# AssuredSAN Storage Management Guide

## For firmware release G222

**Abstract**

This guide is for use by storage administrators to manage a Dot Hill AssuredSAN storage system by using its web interface, WBI.

P/N 83-00006360-12-01
Revision A
January 2016

**Open Source Third Party Licenses and Code**

Dot Hill storage products use open source software components. To view information about open source software licenses and open source code used in Dot Hill storage products, see https://www.dothill.com/support.

# Contents

# Figures

# Tables

# About this guide

This guide provides information about managing a Dot Hill AssuredSAN™ storage system by using its web interface, WBI.

Product information specific to the AssuredSAN 3004 or 4004 series is called out by the product name in bold at the beginning of each relevant paragraph (for instance, "**For AssuredSAN 4004**:"). If there is a mention within a sentence, there will be a callout within the sentence. If there are several paragraphs for a product, a preceding note will indicate the relevant content. If an entire section is specific to a product, the section heading will include a call out.

Otherwise, the content of this guide applies to both systems.

## Intended audience

This guide is intended for storage system administrators.

## Prerequisites

Prerequisites for using this product include knowledge of:

- Network administration
- Storage system configuration
- Storage area network (SAN) management and direct attach storage (DAS)
- Fibre Channel (FC) protocol
- Serial Attached SCSI (SAS) protocol
- Internet SCSI (iSCSI) protocol
- Ethernet protocol

## Related documentation

**Table 1 Related documentation**

| For information about | See |
|---|---|
| Enhancements, known issues, and late-breaking information not included in product documentation | Release Notes |
| Overview of product shipkit contents and setup tasks | Getting Started* |
| Regulatory compliance and safety and disposal information | AssuredSAN Product Regulatory Compliance and Safety* |
| Using a rackmount bracket kit to install an enclosure into a rack | AssuredSAN Rackmount Bracket Kit Installation* *or* AssuredSAN 2-Post Rackmount Bracket Kit Installation* |
| Product hardware setup and related troubleshooting | AssuredSAN 6004 Series Setup Guide<br>AssuredSAN 4004 Series Setup Guide<br>AssuredSAN 3004 Series Setup Guide |
| Obtaining and installing a license to use licensed features | AssuredSAN Obtaining and Installing a License |
| Using the command-line interface (CLI) to configure and manage the product | AssuredSAN CLI Reference Guide |

**Table 1 Related documentation (continued)**

| For information about | See |
|---|---|
| Event codes and recommended actions | AssuredSAN Event Descriptions Reference Guide |
| Identifying and installing or replacing field-replaceable units (FRUs) | AssuredSAN 6004 Series FRU Installation and Replacement Guide<br>AssuredSAN 4004 Series FRU Installation and Replacement Guide<br>AssuredSAN 3004 Series FRU Installation and Replacement Guide |

* Printed document included in product shipkit.

For additional information, see Dot Hill's Customer Resource Center web site: https://crc.dothill.com.

# Document conventions and symbols

**Table 2 Document conventions**

| Convention | Element |
|---|---|
| Colored text | Cross-reference links |
| **Black, underlined** text | Email addresses |
| Green, underlined text | Website addresses |
| **Bold** text | • Keys that are pressed<br>• Text typed into a GUI element, such as a box<br>• GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes |
| *Italic* text | Text emphasis |
| `Monospace` text | • File and directory names<br>• System output<br>• Code<br>• Commands, their arguments, and argument values |
| *`Monospace, italic`* text | • Code variables<br>• Command variables |
| **`Monospace, bold`** text | Emphasis of file and directory names, system output, code, and text typed at the command line |

△ **CAUTION:** Indicates that failure to follow directions could result in damage to equipment or data.

**IMPORTANT:** Provides clarifying information or specific instructions.

**NOTE:** Provides additional information.

**TIP:** Provides helpful hints and shortcuts.

# Part 1: Using WBI v3

Chapters 1-10 describe using the WBI v3 user interface to manage and monitor virtual and linear storage.

# 1 Getting started

The Storage Management Console (SMC) is a web-based application for configuring, monitoring, and managing the storage system. The SMC is a web-based interface (WBI).

There are two user interfaces available for the SMC. RAIDar v2 is the legacy interface for managing linear storage. SMC v3 is the interface for managing virtual storage. For new installations, SMC v3 is the default management mode. For upgrades from a previous release, RAIDar v2 is the default management mode. You can change the default management mode or switch to the other mode for the session.

You can only provision virtual storage with an upgrade license, even though options to provision virtual storage are displayed in the v3 interface.

**For AssuredSAN 3004**: The Full Disk Encryption (FDE) feature is not supported for AssuredSAN 3004 systems.

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

In addition to the SMC, each controller module in the storage system has a CLI and an FTP interface, and SNMP and SMI-S interfaces. For information about using the SMC, FTP, SNMP, and SMI-S, see this guide. For information about using the CLI, see the CLI Reference Guide.

