In the Volumes topic, select a volume in the volumes table.
2. Select **Action > Modify Volume**.
   The Modify Volume panel opens.
3. Optional: In the **New Name** field, type a new name for the volume. A volume name is case-sensitive and can have a maximum of 32 bytes. It cannot already exist in the system or include the following: " , < \
4. Optional: In the **Expand By** field, type the size by which to expand the volume. If overcommitting the physical capacity of the system is not allowed, the value cannot exceed the amount of free space in the storage pool. You can use any of the following units: MiB, GiB, TiB, MB, GB, TB.

   Volume sizes are aligned to 4.2 MB (4 MiB) boundaries. When a volume is created or expanded, if the resulting size is less than 4.2 MB it will be increased to 4.2 MB. A value greater than 4.2 MB will be decreased to the nearest 4.2 MB boundary.
5. Optional: In the Write Policy list, select **Write-back** or **Write-through**.
6. Optional: In the Write Optimization list, select **Standard** or **No-mirror**.
7. Optional: In the Read Ahead Size list, select **Adaptive**, **Disabled**, **Stripe**, or a specific size (512 KB; 1, 2, 4, 8, 16, or 32 MB).
8. Optional: In the Tier Affinity field, select **No Affinity**, **Archive**, or **Performance**. The default is **No Affinity**.
9. Click **OK**.

   If a change to the volume size overcommits the pool capacity, the system prompts you to configure event notification to be warned before the pool runs out of physical storage.
10. If the virtual volume exceeds the capacity:
    a. Click **OK** to continue. Otherwise, click **Cancel**. If you clicked **OK**, the volumes table is updated.
    b. To close the confirmation panel, click **OK**.

Copying a volume or snapshot

You can copy a linear or virtual volume or a virtual snapshot to a new virtual volume.

When using a linear volume as the source, the copy operation creates a transient snapshot, copies the data from the snapshot, and deletes the snapshot when the copy is complete. If the source is a snapshot, the copy operation is performed directly from the source; this source data may change if modified data is to be included in the copy and the snapshot is mounted and in use.

To ensure the integrity of a copy, unmount the source or, at minimum, perform a system cache flush on the host and refrain from writing to the source. Since the system cache flush is not natively supported on all operating systems, it is recommended to unmount temporarily. The copy will contain all data on disk at the time of the request, so if there is data in the OS cache, that data will not be copied. Unmounting the source forces the cache flush from the host OS. After the copy has started, it is safe to remount the source and resume I/O.

To ensure the integrity of a copy of a virtual snapshot with modified data, unmount the snapshot or perform a system cache flush. The snapshot will not be available for read or write access until the copy is complete, at which time you can remount the snapshot. If modified

write data is not to be included in the copy, then you may safely leave the snapshot mounted. During a copy using snapshot modified data, the system takes the snapshot off line.

Copy a virtual volume or snapshot

Perform the following steps to copy a virtual volume or snapshot:

1. In the Volumes topic, select a virtual volume or snapshot.
2. Select **Action > Copy Volume**.
   The Copy Volume panel opens.
3. Optional: In the **New Volume** field, change the name for the new volume. The default is *volume-namecn*, where n starts at 01.

   A volume name is case-sensitive and can have a maximum of 32 bytes. It cannot already exist in the system or include the following: ",<\

   If the name is used by another volume, you are prompted to type a different name.
4. In the **Residing on Pool** field, select the pool in which to create the copy. Selecting **Auto** copies the destination volume to the same pool as the source volume.
5. Click **OK**.
   A confirmation panel appears.
6. Click **OK**.

Abort a volume copy

You can abort a volume copy operation. When the operation is complete, the destination volume is deleted.

1. In the Volumes topic, select a volume that is currently being copied.
2. Select **Menu > Abort Volume Copy**.
3. Click **Yes** to abort the operation.

Adding volumes to a volume group

You can add virtual volumes to a new or existing virtual volume group. All volumes in a volume group must be in the same pool.

To add a volume to a volume group, the volume must have the same mappings as all other members of the group. This means that the volume must be mapped with the same access and port settings to the same initiators, hosts, or host groups.

If the volume group is part of a replication set, you cannot add or remove volumes to or from it. If a volume group is being replicated, the maximum number of volumes that can exist in the group is 16.

NOTE: You cannot map LUN 0 for a SAS initiator. You can create a maximum of 1024 volumes, but because the supported LUN range is 1 through 1023, only 1023 volumes can be mapped using default mapping. Using explicit mapping, all volumes can be mapped.

Add volumes to a volume group

Perform the following steps to add volumes to a volume group:

1. In the Volumes topic, select up to 20 volumes to add to a volume group.
2. Select **Action > Add to Volume Group**.
   The **Add to Volume Group** dialog box is displayed.
3. Perform one of the following:
   - To use an existing volume group, select it from the **Volume Groups** field.
   - To create a volume group, type a name for the volume group in the **Volume Groups** field. A volume group name is case-sensitive and can have a maximum of 32 bytes. It cannot include the following: " , < \
4. Click **OK**.

Removing volumes from a volume group

You can remove volumes from a volume group. You cannot remove all volumes from a group. At least one volume must remain. Removing a volume from a volume group will ungroup the volumes but will not delete them. To remove all volumes from a volume group, see Removing volume groups.

To see more information about a volume, hover the cursor over the volume in the table. Viewing volumes contains more details about the Volume Information panel that appears.

Remove volumes from a volume group

1. In the Volumes topic, select the volumes to remove from a volume group.
2. Select **Action > Remove from Volume Group**. The Remove from Volume Group panel opens and lists the volumes to be removed.
3. Click **OK**. For the selected volumes, the Group value changes to --.

Renaming a volume group

You can rename a volume group unless it is part of a replication set. To see more information about a volume, hover the cursor over the volume in the table. Viewing volumes contains more details about the Volume Information panel that appears, including how to view volumes and volume groups that are part of a replications set.

Rename a volume group

1. In the Volumes topic, select a volume that belongs to the volume group that you want to rename.
2. Select **Action > Rename Volume Group**. The Rename Volume Group panel opens.
3. In the **New Group Name** field, enter a new name for the volume group. A volume group name is case sensitive and can have a maximum of 32 bytes. It cannot include the following: " , < \

   If the name is used by another volume group, you are prompted to enter a different name.
4. Click **OK**. The volumes table is updated.

Remove volume groups

You can remove volume groups. When you remove a volume group, you can optionally delete its volumes. Otherwise, removing a volume group will ungroup its volumes but will not delete them.

CAUTION: Deleting a volume removes its mappings and schedules and deletes its data.

To see more information about a volume, hover the cursor over the volume in the table. Viewing volumes contains more details about the Volume Information panel that appears.

Remove volume groups only

1. In the Volumes topic, select a volume that belongs to each volume group that you want to remove. You can remove 1 through 100 volume groups at a time.
2. Select **Action > Remove Volume Group**. The Remove Volume Group panel opens and lists the volume groups to be removed.
3. Click **OK**. For volumes that were in the selected volume groups, the Volume Groups value changes to --.

Remove volume groups and their volumes

1. Verify that hosts are not accessing the volumes that you want to delete.
2. In the Volumes topic, select a volume that belongs to each volume group that you want to remove. You can remove 1 through 100 volume groups at a time.
3. Select **Action > Remove Volume Group**. The Remove Volume Group panel opens and lists the volume groups to be removed.
4. Select the **Delete Volumes** check box.
5. Click **OK**. A confirmation panel appears.

6. Click **Yes** to continue. Otherwise, click **No**.
   If you clicked Yes, the volume groups and their volumes are deleted and the volumes table is updated.

Rolling back a virtual volume

You can replace the data of a source volume or virtual snapshot with the data of a snapshot that was created from it.

CAUTION: When you perform a rollback, the data that existed on the volume is replaced by the data on the snapshot. All data on the volume written since the snapshot was created is lost. As a precaution, create a snapshot of the volume before starting a rollback.

Only one rollback is allowed on the same volume at one time. Additional rollbacks are queued until the current rollback is complete. However, after the rollback is requested, the volume is available for use as if the rollback has already completed.

For volumes and snapshots, if the contents of the selected snapshot have changed since it was created, the modified contents will overwrite those of the source volume or snapshot during the rollback. Since virtual snapshots are copies of a point in time, they cannot be reverted. If you want a snapshot to provide the capability to "revert" the contents of the source volume or snapshot to when the snapshot was created, create a snapshot for this purpose and archive it so you do not change the contents.

To see more information about a volume, hover the cursor over the volume in the table. See Viewing volumes for more information about the Volume Information panel that appears.

Roll back a volume

Perform the following steps to roll back a volume:

1. Unmount the volume from hosts.
2. In the Volumes topic, select the volume to roll back.
3. Select **Action > Rollback Volume**. The Rollback Volume panel opens and lists snapshots of the volume.
4. Select the snapshot to roll back to.
5. Click **OK**.
   A confirmation panel appears.
6. Click **OK**.
   You can remount the volume after the rollback completes.

Deleting volumes and snapshots

You can delete volumes and snapshots. You can delete a volume that has no child snapshots. You cannot delete a volume that is part of a replication set.

CAUTION: Deleting a volume or snapshot removes its mappings and schedules and deletes its data.

NOTE: To delete a volume with one or more snapshots, or a snapshot with child snapshots, you must delete the snapshots or child snapshots first.

To see more information about a volume or snapshot, hover the cursor over the item in the volumes table.

You can view additional snapshot information by hovering the cursor over the snapshot in the Related Snapshots table. See Viewing volumes for more information about the Volume Information and Snapshot Information panels that appear.

Delete volumes and snapshots

1. Verify that hosts are not accessing the volumes and snapshots that you want to delete.
2. In the Volumes topic, select 1 through 100 items (volumes, snapshots, or both) to delete.
3. Select **Action > Delete Volumes**. The Delete Volumes panel opens with a list of the items to be deleted.
4. Click **Delete**. The items are deleted and the volumes table is updated.

Creating snapshots

You can create snapshots of selected virtual volumes or of virtual snapshots. You can create snapshots immediately or schedule snapshot creation.

If the large pools feature is enabled, through use of the `large-pools` parameter of the set `advanced-settings` CLI command, the maximum number of volumes in a snapshot tree is limited to 9, base volume plus 8 snapshots. The maximum number of volumes per snapshot will decrease to fewer than 9 if more than 3 replication sets are defined for volumes in the snapshot tree. If creating a snapshot will exceed the limit, you will be unable to create the snapshot unless you delete a snapshot first.

To see more information about a volume, snap pool linear storage only, or snapshot, hover the cursor over the item in the volumes table.

You can view additional snapshot information by hovering the cursor over the snapshot in the Snapshots table. Viewing volumes contains more details about the Volume Information and Snapshot Information panels that appear.

Create virtual snapshots

1. In the Volumes topic, select from 1 to 16 virtual volumes or snapshots.

   NOTE: You can also select a combination of virtual volumes and snapshots.

2. Select **Action > Create Snapshot**.
   The Create Snapshots panel opens.
3. Optional: In the **Snapshot Name** field, change the name for the snapshot. The default is `volume-name_sn`, where `n` starts at 0001. A snapshot name is case sensitive and can have a maximum of 32 bytes. It cannot already exist in the system or include the following: " , < \
   If the name is used by another snapshot, you are prompted to enter a different name.
4. Optional: If you want to schedule a create-snapshot task, perform the following:
   - Select the **Scheduled** check box.
   - Optional: Change the default prefix to identify snapshots created by this task. The default is `volumesn`, where `n` starts at 01. The prefix is case sensitive and can have a maximum of 26 bytes. It cannot already exist in the system or include the following: " , < \

   Scheduled snapshots are named `prefix_Sn`, where `n` starts at 0001.

   - Optional: Select the number of snapshots to retain from either 1 through 8 if the large pools feature is enabled, or 1 through 32 if the large pools feature is disabled. The default is 1. When the task runs, the retention count is compared with the number of existing snapshots:
     - If the retention count has not been reached, the snapshot is created.
     - If the retention count has been reached, the oldest snapshot for the volume is unmapped, reset, and renamed to the next name in the sequence.
   - Specify a date and a time at least five minutes in the future to run the task. The date must use the format `yyyy-mm-dd`. The time must use the format hh:mm followed by either AM, PM, or 24H (24-hour clock). For example, 13:00 24H is the same as 1:00 PM.
   - Optional: If you want the task to run more than once, perform the following:
     - Select the **Repeat** check box and specify how often the task should run.
     - Optional: Select the **End** check box to specify when the task should stop running.
     - Optional: Select the **Time Constraint** check box to specify a time range within which the task should run.
     - Optional: Select the **Date Constrain**t check box to specify days when the task should run. Ensure that this constraint includes the start date.
5. Click **OK**.
   - If **Scheduled** is not selected, the snapshot is created.
   - If **Scheduled** is selected, the schedule is created and can be viewed in the Manage Schedules panel. For information on modifying or deleting schedules through this panel, see Managing scheduled tasks.

Resetting a snapshot

As an alternative to taking a new snapshot of a volume, you can replace the data in a standard snapshot with the current data in the source volume. The snapshot name and mappings are not changed.

This feature is supported for all snapshots in a tree hierarchy. However, a virtual snapshot can only be reset to the parent volume or snapshot from which it was created.

CAUTION: To avoid data corruption, unmount a snapshot from hosts before resetting the snapshot.

You can reset a snapshot immediately. You also have the option of scheduling a reset-snapshot task.

To see more information about a snapshot, hover the cursor over the item in the volumes table. You can view different snapshot information by hovering the cursor over the snapshot in the Snapshots table. See Viewing volumes for more details about the Volume Information and Snapshot Information panels that appear.

Reset a snapshot

Perform the following steps to reset a snapshot:

1. Unmount the snapshot from hosts.
2. In the Volumes topic, select a snapshot.
3. Select **Action > Reset Snapshot**.
   The Reset Snapshot panel opens.
4. Optional: To schedule a reset task, perform the following steps:
   - Select the **Schedule** check box.
   - Specify a date and time at least five minutes in the future to run the task. The date must use the format *yyyy-mm-dd*. The time must use the format *hh:mm* and include either **AM, PM**, or **24H** (24-hour clock). For example, 13:00 24H is the same as 1:00 PM.
   - Optional: If you want the task to run more than once:
     - Select the **Repeat** check box and specify how often the task should run.
     - Optional: Specify when the task should stop running.
     - Optional: Specify a time range within which the task should run.
     - Optional: Specify days when the task should run. Ensure that this constraint includes the start date.
5. Click **OK**.
   - If the **Schedule** check box was not selected, a **Confirm Operation** dialog box is displayed.

     Click **OK** to reset the snapshot.

     NOTE: You can remount the snapshot after it is reset.
   - If the **Schedule** check box was selected, the reset snapshot schedule is created and a **Success** dialog box is displayed.

     Click **OK** to close the **Success** dialog box. The schedule can be viewed in the Manage Schedules panel, as described in Managing scheduled tasks.

     NOTE: Remember to unmount the snapshot before the scheduled task runs.

Creating a replication set from the Volumes topic

You can create a replication set, which specifies the components of a replication. The Create Replication Set panel enables you to create replication sets. You can access this panel from both the Replications and Volumes topics.

Performing this action creates the replication set and the infrastructure for the replication set. For a selected volume, snapshot, or volume group, the action creates a secondary volume or volume group and the internal snapshots required to support replications. By default, the secondary volume or volume group and infrastructure are created in the pool corresponding to the one for the primary volume or volume group (A or B). Optionally, you can select the other pool.

A peer connection must be defined to create and use a replication set. A replication set can specify only one peer connection and pool. When creating a replication set, communication between the peer connection systems must be operational during the entire process.

If a volume group is part of a replication set, volumes cannot be added to or deleted from the volume group.

If a replication set is deleted, the internal snapshots created by the system for replication are also deleted. After the replication set is deleted, the primary and secondary volumes can be used like any other base volumes or volume groups.

Primary volumes and volume groups

The volume, volume group, or snapshot that will be replicated is called the *primary volume* or *volume group*. It can belong to only one replication set. If the volume group is already in a replication set, individual volumes may not be included in separate replication sets. Conversely, if a volume that is a member of a volume group is already in a replication set, its volume group cannot be included in a separate replication set.

The maximum number of individual volumes and snapshots that can be replicated is 32 in total. If a volume group is being replicated, the maximum number of volumes that can exist in the group is 16.

Using a volume group for a replication set enables you to make sure that the contents of multiple volumes are synchronized at the same time. When a volume group is replicated, snapshots of all of the volumes are created simultaneously. In doing so, it functions as a consistency group, ensuring consistent copies of a group of volumes. The snapshots are then replicated as a group. Though the snapshots may differ in size, replication of the volume group is not complete until all of the snapshots are replicated.

Secondary volumes and volume groups

When the replication set is created—either through the CLI or the PowerVault Manager —secondary volumes and volume groups are created automatically. Secondary volumes and volume groups cannot be mapped, moved, expanded, deleted, or participate in a rollback operation. Create a snapshot of the secondary volume or volume group and use the snapshot for mapping and accessing data.

Queuing replications

You can specify the action to take when a replication is running and a new replication is requested.

- Discard. Discard the new replication request.
- Queue Latest. Take a snapshot of the primary volume and queue the new replication request. If the queue contained an older replication request, discard that older request. A maximum of one replication can be queued. This is the default.

NOTE: If the queue policy is set to `Queue Latest` and a replication is running and another is queued, you cannot change the queue policy to discard. You must manually remove the queued replication before you can change the policy.

Maintaining replication snapshot history from the Volumes topic

A replication set can be configured to maintain a replication snapshot history. As part of handling a replication, the replication set will automatically take a snapshot of the primary or secondary volumes, or both, thereby creating a history of data that has been replicated over time. This feature can be enabled for a secondary volume or for a primary volume and its secondary volume, but not for a volume group.

When this feature is enabled:

- For a primary volume, when a replication starts it will create a snapshot of the data image being replicated.
- For a secondary volume, when a replication successfully completes it will create a snapshot of the data image just transferred to the secondary volume. (This is in contrast to the primary volume snapshot, which is created before the sync.) If replication does not complete, a snapshot will not be created.
- You can set the number of snapshots to retain from 1 through 16, referred to as the snapshot retention count. This setting applies to management of snapshots for both the primary and secondary volume and can be changed at any time. Its value must be greater than the number of existing snapshots in the replication set, regardless of whether snapshot history is enabled. If you select a snapshot retention count value that is less than the current number of snapshots, an error message is displayed. Thus, you must manually delete the excess snapshots before reducing the snapshot count setting. When the snapshot count is exceeded, the oldest unmapped snapshot will be discarded automatically.
- The snapshots are named `basename_nnnn` where `_nnnn` starts at 0000 and increments for each subsequent snapshot. If primary volume snapshots are enabled, snapshots with the same name will exist on the primary and secondary systems. The snapshot number is incremented each time a replication is requested, whether or not the replication completes — for example, if the replication was queued and subsequently removed from the queue.

- If the replication set is deleted, any existing snapshots automatically created by snapshot history rules will not be deleted. You will be able to manage those snapshots like any other snapshots.
- Manually creating a snapshot will not increase the snapshot count associated with the snapshot history. Manually created snapshots are not managed by the snapshot history feature. The snapshot history feature generates a new name for the snapshot that it intends to create. If a volume of that name already exists, the snapshot history feature will not overwrite that existing volume. Snapshot numbering will continue to increment, so the next time the snapshot history feature runs, the new snapshot name will not conflict with that existing volume name.
- A snapshot created by this feature is counted against the system-wide maximum snapshots limit, with the following result:
  - If the snapshot count is reached before the system limit then the snapshot history is unchanged.
  - If the system limit is reached before the snapshot count then the snapshot history stops adding or updating snapshots.
- A mapped snapshot history snapshot will not be deleted until after it is unmapped.
- The snapshot basename and snapshot retention count settings only take effect when snapshot history is set to secondary or both, although these settings can be changed at any time.
- You can set the retention priority for snapshots to the following. In a snapshot tree, only leaf snapshots can be deleted automatically.

Table 22. Snapshot retention priority

Retention priority	Description
never-delete	Snapshots will never be deleted automatically to make space. The oldest snapshot in the snapshot history will be deleted once the snapshot count has been exceeded. This is the default.
high	Snapshots can be deleted after all eligible medium-priority snapshots have been deleted.
medium	Snapshots can be deleted after all eligible low-priority snapshots have been deleted.
low	Snapshots can be deleted. This parameter is unrelated to snapshot history, and because the default is never delete, snapshot history snapshots will normally not be affected in a low virtual memory situation.

When this option is disabled, snapshot history will not be kept. If this option is disabled after a replication set has been established, any existing snapshots will be kept, but not updated.

Create a replication set from the Volumes topic

1. In the volumes table, select a volume or snapshot to use as the primary volume.
2. Select **Action > Create Replication Set**. The Create Replication Set panel appears.
3. If the selected volume is in a volume group, source options appear.
   - To replicate the selected volume only, select **Single Volume**. This option is the default.
   - To replicate all volumes in the volume group, select **Volume Group**.
4. Enter a name for the replication set. The name is case sensitive and can have a maximum of 32 bytes. It cannot already exist in the system, include leading or trailing spaces, or include the following characters: " , < \
5. Optional: Select a peer system to use as the secondary system for the replication set.
6. Optional: Select a pool on the secondary system. By default, the pool that corresponds with the pool in which the primary volume resides is selected. The selected pool must exist on the remote system.
7. Optional: If **Single Volume** is selected, enter a name for the secondary volume. The default name is the name of the primary volume. The name is case sensitive and can have a maximum of 32 bytes. It cannot already exist on the secondary system or include the following: " , < \
8. Optional: Specify the **Queue Policy** action to take when a replication is running and a new replication is requested.
9. Optional: Select the **Secondary Volume Snapshot History** check box to keep a snapshot history on the secondary system for the secondary volume.
   - Set the **Retention Count** to specify the number of snapshots to retain.
   - Modify the **Snapshot Basename** to change the snapshot name. The name is case sensitive and can have a maximum of 26 bytes. It cannot already exist in the system or include the following characters: " , < \
   - Set the **Retention Priority** to specify the snapshot retention priority.
   - Optional: Select the **Primary Volume Snapshot History** check box to keep a snapshot history for the primary volume on the primary system
10. Optional: Select the **Scheduled** check box to schedule recurring replications.
11. Click **OK**.
12. In the success dialog box:

- If you selected the Scheduled check box, click **OK**. The Schedule Replications panel opens and you can set the options to create a schedule for replications. For more information on scheduling replications, see Initiating or scheduling a replication from the Volumes topic.
- Otherwise, you have the option to perform the first replication. Click **Yes** to begin the first replication, or click **No** to initiate the first replication later.

Initiating or scheduling a replication from the Volumes topic

After you have created a replication set, you can copy the selected volume or volume group on the primary system to the secondary system by initiating replication. The first time that you initiate replication, a full copy of the allocated pages for the volume or volume group is made to the secondary system. Thereafter, the primary system only sends the contents that have changed since the last replication.

You can manually initiate replication or create a scheduled task to initiate it automatically from both the Replications and Volumes topics. You can initiate replications only from a replication set's primary system. For information on modifying or deleting a replication schedule, see Managing replication schedules from the Volumes topic.

NOTE: If you change the time zone of the secondary system in a replication set whose primary and secondary systems are in different time zones, you must restart the system to enable management interfaces to show proper time values for replication operations.

If a replication fails, the system suspends the replication set. The replication operation will attempt to resume if it has been more than 10 minutes since the replication set was suspended. If the operation has not succeeded after six attempts using the 10-minute interval, it will switch to trying to resume if it has been over an hour and the peer connection is healthy.

NOTE: Host port evaluation is done at the start or resumption of each replication operation. At most, two ports will be used. Ports with optimized paths will be used first. Ports with unoptimized paths will be used if no optimized path exists. If only one port has an optimized path, then only that port will be used. The replication will not use another available port until all currently used ports become unavailable.

NOTE: If a single host port loses connectivity, event 112 will be logged. Because a peer connection is likely to be associated with multiple host ports, the loss of a single host port may degrade performance but usually will not cause the peer connection to be inaccessible.

Manually initiate replication from the Volumes topic

NOTE: If CHAP is enabled on one system within a peer connection, be sure that CHAP is configured properly on the corresponding peer system before initiating this operation. For more information about configuring CHAP, see CHAP and replication.

1. In the Volumes topic, select a replication set in the Replication Sets table.
2. Select **Action > Replicate**.
   The Replicate panel opens.
3. Click **OK**.
   - If a replication is not in progress, the local system begins replicating the contents of the replication set volume to the remote system and the status of the replication set changes to **Running**.
   - If a replication is already in progress, then the outcome of this replication request depends upon the Queue Policy setting specified in the Create Replication Set panel. For more information on setting the queue policy, see Queuing replications.

Schedule a replication from the Volumes topic

1. In the Volumes topic, select a replication set in the Replication Sets table.
2. Select **Action > Replicate**. The Replicate panel opens.
3. Select the **Schedule** check box.
4. Enter a name for the replication schedule task. The name is case sensitive and can have a maximum of 32 bytes. It cannot already exist in the system or include the following: " , < \
5. Optional: If you want to create a replication of the last snapshot in the primary volume, select the **Last Snapshot** check box.

6. Specify a date and a time in the future to be the first instance when the scheduled task will run, and to be the starting point for any specified recurrence.
   - To set the **Date** value, enter the current date in the format *YYYY-MM-DD*.
   - To set the **Time** value, enter two-digit values for the hour and minutes and select either **AM, PM**, or **24H** (24-hour clock). The minimum interval is one hour.
7. Optional: If you want the task to run more than once, select the **Repeat** check box.
   - Specify how often the task should repeat. Enter a number and select the appropriate time unit. Replications can recur no less than 30 minutes apart.
   - Either make sure the **End** check box is cleared, which allows the schedule to run indefinitely, or select the check box to specify when the schedule ends. To then specify an end date and time, select the **On** option, and specify when the schedule should stop running, or select the **After** option, and specify the number of replications that can occur before the schedule stops running.
   - Either make sure the **Time Constraint** check box is cleared, which allows the schedule to run at any time, or select the check box to specify a time range within which the schedule should run.
   - Either make sure the **Date Constraint** check box is cleared, which allows the schedule to run on any day, or select the check box to specify the days when the schedule should run.
8. Click **OK**. The schedule is created.

Manage replication schedules from the Volumes topic

You can modify or delete scheduled replication tasks on the primary system.