## Configuring and provisioning a new storage system

### To configure and provision a storage system for the first time

1. Configure your web browser to use the SMC as described in "Web browser requirements and setup" (page 20).
2. Sign in to the SMC; the default user for management is `manage` and the default password is `!manage`. For more information about signing in, see "Signing in and signing out" (page 25).
3. Verify that controller modules have the latest firmware as described in "Updating firmware" (page 71).
4. Use the Configuration Wizard as described in "Using the Configuration Wizard" (page 47).
5. Create virtual and linear disk groups and pools, and add dedicated spares to linear disk groups, as described in "Adding a disk group" (page 89) and "Changing dedicated spares" (page 94).
6. Create volumes and map them to initiators, as described in "Creating a virtual volume" (page 100).
7. From hosts, verify volume mappings by mounting the volumes and performing read/write tests to the volumes.
8. Optionally, for replication of virtual volumes and snapshots, create peer connections and replication sets, as described in "Creating a peer connection" (page 125), "Creating a replication set from the Replications topic" (page 127), and "Creating a replication set from the Volumes topic" (page 111).

## Using the interface

### Web browser requirements and setup

- Use Mozilla Firefox 11 and newer, Google Chrome 17 and newer, Microsoft Internet Explorer 10 and 11, or Apple Safari 5.1 and newer.
- 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 browser's local-intranet security option to medium or medium-low.
  - Verify that the browser is set to allow cookies at least for the IP addresses of the storage-system network ports.

- For Internet Explorer, add each controller's network IP address as a trusted site.
- If the SMC is configured to use HTTPS, ensure that Internet Explorer is set to use either TLS 1.0, TLS 1.1, or TLS 1.2.

## Areas of the SMC v3 interface

The main areas of the interface are the banner, topic tabs, topic pane, and footer, as represented by the following table. For information about a topic tab or an item in the banner or footer, click its link in the table.

The topic pane shows information that relates to the selected topic tab. This area also contains an Action menu that provides access to configuration, provisioning, and other actions. The contents of the Action menu are determined by the user's role, the selected topic, and what (if anything) is selected in the topic pane.

**Table 3 Areas of the SMC v3 interface (v3)**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Banner:** | Product ID | System panel (page 138) | Connection panel (page 139) | Date/time panel (page 139) | User panel (page 140) | Sign Out button (page 25) | Help button (page 23) |
| **Topic tabs:** | Home (page 44) | **Topic pane** | | | | | |
| | System (page 61) | | | | | | |
| | Hosts (page 80) | | | | | | |
| | Pools (page 86) | | | | | | |
| | Volumes (page 97) | | | | | | |
| | Mapping (page 113) | | | | | | |
| | Performance (page 133) | | | | | | |
| **Footer:** | Health panel (page 140) | Event panel (page 141) | Capacity panel (page 142) | Host I/O panel (page 143) | Tier I/O panel (page 143) | Activity panel (page 144) | |

## Tips for using the SMC

- Do not use the browser's Back, Forward, Reload, or Refresh buttons.The SMC has a single page for 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, the SMC 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 the SMC 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 SMC session.
- If your session is inactive for too long, you will be signed out automatically. This timer resets after each action you perform. One minute before automatic sign-out you will be prompted to continue using the SMC.

- 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.

## 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

- To display help for the content in the topic pane, click the help icon in the banner.
- 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 help window and you can open a new help 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.

## Color codes

The interface uses the following color codes to distinguish performance statistics and types of capacity utilization.

### Home topic

**Table 4 Home topic storage space color codes (v3)**

| Color | Meaning |
|---|---|
| System performance statistics | |
| | IOPS |
| | Data throughput (MB/s) |
| Capacity graph, bottom bar | |
| | System physical space available |
| | System physical space used by global spares |
| | System physical space used by linear disk groups |
| | System physical space used by virtual disk groups |
| Capacity graph, top bar | |
| | Linear pool reserved space (RAID parity and metadata) |
| | Linear pool allocated space |
| | Linear pool unallocated space |
| | Virtual pool reserved space (RAID parity and metadata) |
| | Virtual pool allocated space |
| | Virtual pool unallocated space |
| Storage A/B, virtual capacity graph, bottom bar | |
| | Virtual pool usable space (excludes reserved space) |
| Storage A/B, virtual capacity graph, top bar | |
| | Virtual pool allocated space |
| | Virtual pool unallocated space |