Modify scheduled replication tasks from the Volumes topic

1. From the Replication Sets table on the primary system, select a replication set that has an associated schedule.
2. Select **Action > Manage Schedules**. The Manage Schedules panel opens.
3. Select the schedule to modify.
   The schedule settings appear at the bottom of the panel.
4. If you want to create a replication of the last snapshot in the primary volume, select the **Last Snapshot** check box.
   At the time of the replication, the snapshot must exist. This snapshot may have been created either manually or by scheduling the snapshot.
   NOTE: This option is unavailable when replicating volume groups.
5. Specify a date and a time in the future to specify when to run the scheduled task. This date and time is also the starting point for any specified recurrence.
   - To set the **Date** value, enter the current date in the format *YYYY-MM-DD*.
   - To set the **Time** value, enter two-digit values for the hour and minutes and select either **AM, PM**, or **24H** (24-hour clock).
6. If you want the task to run more than once, select the **Repeat** check box.
   - Specify how often the task should repeat. Enter a number, and select the appropriate time unit. Replications can recur no less than 30 minutes apart.
   - To allow the schedule to run without an end date, clear the **End** check box. To specify when the schedule should stop running, select the **End** check box
   - To allow the schedule to run at any time, clear the **Time Constraint** check box. To specify a time range within which the schedule can run, select the **Time Constraint** check box.
   - To allow the schedule to run on any day, clear the **Date Constraint** check box. To specify the days when the schedule can run, select the **Date Constraint** check box.
7. Click **Apply**.
   A confirmation panel appears.
8. Click **OK**.

Delete a schedule from the Volumes topic

Perform the following steps to delete a schedule from the Volumes topic:

1. Select **Action > Manage Schedules**.
   The Manage Schedules panel opens.
2. Select the schedule to delete.
3. Click **Delete Schedule**.
   A confirmation panel appears.
4. Click **OK**.

7

Working in the Mappings topic

Topics:

Viewing mappings

The Mapping topic shows a tabular view of information about mappings that are defined in the system. By default, the table shows 20 entries at a time and is sorted first by host and second by volume.

The mapping table shows the following information:

- Group.Host.Nickname. Identifies the initiators to which the mapping applies:
  - All Other Initiators. The mapping applies to all initiators that are not explicitly mapped with different settings.
  - `initiator-name`—The mapping applies to the initiator only.
  - `initiator-ID`—The mapping applies to the initiator only, and the initiator has no nickname.
  - `host-name.*`—The mapping applies to all initiators in the host.
  - `host-group-name.*.*`—The mapping applies to all hosts in this group.
- Volume. Identifies the volumes to which the mapping applies:
  - `volume-name`—The mapping applies to the volume only.
  - `volume-group-name.*`—The mapping applies to all volumes in the volume group.
- Access. Shows the type of access assigned to the mapping:
  - `read-write`—The mapping permits read and write access to volumes.
  - `read-only`—The mapping permits read access to volumes.
  - `no-access`—The mapping prevents access to volumes.
- LUN. Shows whether the mapping uses a single LUN or a range of LUNs (indicated by *).
- Ports. Lists the controller host ports to which the mapping applies. Each number represents corresponding ports on both controllers.

To display more information about a mapping, see View map details on page 110.

Mapping initiators and volumes

You can map initiators and volumes to control host access to volumes unless the volume is the secondary volume of a replication set. Mapping applies to hosts and host groups as well as initiators, and to virtual snapshots and volume groups as well as volumes. For the purposes of brevity, the terms *initiator* and *volumes* will stand in for all possibilities, unless otherwise stated. By default, volumes are not mapped.

If a volume is mapped to ID All Other Initiators, this is its default mapping. The *default mapping* enables all connected initiators to see the volume using the specified access mode, LUN, and port settings. The advantage of a default mapping is that all connected initiators can discover the volume with no additional work by the administrator. The disadvantage is that all connected initiators can discover the volume with no restrictions. Therefore, this process is not recommended for specialized volumes that require restricted access. Also, to avoid multiple hosts mounting the volume and causing corruption, the hosts must be cooperatively managed, such as by using cluster software.

If multiple hosts mount a volume without being cooperatively managed, volume data is at risk for corruption. To control access by specific hosts, you can create an *explicit mapping*. An explicit mapping can use different access mode, LUN, and port settings to allow or prevent access by a host to a volume, overriding the default mapping. When an explicit mapping is deleted, the volume's default mapping takes effect.

The storage system uses Unified LUN Presentation (ULP), which can expose all LUNs through all host ports on both controllers. The interconnect information is managed in the controller firmware. ULP appears to the host as an active-active storage system where the host can choose any available path to access a LUN regardless of disk group ownership. When ULP is in use, the controllers' operating/

redundancy mode is shown as Active-Active ULP. ULP uses the T10 Technical Committee of INCITS Asymmetric Logical Unit Access (ALUA) extensions, in SPC-3, to negotiate paths with aware host systems. Unaware host systems see all paths as being equal.

If a host group or host is mapped to a volume or volume group, all of the initiators within that group will have an individual map to each volume that makes up the request. As long as the group entity is mapped consistently, that set of individual maps will be represented as a grouped mapping. If any individual map within that group is modified, the grouped mapping will no longer be consistent, and it will no longer appear in the PowerVault Manager. It will be replaced in the PowerVault Manager with all of the individual maps.

CAUTION: Volume mapping changes take effect immediately. Make changes that limit access to volumes when the volumes are not in use. Before changing a LUN, be sure to unmount the volume.

NOTE: The secondary volume of a replication set cannot be mapped. Create a snapshot of the secondary volume or volume group and use the snapshot for mapping and accessing data.

Map initiators and volumes

1. Perform one of the following:
   - In the Hosts topic, select the initiators to map and select **Action > Map Initiators**.
   - In the Volumes topic, select the volumes to map and select **Action > Map Volumes**.
   - In the Mapping topic, select **Map** to create a new mapping.
   - In the Mapping topic, select one or more mappings to modify or delete and select **Action > Map**. You can also create a new mapping.

   The Map panel opens and shows two tables side-by-side that list available initiators and volumes. You can use these tables to create mappings. There is also a table underneath the host and volume tables that lists mappings. After you create a mapping and before you save it, the mapping appears in the mappings table and you can modify its settings or delete it.

   The Available Host Groups, Hosts, and Initiators table shows one or more of the following rows:

Table 23. Available host groups, hosts, and initiators

Row description	Group	Host	Nickname	ID
A row with these values always appears. Select this row to apply map settings to all initiators and create a default mapping.	-	-	(blank)	All Other Initiators
A row with these values appears for an initiator that is grouped into a host. Select this row to apply map settings to all initiators in this host.	-	*host-name*	*	*
A row with these values appears for an initiator that is grouped into a host group. Select this row to apply map settings to all initiators in this host group.	*host-group-name*	*	*	*
A row with these values appears for each initiator. Select this row to apply map settings to this initiator.	- or host - *host-group-name*	- or *host-name*	(blank) or *initiator-nick name*	*initiator-ID*

   The Available Volume Groups and Volumes table shows one or more of the following rows:

Table 24. Available volume groups and volumes

Row description	Group	Name	Type
A row with these values appears for a volume/snapshot that is grouped into a volume group. Select this row to apply map settings to all volumes/ snapshots in this volume group.	*volume-group-name*	*	Group
A row with these values appears for each volume/ snapshot. Select this row to apply map settings to this volume/snapshot.	-	*volume-name*	*volume-type*

- When you select one or more host groups, hosts, or initiators in the Hosts topic, the items appears in the Available Host Groups, Hosts, and Initiators table while all available volumes, volume groups, and snapshots appear in the Available Volume Groups and Volumes table.
- The converse is true when you select one or more volumes, volume groups, or snapshots in the Available Volume Groups and Volumes table.
- When you open the Map panel through the Mapping topic without selecting a mapping, both tables are fully populated with all available items.
- When you select a mapping in the mapping table, it appears in the list of mappings below the above two tables. Also, both tables are fully populated.

2. Perform one of the following:
   - If nothing was pre-selected, select one or more initiators and one or more volumes to map and click the **Map** button.
   - If initiators were pre-selected, select volumes to map to those initiators and click the **Map** button.
   - If volumes were pre-selected, select initiators to map to those volumes and click the **Map** button.
   - If maps were pre-selected, they already appear in the mapping table and a **Map** button appears.

   For each pairing of selected initiators and volumes, a row appears in the mapping table at the bottom of the panel. At this time, no further mappings can be added to the list. Mappings in the list can be modified—including the mapping's mode, LUN, or ports, or they can be deleted.

   NOTE: Once a set of mappings between initiators and volumes have been defined using the Map button, the button changes from Map to Reset. If mappings have been pre-selected, the Reset button, not the Map button, appears.
3. Perform any of the following:
   - To immediately remove a row from the table, in the Action column, select **Remove Row**.
   - To delete an existing mapping, in the Action column, select **Delete**.
   - To edit a mapping, set the following options:
     - **Mode**. The access mode can specify read-write access, read-only access, or no access to a volume. The default is read-write. When a mapping specifies no access, the volume is masked, which means it is not visible to associated initiators. Masking is useful to override an existing default map that allows open access so that access is denied only to specific initiators. To allow access to specific hosts and deny access to all other hosts, create explicit maps to those hosts. For example, an engineering volume could be mapped with read-write access for the engineering server and read-only access for servers used by other departments.
     - **LUN**. The LUN identifies the volume to a host. The default is the lowest available LUN. Both controllers share one set of LUNs, and any unused LUN can be assigned to a mapping. However, each LUN is generally only used once as a default LUN. For example, if LUN 5 is the default for Volume1, no other volume in the storage system can use LUN 5 on the same port as its default LUN. For explicit mappings, the rules differ: LUNs used in default mappings can be reused in explicit mappings for other volumes and other hosts.

       NOTE: When mapping a volume to a host with the Linux ext3 file system, specify read-write access. Otherwise, the file system will be unable to mount the volume and will report an error such as "unknown partition table."
     - **Ports**. Port selections specify controller host ports through which initiators are permitted to access, or are prevented from accessing, the volume. Selecting a port number automatically selects the corresponding port in each controller.
   - To save a new mapping or edits to an existing mapping, in the Action column, select **Save**.
   - To clear the mapping table and discard any changes, click **Reset**.

4. Once the list is correct, to apply changes, click **Apply** or **OK**.
   A confirmation panel appears.

   To discard the changes instead of applying them, click **Reset**.
5. Click **Yes** to continue. Otherwise, click **No**. If you clicked Yes, the mapping changes are processed.
6. To close the panel, click **Cancel**.

Remove mappings

You can remove one or more selected mappings between initiators and volumes.

1. Perform one of the following:
   - In the Mapping topic, select one or more mappings from the table.
   - In the Volumes topic, select at least one mapping in the Related Maps table.
2. Select **Action > Remove Mappings**. The Remove Mappings panel shows the selected mappings.
3. Click **OK**. The selected mappings are removed.

Removing all mappings

You can remove all mappings between initiators and volumes from the system.

1. In the Mapping topic, select one or more mappings from the table.
2. Select **Action > Remove All Mappings**. The Remove All Mappings panel opens.
3. Click **OK**. The mappings are removed from the system.

View map details

In the Hosts, Volumes, and Mapping topics, you can see basic information about mappings between hosts and volumes.

1. Perform one of the following:
   - In the Hosts or Volumes topic, in the Related Maps table, select at least one mapping.
   - In the Mapping topic, in the mapping table, select at least one mapping.
2. Select **Action > View Map Details**. The Map Details panel opens and shows the following information.
   - Host Group. Identifies the host group to which the mapping applies:
     - `-`. The mapping does not apply to a host group.
     - `host-group-name`. The mapping applies to all hosts in this host group.
   - Host. Identifies the host to which the mapping applies:
     - `-`. The mapping does not apply to a host.
     - `host-name`. The mapping applies to all initiators in this host.
   - Nickname. Shows the nickname of the initiator, if a nickname is assigned. Otherwise, this field is blank.
   - Initiator ID. Shows the WWN of an FC or SAS initiator or the IQN of an iSCSI initiator.
   - Volume Group. Identifies the volumes to which the mapping applies:
     - `-`. The mapping does not apply to a volume group.
     - `volume-group-name`. The mapping applies to all volumes in this volume group.
   - Volume. Identifies the volume to which the mapping applies.
   - Access. Shows the type of access assigned to the mapping:
     - `read-write`—The mapping permits read and write access to volumes.
     - `read-only`—The mapping permits read access to volumes.
     - `no-access`—The mapping prevents access to volumes.
   - LUN. Shows whether the mapping uses a single LUN or a range of LUNs (indicated by *). By default, the table is sorted by this column.
   - Ports. Lists the controller host ports to which the mapping applies. Each number represents corresponding ports on both controllers.
3. Click **OK**.

8

Working in the Replications topic

Topics:

About replicating virtual volumes in the Replications topic

Replication for virtual storage provides a remote copy of a volume, volume group, or snapshot—thereafter known as *volume*—on a remote system by periodically updating the remote copy to contain a point-in-time consistent image of a source volume. After an initial image has been replicated, subsequent replications only send changed data to the remote system. All replications, including the initial one, only replicate data that has been written as opposed to using all pages of data from the source. This feature can be used for disaster recovery, to preserve data, and to back data up to off-site locations. It can also be used to distribute data.

Replication prerequisites

To replicate a volume, you must first create a peer connection and replication set. A peer connection establishes bi-directional communication between a local and remote system, both of which must have FC or iSCSI ports and a virtual pool. The system establishes a peer connection by connecting a host port on the local system with a user-specified host port on the remote system, then exchanging information and setting up a long term communication path in-band. Because the communication path establishes a peer connection between the two systems, replications can occur in either direction.

To verify that a host port address is available before creating a peer connection, use the `query peer-connection` CLI command. This command provides information about the remote system, such as inter-connectivity between the two systems, licensing, and pool configuration. For more information on this command, see the *Dell EMC PowerVault ME4 Series Storage System CLI Guide*. For more information on peer connections, see Creating a peer connection, Deleting a peer connection, and Modifying a peer connection.

After you create a peer connection, you can create a replication set. A replication set specifies a volume, snapshot, or multiple volumes in a volume group (hereafter known as *volume*) on one system of the peer connection, known as the primary system in the context of replication, to replicate across the peer connection. When you create a replication set, a corresponding volume is automatically created on the other system of the peer connection, known as the secondary system, along with the infrastructure needed for replication. The infrastructure consists of internal snapshots used for replication operations:

- A replication set for a volume consumes two internal snapshots each for the primary volume and the secondary volume if the queue policy is set to `Discard`, or three each if the queue policy is set to `Queue Latest`.
- A replication set for a volume group consumes two internal volume groups if the queue policy is set to `Discard`, or three if the queue policy is set to `Queue Latest`. Each internal volume group contains a number of volumes equal to the number of volumes in the base volume group.

Internal snapshots and internal volume groups count against system limits, but do not display.

Using a volume group for a replication set enables you to make sure that multiple volumes are synchronized at the same time. When a volume group is replicated, snapshots of all of the volumes are created simultaneously. In doing so, it functions as a consistency group, ensuring consistent copies of a group of volumes. The snapshots are then replicated as a group. Even though the snapshots may differ in size, replication is not complete until all of the snapshots are replicated.

For a replication set, the term `primary` refers to the source volume and the system in which it resides, and the term `secondary` is used for the remote copy and the system in which it resides. The secondary volume is meant to be an exact copy of the primary volume from the last time that replication occurred. To guarantee that the contents from that point in time match, the secondary volume cannot be mapped, rolled back, or modified except through replication.

While you cannot modify the secondary volume, you can create a snapshot of the secondary volume that you can map, roll back, and otherwise treat like any volume or snapshot. You can regularly take snapshots to maintain a history of the replications for backup or archiving, or enable snapshot history for the replication set. These snapshots also can be used in disaster recovery. For more information on replication sets, see "Creating a replication set from the Replications topic, Creating a replication set from the Volumes topic, Modifying a replication set, and Deleting a replication set.

Replication process

After you create a peer connection and replication set, you can then replicate volumes between the systems. The initial replication differs slightly from all subsequent replications in that it copies all of the allocated pages of the primary volume to the secondary volume. Depending on how large your source volume is and the speed of the network connection, this initial replication may take some time.

Subsequent replications are completed by resetting one of the hidden snapshots to contain the contents last replicated and then resetting the other hidden snapshot to the current primary volume contents and comparing the changes. The system writes any changes it finds on the hidden primary snapshot to the hidden secondary snapshot, after which the secondary volume is updated to contain the contents of the secondary volume.

The progress and status of the initial and subsequent replications are tracked and displayed. The timestamps for replication reflect the time zones of the respective systems. When viewed on a secondary system in a different time zone, for example, replication information will reflect the time zone of the secondary system. For more information on replicating, see Stopping a replication, Initiating or scheduling a replication from the Replications topic, Initiating or scheduling a replication from the Volumes topic, Resuming a replication, and Suspending a replication.

You can initiate a replication manually or by using a schedule. When creating a schedule for a replication set, you cannot specify for replication to occur more frequently than once an hour. For more information on scheduling a replication set, see Initiating or scheduling a replication from the Replications topic and Initiating or scheduling a replication from the Volumes topic.

Initial replication

The following illustration shows the internal processes that take place during the initial replication of a single volume.

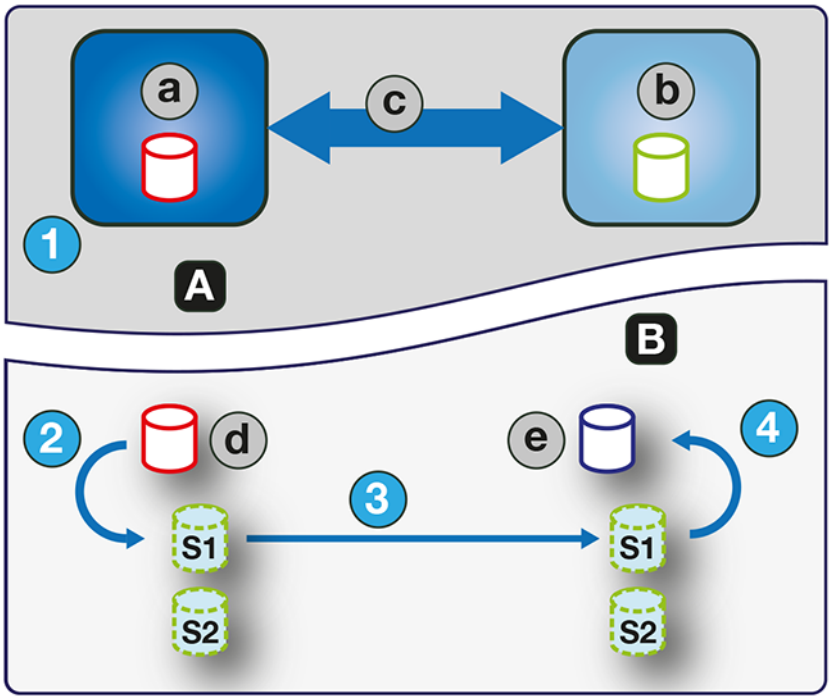


Figure 1. Process for initial replication

A	User view	1	Step 1: User initiates replication for the first time.
B	Internal view	2	Step 2: Current primary volume contents replace S1 contents.
a	Primary system	3	Step 3: S1 contents are fully replicated over the peer connection to counterpart S1, replacing S1 contents.
b	Secondary system	4	Step 4: S1 contents replace the secondary volume contents.
c	Peer connection		
d	Primary volume		
e	Secondary volume		

The two internal snapshots for each volume on the primary and secondary systems all have distinct roles. For both systems, they are labeled S1 (Snapshot 1) and S2 (Snapshot 2) in the two figures above and below. When a replication set is created, the primary volume and its internal snapshots all contain the same data. The secondary volume and its internal snapshots do not contain any data. Between the time that the replication set was created and the initial replication occurs, it is possible that hosts have written additional data to the primary volume.

During initial replication, the following sequence takes place. The user initiates replication on the primary system (step 1). The current primary volume contents, which might be different than when the replication set was created, replace the contents of S1 on the primary system (step 2). The S1 data, which matches that of the primary volume, is replicated in its entirety to its S1 counterpart on the secondary system and replaces the data that the secondary system S1 contains (step 3). The S1 contents on the secondary system replace the contents of the secondary volume (step 4). The contents of the primary and secondary volumes are now synchronized.

Subsequent replications

The following figure illustrates the internal process that take place in replications subsequent to the initial replication of a single volume.

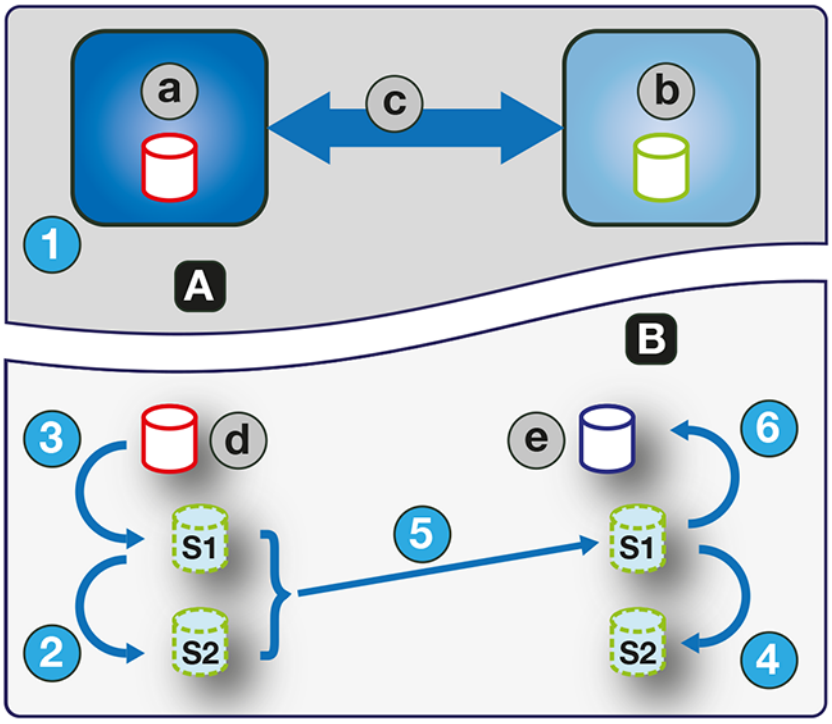


Figure 2. Process for subsequent replications

A	User view	1	Step 1: User initiates replication after the first replication has completed.
B	Internal view	2	Step 2: S1 contents replace S2 contents.
a	Primary system	3	Step 3: Current primary volume contents replace S1 contents.
b	Secondary system	4	Step 4: S1 contents replace the secondary volume contents.
c	Peer connection	5	Step 5: Differences (delta) between S1 and S2 are identified and replicated over the peer connection to counterpart S1.
d	Primary volume	6	Step 6: S1 contents replace the secondary volume contents.
e	Secondary volume		

During the initial replication, the entire contents of the primary volume are replicated to the secondary volume. In subsequent replications, only data that is new or modified since the last replication operation is replicated. This is accomplished by comparing a snapshot of the primary volume data from the last replication with a current snapshot of the primary volume. With the exception of this comparison, the process for both the initial and subsequent replications is similar.

During replications subsequent to the initial replication, the following sequence takes place. The user initiates replication on the primary system (step 1). On the primary system, the S1 contents replace the S2 contents (step 2). (The S2 contents can then be used for comparison during step 5.) The current primary volume contents replace the contents of S1 on the primary system (step 3). On the secondary system, the S1 contents replace the S2 contents (step 4). The S1 contents on the primary system, which match that of the primary volume at the time the replication was initiated, are compared to the S2 contents on the primary system. Only the data that is the delta between S1 and S2 is replicated to its S1 counterpart on the secondary system, which is updated with the delta data. The data comparison and replication occur together (step 5). The S1 contents on the secondary system replace the contents of the secondary volume (step 6). The contents of the primary and secondary volumes are now synchronized.

Internal snapshots

When first created from the primary volume, the internal snapshots consume very little space but will grow as data is written to the volume. Just as with any virtual snapshot, the amount of disk space used by an internal snapshot depends on the difference in the number of shared and unique pages between itself and the volume. The snapshot will not exceed the amount of disk space used by the primary volume. At most, the two internal snapshots together for each volume may consume twice the amount of disk space as the primary volume from which they are snapped.

Even though the internal snapshots are hidden from the user, they do consume snapshot space (and thus pool space) from the virtual pool. If the volume is the base volume for a snapshot tree, the count of maximum snapshots in the snapshot tree may include the internal snapshots for it even though they are not listed. Internal snapshots and internal volume groups count against system limits, but do not display.

Creating a virtual pool for replication

When you create a virtual pool, specify that it has enough space for three times the anticipated size of the primary volume to account for the primary volume plus the same amount of space for each of the two internal snapshots. This is the maximum amount of space that you will need for replication. Also, for a pool on the primary system, allow additional space for other uses of the pool.

Setting up snapshot space management in the context of replication

The snapshot space management feature, accessible only through the CLI, enables users to monitor and control the amount of space that snapshots can consume in a pool. In addition to configuring a snapshot space limit, you can also specify a limit policy to enact when the snapshot space reaches the configured limit. The policy will either notify you via the event log that the percentage has been reached (in which case the system continues to take snapshots, using the general pool space), or notify you and trigger automatic deletion of snapshots. If automatic deletion is triggered, snapshots are deleted according to their configured retention priority. For more information on setting snapshot retention priority, see Maintaining replication snapshot history from the Replications topic.

When you create virtual volumes through the `create volume` and `create volume-set` CLI commands, you can set the retention priority for snapshots of the volume. If automatic deletion of snapshots is enabled, the system uses the retention priority of snapshots to determine which, if any, snapshots to delete. Snapshots are considered to be eligible for deletion if they have any retention priority other than `never-delete`. Snapshots are configured to be eligible for deletion by priority and age. The oldest, lowest priority snapshots are deleted first. Internal replication snapshots and snapshots that are mapped or are not leaves of a volume's snapshot tree are ineligible for deletion. For more information on the `create volume` and `create volume-set` CLI commands, see the *Dell EMC PowerVault ME4 Series Storage System CLI Guide*.

If you are using the replication feature and snapshot space management, there are specific factors to consider when managing snapshot space for the primary and secondary systems, especially when setting up the snapshot space and policies for the pool:

- Make sure that there is enough snapshot space to accommodate the maximum anticipated size of the two internal snapshots, which cannot be deleted, and any other snapshots that you would like to retain.
- To adjust the snapshot space of the pool, increase the value of the limit parameter of the `set snapshot-space` CLI command. For more information on the `set snapshot-space` CLI command, see the *Dell EMC PowerVault ME4 Series Storage System CLI Guide*.
- You can later create more snapshot space by adding disks to the pool to increase its size.

If the internal snapshots are larger than anticipated and take up a lot of snapshot space, you can adjust the snapshot space thresholds or increase the snapshot space to prevent unintentional automatic deletion of snapshots that you want to retain. To monitor the snapshot space for virtual pools, use the show `snapshot-space` CLI command. To monitor the size of the internal snapshots, use the `show snapshots` CLI command with its type parameter set to `replication`. For more information on the show snapshots CLI command, see the *Dell EMC PowerVault ME4 Series Storage System CLI Guide*.

Replication and empty allocated pages

Deleting data from a volume can result in deallocation of pages on that volume. Pages deallocated before the initial replication will not be copied to the secondary volume. Pages deallocated since the last replication cause a page consisting of zeroes to be written to the secondary volume during replication. This can result in a difference in the number of allocated pages between the primary and secondary volumes. A virtual storage background task automatically reclaims pages consisting of all zeroes, eventually freeing up the secondary volume snapshot space that these reclaimed pages consumed. Freeing up this space is not immediate and happens over a period of time.

Disaster recovery

The replication feature supports manual disaster recovery only. It is not integrated with third-party disaster recovery software. Since replication sets of virtual volumes cannot reverse the direction of the replication, carefully consider how the replicated data will be accessed at the secondary backup site when a disaster occurs.

NOTE: Using a volume group in a replication set ensures consistent simultaneous copies of the volumes in the volume group. This means that the state of all replicated volumes can be known when a disaster occurs since the volumes are synchronized to the same point in time.

Accessing the data while keeping the replication set intact

If you want to continue replicating changed data from the primary data center system, you will need to keep the replication set intact. While the data center system is down, you can access the data at the secondary backup system by creating a snapshot of the secondary volume or using the snapshot history snapshot. The snapshot can be mapped either read-only or read-write (but you cannot replicate the changes written to it back to the data center system using the existing replication set).

NOTE: If a system goes down but recovers, the data, peer connection, and replication sets should be intact and replication can resume normally.

Access data at the backup site temporarily

1. Create a snapshot of the secondary volume or use a snapshot history snapshot.
2. Map the snapshot to hosts.
3. When the data center system has recovered, delete the snapshot.

Accessing the data from the backup system as if it were the primary system

If you do not think the data center system can be recovered in time or at all, then you will want to temporarily access the data from the backup system as if it were the primary system. You can again create a snapshot of the secondary volume and map that to hosts, or delete the replication set to allow mapping the secondary volume directly to hosts. Deleting the replication set means the secondary volume becomes a base volume and is no longer the target of a replication. Should the primary volume become available and you want to use it as is in preparation for another disaster, a new replication set with a new secondary volume must be created. Deleting the replication set also enables cleaning up any leftover artifacts of the replication set.

In an emergency situation where no connection is available to the peer system and you do not expect to be able to reconnect the primary and secondary systems, use the local-only parameter of the `delete replication-set`and `delete peer-connection` CLI commands on both systems to delete the replication set and peer connection. Do not use this parameter in normal operating conditions. For more information, see the *Dell EMC PowerVault ME4 Series Storage System CLI Guide*. Other methods for deleting replication sets and peer connections will most likely be ineffective in this situation.

NOTE: While deleting the peer connection for the replication set is unnecessary for making the secondary volume mappable, if you think that it will no longer be operable in the future, delete it when deleting the replication set.

Disaster recovery procedures

In a disaster recovery situation, you might typically perform the tasks in the following order:

1. Transfer operations from the data center system to the backup system (failover).
2. Restore operations to the data center system when it becomes available (failback).
3. Prepare the secondary system for disaster recovery.

Manually transfer operations from the data center system to the backup system

1. Create a snapshot of the secondary volume, use a snapshot history snapshot, or delete the replication set.
2. Map the snapshot or the secondary volume, depending on the option that you choose in step 1, to hosts.

Restore operations to the data center system

1. If the old primary volume still exists on the data center system, delete it. The volume cannot be used as the target—a new "secondary" volume will be created and deleting it will free up available space.

2. Create a peer connection between the backup system and the data center system, if necessary.
3. Create a replication set using the backup system's volume or snapshot as the primary volume and the data center system as the secondary system.
4. Replicate the volume from the backup system to the data center system.

Prepare the backup system for disaster recovery after the replication is complete

1. Delete the replication set.
2. Delete the volume on the backup system. The volume cannot be used as the target of a replication and deleting it will free up space.
3. Create a replication set using the data center system's volume as the primary volume and the backup system as the secondary system.
4. Replicate the volume from the data center system to the backup system.

Viewing replications

The Replications topic shows a tabular view of information about peer connections, replication sets, and snapshot history of local snapshots associated with a selected replication set. For more information about replication, see About replicating virtual volumes on page 31.

Peer Connections table

The Peer Connections table shows the following information. By default, the table shows 10 entries at a time.

- Name. Shows the specified peer connection name.
- Status. Shows the status of the peer connection:
  - `Online`—The systems have a valid connection.
  - `Offline`—No connection is available to the remote system.
- Health. Shows the health of the component: OK, Fault, or Unknown.
- Type. Shows the type of host ports being used for the peer connection: FC or iSCSI.
- Local Ports. Shows the IDs of host ports in the local system.
- Remote Ports. Shows the IDs of host ports in the remote system.

To see more information about a peer connection, hover the cursor over the peer connection in the table. The **Peer Connections** panel that appears contains the following information:

NOTE: If the health is not OK, the health reason and recommended action are shown to help you resolve problems.

Table 25. Peer Connections

Panel	Information displayed
Peer Connections	Name, serial number, connection type, connection status, local host port name and IP address, remote host port name and IP address, health

Replication Sets table

The Replication Sets table shows the following information. By default, the table shows 10 entries at a time.

NOTE: If you change the time zone of the secondary system in a replication set whose primary and secondary systems are in different time zones, you must restart the system to enable management interfaces to show proper time values for replication operations.

- Name. Shows the replication set name.
- Primary Volume. Shows the primary volume name. For replication sets that use volume groups, the primary volume name is `volume-group-name.*` where .* signifies that the replication set contains more than one volume. If the volume is on the local system, the icon appears.

- Secondary Volume. Shows the secondary volume name. For replication sets that use volume groups, the secondary volume name is `volume-group-name.*` where .* signifies that the replication set contains more than one volume. If the volume is on the local system, the icon appears.
- Status. Shows the status of the replication set.
  - `Not Ready` – The replication set is not ready for replications because the system is still preparing the replication set.
  - `Unsynchronized` – The primary and secondary volumes are unsynchronized because the system has prepared the replication set, but the initial replication has not run.
  - `Running` – A replication is in progress.
  - `Ready` – The replication set is ready for a replication.
  - `Suspended` – Replications have been suspended.
  - `Unknown` – This system cannot communicate with the primary system and thus cannot be sure of the current state of the replication set. Check the state of the primary system.
- Last Successful Run. Shows the date and time of the last successful replication.
- Estimated Completion Time. Shows the estimated date and time for the replication in progress to complete.

To see more information about a replication set, hover the cursor over a replication set in the Replication Sets table. The Replication Sets panel that appears contains the following information:

Table 26. Replication Sets

Panel	Information displayed
Replication Set Information	Replication set name and serial number; status; primary volume or volume group name and serial number; secondary volume or volume group name and serial number; peer connection name; queue policy, queue count, secondary volume snapshot history, primary volume snapshot history, retention count, retention priority, snapshot basename, associated schedule name, current run progress, current run start time, current run estimated time to completion, current run transferred data, last successful run, last run start time, last run end time, last run transferred data, last run status, and last run error status

Replication Snapshot History table

The Replication Snapshot History table shows the following information. By default, the table shows 10 entries at a time.

- Local Snapshot Name. Shows the local snapshot name.
- Creation Date/Time. Shows the date and time of the last successful snapshot created.
- Snap Data. Shows the total amount of write data associated with the snapshot.
- Unique Data. Shows the amount of write data that is unique to the snapshot.

To see more information about a snapshot history, hover the cursor over a snapshot set in the Replication Snapshot History table. The Snapshot Information hover panel that appears contains the following information:

Table 27. Replication Snapshot History

Panel	Information displayed
Snapshot information	Name, serial number, status, status reason, retention priority, snapshot data, unique data, shared data, pool, class, number of snaps, number of snapshots in tree, source volume, total size, creation date/time, type, parent volume, base volume, health

Querying a peer connection

You can view information about systems you might use in a peer connection before creating the peer connection, or you can view information about systems currently in a peer connection before modifying the peer connection.

Query a peer connection

1. In the Replications topic, do one of the following to display the Query Peer Connection panel:
   - Select the peer connection to query in the Peer Connections table, then select **Action > Query Peer Connection**. The remote host port address field is pre-populated with the selected peer's remote port address.
   - Select **Action > Query Peer Connection**.

2. If you did not select a peer connection from the Peer Connections table, enter the remote host port address to query in the text box.
3. Click **OK**. A processing dialog box appears while the remote port address is queried. If successful, detailed information about the remote system and controllers is displayed. An error message appears if the operation is unsuccessful.

Creating a peer connection

A peer connection enables bi-directional communication between a local system and a remote system to transfer data between the two systems. Creating a peer connection requires a name for the peer connection and either an IP address of a single available iSCSI host port on the remote system, or a WWN of a single available FC host port on the remote system. Only iSCSI and FC host ports are used for the peer connection.

The peer connection is defined by the ports that connect the two peer systems, as well as the name of the peer connection. The local system uses the remote address to internally run the `query peer-connection` CLI command. The results of the query are used to configure the peer connection.

The prerequisites to create a peer connection are:

- Both systems must have iSCSI or FC host ports. Ports at both ends of the connection must use the same protocol.
- Both systems must be connected to the same fabric or network. For FC, at least one FC switch is required between systems (no direct attach).
- All host port addresses in both systems must be unique, even for ports not in use.
- Each system must have a virtual pool.
- If iSCSI CHAP is configured for the peer connection, the authentication must be valid.
- You must specify the username and password of a user with the manage role on the remote system.

You can create a maximum of four peer connections per storage system. However, only one peer connection is allowed to a particular remote system. Attempting to create a second peer connection to the same system will fail.

While creating the peer connection, the local system receives information about all host ports and IPs on the remote system as well as the remote system's licensing and host port health. It also links host ports of the select host port type on the local system to those on the remote system, so all ports of that type are available as part of the peer connection. Once created, the peer connection exists on both the local and remote systems.

Replications use the bi-directional communication path between the systems when exchanging information and transferring replicated data. Once you create a peer connection, you can use it when creating any replication set. Because the peer connection is bi-directional, replication sets can be created from both systems with replication occurring from either direction.

NOTE: You can use the `query peer-connection` CLI command to determine if the remote system is compatible with your system. This command provides information about the remote system, such as host ports, licensing, and pools. You can run it before creating the peer connection to determine if either system needs to be reconfigured first. You can also run it to diagnose problems if creating a peer connection fails.

To create a peer connection

1. In the Replications topic, select **Action > Create Peer Connection**. The Create Peer Connection panel opens.
2. Enter a name for the peer connection. The name is case sensitive and can have a maximum of 32 bytes. It cannot already exist in the system or include the following: " , < \
3. Enter the destination port address for the remote system.
4. Enter the name and password of a user with the manage role on the remote system.
5. Click **OK**.
6. If the task succeeds, click **OK** in the confirmation dialog. The peer connection is created and the Peer Connections table is updated.

   If the task does not succeed, the Create Peer Connection panel appears with errors in red text. Correct the errors, then click **OK**.

CHAP and replication

If you want to use Challenge Handshake Authentication Protocol (CHAP) for the iSCSI connection between peer systems, see the procedure below to set up CHAP. Make sure that you configure both systems in this way. In a peer connection, both systems will alternately act as an originator (initiator) and recipient (target) of a login request. Peer connections support one-way CHAP only.

If only one system has CHAP enabled and the two systems do not have CHAP records for each other, or the CHAP records have different secrets, the system with CHAP enabled will be able to modify the peer connection. However, it will be unable to perform any other

replication operations, such as creating replication sets, initiating replications, or suspending replication operations. The system that does not have CHAP enabled will be unable to perform any replication operations, including modifying and deleting the peer connection. For full replication functionality for both systems, set up CHAP for a peer connection (see the following procedure).

If the two systems have CHAP records for each other with the same secret, they can perform all replication operations whether or not CHAP is enabled on either system. In other words, even if CHAP is enabled on neither system, only one system, or both systems, either system can work with peer connections, replication sets, and replications.

If you want to use Challenge Handshake Authentication Protocol (CHAP) for the iSCSI connection between peer systems, see the following procedure to set up CHAP. In a peer connection, both systems will alternately act as an initiator and target of a login request. Peer connections support one-way CHAP only.

Set up CHAP for a peer connection using the CLI

1. If you have not already configured CHAP, run `query peer-connection` from either the local system or the remote system to ensure that they have connectivity.
2. If you have an existing peer connection, stop I/O to it.
3. On the local system, use the `create chap-record` command to create a CHAP record for one-way CHAP to allow access by the remote system.
4. On the remote system, use the `create chap-record` command to create a CHAP record for one-way CHAP to the local system. Note that the same CHAP record used from the local system may also be used here but the configuration is still one-way CHAP.
5. On each system, enable CHAP by running: `set iscsi-parameters chap on`

   CAUTION: Enabling or disabling CHAP will cause all iSCSI host ports in the system to be reset and restarted. This may prevent iSCSI hosts from being able to reconnect if their CHAP settings are incorrect.

6. Wait one minute for the commands to complete before attempting to use the peer connection.
7. Run `query peer-connection` from the local system and then from the remote system to ensure communication can be initiated from either system.
   - If both succeed, you can create, set, or perform replication on that peer connection.
   - If either fails, it is likely that you must fix a CHAP configuration issue and then repeat these steps as appropriate. If you need to modify a CHAP record, use the `set chap-record` command.

Modifying a peer connection

You can change the name of a current peer connection or the port address of the remote system from either the local system or the remote system without changing the peer connection configurations. For example, you could configure a peer connection and then move one of the peers to a different network.

Changing the peer connection name will not affect the network connection so any running replications will not be interrupted.

NOTE: Changing the remote port address will modify the network connection, which is permitted only if no replications are running and new replications are prevented from running. For the peer connection, stop any running replications and either suspend its replication sets or make sure its network connection is offline. After you have modified the peer connection, you can resume replication sets. If CHAP is enabled on one system within a peer connection, be sure that CHAP is configured properly on the corresponding peer system before initiating this operation. For more information about configuring CHAP, see CHAP and replication.

Modify a peer connection

1. In the Replications topic, select the peer connection to be modified in the Peer Connections table.
2. Select **Action > Modify Peer Connection**. The Modify Peer Connection panel appears.
3. Change one of the following. You cannot change both:
   - Select **New Name**, then enter a new name for the peer connection. The name is case sensitive and can have a maximum of 32 bytes. It cannot already exist in the system or include the following: " , < \
   - Select **New Remote Address** (FC-WWN or iSCSI-IP), then enter a new address for the remote system.

NOTE: You can change protocols used in the peer connection between FC and iSCSI by modifying the peer connection to use the remote port address of the new protocol.

4. Enter the name and password of a user assigned a manage role on the remote system.
5. Click **OK**. The peer connection is modified and the Peer Connections table is updated.

Deleting a peer connection

You can delete a peer connection if there are no replication sets that belong to the peer connection. If there are replications sets that belong to the peer connection, you must delete them before you can delete the peer connection. For more information, see Deleting a replication set.

NOTE: If the peer connection is down and there is no communication between the primary and secondary systems, use the `local-only` parameter of the `delete replication-set` CLI command to delete the replication set.

NOTE: If CHAP is enabled on one system within a peer connection, be sure that CHAP is configured properly on the corresponding peer system before initiating this operation. For more information about configuring CHAP, see CHAP and replication.

Delete a peer connection

1. In the Replications topic, select the peer connection to be deleted in the Peer Connections table.
2. Select **Action > Delete Peer Connection**.
3. Click **OK**. The peer connection is deleted and the Peer Connections table is updated.

Creating a replication set from the Replications topic

You can create a replication set, which specifies the components of a replication. The Create Replication Set panel enables you to create replication sets. You can access this panel from both the Replications and Volumes topics.

Performing this action creates the replication set and the infrastructure for the replication set. For a selected volume, snapshot, or volume group, the action creates a secondary volume or volume group and the internal snapshots required to support replications. By default, the secondary volume or volume group and infrastructure are created in the pool corresponding to the one for the primary volume or volume group (A or B). Optionally, you can select the other pool.

A peer connection must be defined to create and use a replication set. A replication set can specify only one peer connection and pool. When creating a replication set, communication between the peer connection systems must be operational during the entire process.

If a volume group is part of a replication set, volumes cannot be added to or deleted from the volume group.

If a replication set is deleted, the internal snapshots created by the system for replication are also deleted. After the replication set is deleted, the primary and secondary volumes can be used like any other base volumes or volume groups.

Primary volumes and volume groups

The volume, volume group, or snapshot that will be replicated is called the *primary volume* or *volume group*. It can belong to only one replication set. If the volume group is already in a replication set, individual volumes may not be included in separate replication sets. Conversely, if a volume that is a member of a volume group is already in a replication set, its volume group cannot be included in a separate replication set.

The maximum number of individual volumes and snapshots that can be replicated is 32 in total. If a volume group is being replicated, the maximum number of volumes that can exist in the group is 16.

Using a volume group for a replication set enables you to make sure that the contents of multiple volumes are synchronized at the same time. When a volume group is replicated, snapshots of all of the volumes are created simultaneously. In doing so, it functions as a consistency group, ensuring consistent copies of a group of volumes. The snapshots are then replicated as a group. Though the snapshots may differ in size, replication of the volume group is not complete until all of the snapshots are replicated.

Secondary volumes and volume groups

When the replication set is created—either through the CLI or the PowerVault Manager—secondary volumes and volume groups are created automatically. Secondary volumes and volume groups cannot be mapped, moved, expanded, deleted, or participate in a rollback operation. Create a snapshot of the secondary volume or volume group and use the snapshot for mapping and accessing data.

Queuing replications

You can specify the action to take when a replication is running and a new replication is requested.

- **Discard**. Discard the new replication request.
- **Queue Latest**. Take a snapshot of the primary volume and queue the new replication request. If the queue contained an older replication request, discard that older request. A maximum of one replication can be queued. This is the default.

NOTE: If the queue policy is set to `Queue Latest` and a replication is running and another is queued, you cannot change the queue policy to discard. You must manually remove the queued replication before you can change the policy.

Maintaining replication snapshot history from the Replications topic

A replication set can be configured to maintain a replication snapshot history. As part of handling a replication, the replication set will automatically take a snapshot of the primary and/or secondary volume(s), thereby creating a history of data that has been replicated over time. This feature can be enabled for a secondary volume or for a primary volume and its secondary volume, but not for a volume group. When this feature is enabled:

- For a primary volume, when a replication starts it will create a snapshot of the data image being replicated.
- For a secondary volume, when a replication successfully completes it will create a snapshot of the data image just transferred to the secondary volume. (This is in contrast to the primary volume snapshot, which is created before the sync.) If replication does not complete, a snapshot will not be created.
- You can set the number of snapshots to retain from 1 through 16, referred to as the snapshot retention count. This setting applies to management of snapshots for both the primary and secondary volume and can be changed at any time. Its value must be greater than the number of existing snapshots in the replication set, regardless of whether snapshot history is enabled. If you select a snapshot retention count value that is less than the current number of snapshots, an error message appears. Thus, you must manually delete the excess snapshots before reducing the snapshot count setting. When the snapshot count is exceeded, the oldest unmapped snapshot will be discarded automatically.
- The snapshots are named `basename_nnnn` where _nnnn starts at 0000 and increments for each subsequent snapshot. If primary volume snapshots are enabled, snapshots with the same name will exist on the primary and secondary systems. The snapshot number is incremented each time a replication is requested, whether or not the replication completes — for example, if the replication was queued and subsequently removed from the queue.
- If the replication set is deleted, any existing snapshots automatically created by snapshot history rules will not be deleted. You will be able to manage those snapshots like any other snapshots.
- Manually creating a snapshot will not increase the snapshot count associated with the snapshot history. Manually created snapshots are not managed by the snapshot history feature. The snapshot history feature generates a new name for the snapshot that it intends to create. If a volume of that name already exists, the snapshot history feature will not overwrite that existing volume. Snapshot numbering will continue to increment, so the next time the snapshot history feature runs, the new snapshot name will not conflict with that existing volume name.
- The snapshot basename and snapshot retention count settings only take effect when snapshot history is set to secondary or both, although these settings can be changed at any time.
- A mapped snapshot history snapshot will not be deleted until after it is unmapped.
- A snapshot created by this feature is counted against the system-wide maximum snapshots limit, with the following result:
  - If the snapshot count is reached before the system limit then the snapshot history is unchanged.
  - If the system limit is reached before the snapshot count then the snapshot history stops adding or updating snapshots.
- You can set the retention priority for snapshots to the following. In a snapshot tree, only leaf snapshots can be deleted automatically.
  - **never-delete**. Snapshots will never be deleted automatically to make space. The oldest snapshot in the snapshot history will be deleted once the snapshot count has been exceeded. This is the default.
  - **high**. Snapshots can be deleted after all eligible medium-priority snapshots have been deleted.
  - **medium**. Snapshots can be deleted after all eligible low-priority snapshots have been deleted.

- **low**. Snapshots can be deleted. This parameter is unrelated to snapshot history, and because the default is never delete, snapshot history snapshots will normally not be affected in a low virtual memory situation.

When this option is disabled, snapshot history will not be kept. If this option is disabled after a replication set has been established, any existing snapshots will be kept, but not updated.

Create a replication set from the Replications topic

NOTE: If CHAP is enabled on one system within a peer connection, be sure that CHAP is configured properly on the corresponding peer system before initiating this operation. For more information about configuring CHAP, see CHAP and replication.

1. In the Peer Connections table, select the peer connection to use for the replication set.
2. Select **Action > Create Replication Set**. The Create Replication Set panel appears.
3. Enter a name for the replication set. The name is case sensitive and can have a maximum of 32 bytes. It cannot already exist in the system, include leading or trailing spaces, or include the following characters: " , < \
4. Select whether you want to use a single volume or a volume group, which will filter the entries in the adjacent table.
5. In the table, select the volume or volume group to replicate. This will be the primary volume or volume group.
6. Optional: If **Single Volume** is selected, enter a name for the secondary volume. The default name is the name of the primary volume. The name is case sensitive and can have a maximum of 32 bytes. It cannot already exist on the secondary system or include the following: " , < \
7. Optional: Select a pool on the secondary system. By default, the pool that corresponds with the pool in which the primary volume resides is selected. The selected pool must exist on the remote system.
8. Optional: Specify the Queue Policy action to take when a replication is running and a new replication is requested.
9. Optional: Select the **Secondary Volume Snapshot History** check box to keep a snapshot history on the secondary system for the secondary volume.
   - Set the Retention Count to specify the number of snapshots to retain.
   - Modify the Snapshot Basename to change the snapshot name. The name is case sensitive and can have a maximum of 26 bytes. It cannot already exist in the system or include the following characters: " , < \
   - Set the Retention Priority to specify the snapshot retention priority.
   - Optional: Check **Primary Volume Snapshot History** to keep a snapshot history for the primary volume on the primary system.
10. Optional: Select the **Scheduled** check box to schedule recurring replications.
11. Click **OK**.
12. In the success dialog box:
    - If you selected the **Scheduled** check box, click **OK**. The Schedule Replications panel opens and you can set the options to create a schedule for replications. For more information on scheduling replications, see Initiating or scheduling a replication from the Replications topic.
    - Otherwise, you have the option to perform the first replication. Click **Yes** to begin the first replication, or click **No** to initiate the first replication later.

Modifying a replication set

You can change a replication set's name, queue policy, and snapshot history settings. Volume membership of a replication cannot change for the life of the replication set.

NOTE: If CHAP is enabled on one system within a peer connection, be sure that CHAP is configured properly on the corresponding peer system before initiating this operation. For more information about configuring CHAP, see CHAP and replication.

Modify a replication set

1. In the Replications topic, select the replication set in the Replications Sets table that you want to modify.
2. Select **Action > Modify Replication Set**. The Modify Replication Set panel opens.
3. Enter a new name for the replication set. The name is case sensitive and can have a maximum of 32 bytes. It cannot already exist in the system, include leading or trailing spaces, or include the following: " , < \
4. Specify the Queue Policy action to take when a replication is running and a new replication is requested.

- **Discard**. Discard the new replication request.
- **Queue Latest**. Take a snapshot of the primary volume and queue the new replication request. If the queue contained an older replication request, discard that older request. A maximum of one replication can be queued. If the queue policy is set to `Queue Latest` and a replication is running and another is queued, you cannot change the queue policy to Discard. You must manually remove the queued replication before you can change the policy.

5. Optional: Select the **Secondary Volume Snapshot History** check box to keep a snapshot history on the secondary system for the secondary volume.
   - Set the Retention Count to modify the number of snapshots to retain. Its value must be greater than the number of existing snapshots in the replication set, regardless of whether snapshot history is enabled.

     NOTE: If you reduce the snapshot count setting to a value less than the current number of snapshots, the operation will fail. Thus, you must manually delete the excess snapshots before reducing the snapshot count setting. If you change this parameter while a replication is running, for the current replication it will affect only the secondary system. In this case the value can only be increased, so you might have one less expected snapshot on the primary system than on the secondary system.
   - Set the Snapshot Basename to modify the snapshot name. The name is case sensitive and can have a maximum of 26 bytes. It cannot already exist in the system or include the following characters: " , < \

     NOTE: If you change the Snapshot Basename while a replication is running, for the current replication it will affect the name of the snapshot on the secondary system. For that replication only, the names of the snapshots on the primary and secondary systems will differ.
   - Set the Retention Priority to specify the snapshot retention priority.
   - Optional: Check **Primary Volume Snapshot History** to keep a snapshot history for the primary volume on the primary system.
6. Click **OK**. The name of the replication set is updated in the Replications Sets table.