**Table 4 Home topic storage space color codes (v3) (continued)**

| Color | Meaning |
|---|---|
| Storage A/B, virtual disk group utilization graph | |
| | Performance tier unallocated space |
| | Performance tier allocated space |
| | Standard tier unallocated space |
| | Standard tier allocated space |
| | Archive tier unallocated space |
| | Archive tier allocated space |
| Storage A/B, read cache utilization graph | |
| | Read cache unallocated space |
| | Read cache allocated space |
| Storage A/B, linear capacity graph | |
| | Linear pool allocated space |
| | Linear pool unallocated space |
| Storage A/B, linear disk group utilization graph | |
| | Unallocated space |
| | Allocated space |
| Spares | |
| | Standard tier global spares |
| | Archive tier global spares |

## Create Virtual Volumes panel

**Table 5 Create Virtual Volumes panel storage space color codes (v3)**

| Color | Meaning |
|---|---|
| Virtual capacity graph, top bar | |
| | Virtual pool allocated space |
| | Virtual pool unallocated space |
| | Virtual pool space that would be used by the volumes being created |
| Virtual capacity graph, bottom bar | |
| | Virtual pool usable space (excludes reserved space) |

## Size representations

Parameters such as names of users and volumes have a maximum length in bytes. When encoded in UTF-8, a single character can occupy multiple bytes. Standard US-ASCII characters require 1 byte; most Latin (Western European), Cyrillic, and Arabic characters are encoded with 2 bytes; most Asian characters are 3 bytes.

Operating systems usually show volume size in base 2. Disk drives usually show size in base 10. Memory (RAM and ROM) size is always shown in base 2. In the SMC, the base for entry and display of storage-space sizes can be set per user.

**Table 6 Storage size representations in base 2 and base 10 (v3)**

| Base 2 | | Base 10 | |
|---|---|---|---|
| **Unit** | **Size in bytes** | **Unit** | **Size in bytes** |
| KiB (kibibyte) | 1,024 | KB (kilobyte) | 1,000 |
| MiB (mebibyte) | $1{,}024^2$ | MB (megabyte) | $1{,}000^2$ |
| GiB (gibibyte) | $1{,}024^3$ | GB (gigabyte) | $1{,}000^3$ |
| TiB (tebibyte) | $1{,}024^4$ | TB (terabyte) | $1{,}000^4$ |
| PiB (pebibyte) | $1{,}024^5$ | PB (petabyte) | $1{,}000^5$ |
| EiB (exbibyte) | $1{,}024^6$ | EB (exabyte) | $1{,}000^6$ |

The locale setting determines the character used for the decimal (radix) point, as shown below.

**Table 7 Decimal (radix) point character by locale (v3)**

| Language | Character | Examples |
|---|---|---|
| Arabic, English, Chinese, Japanese, Korean, Russian | Period (.) | 146.81 GB<br>3.0 Gbit/s |
| Dutch, French, German, Italian, Portuguese, Spanish | Comma (,) | 146,81 GB<br>3,0 Gbit/s |

## Signing in and signing out

Multiple users can be signed in to each controller simultaneously.

For each active SMC 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 SMC session, but all instances of Firefox, Chrome, and Safari share the same SMC session.

### To sign in

1. In the web browser address field, type `https://<IP address of a controller network port >` and press **Enter**. (Do not include a leading zero in an IP address. For example, enter 10.1.4.33 and not 10.1.4.**0**33.) The SMC Sign In page is displayed. If the Sign In page does not display, verify that you have entered the correct IP address.

   If the v2 version of the Sign In page appears, to switch to the user interface that manages virtual storage for the session, when the Sign In page opens, perform the following action:

   - In the URL, replace `v2` with `v3`.

2. On the sign-in page, enter the name and password of a configured user. The default user name and password are `manage` and `!manage`. To display the interface in a language other than the user setting, select the language from the Language list.

   Language preferences can be configured for the system and for individual users.

3. Click **Sign In**. If the system is available, the Home page is displayed. Otherwise, a message indicates that the system is unavailable.

When you are ready to end your session, sign out as described below. Do not simply close the browser window.

**To sign out**

1. Click **Sign Out** near the top of the SMC 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 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 on page 34, automated tiered storage on page 35, read cache on page 34, and the quick rebuild feature on page 40.

The legacy linear method maps logical host requests directly to physical storage. In some cases the mapping is 1-to-1, 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 type 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. You can add virtual, linear, and read-cache disk groups to a pool.

All disks in a disk group must be the same type (SAS SSD, enterprise SAS, or midline SAS). 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, regardless of RAID level. 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).

**CAUTION:** The emulation for 512e disks supports backward-compatibility for many applications and legacy operating systems that do not support 4K native disks. However, older versions of application software, such as virtualization software that resides between the operating system and your storage firmware, may not fully support 512e disk emulation. If not, performance degradation might result. Ensure that you have upgraded to the most recent version of any software that might be affected, and see its documentation for further information.

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. Unlike linear pools, multiple disk groups (up to 16) can be added to a single virtual pool. Virtual disk groups that contain SSDs can only be created with a Performance tier license. This restriction does not apply to read-cache disk groups.

**TIP:** For optimal performance, all virtual disk groups in the same tier within a virtual group should have the same RAID level, disk capacity, 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. Otherwise, the data will be lost. When the last disk group is removed, the pool ceases to exist, and will be deleted from the system automatically.

The RAID type for a virtual disk group must be fault tolerant. The supported RAID types for virtual disk groups are: RAID 1, RAID 5, RAID 6, RAID 10. If RAID 10 is specified, the disk group has 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 types for linear disk groups created through the SMC must also must be fault tolerant. The supported RAID types for linear disk groups in the interface are: RAID 1, RAID 5, RAID 6, RAID 10, and RAID 50. 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:** Vdisks created through RAIDar v2 or legacy products display in SMC v3 as linear disk groups. The user interface also shows corresponding linear pools. These disk groups can be used in the same way as any linear disk group created through SMC v3.

### 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 utilizes 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 a single disk in an NRAID configuration.

## 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.

**TIP:** 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
- Suggest the number of disks to select for different RAID levels (virtual disk groups)
- Describe the expansion capability for different RAID levels (linear disk groups)

**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 on this command, see the CLI Reference Guide.

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

**Table 8 Example applications and RAID levels (v3)**

| 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 |

**Table 9 RAID level comparison (v3)**

| 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 performance; protects against single disk failure | High redundancy cost overhead: because all data is duplicated, twice 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 sub-groups | 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 |

**Table 10 Number of disks per RAID level to optimize virtual disk group performance (v3)**

| RAID level | Number of disks (data and parity) |
|---|---|
| 1 | N/A. 2 total. |
| 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) |
| 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 | 16 total (8 RAID-1 subgroups) |

**Table 11 Linear disk group expansion by RAID level (v3)**

| RAID level | Expansion capability | Maximum disks |
|---|---|---|
| NRAID | Cannot expand. | 1 |
| 0, 3, 5, 6 | You can add 1–4 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 |

## About SSDs

The use of SSDs 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. If you have the Performance tier license, you can use SSDs for virtual disk groups for improved read and write performance. You can also use one or two SSDs in read-cache disk groups to increase performance for pools without a Performance tier license. For more information about automated tiered storage, see “About automated tiered storage” (page 35). For more information on read-cache disk groups, see “Read-cache disk groups” (page 28).

The application workload of a system determines the percentage of SSDs of the total disk capacity that is needed for best performance.

### 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 values 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.

### Internal disk management

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

#### 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/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 LBA's 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. The autonomic nature of Dot Hill AssuredSAN real-time tiering does not support static use of the TRIM or UNMAP commands. Dot Hill AssuredSAN firmware does not issue TRIM or UNMAP commands to SSDs.

### 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)

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. So also is the ratio of SSDs to conventional drives. In some environments, a ratio of 10% SSDs to 90% conventional drives, when combined with Dot Hill AssuredSAN real-time tiering, can yield dramatic performance improvements.

Since Dot Hill AssuredSAN real-time tiering automatically moves “hot” data to SSDs and less-used “cool” data to conventional disks, applications and environments that require mission-critical movement of frequently accessed “hot” data might dictate a higher ratio of SSDs to conventional disks, as well as the use of higher DWPD SSDs (such as 8 DWPD or 10 DWPD). For less demanding application environments, the cost savings of upcoming 3 DWPD SSDs may be more attractive.

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 “hot” pages only. Each read-cache disk group consists of one or two SSDs with a maximum capacity of 4TB. A separate copy of the data is also kept in spinning disks. Read cache contents are 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.
- SSDs do 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.

## About pools

A *pool* is an aggregation of one or more drives in the form 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 type that is incorporated as a component of a pool, that stores volume data. For virtual pools, which can have multiple disk groups, volumes are added to a pool and 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 disk groups and resources owned by the failed controller. If a fault-tolerant cabling configuration and 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” (page 89).

### 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 300 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 300 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 512 TiB 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 CLI documentation.

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 which to move 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/sequential 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 1-to-1, while in most cases the mapping is across groups of physical storage devices, or slices of them.

---

**NOTE:** Linear pools display in SMC v3 for vdisks created through RAIDar v2 or legacy products. The user interface shows the vdisks as linear disk groups. These linear pools can be used in the same way as any linear pool created through SMC v3.

---

## 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 the storage for a file system partition you create with your operating system or third-party tools. For more information about mapping, see “About volume mapping” (page 36).

### 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 virtual volumes and snapshots share the same underlying structure, it is possible to create snapshots of other snapshots, not just of volumes.