Deleting a replication set

You can delete a replication set. When you delete a replication set, all infrastructure created by the system (internal snapshots required to support replications) is also deleted. The primary and secondary volumes and volume groups no longer have restrictions and function like all other base volumes, volume groups, and snapshots.

If you want to delete a replication set that has a replication in progress, you must first suspend and then stop the replication for that replication set. For more information, see Stopping a replication or Suspending a replication. When a replication set is deleted, the snapshots created from the snapshot history feature will not be deleted. You will be able to manage those snapshots like any other snapshots. For more information, see Maintaining replication snapshot history from the Replications topic.

NOTE: If the peer connection is down and there is no communication between the primary and secondary systems, use the `local-only` parameter of the `delete replication-set` CLI command on both systems to delete the replication set. For more information, see the *Dell EMC PowerVault ME4 Series Storage System CLI Guide*.

Delete a replication set

1. In the Replications topic, select the replication set to be deleted in the Replication Sets table.
2. Select **Action > Delete Replication Set**.
3. Click **OK**. The replication set is deleted and the Replication Sets table is updated.

Initiating or scheduling a replication from the Replications topic

After you have created a replication set, you can copy the selected volume or volume group on the primary system to the secondary system by initiating replication. The first time that you initiate replication, a full copy of the allocated pages for the volume or volume group is made to the secondary system. Thereafter, the primary system only sends the contents that have changed since the last replication.

You can manually initiate replication or create a scheduled task to initiate it automatically from both the Replications and Volumes topics. You can initiate replications only from a replication set's primary system.

NOTE: If you change the time zone of the secondary system in a replication set whose primary and secondary systems are in different time zones, you must restart the system to enable management interfaces to show proper time values for replication operations.

If a replication fails, the system suspends the replication set. The replication operation will attempt to resume if it has been more than 10 minutes since the replication set was suspended. If the operation has not succeeded after six attempts using the 10-minute interval, it will switch to trying to resume if it has been over an hour and the peer connection is healthy.

NOTE: Host port evaluation is done at the start or resumption of each replication operation.

- **At most, two ports will be used.**
- **Ports with optimized paths will be used first. Ports with unoptimized paths will be used if no optimized path exists. If only one port has an optimized path, then only that port will be used.**
- **The replication will not use another available port until all currently used ports become unavailable.**

NOTE: If a single host port loses connectivity, event 112 will be logged. Because a peer connection is likely to be associated with multiple host ports, the loss of a single host port may degrade performance but usually will not cause the peer connection to be inaccessible.

Manually initiate replication from the Replications topic

If CHAP is enabled on one system within a peer connection, be sure that CHAP is configured properly on the corresponding peer system before initiating this operation. For more information about configuring CHAP, see CHAP and replication.

1. In the Replications topic, select a replication set in the Replication Sets table.
2. Select **Action > Replicate**. The Replicate panel opens.
3. Click **OK**.
   - If a replication is not in progress, the local system begins replicating the contents of the replication set volume to the remote system and the status of the replication set changes to `Running`.
   - If a replication is already in progress, then the outcome of this replication request depends upon the Queue Policy setting specified in the Create Replication Set panel. For more information on setting the queue policy, see Queuing replications.

Schedule a replication from the Replications topic

1. In the Replications topic, select a replication set from the Replication Sets table.
2. Select **Action > Replicate**.
   The Replicate panel opens.
3. Select the **Schedule** check box.
4. Type a name for the replication schedule task. The name is case sensitive and can have a maximum of 32 bytes. It cannot already exist in the system or include the following: " , < \
5. If you want to create a replication of the last snapshot of the primary volume, select the **Last Snapshot** check box.
   At the time of the replication, the snapshot must exist. This snapshot may have been created either manually or by scheduling the snapshot. If no snapshot exists for the volume when the scheduled replication begins, event 362 is logged and the replication fails.
   NOTE: This option is unavailable when replicating volume groups.
6. Specify a date and a time in the future to be the first instance when the scheduled task will run, and to be the starting point for any specified recurrence.
   - To set the **Date** value, enter the current date in the format *YYYY-MM-DD*.
   - To set the Time value, enter two-digit values for the hour and minutes and select either **AM, PM**, or **24H** (24-hour clock). The minimum interval is one hour.
7. If you want the task to run more than once, select the **Repeat** check box.
   - Specify how often the task should repeat. Enter a number and select the appropriate time unit. Replications can recur no less than 30 minutes apart.
   - Either make sure the **End** check box is cleared, which allows the schedule to run indefinitely, or select the check box to specify when the schedule ends. To then specify an end date and time, select the **On** option, and specify when the schedule should stop running. Or, select the **After** option, and specify the number of replications that can occur before the schedule stops running.

- Either make sure the **Time Constraint** check box is cleared, which allows the schedule to run at any time, or select the check box to specify a time range within which the schedule should run.
- Either make sure the **Date Constraint** check box is cleared, which allows the schedule to run on any day, or select the check box to specify the days when the schedule should run.

8. Click **OK**. The schedule is created.

Stopping a replication

You can stop a replication on the primary system of a replication set. For the stop to succeed, the replication set state must be either `Ready` or `Suspended`. Attempting to stop a replication for a replication set that is in a `Ready` or `Unsynchronized` state fails with an error message.

NOTE: If you stop a running replication, the replication set returns to the state it had before replication started: either `Ready` or `Unsynchronized`. If you stop a suspended replication, the state of the replication remains `Suspended`.

NOTE: If you stop the initial replication for a replication set, the snapshot space allocated for that replication in the primary pool and the secondary pool will not be freed. To free that space, either re-run the initial replication or delete the replication set.

Stop a replication

NOTE: If CHAP is enabled on one system within a peer connection, be sure that CHAP is configured properly on the corresponding peer system before initiating this operation. For more information about configuring CHAP, see CHAP and replication.

1. In the Replications topic, select a replication set that is currently being replicated in the Replication Sets table.
2. Select **Action > Abort Replication**.
3. Click **OK**. The replication is terminated.

Suspending a replication

You can suspend replication operations for a specified replication set from its primary system. You can suspend replications from a replication set's primary system only.

When you suspend a replication set, all replications in progress are paused and no new replications are allowed to occur. You can abort suspended replications. After you suspend replication, you must resume it to allow the replication set to resume replications that were in progress and allow new replications to occur. For more information, see Stopping a replication or Resuming a replication.

If replications are attempted during the suspended period (including scheduled replications), the replications will fail.

Suspend a replication

NOTE: If CHAP is enabled on one system within a peer connection, be sure that CHAP is configured properly on the corresponding peer system before initiating this operation. For more information about configuring CHAP, see CHAP and replication.

1. In the Replications topic, select a replication set that is currently being replicated in the Replication Sets table.
2. Select **Action > Suspend Replication**.
3. Click **OK**. The replications on the replication set are suspended and the status of the replication set changes to Suspended.

Resuming a replication

You can resume the replication operations of a specified suspended replication set. You can resume replications from a replication set's primary system only.

When a replication set is suspended, all replications in progress are paused and no new replications are allowed to occur. When you resume replications, all paused replications are resumed and new replications are allowed to occur. If you stopped a replication while the replication set was suspended, the stopped replication does not resume.

Resume a replication

NOTE: If CHAP is enabled on one system within a peer connection, be sure that CHAP is configured properly on the corresponding peer system before initiating this operation. For more information about configuring CHAP, see CHAP and replication.

1. In the Replications topic, select a replication set for which replications were suspended in the Replication Sets table.
2. Select **Action > Resume Replication**.
3. Click **OK**. Replications on the replication set are resumed and the status of the replication set changes to `Running`.

Manage replication schedules from the Replications topic

You can modify or delete scheduled replication tasks on the primary system.

1. In the Replications topic, select a replication set on the primary system that has an associated schedule from the Replication Sets table.
2. Select **Action > Manage Schedules**.
   The **Manage Schedules** panel opens.
3. Select the schedule to modify. Its settings appear at the bottom of the panel.
4. If you want to create a replication of the last snapshot in the primary volume, select the **Last Snapshot** check box.

   NOTE: This option is unavailable when replicating volume groups.

5. Specify a date and a time in the future to be the first instance when the scheduled task will run, and to be the starting point for any specified recurrence.
   - To set the **Date** value, enter the current date in the format *YYYY-MM-DD*.
   - To set the **Time** value, enter two-digit values for the hour and minutes and select either **AM, PM**, or **24H** (24-hour clock).
6. If you want the task to run more than once, select the **Repeat** check box.
   - Specify how often the task should repeat. Enter a number and select the appropriate time unit. Replications can recur no less than 30 minutes apart.
   - Clear the **End** checkbox is cleared to allow the schedule to run without an end date, or select the check box and specify when the schedule should stop running.
   - Clear **Time Constraint** checkbox to allow the schedule to run at any time, or select the check box to specify a time range within which the schedule should run.
   - Clear **Date Constraint** checkbox to allow the schedule to run on any day, or select the check box to specify the days when the schedule should run.
7. Click **Apply**.
   A confirmation panel appears.
8. Click **OK**.

Delete a replication schedule

Perform the following steps to delete a replication schedule:

1. From the Replication Sets table on the primary system, select a replication set that has an associated schedule.
2. Select **Action > Manage Schedules**. The **Manage Schedules** panel opens.
3. Select the schedule to delete.
4. Click **Delete Schedule**.
   A confirmation panel appears.
5. Click **OK**.

9

Working in the Performance topic

Topics:

Viewing performance statistics

The Performance topic shows performance statistics for the following types of components: disks, disk groups, virtual pools, virtual tiers, host ports, controllers, and volumes. For more information about performance statistics, see About performance statistics.

You can view current statistics in tabular format for all component types, and historical statistics in graphical format for disks, disk groups, and virtual pools and tiers.

View performance statistics

1. In the Performance topic, select a component type from the Show list. The components table shows information about each component of that type in the system.
2. Select one or more components in the list.
3. Click **Show Data**. The Current Data area shows the sample time, which is the date and time when the data sample was collected. It also shows the total duration of all data samples, which is the time period between collection and display of the current sample, the previous sample, if any, and a table of current performance statistics for each selected component.
4. To view graphs of historical data for the selected disks, disk groups, virtual pools, or virtual tiers, select the **Historical Data** check box. The Historical Data area shows the time range of samples whose data is represented by the graphs, and the Total IOPS graph by default.
5. To specify either a time range or a count of historical statistics samples to display, perform the following:
   - Click **Set time** range. The Update Historical Statistics panel opens and shows the default count value of 100.
   - To specify a count, in the Count field, enter a value in the range of 5–100 and click **OK**.
   - To specify a time range, perform the following:
     - Select the **Time Range** check box.
     - Set date/time values for the starting and ending samples. The values must be between the current date/time and 6 months in the past. The ending values must be more recent than the starting values.

       NOTE: If you specify a time range, it is recommended to specify a range of 24 hours or less.
     - Click **OK**. In the Historical Data area, the Time Range values are updated to show the times of the oldest and newest samples displayed, and the graph for the selected components is updated.
6. To view different historical statistics, select a graph from the Statistics list. For a description of each graph, see Historical performance graphs on page 128.
7. To hide the legend in the upper right corner of a historical statistics graph, clear the **Show Legend** check box.

Historical performance graphs

The following table describes the graphs of historical statistics that are available for each component type. In the graphs, measurement units are automatically scaled to best represent the sample data within the page space.

Table 28. Historical performance

System component	Graph	Description
Disk, group, pool, tier	Total IOPS	Total number of read and write operations per second since the last sampling time.
Disk, group, pool, tier	Read IOPS	Number of read operations per second since the last sampling time.
Disk, group, pool, tier	Write IOPS	Number of write operations per second since the last sampling time.
Disk, group, pool, tier	Data Throughput	Overall rate at which data was read and written since the last sampling time.
Disk, group, pool, tier	Read Throughput	Rate at which data was read since the last sampling time.
Disk, group, pool, tier	Write Throughput	Rate at which data was written since the last sampling time.
Disk, group, pool, tier	Total I/Os	Number of read and write operations since the last sampling time.
Disk, group, pool, tier	Number of Reads	Number of read operations since the last sampling time.
Disk, group, pool, tier	Number of Writes	Number of write operations since the last sampling time.
Disk, group, pool, tier	Data Transferred	Total amount of data read and written since the last sampling time.
Disk, group, pool, tier	Data Read	Amount of data read since the last sampling time.
Disk, group, pool, tier	Data Written	Amount of data written since the last sampling time.
Disk, group	Average Response Time	Average response time for reads and writes since the last sampling time.
Disk, group	Average Read Response Time	Average response time for reads since the last sampling time.
Disk, group	Average Write Response Time	Average response time for writes since the last sampling time.
Disk, group	Average I/O Size	Average size of reads and writes since the last sampling time.
Disk, group	Average Read I/O Size	Average size of reads since the last sampling time.
Disk, group	Average Write I/O Size	Average size of writes since the last sampling time.
Disk, group	Number of Disk Errors	Number of disk errors since the last sampling time.
Disk, group	Queue Depth	Average number of pending I/O operations being serviced since the last sampling time. This value represents periods of activity only and excludes periods of inactivity.
Pool, tier	Number of Allocated Pages	Number of 4-MB pages allocated to volumes, based on writes to those volumes. Creating a volume does not cause any allocations. Pages are allocated as data is written.

Table 28. Historical performance (continued)

System component	Graph	Description
Tier	Number of Page Moves In	Number of pages moved into this tier from a different tier.
Tier	Number of Page Moves Out	Number of pages moved out of this tier to other tiers.
Tier	Number of Page Rebalances	Number of pages moved between disk groups in this tier to automatically load balance.
Tier	Number of Initial Allocations	Number of pages that are allocated as a result of host writes. This number does not include pages allocated as a result of background tiering page movement. (Tiering moves pages from one tier to another, so one tier will see a page deallocated, while another tier will show pages allocated; these background moves are not considered "initial allocations.")
Tier	Number of Unmaps	Number of 4-MB pages that are automatically reclaimed and deallocated because they are empty (they contain only zeroes for data).
Tier	Number of RFC Copies	Number of 4-MB pages copied from spinning disks to SSD read cache (read flash cache).
Tier	Number of Zero-Pages Reclaimed	Number of empty (zero-filled) pages that were reclaimed during this sample period.

Updating historical statistics

The Performance topic can show historical performance statistics for the following types of components: disks, disk groups, and virtual pools and tiers. By default, the newest 100 samples are shown. For more information about performance statistics, see About performance statistics.

Update displayed historical statistics

1. Display a historical statistics graph as described in Viewing performance statistics.
2. Select **Action > Update Historical Statistics**.
   The Update Historical Statistics panel opens and shows the default count value of 100.
3. To specify a count, in the **Count** field enter a value in the range of 5 to 100 and click **OK**.
4. To specify a time range, perform the following:
   - Select the **Time Range** check box.
   - Set date/time values for the starting and ending samples. The values must be between the current date/time and 6 months in the past. The ending values must be more recent than the starting values.

     NOTE: If you specify a time range, it is recommended to specify a range of 24 hours or less.
   - Click **OK**.

   In the Historical Data area of the Performance topic, the Time Range values are updated to show the times of the oldest and newest samples displayed. The graph for the selected components is updated.

Exporting historical performance statistics

You can export historical performance statistics in CSV format to a file on the network. You can then import the data into a spreadsheet or other third-party application.

The number of data samples downloaded is fixed at 100 to limit the size of the data file to be generated and transferred. The default is to retrieve all the available data, up to six months, aggregated into 100 samples. You can specify a different time range by specifying a start and end time. If the specified time range spans more than 100 15-minute samples, the data will be aggregated into 100 samples.

The resulting file will contain a row of property names and a row for each data sample.

Export historical performance statistics

1. In the Performance topic, from the Show list, select **Disks, Disk Groups, Virtual Pools**, or **Virtual Tiers**.
2. Select at least one component.

   NOTE: Statistics are exported for all disks, regardless of which components are selected.

3. Select **Action > Export Historical Statistics**.
   The Export Historical Statistics panel opens.
4. To specify a time range, perform the following:
   - Select the **Time Range** check box.
   - Set date/time values for the starting and ending samples. The values must be between the current date/time and 6 months in the past. The ending values must be more recent than the starting values.

     NOTE: If you specify a time range, it is recommended to specify a range of 24 hours or less.
5. Click **OK**.

   NOTE: In Microsoft Internet Explorer, if the download is blocked by a security bar, select its Download File option. If the download does not succeed the first time, return to the Export Historical Statistics panel and retry the export operation.

6. When prompted to open or save the file, click **Save**.
   - If you are using Firefox or Chrome and have a download directory set, the file `Disk_Performance.csv` is saved there.
   - Otherwise, you are prompted to specify the file location and name. The default file name is `Disk_Performance.csv`. Change the name to identify the system, controller, and date.
7. Click **OK**.

Resetting performance statistics

You can reset (clear) the current or historical performance statistics for all components. When you reset statistics, an event is logged and new data samples will continue to be stored every five minutes.

Reset performance statistics

1. In the Performance topic, select **Action > Reset All Statistics**.
   The Reset All Statistics panel opens.
2. Perform one of the following:
   - To reset current statistics, select **Current Data**.
   - To reset historical statistics, select **Historical Data**.
3. Click **OK**.
   A confirmation panel appears.
4. Click **Yes** to continue. Otherwise, click **No**. If you clicked Yes, the statistics are cleared.

10

Working in the banner and footer

Topics:

Banner and footer overview

The banner of the PowerVault Manager interface contains four panels that are next to each other:

- The system panel shows system and firmware information.
- The connection information panel shows information about the link between the PowerVault Manager and the storage system.
- The system date/time panel shows system date and time information.
- The user information panel shows the name of the logged-in user.

The footer of the PowerVault Manager interface contains six panels that are next to each other:

- The system health panel shows the current health of the system and each controller.
- The event panel shows the last 1,000 or fewer events (organized by event type) that the system has logged.
- The capacity utilization panel shows a pair of color-coded bars that represent the physical capacity of the system and how the capacity is allocated and used.
- The host I/O panel shows a pair of color-coded bars for each controller that has active I/O, which represent the current IOPS for all ports and the current data throughput (MB/s) for all ports.
- The tier I/O panel shows a color-coded bar for each virtual pool (A, B, or both) that has active I/O.
- The activity panel shows notifications of recent system activities.

If you hover your cursor over any of these panels except for the activity panel, an additional panel with more detailed information appears. Some of these panels have menus that enable you to perform related tasks. There are two icons for panels that have a menu: for the banner and for the footer. Click anywhere in the panel to display the menu.

Viewing system information

The system panel in the banner shows the system name and the firmware bundle version installed for the controller that you are accessing.

Hover the cursor over this panel to display the System Information panel, which shows the system name, vendor, location, contact, and information. It also shows the firmware bundle version for each controller (A and B) and the service tag identifier.

The icon indicates that the panel has a menu. Click anywhere in the panel to display a menu to change system information settings and system services settings, update firmware, restart or shut down controllers (page 83) and view SSL certificate information.

Viewing certificate information

By default, the system generates a unique SSL certificate for each controller. For the strongest security, you can replace the default system-generated certificate with a certificate issued from a trusted certificate authority.

The Certificate Information panel shows information for the active SSL certificates that are stored on the system for each controller. Tabs A and B contain unformatted certificate text for each of the corresponding controllers. The panel also shows one of the following status values as well as the creation date for each certificate:

- Customer-supplied. Indicates that the controller is using a certificate that you have uploaded.
- System-generated. Indicates that the controller is using an active certificate and key that were created by the controller.
- Unknown status. Indicates that the controller's certificate cannot be read. This most often occurs when a controller is restarting, the certificate replacement process is still in process, or you have selected the tab for a partner controller in a single-controller system.

You can use your own certificates by uploading them through FTP or SFTP or by using the `contents` parameter of the `create certificate` CLI command to create certificates with your own unique certificate content. For a new certificate to take effect, you must first restart the controller for it. For information on how to restart a controller, see Restarting or shutting down controllers.

To verify that the certificate replacement was successful and the controller is using the certificate that you have supplied, make sure the certificate status is `customer-supplied`, the creation date is correct, and the certificate content is the expected text.

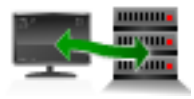
View certificate information

1. In the banner, click the system panel and select **Show Certificate Info**.
   The Certificate Information panel opens.
2. After you have finished viewing certificate information, click **Close**.

Viewing connection information

The icon in the connection panel in the banner shows the current state of the management link between the PowerVault Manager and the storage system. The connection information table shows the icon that appears for each state.

Table 29. Connection information

Icon	Meaning
	The management link is connected and the system is up. Animation shows when data is being transferred.
	The management link is connected but the system is down.
	The management link is not connected.

Hover the cursor over this panel to display the Connection Information panel, which shows the connection and system states.

Viewing system date and time information

The date/time panel in the banner shows the system date and time in the following format:

`YYYY-MM-DD`

`HH:MM:SS`

The icon indicates that the panel has a menu. Click anywhere in the panel to display a menu to change date and time settings.

Changing date and time settings

You can change the storage system date and time, which appear in the date/time panel in the banner. It is important to set the date and time so that entries in system logs and notifications have correct time stamps.

You can set the date and time manually or configure the system to use NTP to obtain them from a network-attached server. When NTP is enabled, and if an NTP server is available, the system time and date can be obtained from the NTP server. This allows multiple storage devices, hosts, log files, and so forth to be synchronized. If NTP is enabled but no NTP server is present, the date and time are maintained as if NTP was not enabled.

NTP server time is provided in the UTC time scale, which provides several options:

- To synchronize the times and logs between storage devices installed in multiple time zones, set all the storage devices to use UTC.
- To use the local time for a storage device, set its time zone offset.
- If a time server can provide local time rather than UTC, configure the storage devices to use that time server, with no further time adjustment.

Whether NTP is enabled or disabled, the storage system does not automatically make time adjustments for Daylight Saving Time. You must make that adjustment manually.

NOTE: If you change the time zone of the secondary system in a replication set whose primary and secondary systems are in different time zones, you must restart the system to enable management interfaces to show proper time values for replication operations.

Use manual date and time settings

Perform the following steps to manually set the date and time settings:

1. In the banner, click the date/time panel and select **Set Date and Time**.
   The Date and Time panel opens.
2. Clear the **Network Time Protocol (NTP)** checkbox.
3. To set the Date value, type the current date in the format `YYYY-MM-DD`.
4. To set the Time value, type the current time in the format `HH:MM`.
   NOTE: The system time uses a 24-hour clock.
5. Perform one of the following:
   - To save your settings and continue configuring your system, click **Apply**.
   - To save your settings and close the panel, click **Apply and Close**.

   A confirmation panel appears.
6. Click **OK**.

Obtain the date and time from an NTP server

1. In the banner, click the date/time panel and select Set **Date and Time**.
   The Set Date and Time panel opens.
2. Select the **Network Time Protocol (NTP)** check box.
3. Perform one of the following:
   - To have the system retrieve time values from a specific NTP server, enter its IP address in the NTP Server Address field.
   - To have the system listen for time messages sent by an NTP server in broadcast mode, clear the NTP Server Address field.
4. In the NTP Time Zone Offset field, enter the time zone as an offset in hours, and optionally, minutes, from UTC. For example, the Pacific Time Zone offset is -8 during Pacific Standard Time or -7 during Pacific Daylight Time. The offset for Bangalore, India is +5:30.
5. Perform one of the following:
   - To save your settings and continue configuring your system, click **Apply**.
   - To save your settings and close the panel, click **Apply and Close**.

   A confirmation panel appears.
6. Click **Yes** to save your changes. Otherwise, click **No**.

Viewing user information

The user panel in the banner shows the name of the signed-in user.

Hover the cursor over this panel to display the User Information panel, which shows the roles, accessible interfaces, and session timeout for this user.

The icon indicates that the panel has a menu. Click anywhere in the panel to change settings for the signed-in user (`monitor` role) or to manage all users (`manage` role). For more information on user roles and settings, see Managing users.

Viewing health information

The health panel in the footer shows the current health of the system and each controller.

Hover the cursor over this panel to display the System Health panel, which shows the health state. If the system health is not OK, the System Health panel also shows information about resolving problems with unhealthy components.

The icon indicates that the panel has a menu. Click anywhere in the panel to display a menu to change notification settings, save log data, and view system information.

Saving log data to a file

To help service personnel diagnose a system problem, you might be asked to provide system log data. Using the PowerVault Manager, you can save the following log data to a compressed zip file:

- Device status summary, which includes basic status and configuration data for the system
- The event log from each controller
- The debug log from each controller
- The boot log, which shows the startup sequence, from each controller
- Critical error dumps from each controller, if critical errors have occurred
- CAPI traces from each controller

NOTE: The controllers share one memory buffer for gathering log data and for loading firmware. Do not try to perform more than one log saving operation at a time, or to perform a firmware update operation while performing a log saving operation.

Save log data from the storage system to a network location

1. In the footer, click the health panel and select **Save Logs**. The Save Logs panel opens.
2. Enter your name, email address, and phone number so support personnel will know who provided the data.

   The contact name value can include a maximum of 100 bytes, using all characters except the following: " ' ` &

   The email address can include a maximum of 100 characters., except the following: " < > \

   The phone number value can include only digits and no other characters.
3. Enter comments describing the problem and specifying the date and time when the problem occurred. This information helps service personnel when they analyze the log data. Comment text can include a maximum of 500 bytes.
4. Click **OK**. Log data is collected, which takes several minutes.

   NOTE: In Microsoft Internet Explorer, if the download is blocked by a security bar, select its Download File option. If the download does not succeed the first time, return to the Save Logs panel and retry the save operation.
5. When prompted to open or save the file, click **Save**.
   - If you are using Chrome, `store.zip` is saved to the downloads folder.
   - If you are using Firefox and have a download folder set, `store.zip` is saved to that folder.
   - Otherwise, you are prompted to specify the file location and name. The default file name is `store.zip`. Change the name to identify the system, controller, and date.

   NOTE: The file must be uncompressed before the files it contains can be examined. The first file to examine for diagnostic data is `store_yyyy_mm_dd__hh_mm_ss.logs`.

Viewing event information

If you are having a problem with the system, review the event log before calling technical support. Information shown in the event log might enable you to resolve the problem.

To view the event log, in the footer, click the events panel and select **Show Event List**. The Event Log Viewer panel opens. The panel shows a tabular view of the 1000 most recent events logged by either controller. All events are logged, regardless of notification settings. For information about notification settings, see Setting system notification settings on page 45.

The event panel in the footer shows the numbers of the following types of events that the system has logged:

- Sev. One of the following severity icons:
  - **Critical**. A failure occurred that may cause a controller to shut down. Correct the problem *immediately*.
  - **Error**. A failure occurred that may affect data integrity or system stability. Correct the problem as soon as possible.
  - **Warning**. A problem occurred that may affect system stability but not data integrity. Evaluate the problem and correct it if necessary.
  - **Informational**. A configuration or state change occurred, or a problem occurred that the system corrected. No action is required.
  - **Resolved**. A condition that caused an event to be logged has been resolved. No action is required.
- Date/Time. The date and time when the event occurred, shown in the format *year-month-day hour:minutes:seconds*. Time stamps have one-second granularity.
- ID. The event ID. The prefix A or B identifies the controller that logged the event.
- Code. An event code that helps you and support personnel diagnose problems.
- Message. Brief information about the event. Click the message to show or hide additional information and recommended actions.
- Ctrl. The ID of the controller that logged the event.

Hover the cursor over the left side of this area to display the Critical & Error Event Information panel, which shows:

- The number of events with Critical and Error severity that have occurred in the past 24 hours or in the last 1000 events
- The date and time when the last most-severe event occurred

The icon indicates that the panel has a menu. Click anywhere in the panel to display a menu to view the most recent 1000 events on Viewing the event log on page 136 and set up system notification settings on Setting system notification settings on page 45.

When reviewing the event log, look for recent Critical, Error, or Warning events. For each, click the message to view additional information and recommended actions. Follow the recommended actions to resolve the problems.

Viewing the event log

If you are having a problem with the system, review the event log before calling technical support. Information shown in the event log might enable you to resolve the problem.

To view the event log, in the footer, click the events panel and select **Show Event List**. The Event Log Viewer panel opens. The panel shows a tabular view of the 1000 most recent events logged by either controller. All events are logged, regardless of notification settings. For information about notification settings, see Setting system notification settings on page 45.

For each event, the panel shows the following information:

- Sev. One of the following severity icons:
  - **Critical**. A failure occurred that may cause a controller to shut down. Correct the problem *immediately*.
  - **Error**. A failure occurred that may affect data integrity or system stability. Correct the problem as soon as possible.
  - **Warning**. A problem occurred that may affect system stability but not data integrity. Evaluate the problem and correct it if necessary.
  - **Informational**. A configuration or state change occurred, or a problem occurred that the system corrected. No action is required.
  - **Resolved**. A condition that caused an event to be logged has been resolved. No action is required.
- Date/Time. The date and time when the event occurred, shown in the format *year-month-day hour:minutes:seconds*. Time stamps have one-second granularity.
- ID. The event ID. The prefix A or B identifies the controller that logged the event.
- Code. An event code that helps you and support personnel diagnose problems.
- Message. Brief information about the event. Click the message to show or hide additional information and recommended actions.
- Ctrl. The ID of the controller that logged the event.

When reviewing the event log, look for recent Critical, Error, or Warning events. For each, click the message to view additional information and recommended actions. Follow the recommended actions to resolve the problems.

Resources for diagnosing and resolving problems

- The troubleshooting chapter and LED descriptions appendix in your product's Deployment Guide
- The topics about verifying component failure in your product's FRU Installation and Replacement Guide
- The full list of event codes, descriptions, and recommended actions in your product's event documentation

Viewing capacity information

The capacity panel in the footer shows a pair of color-coded bars. The lower bar represents the physical capacity of the system, and the upper bar identifies how the capacity is allocated and used.

Hover the cursor over a segment to see the storage type and size that is represented by that segment. For instance, in a system where storage is being used, the bottom bar has color-coded segments that show the total unused disk space and space that is used by disk groups. The total of these segments is equal to the total disk capacity of the system.

Hover the cursor over a segment to see the storage type and size that is represented by that segment. For instance, in a system where both virtual and linear storage is being used, the bottom bar has color-coded segments that show the total unused disk space that is allotted for virtual and linear disk groups and the space that is used by the disk groups. The total of these segments is equal to the total disk capacity of the system.

In this same system, the top bar has color-coded segments for reserved, allocated, and unallocated space for disk groups. If very little disk group space is used for any of these categories, it will not be visually represented.

In this same system, the top bar has color-coded segments for reserved, allocated, and unallocated space for virtual and linear disk groups. If very little disk group space is used for any of these categories, it will not be visually represented.

Reserved space refers to space that is unavailable for host use. It consists of RAID parity and the metadata that is needed for internal management of data structures. The terms allocated space and unallocated space have different meanings for the virtual and linear storage technologies. For virtual storage, allocated space refers to the amount of space that is consumed by data that is written to the pool. Unallocated space is the difference between the space that is designated for all volumes and the allocated space.

Reserved space refers to space that is unavailable for host use. It consists of RAID parity and the metadata that is needed for internal management of data structures. The terms allocated space and unallocated space have different meanings for the virtual and linear storage technologies. Allocated space, for virtual storage, refers to the amount of space that is consumed by data that is written to the pool. Unallocated space is the difference between the space that is designated for all volumes and the allocated space.

For linear storage, allocated space is the space that is designated for all volumes. (When a linear volume is created, space equivalent to the volume size is reserved for it. This is not the case for virtual volumes.) Unallocated space is the difference between the overall and allocated space.

Hover the cursor over a segment of a bar to see the storage size represented by that segment. Point anywhere in this panel to see the following information about capacity utilization in the Capacity Utilization panel:

- **Total Disk Capacity**: The total physical capacity of the system
- **Unused**: The total unused disk capacity of the system
- **Global Spares**: The total global spare capacity of the system
- **Virtual/Linear Disk Groups**: The capacity of the disk groups, both total and by pool.
- **Reserved**: The reserved space for the disk groups, both total and by pool
- **Allocated**: The allocated space for the disk groups, both total and by pool
- **Unallocated**: The unallocated space for the disk groups, both total and by pool
- **Uncommitted**: For virtual disk groups, the uncommitted space in each pool (total space minus the allocated and unallocated space) and total uncommitted space

Viewing host information

The host I/O panel in the footer shows a pair of color-coded bars for each controller that has active I/O. In each pair, the upper bar represents the current IOPS for all ports, which is calculated over the interval since these statistics were last requested or reset, and the lower bar represents the current data throughput (MB/s) for all ports, which is calculated over the interval since these statistics were last requested or reset. The pairs of bars are sized to represent the relative values for each controller.

Hover the cursor over a bar to see the value represented by that bar.

Hover the cursor anywhere in the panel to display the Host I/O Information panel, which shows the current port IOPS and data throughput (MB/s) values for each controller.

Viewing tier information

The tier I/O panel in the footer shows a color-coded bar for each virtual pool (A, B, or both) that has active I/O. The bars are sized to represent the relative IOPS for each pool. Each bar contains a segment for each tier that has active I/O. The segments are sized to represent the relative IOPS for each tier.

Hover the cursor over a segment to see the value represented by that segment.

Hover the cursor anywhere in this panel to display the Tier I/O Information panel, which shows the following details for each tier in each virtual pool:

- Current IOPS for the pool, calculated over the interval since these statistics were last requested or reset.
- Current data throughput (MB/s) for the pool, calculated over the interval since these statistics were last requested or reset.

The panel also contains combined total percentages of IOPS and current data throughput (MB/s) for both pools.

Viewing recent system activity

The activity panel in the footer shows notifications of recent system activities, such as the loading of configuration data upon sign-in, events with the Resolved status, and scheduled tasks.

To view past notifications for this PowerVault Manager session, click the activity panel in the footer and select Notification History. For more information, see Viewing the notification history.

Viewing the notification history

The Notification History panel shows past activity notifications for this PowerVault Manager session. You can page through listed items by using the following buttons:

 Show next set of items

 Reached end of list

 Show previous set of items

 Reached start of list

When you sign out, the list is cleared.

View notification history

1. Click the activity panel in the footer and select **Notification History**.
   The Notification History panel opens.
2. View activity notifications, using the navigation buttons.
3. Click **Close** when you are finished.

A

Other management interfaces

Topics:

SNMP reference

This appendix describes the Simple Network Management Protocol (SNMP) capabilities that Dell EMC storage systems support. This includes standard MIB-II, the FibreAlliance SNMP Management Information Base (MIB) version 2.2 objects, and enterprise traps.

The storage systems can report their status through SNMP. SNMP provides basic discovery using MIB-II, more detailed status with the FA MIB 2.2, and asynchronous notification using enterprise traps.

SNMP is a widely used network monitoring and control protocol. It is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite.

SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Data is passed from SNMP agents reporting activity on each network device to the workstation console used to oversee the network. The agents return information contained in a Management Information Base (MIB), which is a data structure that defines what is obtainable from the device and what can be controlled (turned on and off, etc.).

Supported SNMP versions

The storage systems allow use of SNMPv2c or SNMPv3. SNMPv2c uses a community-based security scheme. For improved security, SNMPv3 provides authentication of the network management system that is accessing the storage system, and encryption of the information transferred between the storage system and the network management system.

When SNMPv3 is disabled, SNMPv2c will be active. When SNMPv3 is enabled, SNMPv2c will only have access to the MIB-II common system information. This allows device discovery.

Whether you use SNMPv2c or v3, note that the only SNMP-writable information is the system contact, name, and location. System data, configuration, and state cannot be changed via SNMP.

Standard MIB-II behavior

MIB-II is implemented to support basic discovery and status.

An SNMP object identifier (OID) is a number assigned to devices in a network for identification purposes. OID numbering is hierarchical. Using the IETF notation of digits and dots resembling very long IP addresses, various registries such as ANSI assign high-level numbers to vendors and organizations. They, in turn, append digits to the number to identify individual devices or software processes.

The system object identifier (`sysObjectID`) for Dell EMC storage systems is 1.3.6.1.4.1.674. System uptime is an offset from the first time this object is read.

In the system group, all objects can be read. The contact, name, and location objects can be set.

In the interfaces group, an internal PPP interface is documented, but it is not reachable from external to the device.

The address translation (at) and external gateway protocol (egp) groups are not supported.

Enterprise traps

Traps can be generated in response to events occurring in the storage system. These events can be selected by severity and by individual event type. A maximum of three SNMP trap destinations can be configured by IP address.

Enterprise event severities are informational, minor, major, and critical. There is a different trap type for each of these severities. The trap format is represented by the enterprise traps MIB. Information included is the event ID, the event code type, and a text description generated from the internal event. Equivalent information can also be sent using email or popup alerts to users who are logged in to the PowerVault Manager.

FA MIB 2.2 SNMP behavior

The FA MIB 2.2 objects are in compliance with the FibreAlliance MIB v2.2 Specification (FA MIB2.2 Spec).

FA MIB 2.2 was never formally adopted as a standard, but it is widely implemented and contains many elements useful for storage products. This MIB generally does not reference and integrate with other standard SNMP information. It is implemented under the experimental subtree.

Significant status within the device includes such elements as its temperature and power sensors, the health of its storage elements such as virtual disks, and the failure of any redundant component including an I/O controller. While sensors can be individually queried, for the benefit of network management systems all the above elements are combined into an "overall status" sensor. This is available as the unit status (`connUnitStatus` for the only unit).

The revisions of the various components within the device can be requested through SNMP.

The port section is only relevant to products with Fibre Channel host ports.

The event table allows 400 recently-generated events to be requested. Informational, minor, major, or critical event types can be selected. Whichever type is selected enables the capture of that type and more severe events. This mechanism is independent of the assignment of events to be generated into traps.

The traps section is not supported. It has been replaced by an ability to configure trap destinations using the CLI or the PowerVault Manager. The statistics section is not implemented.

The following table lists the MIB objects, their descriptions and the value set in ME4 Series storage systems. Unless specified otherwise, objects *are not* settable.

Table 30. FA MIB 2.2 objects, descriptions, and values

Object	Description	Value
`RevisionNumber`	Revision number for this MIB	220
`UNumber`	Top-level URL of this device, for example, `http://10.1.2.3`. If a web server is not present on the device, this string is empty in accordance with the FA MIB2.2 Spec.	Default: `http://10.0.0.1`
`StatusChangeTime`	`sysuptime` timestamp of the last status change event, in centiseconds. `sysuptime` starts at 0 when the Storage Controller boots and keeps track of the up time. `statusChangeTime` is updated each time an event occurs.	0 at startup
`ConfigurationChangeTime`	`sysuptime` timestamp of the last configuration change event, in centiseconds. `sysuptime` starts at 0 when the Storage Controller boots and keeps track of the up time. configurationChangeTime is updated each time an event occurs.	0 at startup
`ConnUnitTableChangeTime`	`sysuptime` timestamp of the last update to the `connUnitTable` (an entry was either added or deleted), in centiseconds.	0 always (entries are not added to or deleted from the `connUnitTable`)
connUnit Table	**Includes the following objects as specified by the FA MIB2.2 Spec:**	

Table 30. FA MIB 2.2 objects, descriptions, and values (continued)

Object	Description	Value
connUnitId	Unique identification for this connectivity unit	Total of 16 bytes comprised of 8 bytes of the node WWN or similar serial number-based identifier (for example,1000005013b05211) with the trailing 8 bytes equal to zero
connUnitGlobalId	Same as connUnitId	Same as connUnitId
connUnitType	Type of connectivity unit	storage-subsystem (11)
connUnitNumports	Number of host ports in the connectivity unit	Number of host ports
connUnitState	Overall state of the connectivity unit	online (2) or unknown (1), as appropriate
connUnitStatus	Overall status of the connectivity unit	ok (3), warning (4), failed (5), or unknown (1), as appropriate
connUnitProduct	Connectivity unit vendor's product model name	Model string
connUnitSn	Serial number for this connectivity unit	Serial number string
connUnitUpTime	Number of centiseconds since the last unit initialization	0 at startup
connUnitUrl	Same as systemURL	Same as systemURL
connUnitDomainId	Not used; set to all 1s as specified by the FA MIB2.2 Spec	0xFFFF
connUnitProxyMaster	Stand-alone unit returns yes for this object	yes (3) since this is a stand-alone unit
connUnitPrincipal	Whether this connectivity unit is the principal unit within the group of fabric elements. If this value is not applicable, returns unknown.	unknown (1)
connUnitNumSensors	Number of sensors in the connUnitSensorTable	33
connUnitStatusChangeTime	Same as statusChangeTime	Same as statusChangeTime
connUnitNumRevs	Number of revisions in the connUnitRevsTable	16
connUnitNumZones	Not supported	0
connUnitModuleId	Not supported	16 bytes of 0s
connUnitName	Settable: Display string containing a name for this connectivity unit	Default: Uninitialized Name
connUnitInfo	Settable: Display string containing information about this connectivity unit	Default: Uninitialized Info
connUnitControl	Not supported	invalid (2) for an SNMP GET operation and not settable through an SNMP SET operation.
connUnitContact	Settable: Contact information for this connectivity unit	Default: Uninitialized Contact
connUnitLocation	Settable: Location information for this connectivity unit	Default: Uninitialized Location

Table 30. FA MIB 2.2 objects, descriptions, and values (continued)

Object	Description	Value
connUnitEventFilter	Defines the event severity that will be logged by this connectivity unit. Settable only through the PowerVault Manager.	Default: info (8)
connUnitNumEvents	Number of events currently in the connUnitEventTable	Varies as the size of the Event Table varies
connUnitMaxEvents	Maximum number of events that can be defined in the connUnitEventTable	400
connUnitEventCurrID	Not supported	0
connUnitRevs Table	**Includes the following objects as specified by the FA MIB2.2 Spec:**	
connUnitRevsUnitId	connUnitId of the connectivity unit that contains this revision table	Same as connUnitId
connUnitRevsIndex	Unique value for each connUnitRevsEntry between 1 and connUnitNumRevs	See External details for certain FA MIB 2.2 objects
connUnitRevsRevId	Vendor-specific string identifying a revision of a component of the connUnit	String specifying the code version. Reports "Not Installed or Offline" if module information is not available.
connUnitRevsDescription	Display string containing description of a component to which the revision corresponds	See External details for certain FA MIB 2.2 objects
connUnitSensor Table	**Includes the following objects as specified by the FA MIB2.2 Spec:**	
connUnitSensorUnitId	connUnitId of the connectivity unit that contains this sensor table	Same as connUnitId
connUnitSensorIndex	Unique value for each connUnitSensorEntry between 1 and connUnitNumSensors	See External details for certain FA MIB 2.2 objects
connUnitSensorName	Display string containing textual identification of the sensor intended primarily for operator use	See External details for certain FA MIB 2.2 objects
connUnitSensorStatus	Status indicated by the sensor	ok (3), warning (4), or failed (5) as appropriate for FRUs that are present, or other (2) if FRU is not present.
connUnitSensorInfo	Not supported	Empty string
connUnitSensorMessage	Description the sensor status as a message	connUnitSensorName followed by the appropriate sensor reading. Temperatures display in both Celsius and Fahrenheit. For example, CPU Temperature (Controller Module A): 48C 118F). Reports "Not installed" or "Offline" if data is not available.
connUnitSensorType	Type of component being monitored by this sensor	See External details for certain FA MIB 2.2 objects
connUnitSensor Characteristic	Characteristics being monitored by this sensor	See External details for certain FA MIB 2.2 objects
connUnitPort Table	**Includes the following objects as specified by the FA MIB2.2 Spec:**	
connUnitPortUnitId	connUnitId of the connectivity unit that contains this port	Same as connUnitId

Table 30. FA MIB 2.2 objects, descriptions, and values (continued)

Object	Description	Value
connUnitPortIndex	Unique value for each connUnitPortEntry between 1 and connUnitNumPorts	Unique value for each port, between 1 and the number of ports
connUnitPortType	Port type	not-present (3), or n-port (5) for point-to-point topology, or l-port (6)
connUnitPortFCClassCap	Bit mask that specifies the classes of service capability of this port. If this is not applicable, returns all bits set to zero.	Fibre Channel ports return 8 for class-three
connUnitPortFCClassOp	Bit mask that specifies the classes of service that are currently operational. If this is not applicable, returns all bits set to zero.	Fibre Channel ports return 8 for class-three
connUnitPortState	State of the port hardware	unknown (1), online (2), offline (3), bypassed (4)
connUnitPortStatus	Overall protocol status for the port	unknown (1), unused (2), ok (3), warning (4), failure (5), notparticipating(6), initializing (7), bypass (8)
connUnitPortTransmitterType	Technology of the port transceiver	unknown (1) for Fibre Channel ports
connUnitPortModuleType	Module type of the port connector	unknown (1)
connUnitPortWwn	Fibre Channel World Wide Name (WWN) of the port if applicable	WWN octet for the port, or empty string if the port is not present
connUnitPortFCId	Assigned Fibre Channel ID of this port	Fibre Channel ID of the port. All bits set to 1 if the Fibre Channel ID is not assigned or if the port is not present
connUnitPortSn	Serial number of the unit (for example, for a GBIC). If this is not applicable, returns an empty string.	Empty string
connUnitPortRevision	Port revision (for example, for a GBIC)	Empty string
connUnitPortVendor	Port vendor (for example, for a GBIC)	Empty string
connUnitPortSpeed	Speed of the port in KByte per second (1 KByte = 1000 Byte)	Port speed in KByte per second, or 0 if the port is not present
connUnitPortControl	Not supported	invalid (2) for an SNMP GET operation and not settable through an SNMP SET operation
connUnitPortName	String describing the addressed port	See External details for certain FA MIB 2.2 objects
connUnitPortPhysicalNumber	Port number represented on the hardware	Port number represented on the hardware
connUnitPortStatObject	Not supported	0 (No statistics available)
connUnitEvent Table	**Includes the following objects as specified by the FA MIB2.2 Spec:**	
connUnitEventUnitId	connUnitId of the connectivity unit that contains this port	Same as connUnitId
connUnitEventIndex	Index into the connectivity unit's event buffer, incremented for each event	Starts at 1 every time there is a table reset or the unit's event table reaches its maximum index value
connUnitEventId	Internal event ID, incremented for each event, ranging between 0 and connUnitMaxEvents	Starts at 0 every time there is a table reset or connUnitMaxEvents is reached

Table 30. FA MIB 2.2 objects, descriptions, and values (continued)

Object	Description	Value
connUnitREventTime	Real time when the event occurred, in the following format: DDMMYYYY HHMMSS	0 for logged events that occurred prior to or at startup
connUnitSEventTime	sysuptime timestamp when the event occurred	0 at startup
connUnitEventSeverity	Event severity level	error (5), warning (6) or info (8)
connUnitEventType	Type of this event	As defined in CAPI
connUnitEventObject	Not used	0
connUnitEventDescr	Text description of this event	Formatted event, including relevant parameters or values
connUnitLink Table	**Not supported**	**N/A**
connUnitPortStatFabric Table	**Not supported**	**N/A**
connUnitPortStatSCSI Table	**Not supported**	**N/A**
connUnitPortStatLAN Table	**Not supported**	**N/A**
SNMP Traps	**The following SNMP traps are supported:**	
trapMaxClients	Maximum number of trap clients	3
trapClientCount	Number of trap clients currently enabled	1 if traps enabled; 0 if traps not enabled
connUnitEventTrap	This trap is generated each time an event occurs that passes the connUnitEventFilter and the trapRegFilter	N/A
trapReg Table	**Includes the following objects per the FA MIB2.2 Spec**	
trapRegIpAddress	IP address of a client registered for traps	IP address set by user
trapRegPort	User Datagram Protocol (UDP) port to send traps to for this host	162
trapRegFilter	Settable: Defines the trap severity filter for this trap host. The connUnit will send traps to this host that have a severity level less than or equal to this value.	Default: warning (6)
trapRegRowState	Specifies the state of the row	READ: rowActive (3) if traps are enabled. Otherwise rowInactive(2) WRITE: Not supported

External details for certain FA MIB 2.2 objects

Tables in this section specify values for certain objects described in the following table:

Table 31. connUnitRevsTable index and description values

connUnitRevsIndex	connUnitRevsDescription
1	CPU TypeforStorageController(Controller A)
2	Bundle revisionforController(Controller A)
3	Build dateforStorageController(Controller A)

Table 31. connUnitRevsTable index and description values (continued)

connUnitRevsIndex	connUnitRevsDescription
4	Code revisionforStorageController(Controller A)
5	Code baselevelforStorageController(Controller A)
6	FPGA code revisionfor Memory Controller(Controller A)
7	Loader code revisionforStorageController(Controller A)
8	CAPI revision (Controller A)
9	Code revisionfor Management Controller(Controller A)
10	Loader code revisionfor Management Controller(Controller A)
11	Code revisionfor Expander Controller(Controller A)
12	CPLD code revision(Controller A)
13	Hardware revision (Controller A)
14	Host interface module revision(Controller A)
15	HIM revision(Controller A)
16	Backplane type (Controller A)
17	Host interfacehardware(chip)revision(Controller A)
18	Disk interface hardware (chip) revision (Controller A)
19	CPU TypeforStorageController(Controller B)
20	Bundle revisionforController(Controller B)
21	Build dateforStorageController(Controller B)
22	Code revisionforStorageController(Controller B)
23	Code baselevelforStorageController(Controller B)
24	FPGA code revisionfor Memory Controller(Controller B)
25	Loader code revisionforStorageController(Controller B)
26	CAPI revision (Controller B)
27	Code revisionfor Management Controller(Controller B)
28	Loader code revisionfor Management Controller(Controller B)
29	Code revisionfor Expander Controller(Controller B)
30	CPLD code revision(Controller B)
31	Hardware revision (Controller B)
32	Host interface module revision(Controller B)
33	HIM revision(Controller B)
34	Backplane type (Controller B)
35	Host interfacehardware(chip)revision(Controller B)
36	Disk interface hardware (chip) revision (Controller B)

External details for connUnitSensorTable

Table 32. connUnitSensorTable index, name, type, and characteristic values

connUnitSensorIndex	connUnitSensorName	connUnitSensorType	connUnitSensor Characteristic
1	Onboard Temperature 1 (Controller A)	board(8)	temperature(3)
2	Onboard Temperature 1 (Controller B)	board(8)	temperature(3)
3	Onboard Temperature 2 (Controller A)	board(8)	temperature(3)
4	Onboard Temperature 2 (Controller B)	board(8)	temperature(3)
5	Onboard Temperature 3 (Controller A)	board(8)	temperature(3)
6	Onboard Temperature 3 (Controller B)	board(8)	temperature(3)
7	Disk Controller Temperature (Controller A)	board(8)	temperature(3)
8	Disk Controller Temperature (Controller B)	board(8)	temperature(3)
9	Memory ControllerTemperature(Controller A)	board(8)	temperature(3)
10	Memory ControllerTemperature(Controller B)	board(8)	temperature(3)
11	Capacitor Pack Voltage (Controller A)	board(8)	power(9)
12	Capacitor Pack Voltage (Controller B)	board(8)	power(9)
13	Capacitor Cell 1 Voltage(Controller A)	board(8)	power(9)
14	Capacitor Cell 1 Voltage(Controller B)	board(8)	power(9)
15	Capacitor Cell 2 Voltage(Controller A)	board(8)	power(9)
16	Capacitor Cell 2 Voltage(Controller B)	board(8)	power(9)
17	Capacitor Cell 3 Voltage(Controller A)	board(8)	power(9)
18	Capacitor Cell 3 Voltage(Controller B)	board(8)	power(9)
19	Capacitor Cell 4 Voltage(Controller A)	board(8)	power(9)
20	Capacitor Cell 4 Voltage(Controller B)	board(8)	power(9)
21	Capacitor Charge Percent (Controller A)	board(8)	other(2)

Table 32. connUnitSensorTable index, name, type, and characteristic values (continued)

connUnitSensorIndex	connUnitSensorName	connUnitSensorType	connUnitSensor Characteristic
22	Capacitor Charge Percent (Controller B)	board(8)	other(2)
23	Overall Status	enclosure(7)	other(2)
24	Upper IOM Temperature(Controller A)	enclosure(7)	temperature(3)
25	Lower IOM Temperature(Controller B)	enclosure(7)	temperature(3)
26	Power Supply 1 (Left)Temperature	power-supply(5)	temperature(3)
27	Power Supply 2 (Right)Temperature	power-supply(5)	temperature(3)
28	Upper IOM Voltage, 12V (Controller A)	enclosure(7)	power(9)
29	Upper IOM Voltage, 5V (Controller A)	enclosure(7)	power(9)
30	Lower IOM Voltage, 12V (Controller B)	enclosure(7)	power(9)
31	Lower IOM Voltage, 5V (Controller B)	enclosure(7)	power(9)
32	Power Supply 1 (Left)Voltage, 12V	power-supply(5)	power(9)
33	Power Supply 1 (Left)Voltage, 5V	power-supply(5)	power(9)
34	Power Supply 1 (Left)Voltage, 3.3V	power-supply(5)	power(9)
35	Power Supply 2 (Right)Voltage, 12V	power-supply(5)	power(9)
36	Power Supply 2 (Right)Voltage, 5V	power-supply(5)	power(9)
37	Power Supply 2 (Right)Voltage, 3.3V	power-supply(5)	power(9)
38	Upper IOM Voltage, 12V (Controller A)	enclosure(7)	currentValue(6)
39	Lower IOM Voltage, 12V (Controller B)	enclosure(7)	currentValue(6)
40	Power Supply 1 (Left)Current,12V	power-supply(5)	currentValue(6)
41	Power Supply 1 (Left)Current, 5V	power-supply(5)	currentValue(6)
42	Power Supply 2 (Right)Current,12V	power-supply(5)	currentValue(6)
43	Power Supply 2 (Right)Current, 5V	power-supply(5)	currentValue(6)

External details for connUnitPortTable

Table 33. connUnitPortTable index and name values

connUnitPortIndex	connUnitPortName
0	Host Port 0 (Controller A)
1	Host Port 1 (Controller B)
2	Host Port 2 (Controller B)
3	Host Port 3 (Controller B)

Configure SNMP event notification in the PowerVault Manager

1. Verify that the storage system's SNMP service is enabled. See Enable or disable system-management settings.
2. Configure and enable SNMP traps. See Setting system notification settings.
3. Optionally, configure a user account to receive SNMP traps. See Adding, modifying, and deleting users.