### Volume groups

For ease of management related to virtual storage, you can group 1–20 virtual 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.

**IMPORTANT:** Volume groups only apply 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. These blocks have a fixed (static) mapping between the logical data presented to hosts and the physical location where it is stored.

It is only possible to take snapshots of linear volumes, but not of linear snapshots.

**NOTE:** Volumes created through RAIDar v2 or legacy products display in SMC v3 as linear volumes. These linear volumes can be used in the same way as any linear volume created through SMC v3.

## About volume cache options

You can set options that optimize reads and writes performed for each volume.

### 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. If used incorrectly, you might hinder system performance.

You can change the write-back cache setting for a volume when modifying it. *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 operation and 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.

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.

**TIP:** 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

**CAUTION:** 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 non-RAID 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 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 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 (space) associated with that data will be deallocated (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 (ATS) 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:

- Frequently accessed, “hot” data can move to disks with higher performance, lower capacity, and higher costs.
- Infrequently accessed, “cool” data can move to disks with higher capacity, 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 SAS SSDs, which provide the best performance but also the highest cost.
- 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.

Some advantages of using ATS are:

- Because a virtual pool can have multiple disk groups, each belonging to a different tier, a virtual pool can provide multiple tiers of storage.
- The I/O load is automatically balanced between components in a tier.
- Virtual disk groups can be added or removed without disrupting I/O. Data in virtual disk groups that are being removed is automatically migrated to other disk groups as long as the other disk groups have enough storage space for it. If they do not have the space, the system will not delete the disk groups until enough data is removed.

### Volume tier affinity feature

The volume tier affinity feature enables tuning the tier-migration algorithm for a virtual volume when creating or modifying the volume so that the volume data automatically moves to a specific tier, if possible. If space is not available in a volume's preferred tier, another tier will be used. There are three volume tier affinity settings:

- 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 will swap into higher performing tiers based on frequency of access and tier space availability.
- Archive—This setting prioritizes the volume data to the least performing tier available. Volume data can move to higher performing tiers based on frequency of access and available space in the tiers.
- Performance—This setting prioritizes volume data to the higher performing tiers. If no space is available, lower performing tier space is used. Performance affinity volume data will swap into higher tiers based upon frequency of access or when space is made available.

## 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, or a port in a network switch.

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. A maximum of 512 names can be assigned.

For ease of management, you can group 1–128 initiators that represent a server or switch into a host. Further, you can group 1–256 hosts into a host group. Doing so 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 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 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 (hereafter called “hosts”) enable the 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.

Default mapping is expected by some operating systems, such as Microsoft Windows, which can immediately discover the volume. 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 initiators, 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 an initiator 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 can only be 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 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.

**TIP:** When an explicit mapping is deleted, the volume's default mapping takes effect. Therefore, it is recommended to use the same LUN for explicit mappings as for the default mapping.

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 snapshots

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.

With a license, you can create up to 1024 snapshots. Other than the overall maximum number of snapshots, there are no restrictions on the number of virtual or linear snapshots that you can create. When you reach the maximum number of base snapshots, before you can create a new snapshot you must either delete an existing snapshot or purchase and install a license that increases the maximum number of snapshots.

The system can create both virtual and linear snapshots. When you create a snapshot of a virtual volume, the result is a virtual snapshot. When you create a snapshot of a linear volume, the result is a linear snapshot. The methods by which virtual and linear snapshots are created vary, reflecting the differences between the two storage technologies. The virtual technology streamlines the underlying process of creating snapshots, delivering improved speed and efficiency. For both virtual and linear snapshots, once a snapshot has been created, the source volume cannot be expanded.

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.

Virtual and linear snapshots both 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. This feature operates differently depending on the storage technology for the snapshot.

Virtual and linear snapshots also share the reset snapshot feature, which enables you to replace the data in a snapshot with the current data in the source volume. You can use it to update an existing snapshot with the data contained in the current source volume or snapshot. When you reset a snapshot, the snapshot name and mappings are not changed.

Automatically deleting snapshots is not currently unavailable.

### Virtual snapshots

The process of 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 snapshot is modified.) There are no intermediate steps needed like designating the volume for snapshot capability. 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, they 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 virtual 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.

## Linear snapshots

For linear snapshots, each pool has reserved space, called a snap pool, that stores pointers to source-volume data for snapshots. Any unique data written to a snapshot is stored in the snap pool.

The snapshot feature for linear snapshots uses the single copy-on-write method to capture only data that has changed. If a block is to be overwritten on the master volume, and a snapshot depends on the existing data in the block being overwritten, the data is copied from the master volume to the snap pool before the data is changed. All snapshots that depend on the older data are able to access it from the same location in the snap pool. This reduces the impact of snapshots when writing to a master volume. In addition, only a single copy-on-write operation is performed on the master volume.