SNMP management

To view and set system group objects, SNMP must be enabled in the storage system. See Enable or disable system-management settings on page 44. To use SNMPv3, it must be configured in both the storage system and the network management system that intends to access the storage system or receive traps from it. In the storage system, SNMPv3 is configured through the creation and use of SNMP user accounts, as described in Adding, modifying, and deleting users on page 40. The same users, security protocols, and passwords must be configured in the network management system.

To obtain the MIB, see www.dell.com/support.

Using FTP and SFTP

Although the PowerVault Manager is the preferred interface for downloading log data and historical disk-performance statistics and updating firmware, you can also use FTP and SFTP to do these tasks, and to install security certificates and keys.

NOTE: SFTP is enabled by default and FTP is disabled by default.

NOTE: Do not attempt to do more than one of the operations in this appendix at the same time. They can interfere with each other and the operations may fail. Specifically, do not try to do more than one firmware update at the same time or try to download system logs while doing a firmware update.

Downloading system logs

To help service personnel diagnose a system problem, you might be asked to provide system log data. You can download this data by accessing the system's FTP or SFTP interface and running the `get logs` command. When both controllers are online, regardless of operating mode, `get logs` will download a single, compressed zip file that includes:

- Device status summary, which includes basic status and configuration data for the system
- Each controller's MC logs
- Each controller's event log
- Each controller's debug log
- Each controller's boot log, which shows the startup sequence
- Critical error dumps from each controller, if critical errors have occurred
- CAPI traces from each controller

Use a command-line-based FTP/SFTP client. A UI-based FTP/SFTP client might not work.

Download system logs

Perform the following steps to download the system logs:

1. In the PowerVault Manager, prepare to use FTP/SFTP:
   a. Determine the network-port IP addresses of the system controllers. See Configuring controller network ports.
   b. Verify that the FTP/SFTP service is enabled on the system. See Enable or disable system-management settings.
   c. Verify that the user you will log in as has permission to use the FTP interface. See Adding, modifying, and deleting users.
2. Open a Command Prompt (Windows) or a terminal window (UNIX) and go to the destination directory for the log file.
3. Using the FTP/SFTP port specified in the system services settings, enter:

   `sftp controller-network-address -P port` or

   `ftp controller-network-address`

   `sftp 10.235.216.152 -P 1022` or

   `ftp 10.1.0.9`
4. Log in as a user that has permission to use the FTP/SFTP interface.
5. Enter:

   `get logs filename.zip`

   where *filename* is the file that contains the logs. Dell EMC recommends using a filename that identifies the system, controller, and date.

   `get logs Storage2_A_20120126.zip`

   In FTP, wait for the message `Operation Complete` to appear. No messages are displayed in SFTP; instead, the `get` command returns once the logs collection is finished.
6. Quit the FTP/SFTP session.

NOTE: The log files must be extracted from .zip file to view them. To examine diagnostic data, view *store_yyyy_mm_dd__hh_mm_ss.logs* file first.

Transferring log data to a log-collection system

If the log-management feature is configured in pull mode, a log-collection system can access the storage system's FTP or SFTP interface and use the get `managed-logs` command to retrieve untransferred data from a system log file. This command retrieves the untransferred data from the specified log to a compressed zip file on the log-collection system. Following the transfer of a log's data, the log's capacity status is reset to zero indicate that there is no untransferred data. Log data is controller specific.

For an overview of the log-management feature, see About managed logs.

Use a command-line-based FTP/SFTP client. A UI-based FTP client might not work.

Transfer log data to a log-collection system

Perform the following steps to transfer log data to a log-collection system:

1. In the PowerVault Manager, prepare to use FTP/SFTP:
   a. Determine the network-port IP addresses of the system controllers. See Configuring controller network ports.
   b. Verify that the FTP/SFTP service is enabled on the system. See Enable or disable system-management settings.
   c. Verify that the user you will log in as has permission to use the FTP/SFTP interface. See Adding, modifying, and deleting users.
2. On the log-collection system, open a Command Prompt (Windows) or a terminal window (UNIX) and go to the destination directory for the log file.
3. Enter:

   `sftp controller-network-address -P port` or

   `ftp controller-network-address`

   `sftp 10.235.216.152 -P 1022` or

   `ftp 10.1.0.9`
4. Log in as a user that has permission to use the FTP/SFTP interface.

5. Enter:

   `get managed-logs:log-type filename.zip`

   where:

   - `log-type` specifies the type of log data to transfer:
     - `crash1, crash2, crash3, or crash4`: One of the Storage Controller's four crash logs.
     - `ecdebug`: Expander Controller log.
     - `mc`: Management Controller log.
     - `scdebug`: Storage Controller log.
   - *filename* is the file that contains the transferred data. Dell EMC recommends using a filename that identifies the system, controller, and date.

   ```
   get managed-logs:scdebug Storage2-A_scdebug_2011_08_22.zip
   ```

   In FTP, wait for the message `Operation Complete` to appear. No messages are displayed in SFTP; instead, the `get` command returns once the data transfer is finished.
6. Quit the FTP/SFTP session.

   NOTE: The log files must be extracted from .zip file to view them.

Downloading historical disk-performance statistics

You can access the storage system's FTP/SFTP interface and use the `get perf` command to download historical disk-performance statistics for all disks in the storage system. This command downloads the data in CSV format to a file, for import into a spreadsheet or other third-party application.

The number of data samples downloaded is fixed at 100 to limit the size of the data file to be generated and transferred. The default is to retrieve all the available data (up to six months) aggregated into 100 samples. You can specify a different time range by specifying a start and end time. If the specified time range spans more than 100 15-minute samples, the data will be aggregated into 100 samples.

The resulting file will contain a row of property names and a row for each data sample, as shown in the following example. For property descriptions, see the topic about the `disk-hist-statistics` basetype in the *Dell EMC PowerVault ME4 Series Storage System CLI Guide*.

```
"sample-time","durable-id","serial-number","number-of-ios", ...
"2012-01-26 01:00:00","disk_1.1","PLV2W1XE","2467917", ...
"2012-01-26 01:15:00","disk_1.1","PLV2W1XE","2360042", ...
...
```

Use a command-line-based FTP/SFTP client. A UI-based FTP/SFTP client might not work.

Retrieve historical disk-performance statistics

Perform the following steps to retrieve historical disk-performance statistics:

1. In the PowerVault Manager, prepare to use FTP/SFTP:
   a. Determine the network-port IP addresses of the system controllers. See Configuring controller network ports.
   b. Verify that FTP/SFTP service is enabled on the system. See Enable or disable system-management settings.
   c. Verify that the user you plan to use has FTP/SFTP interface permissions. See Adding, modifying, and deleting users.
2. Open a Command Prompt (Windows) or a terminal window (UNIX) and go to the destination directory for the log file.
3. Type:

   `sftp controller-network-address -P port` or `ftp controller-network-address`

   For example:

   `sftp 10.235.216.152 -P 1022` or

   `ftp 10.1.0.9`
4. Log in as a user that has permission to use the FTP/SFTP interface.
5. Type:

   `get perf:date/time-range filename.csv`

   where:

- *date/time-range* is optional and specifies the time range of data to transfer, in the format: *start.yyyy-mm-dd.hh:mm.[AM|PM].end.yyyy-mm-dd.hh:mm.[AM|PM]*. The string must contain no spaces.
- *filename.csv* is the file that contains the data. Dell EMC recommends using a filename that identifies the system, controller, and date.

```
get perf:start.2019-01-26.12:00.PM.end.2019-01-26.23:00.PM Storage2_A_20120126.csv
```

In FTP, wait for the message `Operation Complete` to appear. No messages are displayed in SFTP; instead, the `get` command returns once the download is finished.

6. Quit the FTP/SFTP session.

Downloading system heat map data

If requested by support engineers for analysis, you can download cumulative I/O density data, also known as heat map data, from the system. To gather this data, access the storage system FTP/SFTP interface and use the get logs command with the heatmap option to download a log file in CSV format. The file contains data for the past seven days from both controllers.

1. In the PowerVault Manager, prepare to use FTP/SFTP:
   a. Determine the network-port IP addresses of the system controllers. See Configuring controller network ports.
   b. Verify that the FTP/SFTP service is enabled on the system. See Enable or disable system-management settings.
   c. Verify that the user you plan to use has FTP/SFTP interface permissions. See Adding, modifying, and deleting users.
2. Open a Command Prompt (Windows) or a terminal window (UNIX) and navigate to the destination directory for the log file.
3. Type:

   `sftp controller-network-address -P port` or

   `ftp controller-network-address`

   For example:

   `sftp 10.235.216.152 -P 1022` or

   `ftp 10.1.0.9`
4. Log in as a user that has permission to use the FTP/SFTP interface.
5. Type:

   `get logs:heatmap filename.csv`

   where: *filename.csv* is the file that contains the data.

   For example:

   `get logs:heatmap IO_density.csv`

   In FTP, wait for the message `Operation Complete` to appear. No messages are displayed in SFTP; instead, the `get` command will return once the download is finished.
6. Quit the FTP/SFTP session.

Updating firmware

You can update the versions of firmware in controller modules, expansion modules in drive enclosures, and disks.

If you have a dual-controller system and the Partner Firmware Update (PFU) option is enabled, updating the firmware on one controller causes the system to automatically update the firmware on the partner controller. If PFU is disabled, after updating firmware on one controller you must log into the IP address of the partner controller and perform the firmware update on that controller.

- Ensure that the storage system is in a healthy state before starting firmware update. If the health of the system is Fault, the firmware update cannot proceed. You must resolve the problem specified by the Health Reason value on the System Overview panel before you can update the firmware.
- If any unwritten cache data is present, firmware update will not proceed. Before you can update firmware, unwritten data must be removed from cache. For more information about the `clear cache` command, see the *Dell EMC PowerVault ME4 Series Storage System CLI Guide*.
- If a disk group is quarantined, contact technical support for help resolving the problem that is causing the component to be quarantined before updating the firmware.

- To ensure success of an online update, select a period of low I/O activity. This helps the update complete as quickly as possible and avoids disruptions to host and applications due to timeouts. Attempting to update a storage system that is processing a large, I/O-intensive batch job will likely cause hosts to lose connectivity with the storage system.

Updating controller module firmware

In a dual-controller system, both controller modules should run the same firmware version. Storage systems in a replication set should run the same or compatible firmware versions. You can update the firmware in each controller module by loading a firmware file obtained from the enclosure vendor.

Update controller module firmware

Perform the following steps to update the controller module firmware:

1. Obtain the appropriate firmware file, and download it to your computer or network.
2. In the PowerVault Manager, prepare to use FTP/SFTP:
   a. Determine the network-port IP addresses of the system controllers. See Configuring controller network ports.
   b. Verify that the FTP/SFTP service is enabled on the system. See Enable or disable system-management settings.
   c. Verify that the user you plan to use has manage role permissions and FTP/SFTP interface permissions. See Adding, modifying, and deleting users.
3. If the storage system has a single controller, stop I/O to disk groups before starting the firmware update.
4. Open a Command Prompt (Windows) or a terminal window (UNIX) and go to the directory containing the firmware file to load.
5. Type:

   `sftp` *`controller-network-address`* `-P` *`port`* or `ftp` *`controller-network-address`*

   For example:

   `sftp 10.235.216.152 -P 1022` or

   `ftp 10.1.0.9`
6. Log in as a user with manage role permissions and FTP/SFTP interface permissions.
7. Type:

   `put` *`firmware-file`* `flash`

   CAUTION: Do not perform a power cycle or controller restart during a firmware update. If the update is interrupted or there is a power failure, the module might become inoperative. If this issue occurs, contact technical support. The module might need to be returned to the factory for reprogramming.

   NOTE: If you attempt to load an incompatible firmware version, the message `*** Code Load Fail. Bad format image. ***` is displayed and after a few seconds the FTP/SFTP prompt is redisplayed. The code is not loaded.

   Firmware update typically takes 10 minutes for a controller having current CPLD firmware, or 20 minutes for a controller with downlevel CPLD firmware. If the controller enclosure has attached enclosures, allow additional time for each enclosure management processor (EMP) to be updated in the expansion module. It typically takes 2.5 minutes for each EMP in a drive enclosure.

   NOTE: If you are using a Windows FTP/SFTP client, during firmware update a client-side FTP/SFTP application issue or timeout setting can cause the FTP/SFTP session to be aborted. If this issue persists, try using the PowerVault Manager to perform the update, use another client, or use another FTP/SFTP application.

   If the Storage Controller cannot be updated, the update operation is canceled. If the FTP/SFTP prompt does not return, quit the FTP/SFTP session and log in again. Verify that you specified the correct firmware file and repeat the update. If this problem persists, contact technical support.

   When firmware update on the local controller is complete, the FTP session returns to the `sftp>` prompt, and the FTP/SFTP session to the local MC is closed. Use a management interface to monitor the system and determine when the update is complete.

   If the Partner Firmware Update (PFU) feature is enabled, allow an extra 5 minutes to 20 minutes for both controllers to be updated.
8. Quit the FTP/SFTP session.
9. Clear your web browser cache, and then sign in to the PowerVault Manager.

   If PFU is running on the controller you sign in to, a dialog box shows PFU progress and prevents you from performing other tasks until PFU is complete.

NOTE: If PFU is enabled for the system, after firmware update has completed on both controllers, check the system health. If the system health is Degraded and the health reason indicates that the firmware version is incorrect, verify that you specified the correct firmware file. If this problem persists, contact technical support.

Updating expansion module firmware

An expansion enclosure can contain one or two expansion modules. Each expansion module contains an enclosure management processor (EMP). When you update controller-module firmware, all expansion modules are automatically updated to a compatible firmware version.

Update expansion-module and drawer firmware

Perform the following steps to update the expansion-module and drawer firmware:

1. Obtain the appropriate firmware file, and download it to your computer or network.
2. In the PowerVault Manager, prepare to use FTP:
   a. Determine the network-port IP addresses of the system controllers. See Configuring controller network ports.
   b. Verify that the FTP service is enabled on the system. See Enable or disable system-management settings.
   c. Verify that the user you plan to use has manage role permissions and FTP interface permissions. See Adding, modifying, and deleting users.
3. If you want to update all expansion modules, go to the next step. Otherwise, in the PowerVault Manager, determine the address of each expansion module to update:
   a. In the Configuration View panel, select a drive enclosure.
   b. In the enclosure properties table, note each EMP bus ID and target ID values. For example, 0 and 63, and 1 and 63. Bus 0 is the bus that is native to a given controller, while bus 1 is an alternate path through the partner controller. Dell EMC recommends performing update tasks consistently through one controller to avoid confusion.
4. If the system has a single controller, stop I/O to disk groups before starting the firmware update.
5. Open a Command Prompt (Windows) or a terminal window (UNIX) and go to the directory containing the firmware file to load.
6. Type:

   ```
   ftp controller-network-address
   ```

   For example:

   ```
   ftp 10.1.0.9
   ```
7. Log in as an FTP user with manage role permissions and FTP/SFTP interface permissions.
8. Perform either of the following tasks:
   - To update all expansion modules, type:

     ```
     put firmware-file encl
     ```
   - To update specific expansion modules, enter:

     ```
     put firmware-file encl:EMP-bus-ID:EMP-target-ID
     ```

   CAUTION: Do not perform a power cycle or controller restart during the firmware update. If the update is interrupted or there is a power failure, the module might become inoperative. If this issue occurs, contact technical support. The module might need to be returned to the factory for reprogramming.

   It typically takes 2.5 minutes to update each EMP in a drive enclosure. Wait for a message that the code load has completed.

   NOTE: If the update fails, verify that you specified the correct firmware file and try the update a second time. If it fails again, contact technical support.
9. If you are updating specific expansion modules, repeat step 8 for each remaining expansion module that needs to be updated.
10. Quit the FTP session.
11. Verify that each updated expansion module has the correct firmware version.

Updating disk firmware

You can update disk firmware by loading a firmware file obtained from your reseller.

A dual-ported disk can be updated from either controller.

NOTE: Disks of the same model in the storage system must have the same firmware revision.

You can specify to update all disks or only specific disks. If you specify to update all disks and the system contains more than one type of disk, the update will be attempted on all disks in the system. The update will only succeed for disks whose type matches the file, and will fail for disks of other types.

Prepare for update

1. Obtain the appropriate firmware file and download it to your computer or network.
2. Check the disk manufacturer's documentation to determine whether disks must be power cycled after firmware update.
3. If you want to update all disks of the type that the firmware applies to, continue with the next step. Otherwise, in the PowerVault Manager, for each disk to update:
   a. Determine the enclosure number and slot number of the disk.
   b. If the disk is associated with a disk group and is single ported, determine which controller owns the disk group.
4. In the PowerVault Manager, prepare to use FTP/SFTP:
   a. Determine the network-port IP addresses of the system's controllers.
   b. Verify that the system's FTP/SFTP service is enabled.
   c. Verify that the user you will log in as has permission to use the FTP interface. The same setting allows a user to transfer files using both FTP and SFTP.
5. Stop I/O to the storage system. During the update all volumes will be temporarily inaccessible to hosts. If I/O is not stopped, mapped hosts will report I/O errors. Volume access is restored after the update completes.

Update disk firmware

Perform the following steps to update disk firmware:

1. Obtain the appropriate firmware file, and download it to your computer or network.
2. In the PowerVault Manager, prepare to use FTP:
   a. Determine the network-port IP addresses of the system controllers. See Configuring controller network ports.
   b. Verify that the FTP/SFTP service is enabled on the system. See Enable or disable system-management settings.
   c. Verify that the user you plan to use has manage role permissions and FTP/SFTP interface permissions. See Adding, modifying, and deleting users.
3. Open a Command Prompt (Windows) or a terminal window (UNIX) and go to the directory containing the firmware file to load.
4. Type:

   `sftp` *`controller-network-address`* `-P` *`port`* or

   `ftp` *`controller-network-address`*

   For example:

   `sftp 10.235.216.152 -P 1022` or

   `ftp 10.1.0.9`
5. Log in as a user with manage role permissions and FTP/SFTP interface permissions.
6. Perform either of the following tasks:
   - To update all disks of the type that the firmware applies to, type:

     `put` *`firmware-file`* `disk`

     For example:

     `put AS10.bin disk`
   - To update specific disks, type:

     `put` *`firmware-file`* `disk:`*`enclosure-ID`*`:`*`slot-number`*

     For example:

     `put AS10.bin disk:1:11`

   CAUTION: Do not power cycle enclosures, or restart a controller during the firmware update. If the update is interrupted or there is a power failure, the disk might become inoperative. If this issue occurs, contact technical support.

   It typically takes several minutes for the firmware to load. In FTP, wait for the message `Operation Complete` to appear. No messages are displayed in SFTP.

NOTE: If the update fails, verify that you specified the correct firmware file and try the update a second time. If it fails again, contact technical support.

7. If you are updating specific disks, repeat step 4 for each remaining disk to update.
8. Quit the FTP/SFTP session.
9. If the updated disks must be power cycled:
   a. Shut down both controllers by using the PowerVault Manager.
   b. Power cycle all enclosures as described in the *Dell EMC PowerVault ME4 Series Storage System Deployment Guide*.
10. Verify that each disk has the correct firmware revision.

Installing a security certificate

The storage system supports use of unique certificates for secure data communications, to authenticate that the expected storage systems are being managed. Use of authentication certificates applies to the HTTPS protocol, which is used by the web server in each controller module.

As an alternative to using the CLI to create a security certificate on the storage system, you can use FTP/SFTP to install a custom certificate on the system. A certificate consists of a certificate file and an associated key file. The certificate can be created by using OpenSSL, for example, and is expected to be valid. If you replace the controller module in which a custom certificate is installed, the partner controller will automatically install the certificate file to the replacement controller module.

Install a security certificate

Perform the following steps to install a security certificate:

1. In the PowerVault Manager, prepare to use FTP/SFTP:
   a. Determine the network-port IP addresses of the system controllers. See Configuring controller network ports.
   b. Verify that the FTP/SFTP service is enabled on the system. See Enable or disable system-management settings.
   c. Verify that the user you plan to use has manage role permissions and FTP/SFTP interface permissions. See Adding, modifying, and deleting users.
2. Open a Command Prompt (Windows) or a terminal window (UNIX) and go to the directory that contains the certificate files.
3. Type:

   `sftp` *`controller-network-address`* `-P` *`port`* or

   `ftp` *`controller-network-address`*

   For example:

   `sftp 10.235.216.152 -P 1022` or

   `ftp 10.1.0.9`
4. Log in as a user with manage role permissions and FTP/SFTP interface permissions.
5. Type:

   `put` *`certificate-file-name`* `cert-file`

   where *certificate-file-name* is the name of the certificate file for your specific system.
6. Type:

   `put` *`key-file-name`* `cert-key-file`

   where `key-file-name` is the name of the security key file for your specific system.
7. Restart both Management Controllers to have the new security certificate take effect.

Using SMI-S

This appendix provides information for network administrators who are managing the storage system from a storage management application through the Storage Management Initiative Specification (SMI-S). SMI-S is a Storage Networking Industry Association (SNIA) standard that enables interoperable management for storage networks and storage devices.

NOTE: SMI-S is not supported for a system with 5U84 enclosures.

SMI-S replaces multiple disparate managed object models, protocols, and transports with a single object-oriented model for each type of component in a storage network. The specification was created by SNIA to standardize storage management solutions. SMI-S enables management applications to support storage devices from multiple vendors quickly and reliably because they are no longer proprietary. SMI-S detects and manages storage elements by type, not by vendor.

The key SMI-S components are:

- Web-based Enterprise Management (WBEM). A set of management and internet standard technologies developed to unify the management of enterprise computing environments. WBEM includes the following specifications:
  - CIM XML: defines XML elements, conforming to DTD, which can be used to represent CIM classes and instances
  - CIMxml Operations over HTTP/HTTPS: defines a mapping of CIM operations onto HTTP/HTTPS; used as a transport mechanism
- Common Information Model (CIM). The data model for WBEM. Provides a common definition of management information for systems, networks, applications and services, and allows for vendor extensions. SMI-S is the interpretation of CIM for storage. It provides a consistent definition and structure of data, using object-oriented techniques. The standard language used to define elements of CIM is MOF.
- Service Location Protocol (SLP). Enables computers and other devices to find services in a local area network without prior configuration. SLP has been designed to scale from small, unmanaged networks to large enterprise networks.

Embedded SMI-S array provider

The embedded SMI-S array provider provides an implementation of SMI-S 1.5 using `cim-xml` over HTTP/HTTPS. The provider supports the Array and Server profiles with additional (or supporting) subprofiles. The Server profile provides a mechanism to tell the client how to connect and use the embedded provider. The Array profile has the following supporting profiles and subprofiles:

- Array profile
- Block Services package
- Physical Package package
- Health package
- Multiple Computer System subprofile
- Masking and Mapping profile
- FC Initiator Ports profile
- SAS Initiator Ports profile
- iSCSI Initiator Ports profile
- Disk Drive Lite profile
- Extent Composition subprofile
- Storage Enclosure profile
- Fan profile
- Power Supply profile
- Sensors profile
- Access Points subprofile
- Location subprofile
- Software Inventory subprofile
- Block Server Performance subprofile
- Copy Services subprofile
- Job Control subprofile
- Storage Enclosure subprofile (if expansion enclosures are attached)
- Disk Sparing subprofile
- Object Manager Adapter subprofile
- Thin Provisioning profile
- Pools from Volumes profile

The embedded SMI-S provider supports:

- HTTPS using SSL encryption on the default port 5989, or standard HTTP on the default port 5988. Both ports cannot be enabled at the same time.
- SLPv2
- CIM Alert and Lifecycle indications
- Microsoft Windows Server 2012 Server Manager and System Center Virtual Machine Manager

SMI-S implementation

SMI-S is implemented with the following components:

- CIM server (called a CIM Object Manager or CIMOM), which listens for WBEM requests (CIM operations over HTTP/HTTPS) from a CIM client, and responds.
- CIM provider, which communicates to a particular type of managed resource—for example, storage systems—and provides the CIMOM with information about them. In theory, providers for multiple types of devices—for example, storage systems and Brocade switches—can be plugged into the same CIMOM. However, in practice, all storage vendors provide the CIMOM and a single provider together, and they do not co-exist well with solutions from other vendors.

These components may be provided in several different ways:

- Embedded agent: The hardware device has an embedded SMI-S agent. No other installation of software is required to enable management of the device.
- SMI solution: The hardware or software ships with an agent that is installed on a host. The agent needs to connect to the device and obtain unique identifying information.

SMI-S architecture

The architecture requirements for the embedded SMI-S Array provider are to work within the Management Controller (MC) architecture, use limited disk space, use limited memory resources and be as fast as a proxy provider running on a server. The CIMOM used is the open source SFCB CIMOM.

SFCB is a lightweight CIM daemon that responds to CIM client requests and supports the standard CIM XML over http/https protocol. The provider is a Common Management Protocol Interface (CMPI) provider and uses this interface. To reduce the memory footprint, a third-party package called CIMPLE is used. For more information on SFCB go to http://sourceforge.net/projects/sblim/files/sblim-sfcb.

About the SMI-S provider

NOTE: SMI-S is not supported for a system with 5U84 enclosures.

The provider is a SMI-S 1.5 provider which passes CTP 1.5 tests. Full provisioning is supported.

The SMI-S provider is a full-fledged embedded provider implemented in the firmware. It provides an industry-standard WBEM-based management framework. SMI-S clients can interact with this embedded provider directly and do not need an intermediate proxy provider. The provider supports active management features such as RAID provisioning.

The CNC and SAS system is supported. The classes for Dell EMC are `SMI_XXX`. The device namespace for Dell EMC is `/root/smis`.

The embedded CIMOM can be configured either to listen to secure SMI-S queries from the clients on port 5989 and require credentials to be provided for all queries, or to listen to unsecure SMI-S queries from the clients on port 5988. This provider implementation complies with the SNIA SMI-S specification version 1.5.0.

NOTE: Port 5989 and port 5988 cannot be enabled at the same time.

The namespace details are given below.

- Implementation Namespace - `root/smis`
- Interop Namespace - `root/interop`

The embedded provider set includes the following providers:

- Instance Provider
- Association Provider
- Method Provider
- Indication Provider

The embedded provider supports the following CIM operations:

- `getClass`
- `enumerateClasses`
- `enumerateClassNames`
- `getInstance`
- `enumerateInstances`

- enumerateInstaneceNames
- associators
- associatorNames
- references
- referenceNames
- invokeMethod

SMI-S profiles

SMI-S is organized around profiles, which describe objects relevant for a class of storage subsystem. SMI-S includes profiles for arrays, FC HBAs, FC switches, and tape libraries. Profiles are registered with the CIM server and advertised to clients using SLP.

Table 34. Supported SMI-S profiles

Profile/subprofile/package	Description
Array profile	Describes RAID arraysystems. It provides a high-leveloverview of the arraysystem.
Block Services package	Defines a standardexpression of existingstoragecapacity, the assignment of capacitytoStoragePools,andallocationofcapacityto be usedbyexternaldevices or applications.
Physical Package package	Models information about a storagesystem'sphysical package and optionally about internalsub-packages.
Health package	Defines thegeneralmechanismsusedinexpressinghealthinSMI-S.
Server profile	Defines the capabilities of a CIM object manager based on the communication mechanisms that it supports.
FC InitiatorPortsprofile	Models the FibreChannel-specificaspects of a targetstoragesystem.
SAS Initiator Ports subprofile	Models the SAS-specific aspects of a targetstoragesystem.
iSCSI InitiatorPortssubprofile	Models the iSCSI-specificaspects of a targetstoragesystem.
Access Points subprofile	Provides addresses of remoteaccesspointsformanagementservices.
Fan profile	Specializes the DMTF Fan profile by adding indications.
Power Supply profile	Specializes the DMTF Power Supply profile by adding indications.
Profile Registration profile	Models the profiles registered in the object manager and associations between registration classes and domain classes implementing the profile.
Software subprofile	Models software or firmware installed on the system.
Masking and Mapping profile	Models device mapping and masking abilities for SCSI systems.
Disk Drive Lite profile	Models disk drive devices.
Extent Composition	Provides an abstraction of how it virtualizes exposable block storage elements from the underlying Primordial storage pool.
Location subprofile	Models the location details of product and its sub-components.
Sensors profile	Specializes the DMTF Sensors profile.
Software Inventory profile	Models installed and available software and firmware.
Storage Enclosure profile	Describes an enclosure that contains storage elements (e.g., disk or tape drives) and enclosure elements (e.g., fans and power supplies).
Multiple Computer System subprofile	Models multiple systems that cooperate to present a " virtual " computer system with additional capabilities or redundancy.
Copy Services subprofile	Provides the ability to create and delete local snapshots and local volume copies (clones), and to reset the synchronization state between a snapshot and its source volume.
Job Control subprofile	Provides the ability to monitor provisioning operations, such as creating volumes and snapshots, and mapping volumes to hosts.

Table 34. Supported SMI-S profiles (continued)

Profile/subprofile/package	Description
Disk Sparing subprofile	Provides the ability to describe the current spare disk configuration, to allocate/de-allocate spare disks, and to clear the state of unavailable disk drives.
Object Manager Adapter subprofile	Allows the client to manage the Object Manager Adapters of a SMI Agent. In particular, it can be used to turn the indication service on and off.
Thin Provisioning profile	Specializes the Block Services Package to add support for thin provisioning of volumes. SMI-S does not support the creation of virtual pools. However, a client can create virtual volumes.
Pools from Volumes profile	Models a pool created from other volumes. This profile is used in conjunction with the Thin Provisioning profile to model virtual storage pools.

Block Server Performance subprofile

The implementation of the block server performance subprofile allows use of the `CIM_BlockStorageStatisticalData` classes and their associations, and the `GetStatisticsCollection, CreateManifestCollection, AddOrModifyManifest` and `RemoveManifest` methods.

The Block Server Performance subprofile collection of statistics updates at 60-second intervals.

CIM

Supported CIM operations

SFCB provides a full set of CIM operations including `GetClass, ModifyClass, CreateClass, DeleteClass, EnumerateClasses, EnumerateClassNames, GetInstance, DeleteInstance, CreateInstance, ModifyInstance, EnumerateInstances, EnumerateInstanceNames, InvokeMethod (MethodCall), ExecQuery, Associators, AssociatorNames, References, ReferenceNames, GetQualifier, SetQualifier, DeleteQualifier, EnumerateQualifiers, GetProperty` and `SetProperty`.

CIM Alerts

The implementation of alert indications allows a subscribing CIM client to receive events such as FC cable connects, Power Supply events, Fan events, Temperature Sensor events and Disk Drive events.

If the storage system's SMI-S interface is enabled, the system will send events as indications to SMI-S clients so that SMI-S clients can monitor system performance. For information about enabling the SMI-S interface, see SMI-S configuration.

In a dual-controller configuration, both controller A and B alert events are sent via controller A's SMI-S provider.

The event categories in the following table pertain to FRU assemblies and certain FRU components.

Table 35. CIM Alertindicationevents

FRU/Event category	Corresponding SMI-S class	Operational status values that would trigger alert conditions
Controller	SMI_Controller	Down, NotInstalled, OK
Hard Disk Drive	SMI_DiskDrive	Unknown, Missing, Error, Degraded, OK
Fan	SMI_PSUFan	Error, Stopped, OK
Power Supply	SMI_PSU	Unknown, Error, Other, Stressed, Degraded, OK
Temperature Sensor	SMI_OverallTempSensor	Unknown, Error, Other, Non-Recoverable Error, Degraded, OK
Battery/Super Cap	SMI_SuperCap	Unknown, Error, OK
FC Port	SMI_FCPort	Stopped, OK

Table 35. CIM Alertindicationevents (continued)

FRU/Event category	Corresponding SMI-S class	Operational status values that would trigger alert conditions
SAS Port	SMI_SASTargetPort	Stopped, OK
iSCSI Port	SMI_ISCSIEthernetPort	Stopped, OK

Life cycle indications

The SMI-S interface provides CIM life cycle indications for changes in the physical and logical devices in the storage system. The SMI-S provider supports all mandatory elements and certain optional elements in SNIA SMI-S specification version 1.5.0. CIM Query Language (CQL) and Windows Management Instrumentation Query Language (WQL) are both supported, with some limitations to the CQL indication filter. The provider supports additional life cycle indications that the Windows Server 2012 operating system requires.

Table 36. Life cycle indications

Profile or subprofile	Element description and name	WQL or CQL
Block Services	`SELECT * FROM CIM_InstCreationWHERESourceInstanceISACIM_StoragePool` Send lifecycleindication when a disk group is created or deleted.	Both
Block Services	`SELECT * FROM CIM_InstCreationWHERESourceInstanceISACIM_StorageVolume` Send lifecycleindication when a volume iscreated or deleted.	Both
Block Services	`SELECT * FROM CIM_InstModificationWHERESourceInstance ISA CIM_LogicalDevice` Send lifecycleindication when disk drive(or any logical device)status changes.	Both
Copy Services	`SELECT * FROM CIM_InstModificationWHERESourceInstance ISA CIM_StorageSynchronized AND SourceInstance.SyncState<> PreviousInstance.SyncState` Send lifecycleindication when the snapshotsynchronizationstatechanges.	CQL
Disk Drive Lite	`SELECT * FROM CIM_InstCreation WHERE SourceInstance ISA CIM_DiskDrive` Send life cycle indication when a disk drive is inserted or removed.	Both
Job Control	`SELECT * FROM CIM_InstModification WHERE SourceInstance ISA CIM_ConcreteJob AND SourceInstance.OperationalStatus=17 AND SourceInstance.OperationalStatus=2` Send life cycle indication when a create or delete operation completes for a volume, LUN, or snapshot.	WQL
Masking and Mapping	`SELECT * FROM CIM_InstCreation WHERE SourceInstance ISA CIM_AuthorizedSubject` Send life cycle indication when a host privilege is created or deleted.	Both
Masking and Mapping	`SELECT * FROM CIM_InstCreation WHERE SourceInstance ISA CIM_ProtocolController` Send life cycle indication when create/delete storage hardware ID (add/remove hosts).	Both
Masking and Mapping	`SELECT * FROM CIM_InstCreation WHERE SourceInstance ISA CIM_ProtocolControllerForUnit` Send life cycle indication when a LUN is created, deleted, or modified.	Both
Multiple Computer System	`SELECT * FROM CIM_InstCreation WHERE SourceInstance ISA CIM_ComputerSystem` Send life cycle indication when a controller is powered on or off.	Both

Table 36. Life cycle indications (continued)

Profile or subprofile	Element description and name	WQL or CQL
Multiple Computer System	`SELECT * FROM CIM_InstModification WHERE SourceInstance ISA CIM_ComputerSystem AND SourceInstance.OperationalStatus <> PreviousInstance.OperationalStatus` Send life cycle indication when a logical component degrades or upgrades the system.	WQL
Multiple Computer System	`SELECT * FROM CIM_InstModification WHERE SourceInstance ISA CIM_RedundancySet AND SourceInstance.RedundancyStatus <> PreviousInstance.RedundancyStatus` Send life cycle indication when the controller active-active configuration changes.	WQL
Target Ports	`SELECT * FROM CIM_InstCreation WHERE SourceInstance ISA CIM_FCPort` Send life cycle indication when a target port is created or deleted.	Both
Target Ports	`SELECT * FROM CIM_InstModification WHERE SourceInstance ISA CIM_FCPort AND SourceInstance.OperationalStatus <> PreviousInstance.OperationalStatus` Send life cycle indication when the status of a target port changes.	WQL

SMI-S configuration

In the default SMI-S configuration, the secure SMI-S protocol is enabled. The secure SMI-S protocol is the recommended protocol for SMI-S.

Table 37. CLI commands for SMI-S protocol configuration

Action	CLI command
Enable secure SMI-S port 5989 (and disable port 5988)	set protocols smis enabled
Disable secure SMI-S port 5989	set protocols smis disabled
Enable unsecure SMI-S port 5988 (and disable port 5989)	set protocols usmis disabled
Enable unsecure SMI-S port 5988	set protocol usmis enabled
See the current status	show protocols
Reset all configurations	reset smis-configurations

Configure access to the SMI-S interface for other users

1. Log in as a user with the manage role that also has access to the SMI-S interface.
2. If the user does not exist, create the user using the following command:

```
create user interfaces wbi,cli,smis,ftp roles manage username
```

3. Type the following command to configure access to the SMI-S interface for another user:

```
set user username2 interfaces wbi,cli,smis,ftp
```

Listening for managed-logs notifications

For use with the storage system's managed logs feature, the SMI-S provider can be set up to listen for notifications that log files have filled to a point that are ready to be transferred to a log-collection system.

1. In the CLI, enter this command:`set advanced-settings managed-logs enabled`.

2. In an SMI-S client:
   a. Subscribe using the `SELECT * FROM CIM_InstCreation WHERE SourceInstance ISA CIM_LogicalFile` filter.
   b. Subscribe using the `SELECT * FROM CIM_InstDeletion WHERE SourceInstance ISA CIM_LogicalFile` filter.

For more information about the managed logs feature, see About managed logs.

Testing SMI-S

Use an SMI-S certified client for SMI-S 1.5. Common clients include Microsoft System Center, IBM Tivoli, EMC CommandCenter and CA Unicenter. Common WBEM CLI clients are Pegasus `cimcli` and Sblim's wbemcli.

To certify that the array provider is SMI-S 1.5 compliant, SNIA requires that the providers pass the Conformance Test Program (CTP) tests.

The `reset smis-configuration` command enables the restoration of your original SMI-S configuration.

Troubleshooting

Table 38. Troubleshooting

Problem	Cause	Solution
Unable to connect to the embedded SMI-S Array provider.	SMI-S protocol is not enabled.	Log in to the array as manage and type: `set protocolsmis enabled`
HTTP Error (Invalid username/ password or 401 Unauthorized).	User preferences are configurable for each user on the storage system.	Check that the user has access to the smis interface and set the user preferences to support the smis interface, if necessary. See Adding,modifying,and deleting users for instructions on how to add users. Also verify the supplied credentials.
Want to connect securely as user name my_xxxx.	Need to add user.	Log in to the array as manage . Type: `create user level manage my_xxxuser` and then type: `set user my_xxxuser interfaces wbi,cli,smis`
Unable to discover via SLP.	SLP multicast has limited range(known as hops).	Move the client closer to the array or set up a SLP DA server or using unicast requests.
Unable to determine if SMI-S is running.	Initial troubleshooting.	Use a Common Information Model (CIM) client tool, such as wbemcli, to troubleshoot.
SMI-S is not responding to client requests.	SMI-S configuration may have become corrupted.	Use the CLI command `reset smis-configuration`. For more information, see the *Dell EMC PowerVault ME4 Series Storage System CLI Guide*.

Using SLP

ME4 Series storage systems support Service Location Protocol (SLP, srvloc), which is a service discovery protocol that allows computers and other devices to find services in a LAN without prior configuration. SLP is open for use on all operating systems, and does not require formal licensing.

SLP is based on User Datagram Protocol (UDP) and can use Transmission Control Protocol (TCP) if needed. SLP listens on port 427. When a client, or User Agent (UA), connects to a network, the client queries for Directory Agents (DA) on the network. If no DA responds, the client assumes a DA-less network and sends a multicast UDP query. All Service Agents (SA) that contain query matches will send a UDP answer to the client. If the answer message is too large, the client can repeat the query using TCP.

In a network with DAs, each SA must register all services with a DA. Then the clients will query the DAs, who will respond to the query with its cached SA information.

Through use of DAs, SLP can also scale beyond the local area network to large enterprise, which is an enterprise IT issue. Consult the IETF RFC2165.

When SLP is enabled, the storage system will advertise the interfaces shown in Table 39. Interfaces advertised by SLP on page 163 and populate the configuration attributes shown in Table 40. SLP attributes shown for a storage system on page 163.

You can enable or disable the SLP service in the PowerVault Manager, as described in Enable or disable system-management settings on page 44, or by using the CLI `set protocols` command, as described in the *Dell EMC PowerVault ME4 Series Storage System CLI Guide*.

If the SLP service is enabled, you can test it by using an open source tool, such as slptool from www.openslp.org.

Table 39. Interfaces advertised by SLP

Interface (protocol) description	Advertisement string
HTTP	`service:api:http`
HTTPS	`service:api:https`
Telnet	`service:ui:telnet`
SSH	`service:ui:ssh`
FTP/SFTP (firmware upgrade)	`service:firmware-update:ftp/sftp`
SNMP	`service:api:snmp`

Table 40. SLP attributes shown for a storage system

SLP attribute	Corresponding property shown by the CLI show systemdetail command in XML API mode
`x-system-name`	`system-name`
`x-system-contact`	`system-contact`
`x-system-location`	`system-location`
`x-system-information`	`system-information`
`x-midplane-serial-number`	`midplane-serial-number`
`x-vendor-name`	`vendor-name`
`x-product-id`	`product-id`
`x-product-brand`	`product-brand`
`x-wwnn`	`current-node-wwn`
`x-platform-type`	`platform-type`
`x-bundle-version`	no correspondingproperty
`x-build-date`	no correspondingproperty
`x-mac-address`	no correspondingproperty
`x-top-level-assembly-part-number`	no correspondingproperty
`x-top-level-assembly-serial-number`	no correspondingproperty

B

Administering a log-collection system

A log-collection system receives log data that is incrementally transferred from a storage system for which the managed logs feature is enabled, and is used to integrate that data for display and analysis. For information about the managed logs feature, see About managed logs.

Over time, a log-collection system can receive many log files from one or more storage systems. The administrator organizes and stores these log files on the log-collection system. Then, if a storage system experiences a problem that needs analysis, that system's current log data can be collected and combined with the stored historical log data to provide a long-term view of the system's operation for analysis.

The managed logs feature monitors the following controller-specific log files:

- Expander Controller (EC) log, which includes EC debug data, EC revisions, and PHY statistics
- Storage Controller (SC) debug log and controller event log
- SC crash logs, which include the SC boot log
- Management Controller (MC) log

Each log-file type also contains system-configuration information.

Topics:

How log files are transferred and identified

Log files can be transferred to the log-collection system in two ways, depending on whether the managed logs feature is configured to operate in `push mode` or pull mode:

- In push mode, when log data has accumulated to a significant size, the storage system sends notification events with attached log files through email to the log-collection system. The notification specifies the storage-system name, location, contact, and IP address, and contains a single log segment in a compressed zip file. The log segment will be uniquely named to indicate the log-file type, the date/time of creation, and the storage system. This information will also be in the email subject line. The file name format is `logtype_yyyy_mm_dd__hh_mm_ss.zip`.
- In pull mode, when log data has accumulated to a significant size, the system sends notification events via email, SMI-S, or SNMP traps, to the log-collection system. The notification will specify the storage-system name, location, contact, and IP address and the log-file type (region) that needs to be transferred. The storage system's FTP/SFTP interface can be used to transfer the appropriate logs to the log-collection system, as described in Transferring log data to a log-collection system.

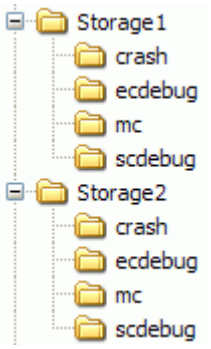
Log-file details

- SC debug-log records contain date/time stamps of the form *mm/dd hh:mm:ss*.
- SC crash logs (diagnostic dumps) are produced if the firmware fails. Upon restart, such logs are available, and the restart boot log is also included. The four most recent crash logs are retained in the storage system.
- When EC debug logs are obtained, EC revision data and SAS PHY statistics are also provided.
- MC debug logs transferred by the managed logs feature are for five internal components: `appsv, mccli, logc, web, and snmpd`. The contained files are log-file segments for these internal components and are numbered sequentially.

Storing log files

It is recommended to store log files hierarchically by storage-system name, log-file type, and date/time. Then, if historical analysis is required, the appropriate log-file segments can easily be located and can be concatenated into a complete record.

For example, assume that the administrator of a log-collection system has created the following hierarchy for logs from two storage systems named Storage1 and Storage2:



In push mode, when the administrator receives an email with an attached ecdebug file from Storage1, the administrator would open the attachment and unzip it into the `ecdebug` subdirectory of the `Storage1` directory.

In pull mode, when the administrator receives notification that an SC debug log needs to be transferred from `Storage2`, the administrator would use the storage system's FTP/SFTP interface to get the log and save it into the scdebug subdirectory of the Storage2 directory.

C

Best practices

This appendix describes best practices for configuring and provisioning a storage system.

Topics:

Pool setup

In a storage system with two controller modules, try to balance the workload of the controllers. Each controller can own one virtual pool. Having the same number of disk groups and volumes in each pool will help balance the workload, increasing performance.

RAID selection

A pool is created by adding disk groups to it. Disk groups are based on RAID technology.

The following table describes the characteristics and use cases of each RAID level:

RAID level	Protection	Performance	Capacity	Application use cases	Suggested disk speed
RAID 1/RAID 10	Protects against up to one disk failure per mirror set	Great random I/O performance	Poor: 50% fault tolerance capacity loss	Databases, OLTP, Exchange Server	10K, 15K, 7K
RAID 5	Protects against up to one disk failure per RAID set	Good sequential I/O performance, moderate random I/O performance	Great: One-disk fault tolerance capacity loss	Big data, media and entertainment (ingest, broadcast, and past production)	10K, 15K, lower capacity 7K
RAID 6	Protects against up to two disk failures per RAID set	Moderate sequential I/O performance, poor random I/O performance	Moderate: Twodisk fault tolerance capacity loss	Archive, parallel distributed file system	High capacity 7K

Disk count per RAID level

The controller breaks virtual volumes into 4-MB pages, which are referenced paged tables in memory. The 4-MB page is a fixed unit of allocation. Therefore, 4-MB units of data are pushed to a disk group. A write performance penalty is introduced in RAID-5 or RAID-6 disk groups when the stripe size of the disk group isn't a multiple of the 4-MB page.

- Example 1: Consider a RAID-5 disk group with five disks. The equivalent of four disks provide usable capacity, and the equivalent of one disk is used for parity. Parity is distributed among disks. The four disks providing usable capacity are the data disks and the one disk providing parity is the parity disk. In reality, the parity is distributed among all the disks, but conceiving of it in this way helps with the example.

  Note that the number of data disks is a power of two (2, 4, and 8). The controller will use a 512-KB stripe unit size when the data disks are a power of two. This results in a 4-MB page being evenly distributed across two stripes. This is ideal for performance.

- Example 2: Consider a RAID-5 disk group with six disks. The equivalent of five disks now provide usable capacity. Assume the controller again uses a stripe unit of 512-KB. When a 4-MB page is pushed to the disk group, one stripe will contain a full page, but the controller must read old data and old parity from two of the disks in combination with the new data in order to calculate new parity. This is known as a read-modify-write, and it's a performance killer with sequential workloads. In essence, every page push to a disk group would result in a read-modify-write.

  To mitigate this issue, the controllers use a stripe unit of 64-KB when a RAID-5 or RAID-6 disk group isn't created with a power-of-two data disks. This results in many more full-stripe writes, but at the cost of many more I/O transactions per disk to push the same 4-MB page.

The following table shows recommended disk counts for RAID-6 and RAID-5 disk groups. Each entry specifies the total number of disks and the equivalent numbers of data and parity disks in the disk group. Note that parity is actually distributed among all the disks.

Table 41. Recommended disk group sizes

RAID level	Total disks	Data disks (equivalent)	Parity disks (equivalent)
RAID 6	4	2	2
	6	4	2
	10	8	2
RAID 5	3	2	1
	5	4	1
	9	8	1

To ensure best performance with sequential workloads and RAID-5 and RAID-6 disk groups, use a power-of-two data disks.

Disk groups in a pool

For better efficiency and performance, use similar disk groups in a pool.

- Disk count balance: For example, with 20 disks, it is better to have two 8+2 RAID-6 disk groups than one 10+2 RAID-6 disk group and one 6+2 RAID-6 disk group.
- RAID balance: It is better to have two RAID-5 disk groups than one RAID-5 disk group and one RAID-6 disk group.
- In terms of the write rate, due to wide striping, tiers and pools are as slow as their slowest disk groups.
- All disks in a tier should be the same type. For example, use all 10K disks or all 15K disks in the Standard tier.

Create more small disk groups instead of fewer large disk groups.

- Each disk group has a write queue depth limit of 100. This means that in write-intensive applications this architecture will sustain bigger queue depths within latency requirements.
- Using smaller disk groups will cost more raw capacity. For less performance-sensitive applications, such as archiving, bigger disk groups are desirable.

Tier setup

In general, it is best to have two tiers instead of three tiers. The highest tier will nearly fill before using the lowest tier. The highest tier must be 95% full before the controller will evict cold pages to a lower tier to make room for incoming writes.

Typically, you should use tiers with SSDs and 10K/15K disks, or tiers with SSDs and 7K disks. An exception may be if you need to use both SSDs and faster spinning disks to hit a combination of price for performance, but you cannot hit your capacity needs without the 7K disks; this should be rare.

Multipath configuration

ME4 Series storage systems comply with the SCSI-3 standard for Asymmetrical Logical Unit Access (ALUA).

ALUA compliant storage systems will provide optimal and non-optimal path information to the host during device discovery, but the operating system must be directed to use ALUA. You can use the following procedures to direct Windows and Linux systems to use ALUA.

Use one of the following procedures to enable MPIO.

Enabling MPIO on Windows

1. Start Server Manager if it is not already running.
2. In the Manage menu, select **Add Roles and Features**.
3. In the Add Roles and Features Wizard, select **Role-based or Feature Based Installation**.
4. Click **Next**.
5. Select the server from the pool and then click **Next**.
6. Click **Next** again to go to the feature selection window.
7. Select the **Multipath IO** checkbox and then click **Next**.
8. Click **Install**.
9. When prompted, reboot the system.

   When the reboot is complete, MPIO is ready to use.

Enabling MPIO on Linux

1. Run the following command to ensure that the multipath daemon is installed and set to start at run-time:

   ```
   chkconfig multipathd on
   ```

2. Ensure the correct entries exist in the /etc/multipath.conf file on each OSS/MDS host. Create a separate device entry for the ME4 Series storage system. The following table specifies four attributes that should be set. Run the following command to obtain the exact vendor and product ID values:

   ```
   multipath -v3
   ```

Attribute	Value
prio	alua
failback	immediate
vendor	*vendor-name*
product	*product-ID*

3. Run the following command to reload the multipath.conf file:

   ```
   service multipathd reload
   ```

4. Run the following command to determine if the multipath daemon used ALUA to obtain the optimal/non-optimal paths:

   ```
   multipath -v3 | grep alua
   ```

   You should see output stating that ALUA was used to configure the path priorities. For example:

   ```
   Oct 01 14:28:43 | sdb: prio = alua (controller setting) Oct 01 14:28:43 | sdb: alua prio =
   130
   ```

Physical port selection

In a system configured to use either all FC or all iSCSI ports, use the ports in the following order:

1. A0,B0
2. A2,B2
3. A1,B1
4. A3,B3

The reason for doing so is that each pair of ports (A0,A1 or A2,A3) are connected to a dedicated CNC chip. If you are not using all four ports on a controller, it is best to use one port from each pair (A0,A2) to ensure better I/O balance on the front end.