For linear snapshots that have been made accessible as read-write, the rollback feature enables you to revert the data in a source volume to the data that existed when a specified snapshot was created (preserved data). It can also include data that has been modified (write data) in the snapshot since the snapshot was created. For example, you might want to create a snapshot, mount that snapshot for read/write, and then install new software on that snapshot for test purposes. If the software installation is successful, you can roll back the standard volume to the contents of the modified snapshot (preserved data plus write data).

Linear snapshot operations are I/O-intensive. Every write to a unique location in a standard volume after a snapshot is created will cause an internal read and write operation to occur in order to preserve the snapshot data.

---

**NOTE:** Snapshots created through RAIDar v2 or legacy products display in SMC v3 as linear snapshots. These linear snapshots can be used in the same way as any linear snapshot created through SMC v3.

---

## About copying volumes

For linear storage, the volume copy feature is a licensed feature that enables you to copy a linear volume or snapshot to a new linear volume through the SMC. For virtual storage, it is accessible without a license and enables you to copy a virtual base volume or snapshot to a new virtual volume through the CLI, but not through the SMC. The volume copy feature creates a complete “physical” copy of a source volume or a 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 information about viewing the status of licensed features in your system, see Installing a license. For more information about using the SMC to create a copy of a linear volume or snapshot, see “Copying a volume or snapshot” (page 105). For more information about using the CLI to create a copy of a virtual base volume or snapshot, see the CLI Reference Guide.

## About reconstruction and copyback

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 component. Component 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. To start reconstruction manually, replace each failed disk and designate each replacement disk as a spare. If you have configured the dynamic spares feature through the CLI, reconstruction will automatically start for linear 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.

For virtual storage only, reconstruction of all disk groups uses a quick-rebuild feature. For more information on quick rebuild, see “About quick rebuild” (page 40).

For both virtual and linear storage, 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 Setup Guide.

---

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

---

When reconstruction is complete, you can remove the failed disk and replace it with a new disk of the same type in the same slot. When the system detects the new disk, it initiates a copyback operation, which copies all data to the new disk from the spare disk that replaced the failed disk. When the copyback operation is complete, the spare disk is freed so that it can be used for a subsequent disk failure.

## About quick rebuild

Quick rebuild is a feature for virtual storage that reduces the time that user data is less than fully fault-tolerant after a disk failure in a disk group. Taking advantage of virtual storage knowledge of where user data is written, quick rebuild only rebuilds 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, a scrub starts on the disk group within a few minutes after the quick rebuild completes.

## 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 from host to disk, 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” (page 133), “Updating historical statistics” (page 135), “Exporting historical performance statistics” (page 136), and “Resetting performance statistics” (page 136).

## About firmware update

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.AssuredSAN products use a new controller-module firmware-update algorithm that supports the following scenarios for a dual-controller system:

- 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.

When you update controller firmware, the Partner Firmware Update (PFU) option, which is enabled by default, ensures 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 newer firmware version in controller A is transferred to controller B.

For information about the procedures to update firmware in controller modules, expansion modules, drawers, and disk drives, see “Updating firmware” (page 71). 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 before any data is lost. The transfer does not remove any data from the logs in the storage system. This feature is disabled by default.

The *log-collection system* is a host computer that is designated to receive the log data transferred from the storage system. Because log data is transferred incrementally, the log-collection system is responsible for integrating the log data for display and analysis.

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/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, SNMP, or SMI-S to the log-collection system, which can then use FTP 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 (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 SMC or the `get logs` command in the FTP 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” (page 140). For information about using the FTP interface, see “Using FTP” (page 302).

## About replicating virtual volumes

Replication for virtual storage is a licensed feature that 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” (page 118).

## About the Full Disk Encryption feature (for AssuredSAN 4004 only)

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 without needing the correct passphrase. Repurposing erases all data and unsecures the system and disks.

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 (for AssuredSAN 4004 only)” (page 75).

## 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, data is held in controller cache until it is written to disk. In write-through mode, data is written directly 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. This can result in data becoming unavailable or, in some cases, volume unavailability.

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

To avoid the possibility of 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 initiators, hosts, and host groups” (page 35). For more information about changing cache settings for a volume, see “Modifying a volume” (page 103).

## About SAS cabling (for AssuredSAN 3004 only)

For systems with a 2-port SAS controller module, host ports can be configured through the SMC or CLI to use fan-out cables or standard cables. A standard cable can connect one port on a SAS host to one controller port, using four PHY lanes per port. A fan-out cable can connect one port on each of two SAS hosts to one controller port, using two PHY lanes per port. Using fan-out instead of standard cables doubles the number of hosts that can be attached to a single system. It will also halve the maximum bandwidth available to each host, but overall bandwidth available to all hosts is unchanged. Configuration must be the same for all ports on both controllers, so a mix of standard and fan-out cables cannot be used on one system. Use of fan-out cables is enabled by default.