D

System configuration limits

The following table lists the system configuration limits for ME4 Series storage systems:

Table 42. ME4 Series system configuration limits

Feature	Value
Enclosures and disks	
Maximum enclosures and disks per system 2U12	Supported configurations: 2U12 controller enclosure + nine 2U12 expansion enclosures = 120 2U12 controller enclosure + nine 2U24 expansion enclosures = 228 2U12 controller enclosure + three 5U84 expansion enclosures = 264 2U24 controller enclosure + nine 2U12 expansion enclosures = 132 2U24 controller enclosure + nine 2U24 expansion enclosures = 240 2U24 controller enclosure + three 5U84 expansion enclosures = 276 5U84 controller enclosure + three 5U84 expansion enclosures = 336
Disk groups and pools	
Maximum virtual pools per controller module	1
Maximum usable virtual pool size per controller module	512 TiB with the large pools feature disabled in the CLI; 1 PB with the large pools feature enabled in the CLI
Maximum disk-group size	Unlimited (non-ADAPT); 1 PB (ADAPT)
Maximum disk groups per pool	16
Maximum virtual disk groups per controller module	16
Maximum linear disk groups per controller module	32
Minimum/maximum disks per virtual disk group	NRAID (non-RAID): 1/1 (read cache only)
	RAID 0: 2/2 (read cache only)
	RAID 1: 2/2
	RAID 3: Not supported
	RAID 5: 3/16
	RAID 6: 4/16
	RAID 10: 4/16
	RAID 50: Not supported
	ADAPT: 12/128
Minimum/maximum disks per linear disk group	NRAID (non-RAID): 1/1
	RAID 0: 2/16
	RAID 1: 2/2

Table 42. ME4 Series system configuration limits (continued)

	RAID 3:3/16
	RAID 5: 3/16
	RAID 6: 4/16
	RAID 10: 4/16
	RAID 50: 6/32
	ADAPT:12/128
Maximum dedicated spares per linear disk group	4
Maximum global spares per system	64
Maximum ADAPT groups per controller module	4
Maximum ADAPT single disk size	64 TiB
Maximum ADAPT disk group size	1 PiB
ADAPT stripe width	8+2
Volumes, initiators, hosts, and mapping	
Maximum virtual volumes per system	1024
Maximum linear volumes per system	512 (recommended)
Maximum volume size	128 TiB (approximately 140 TB)
Maximum mappable volumes (LUNs) per disk group	128
Maximum mappable virtual volumes (LUNs) per pool	512
Maximum mappable linear volumes (LUNs) per pool	128
Maximum mappable volumes (LUNs) per controller module	512
Maximum virtual volumes per pool	1024 (512 base volumes and 512 snapshots)
Maximum linear volumes per pool	1024
Maximum virtual volumes per volume group	1024
Maximum volume groups per controller module	256
Maximum volumes per replication volume group	16
Maximum volumes per host port	1024 (Microsoft Windows limits access to 256)
Maximum initiators per volume	128
Maximum initiators per host port	1024
Maximum initiators per controller module	4096
Maximum initiators per host	128
Maximum hosts per host group	256
Maximum host groups per system	32
Maximum commands per LUN (preferred path)	4096
Maximum queue depth per host port	1024
Maximum host-port link speed	16 Gb FC with capable, qualified SFP+ transceiver 10 GbE iSCSI with capable, qualified SFP + transceiver (CNC only) 12 Gb SAS

Table 42. ME4 Series system configuration limits (continued)

Supported FC/iSCSI module host-port configurations, per controller module	4 ports FC
	4 ports iSCSI
	2 ports FC and 2 ports iSCSI
Virtual volume snapshots	
Maximum snapshots per pool	512
Maximum base volumes per system	1024
Maximum base snapshots per snappable volume	254 in the volume's snapshot tree with the large pools feature disabled in the CLI 8 in the volume's snap shot tree with the large pools feature enabled in the CLI
Maximum mappable snapshots per system	1024
Virtual volume replication	
Maximum number of peer connections per system	4
Maximum number of replicated volumes per system	32
Maximum number of replication sets for a volume	1
Maximum number of volumes for a replicated volume group	16, if no other volumes belong to a replication set
Minimum replication frequency that can be scheduled	1
Embedded SMI-S provider	
Maximum mapping paths (where a path is a volume presented through a host port to an initiator) **NOTE: SMI-S is not supported for a system with 5U84 enclosures.**	250
Miscellaneous	
Maximum SCSI reservations	Per controller module: 1024
	Per LUN: 1
Maximum SCSI registrations for virtual storage	Per system: 32768
	Per LUN: 4096
Maximum SCSI registrations for linear storage	Per system: 32768
	Per FC LUN: 128
	Per iSCSI LUN: 85–128 depending on IQN length
	Per SAS LUN: 128

E

Glossary of terms

The following table lists definitions of the terms used in ME4 Series publications:

Table 43. Glossary of ME4 Series terms

Term	Definition
2U12	An enclosure that is two rack units in height and can contain 12 disks.
2U24	An enclosure that is two rack units in height and can contain 24 disks.
5U84	An enclosure that is five rack units in height and can contain 84 disks.
AES	Advanced Encryption Standard.
AFA	All-flash array. A storage system that uses only SSDs, without tiering.
all-flash array	See also AFA.
allocated page	A page of virtual pool space that has been allocated to a volume to store data.
allocation rate	The rate, in pages per minute, at which a virtual pool is allocating pages to its volumes because they need more space to store data.
ALUA	Asymmetric Logical Unit Access.
array	See storage system.
ASC/ASCQ	Additional Sense Code/Additional Sense Code Qualifier. Information on sense data returned by a SCSI device.
automated tiered storage	A virtual-storage feature that automatically uses the appropriate tier of disks to store data based on how frequently the data is accessed. This enables higher-cost, higher-speed disks to be used only for frequently needed data, while infrequently needed data can reside in lower-cost, lower-speed disks.
auto-write-through	See AWT
available disk	A disk that is not a member of a disk group, is not configured as a spare, and is not in the leftover state. It is available to be configured as a part of a disk group or as a spare. See also compatible disk, dedicated spare, dynamic spare, global spare.
AWT	Auto-write-through. A setting that specifies when the RAID controller cache mode automatically changes from write-back to write-through
base volume	A virtual volume that is not a snapshot of any other volume, and is the root of a snapshot tree. canister See IOM.
CAPI	Configuration Application Programming Interface. A proprietary protocol used for communication between the Storage Controller and the Management Controller in a controller module. CAPI is always enabled.
CHAP	Challenge-Handshake Authentication Protocol.
chassis	The sheet metal housing of an enclosure.
child volume	The snapshot of a parent volume in a snapshot tree. See parent volume.
chunk size	The amount of contiguous data that is written to a disk group member before moving to the next member of the disk group.
CIM Common Information Model	The data model for WBEM. It provides a common definition of management information for systems, networks, applications and services, and allows for vendor extensions.
CIMOM Common Information Model Object Manager	A component in CIM that handles the interactions between management applications and providers.

Table 43. Glossary of ME4 Series terms (continued)

Term	Definition
CNC Converged Network Controller	A controller module whose host ports can be set to operate in FC or iSCSI mode, using qualified SFP and cable options. Changing the host-port mode is also known as changing the ports' personality.
compatible disk	A disk that can be used to replace a failed member disk of a disk group because it has at least the same capacity as, and is of the same type (enterprise SAS, for example) as, the disk that failed. See also available disk, dedicated spare, dynamic spare, global spare.
controller A (or B)	A short way of referring to controller module A (or B). controller enclosure An enclosure that contains one or two controller modules.
controller module	A FRU that contains the following subsystems and devices: a Storage Controller processor; a Management Controller processor; a SAS expander and Expander Controller processor; management interfaces; cache protected by a supercapacitor pack and flash memory; host, expansion, network, and service ports; and midplane connectivity.
CPLD	Complex programmable logic device.
CQL	CIM Query Language.
CRC	Cyclic Redundancy Check.
CRU customer-replaceable unit	A product module that can be ordered as a SKU and replaced in an enclosure by customers or by qualified service personnel, without having to send the enclosure to a repair facility. See also FRU.
CSV Comma-separated values	A format to store tabular data in plain-text form.
DAS Direct Attached Storage	A dedicated storage device that connects directly to a host without the use of a switch.
deallocation rate	The rate, in pages per minute, at which a virtual pool is deallocating pages from its volumes because they no longer need the space to store data.
dedicated spare	A disk that is reserved for use by a specific linear disk group to replace a failed disk. See also available disk, compatible disk, dynamic spare, global spare.
default mapping	Host-access settings that apply to all initiators that are not explicitly mapped to that volume using different settings. See also explicit mapping, masking.
DES	Data Encryption Standard.
DHCP	Dynamic Host Configuration Protocol. A network configuration protocol for hosts on IP networks.
disk group	A group of disks that is configured to use a specific RAID level and provides storage capacity for a pool. See also linear disk group, virtual disk group, read cache.
drain	The automatic movement of active volume data from a virtual disk group to other disk-group members within the same pool.
drawer	In a 5U84 enclosure, one of two FRUs that each holds 42 disks. drive enclosure See expansion enclosure. See also EBOD, JBOD.
drive spin down	See DSD.
DSD	Drive spin down. A power-saving feature available for non-ADAPT linear disk groups that monitors disk activity in the storage system and spins down inactive spinning disks based on user-selectable policies. Drive spin down is not applicable to disks in virtual pools.
DSP	Digital signal processor.
dual-port disk	A disk that is connected to both controllers so it has two data paths, achieving fault tolerance. dynamic spare An available compatible disk that is automatically assigned, if the dynamic spares option is enabled, to replace a failed disk in a disk group with a fault-tolerant RAID level. See also available disk, compatible disk, dedicated spare, global spare.
EBOD	Expanded Bunch of Disks. Expansion enclosure attached to a controller enclosure.
EC	Expander Controller. A processor (located in the SAS expander in each controller module and expansion module) that controls the SAS expander and provides SES functionality. See also EMP.
EEPROM	Electrically erasable programmable ROM.

Table 43. Glossary of ME4 Series terms (continued)

Term	Definition
EMP	Enclosure management processor. An Expander Controller subsystem that provides SES data such as temperature, power supply and fan status, and the presence or absence of disks.
enclosure	A physical storage device that contains I/O modules, disk drives, and other FRUs. See also controller enclosure, expansion enclosure.
enclosure management processor	See EMP.
ESD	Electrostatic discharge.
ESM	Environmental Service Module. See IOM.
Expander Controller	See EC.
expansion enclosure	An enclosure that contains one or two expansion modules. Expansion enclosures can be connected to a controller enclosure to provide additional storage capacity. See also EBOD, JBOD.
expansion module	A FRU that contains the following subsystems and devices: a SAS expander and Expander Controller processor; host, expansion, and service ports; and midplane connectivity.
explicit mapping	Access settings for an initiator to a volume that override the volume's default mapping. See also default mapping, masking.
failback	See recovery.
failover	In an active-active configuration, failover is the act of temporarily transferring ownership of controller resources from an offline controller to its partner controller, which remains operational. The resources include pools, volumes, cache data, host ID information, and LUNs and WWNs. See also recovery.
fan module	The fan FRU used in 5U84 enclosures. There are five in each enclosure, separate from the PSUs. FC Fibre Channel.
FC-AL	Fibre Channel Arbitrated Loop. The FC topology in which devices are connected in a one-way loop.
FDE	Full Disk Encryption. A feature that secures all the user data on a storage system. See also lock key, passphrase, repurpose, SED.
FPGA	Field-programmable gate array. An integrated circuit designed to be configured after manufacturing.
FRU	field-replaceable unit. A product module that can be replaced in an enclosure by qualified service personnel only, without having to send the enclosure to a repair facility. Product interfaces use the term "FRU" to refer to both FRUs and CRUs. See CRU.
Full Disk Encryption	See FDE.
GEM	Generic Enclosure Management. The firmware responsible for managing enclosure electronics and environmental parameters. GEM is used by the Expander Controller.
global spare	A compatible disk that is reserved for use by any disk group with a fault-tolerant RAID level to replace a failed disk. See also available disk, compatible disk, dedicated spare, dynamic spare.
HBA	Host bus adapter. A device that facilitates I/O processing and physical connectivity between a host and the storage system.
host	A user-defined group of initiators that represents a server.
host group	A user-defined group of hosts for ease of management, such as for mapping operations. host port A port on a controller module that interfaces to a host computer, either directly or through a network switch.
initiator	An external port to which the storage system is connected. The external port may be a port in an I/O adapter in a server, or a port in a network switch.
I/O Manager	An SNMP MIB term for a controller module.
I/O module	See IOM
IOM	Input/output module, or I/O module. An IOM can be either a controller module or an expansion module.

Table 43. Glossary of ME4 Series terms (continued)

Term	Definition
IOPS	I/O operations per second.
IQN	iSCSI Qualified Name.
iSCSI	Internet SCSI.
iSNS	Internet Storage Name Service.
JBOD	“Just a bunch of disks.” See expansion enclosure.
LBA	Logical block address. The address used for specifying the location of a block of data.
leftover	The state of a disk that the system has excluded from a disk group because the timestamp in the disk’s metadata is older than the timestamp of other disks in the disk group, or because the disk was not detected during a rescan. A leftover disk cannot be used in another disk group until the disk’s metadata is cleared. For information and cautions about doing so, see documentation topics about clearing disk metadata.
LFF	Large form factor.
linear	The storage-class designation for logical components such as volumes that do not use paged-storage technology to virtualize data storage. The linear method stores user data in sequential, fully allocated physical blocks, using a fixed (static) mapping between the logical data presented to hosts and the physical storage where it is stored.
linear disk	group For linear storage, a group of disks that is configured to use a specific RAID level. The number of disks that a linear disk group can contain is determined by its RAID level. Any supported RAID level can be used. When a linear disk group is created, a linear pool with the same name is also created to represent the volume-containment properties of the disk group. See also linear pool.
linear pool	For linear storage, a container for volumes that is composed of one linear disk group.
LIP	Loop Initialization Primitive. An FC primitive used to determine the loop ID for a controller. lock key A system-generated value that manages the encryption and decryption of data on FDE-capable disks. See also FDE, passphrase.
loop	See FC-AL.
LUN	Logical Unit Number. A number that identifies a mapped volume to a host system.
MAC address	Media Access Control Address. A unique identifier assigned to network interfaces for communication on a network.
Management Controller	See MC.
map/mapping	Settings that specify whether a volume is presented as a storage device to a host system, and how the host system can access the volume. Mapping settings include an access type (read-write, read-only, or no access), controller host ports through which initiators may access the volume, and a LUN that identifies the volume to the host system. See also default mapping, explicit mapping, masking.
masking	A volume-mapping setting that specifies no access to that volume by hosts. See also default mapping, explicit mapping.
MC	Management Controller. A processor (located in a controller module) that is responsible for human-computer interfaces, such as the PowerVault Manager, and computer-computer interfaces, such as SNMP, and interacts with the Storage Controller. See also EC, SC.
metadata	Data in the first sectors of a disk that stores disk-, disk-group-, and volume-specific information including disk group membership or spare identification, disk group ownership, volumes and snapshots in the disk group, host mapping of volumes, and results of the last media scrub.
MIB	Management Information Base. A database used for managing the entities in SNMP. midplane The printed circuit board to which components connect in the middle of an enclosure. mount To enable access to a volume from a host OS. See also host, map/mapping, volume.
midplane	The printed circuit board to which components connect in the middle of an enclosure.
mount	To enable access to a volume from a host OS. See also host, map/mapping, volume.

Table 43. Glossary of ME4 Series terms (continued)

Term	Definition
network port	The Ethernet port on a controller module through which its Management Controller is connected to the network.
NTP	Network time protocol.
NV device	Nonvolatile device. The CompactFlash memory card in a controller module. OID Object Identifier. In SNMP, an identifier for an object in a MIB.
orphan data	See unwritable cache data.
overcommit	A setting that controls whether a virtual pool is allowed to have volumes whose total size exceeds the physical capacity of the pool.
overcommitted	The amount of storage capacity that is allocated to virtual volumes exceeds the physical capacity of the storage system.
page	A range of contiguous LBAs in a virtual disk group.
paged storage	A method of mapping logical host requests to physical storage that maps the requests to virtualized “pages” of storage that are in turn mapped to physical storage. This provides more flexibility for expanding capacity and automatically moving data than the traditional, linear method in which requests are directly mapped to storage devices. Paged storage is also called virtual storage.
parent volume	A virtual volume that has snapshots (can be either a base volume or a base snapshot volume). The parent of a snapshot is its immediate ancestor in the snapshot tree.
partner firmware update	See PFU.
passphrase	A user-created password that allows users to manage lock keys in an FDE-capable system. See also FDE, lock key.
PCB	Printed circuit board.
PCBA	Printed circuit board assembly.
PCM	Power and cooling module FRU. A power supply module that includes an integrated fan. See also PSU.
PDU	Power distribution unit. The rack power-distribution source to which a PCM or PSU connects. peer connection The configurable entity defining a peer-to-peer relationship between two systems for the purpose of establishing an asynchronous replication relationship. See also peer system.
peer system	A remote storage system that can be accessed by the local system and is a candidate for asynchronous replications. Both systems in a peer connection are considered peer systems to each other, and they both maintain a peer connection with the other. Asynchronous replication of volumes may occur in either direction between peer systems configured in a peer connection. See also peer connection.
PFU	Partner firmware update. The automatic update of the partner controller when the user updates firmware on one controller.
PGR	Persistent group reservations.
PHY	One of two hardware components that form a physical link between devices in a SAS network that enables transmission of data.
point-to-point	Fibre Channel Point-to-Point topology in which two ports are directly connected. pool See linear pool, virtual pool.
POST	Power-on self test. Tests that run immediately after a device is powered on.
primary system	The storage system that contains a replication set’s primary volume. See also replication set, secondary system.
primary volume	The volume that is the source of data in a replication set and that can be mapped to hosts. The primary volume exists in a primary (linear storage) or pool (virtual storage) in the primary storage system.
PSU	Power supply unit

Table 43. Glossary of ME4 Series terms (continued)

Term	Definition
quick rebuild	A virtual-storage feature that reduces the time that user data is less than fully fault-tolerant after a disk failure in a disk group. The quick-rebuild process rebuilds only data stripes that contain user data. Data stripes that have not been allocated to user data are rebuilt in the background.
RAID head	See controller enclosure.
RBOD	"RAID bunch of disks." See controller enclosure.
read cache	A special disk group, comprised of SSDs, that can be added to a virtual pool for the purpose of speeding up read access to data stored on spinning disks elsewhere in the pool. Read cache is also referred to as read flash cache.
read flash cache	See read cache.
recovery	In an active-active configuration, recovery is the act of returning ownership of controller resources to a controller which was offline from its partner controller. The resources include volumes, cache data, host ID information, and LUNs and WWNs. See also read cache.
remote syslog support	See syslog.
replication	Asynchronous replication of block-level data from a volume in a primary system to a volume in a secondary system by creating an internal snapshot of the primary volume and copying the snapshot data to the secondary system via Fibre Channel or iSCSI links.
replication set	For virtual replication, a container that houses the infrastructure upon which replications are performed. It defines a relationship between a primary and secondary volume for the purposes of maintaining a remote copy of the primary volume on a peer system. See primary volume, secondary volume.
replication snapshot history	As part of handling a replication, the replication set will automatically take a snapshot of the primary and/or secondary volume, thereby creating a history of data that has been replicated over time. This feature can be enabled for a secondary volume or for a primary volume and its secondary volume, but not for a volume group.
repurpose	A method by which all data on a system or disk is erased in an FDE-capable system. Repurposing unsecures the system and disks without needing the correct passphrase. See also FDE, passphrase.
RFC	Read flash cache. See read cache.
SAS	Serial Attached SCSI.
SBB	Storage Bridge Bay. A specification that standardizes physical, electrical, and enclosure-management aspects of storage enclosure design.
SC	Storage Controller. A processor (located in a controller module) that is responsible for RAID controller functions. The SC is also referred to as the RAID controller. See also EC, MC.
secondary system	The storage system that contains a replication set's secondary volume. See also replication set, primary system.
secondary volume	The volume that is the destination for data in a replication set and that is not accessible to hosts. The secondary volume exists in a secondary (linear storage) or pool (virtual storage) in a secondary storage system.
secret	For use with CHAP, a password that is shared between an initiator and a target to enable authentication.
SED	Self-encrypting drive. A disk drive that provides hardware-based data encryption and supports use of the storage system's Full Disk Encryption feature. See also FDE.
SEEPROM	Serial electrically erasable programmable ROM. A type of nonvolatile (persistent if power removed) computer memory used as FRU ID devices.
SES	SCSI Enclosure Services. The protocol that allows the initiator to communicate with the enclosure using SCSI commands.
SFCB	Small Footprint CIM Broker.
SFF	Small form factor.

Table 43. Glossary of ME4 Series terms (continued)

Term	Definition
SFTP	SSH File Transfer Protocol. A secure secondary interface for installing firmware updates, downloading logs, and installing security certificates and keys. All data sent between the client and server will be encrypted.
SHA	Secure Hash Algorithm.
shelf	See enclosure.
sideplane	A printed circuit board to which components connect longitudinally within an enclosure.
SLP	Service Location Protocol. Enables computers and other devices to find services in a local area network without prior configuration.
SMART	Self-Monitoring Analysis and Reporting Technology. A monitoring system for disk drives that monitors reliability indicators for the purpose of anticipating disk failures and reporting those potential failures.
SMC	Storage Management Console. The web application that is embedded in each controller module and is the primary management interface for the storage system.
SMI-S	Storage Management Initiative - Specification. The SNIA standard that enables interoperable management of storage networks and storage devices. The interpretation of CIM for storage. It provides a consistent definition and structure of data, using object-oriented techniques. SMI-S is not supported for a system with 5U84 enclosures.
snapshot	A point-in-time copy of the data in a source volume that preserves the state of the data as it existed when the snapshot was created. Data associated with a snapshot is recorded in both the source volume and in its associated snap pool. A snapshot can be mapped and written to. Snapshots that can be mapped to hosts are counted against the snapshot limit, whereas transient and unmappable snapshots are not.
snapshot tree	A group of virtual volumes that are interrelated due to creation of snapshots. Since snapshots can be taken of existing snapshots, volume inter-relationships can be thought of as a “tree” of volumes. A tree can be 254 levels deep. See also base volume, child volume, parent volume, source volume.
SNIA	Storage Networking Industry Association. An association regarding storage networking technology and applications.
source volume	A volume that has snapshots. Used as a synonym for parent volume. SSD Solid-state drive.
SSH	Secure Shell. A network protocol for secure data communication.
SSL	Secure Sockets Layer. A cryptographic protocol that provides security over the internet.
standard volume	A volume that can be mapped to initiators and presented as a storage device to a host system, but is not enabled for snapshots.
Storage Controller	See SC.
storage system	A controller enclosure with at least one connected expansion enclosure. Product documentation and interfaces use the terms storage system and system interchangeably.
syslog	A protocol for sending event messages across an IP network to a logging server. This feature supports User Datagram Protocol (UDP) but not Transmission Control Protocol (TCP).
thin provisioning	A virtual-storage feature that allows actual storage for a virtual volume to be assigned as data is written, rather than storage being assigned immediately for the eventual size of the volume. This allows the storage administrator to overcommit physical storage, which in turn allows the connected host system to operate as though it has more physical storage available than is actually allocated to it. When physical resources fill up, the storage administrator can add storage capacity on demand.
tier	A homogeneous group of disks, typically of the same capacity and performance level, that comprise one or more virtual disk groups in the same pool. Tiers differ in their performance, capacity, and cost characteristics, which forms the basis for the choices that are made with respect to which data is placed in which tier. The predefined tiers are:

Table 43. Glossary of ME4 Series terms (continued)

Term	Definition
	• Performance, which uses SSDs (high speed) • Standard, which uses enterprise-class spinning SAS disks (10k/15k RPM, higher capacity) • Archive, which uses midline spinning SAS disks (<10k RPM, high capacity).
tier migration	The automatic movement of blocks of data, associated with a single virtual volume, between tiers based on the access patterns that are detected for the data on that volume.
tray	See enclosure.
ULP	Unified LUN Presentation. A RAID controller feature that enables a host system to access mapped volumes through any controller host port. ULP incorporates ALUA extensions.
undercommitted	The amount of storage capacity that is allocated to volumes is less than the physical capacity of the storage system.
unmount	To remove access to a volume from a host OS.
unwritable cache data	Cache data that has not been written to disk and is associated with a volume that no longer exists or whose disks are not online. If the data is needed, the volume's disks must be brought online. If the data is not needed it can be cleared, in which case it will be lost and data will differ between the host system and disk. Unwritable cache data is also called orphan data.
UPS	Uninterruptible power supply.
UTC	Coordinated Universal Time.
UTF-8	UCS transformation format - 8-bit. A variable-width encoding that can represent every character in the Unicode character set used for the PowerVault Manager and CLI.
vdisk	See linear disk group.
virtual	The storage-class designation for logical components such as volumes that use paged-storage technology to virtualize data storage. See paged storage.
virtual disk group	A group of disks that is configured to use a specific RAID level. The number of disks that a virtual disk group can contain is determined by its RAID level. A virtual disk group can be added to a new or existing virtual pool. See also virtual pool.
virtual pool	A container for volumes that is composed of one or more virtual disk groups.
volume	A logical representation of a fixed-size, contiguous span of storage that is presented to host systems for the purpose of storing data.
volume copy	An independent copy of the data in a linear volume. The capability to copy volumes makes use of snapshot functionality.
volume group	A user-defined group of volumes for ease of management, such as for mapping operations.
VPD	Vital Product Data. Data held on an EEPROM in an enclosure or FRU that is used by GEM to identify and control the component.
WBEM	Web-Based Enterprise Management.
WBI	Web-browser interface, called PowerVault Manager. The primary interface for managing the storage system. A user can enable the use of HTTP, HTTPS for increased security, or both.
WWN	World Wide Name. A globally unique 64-bit number that identifies a device used in storage technology.
WWNN	World Wide Node Name. A globally unique 64-bit number that identifies a device.
WWPN	World Wide Port Name. A globally unique 64-bit number that identifies a port.