Once you have switched the configuration through the firmware, you can disconnect the existing cables and switch to the other type of cables. For information on how to connect and disconnect cables, refer to your product's Setup Guide.

If you connect a cable that does not match the cable type for the configuration, an event will be logged that indicates a mismatch has occurred. Also, while I/O will occur, half of the PHY lanes for each port will be disabled. The Ports hover panel accessed through the Home topic will reflect that the port is in a degraded state. If a cable mismatch occurs, change the port mode of the system using the Host Ports Settings panel or connect cables of the appropriate type for the configuration.

For more information on checking port properties through the Home topic, see “Port information” (page 44).

When configuring the host-interface settings for a 2-port SAS controller module, the current link speed, number of PHY lanes expected for the SAS port, and number of PHY lanes active for each SAS port are displayed. The number of ports that appear depends on the configuration. Changing the host-interface settings interrupts I/O and restarts the storage controllers. For more information on how to configure host ports for use with SAS fan-out cables, see “To change host interface settings for 2-port SAS controller modules (for AssuredSAN 3004 only)” (page 68).

# 2 Working in the Home topic

## Viewing overall system status

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

### 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 or switch. 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 type (protocol) of each host port in controller A. The port icon indicates whether the port is active or inactive:

| | |
|---|---|
|  | FC port is active. |
|  | FC port is connected. |
|  | FC port is disconnected. |
|  | iSCSI port is active. |
|  | iSCSI port is connected. |
|  | iSCSI port is disconnected. |
|  | SAS port is active. |
|  | SAS port is connected. |
|  | SAS port is disconnected. |

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.

| | |
|---|---|
| Port Information | FC port: Name, type, ID (WWN), status, configured speed, actual speed, topology, and health.<br><br>iSCSI IPv4 port: Name, type, ID (IQN), status, actual speed, IP version, IP address, gateway, netmask, and health.<br><br>SAS port: Name, type, ID (WWN), status, configured speed, actual speed, cable type, health |

The area between the blocks displays the following statistics, which 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 SMC 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.

**For AssuredSAN 3004**: For a system with a 2-port SAS controller module, host ports can be configured to use fan-out cables or standard cables. If fan-out cables are connected to SAS ports that are configured to use them, fan-out cable icons appear between the depicted SAS ports.

## 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, global spares, and unused disk space, if any. The upper bar identifies how the capacity is allocated and used. If the system has both virtual and linear storage, the bars proportionally reflect virtual and linear storage. The right side of the bars represents virtual storage capacity and the left side represents linear storage capacity. For color-code descriptions, see "Color codes" (page 23).

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 needed for internal management of data structures. The terms allocated space and unallocated space have different meanings for the two storage technologies.

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 yet been allocated by 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 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, the right upper bar will be longer than the lower bar.

Hover the cursor over a segment of a bar to see the storage size represented by that segment. Point anywhere in this block to see the following information about capacity utilization in the Capacity Utilization panel (with the exception of uncommitted space, there are equivalent sections for virtual and linear disk groups if your system has both virtual and linear storage):

- 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 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. For virtual storage, the Storage A block shows information for 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 color-code descriptions, see "Color codes" (page 23).

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.

For virtual and linear storage, the number of volumes and snapshots for the pool (s) owned by the controller displays above the top horizontal bar.

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.

| | |
|---|---|
| Storage Information for a virtual pool | Owner, storage type, total size, allocated size, snapshot size, available size, allocation rate, and deallocation rate<br><br>For each tier: Pool percentage, number of disks, total size, allocated size, unallocated size, number of reclaimed pages, and health<br><br>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. |
| Storage Information for a linear pool | Owner, storage type, total size, allocated size, snapshot size, and available size<br><br>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 one system into another system, the latter system will attempt 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 `NewSystem` has pool A and you insert a disk group that came from pool A on `OldSystem`, the imported pool A from `OldSystem` will be offline.

To avoid this, do either of the following:

- Physically remove all disks for the existing pool, which will remove the pool, and then insert the imported disks.

  **CAUTION:** This is an offline operation. Removing a virtual disk group or pool while the system is online may result in RAID corruption and possible data loss. Power off the system before removing the existing pool.

- Delete the existing pool and then insert the imported disks.

  **CAUTION:** Deleting a pool will delete all the data it contains

Either method will allow the system to create pool A for the new disk group without conflict, allowing the imported disk group's data to be accessible. If you are unable to find a pool with a duplicate name, or are unsure of how to safely proceed, please download logs from the system and contact technical support for assistance.

# Using the Configuration Wizard

The Configuration Wizard helps you initially configure the system or change system configuration settings.

When you complete this wizard you are given the option to start creating disk groups.

## Using the Configuration Wizard

You can use the Configuration Wizard to perform the following:

- Change the system date and time settings
- Change passwords for the default users, providing they still exist
- Configure each controller's network port
- Enable or disable system-management services
- Enter information to identify the system
- Configure event notification
- Configure controller host ports (if applicable)

The wizard guides you through each step. As you complete a step, it is highlighted at the bottom of the panel. For each step, you can view help by clicking the help icon . At any point, you can cancel the wizard and discard changes.

To use the Configuration Wizard, perform one of the following:

- Point to the Home tab, and select **Configuration Wizard**.
- In the Home topic, select **Action > Configuration Wizard**.

When the Configuration Wizard panel opens, click **Next** to proceed to the next step.

## Using the Configuration Wizard: Set Date and Time

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, such as for Daylight Saving Time. You must make such adjustments manually.

---

**NOTE:** If you make changes in this step, they will be applied when you click **Next**. Changes made in other steps will be applied when you complete the wizard.

---

### To use manual date and time settings

1. Clear the **Network Time Protocol (NTP)** check box.
2. To set the Date value, enter the current date in the format *YYYY-MM-DD*.
3. To set the Time value, enter two-digit values for the hour and minutes and select either **AM**, **PM**, or **24H** (24-hour clock).
4. Click **Next** to proceed to the next step.

### To obtain the date and time from an NTP server

1. Select the **Network Time Protocol (NTP)** check box.
2. Perform one of the following:
   - To have the system retrieve time values from a specific NTP server, enter its 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.
3. 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.
4. Click **Next** to proceed to the next step.

## Using the Configuration Wizard: Password Setup

The system provides the default users `manage` and `monitor`.

1. To secure the storage system, enter and confirm a new password for each default user.

   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, and one non-alphabetic character. A password can include printable UTF-8 characters except for the following: a space or " , < > \
2. Click **Next** to proceed to the next step.

## Using the Configuration Wizard: Network configuration

You can change addressing parameters for the network port in each controller module. You can set static IP values or use DHCP. When setting static IP values, you can use either IPv4 or IPv6 format.

In DHCP mode, the system obtains values for the network port IP address, subnet mask, and gateway from a DHCP server if one 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.

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 in the storage system, the following initial values are set and remain set until the system is able to 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: 0.0.0.0

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. This 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.

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

### To use DHCP

1. Set IP address source to DHCP. The new IP values will not appear until the Configuration Wizard is completed and you have logged in again to the new IP addresses.
2. Record the new addresses.
3. Click **Next** to proceed to the next step.

### To use static IP values:

1. Determine the IP address, subnet mask, and gateway values to use for each network port.
2. Set IP address source to manual.
3. To specify addresses in IPv6 format instead of the default format, IPv4, select the **IPv6** check box. IPv4 uses 32-bit addresses. IPv6 uses 128-bit addresses.

   **NOTE:** IPv6 for controller module network ports is not supported in this release.

4. Enter IP address, subnet mask, and gateway values for each controller. You must set a unique IP address for each controller.

   **NOTE:** The following IP addresses are reserved for internal use by the storage system: 192.168.200.253, 192.168.200.254, 172.22.255.253, 172.22.255.254, and 127.0.0.1

5. Record the IP values you assign.
6. Click **Next** to proceed to the next step.

## Using the Configuration Wizard: Enable system-management services

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.

If a service is disabled, it continues to run but cannot be accessed. To allow specific users to access the SMC (the web browser interface), CLI, FTP, or SMI-S, see "Adding, modifying, and deleting users" (page 56).

### To change system services settings

1. 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, HTTPS for increased security, or of both. Also, if you choose to disable the SMC, the change does not take effect until the Configuration Wizard has finished and you have logged in again. If you disable both, you will lose access to this interface.
     - Default Management Mode. The default version of the SMC that opens when you access it. Select **v2** for the interface that manages legacy linear storage, or **v3** for the new interface that manages virtual storage.
   - Command Line Interface (CLI). An advanced-user interface that is used to manage the system and can be used to write scripts. You can enable use of SSH (secure shell) for increased security, Telnet, or both.
   - 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 via 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.
   - File Transfer Protocol (FTP). A secondary interface for installing firmware updates, downloading logs, and installing a license.
   - 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.
   - Activity Progress Reporting. Provides access to the activity progress interface via 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. In addition, 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.
2. Click **Next** to proceed to the next step.

## Using the Configuration Wizard: System information

### To change system information settings

1. Set the system name, contact, location, and information (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: " < > \
2. Click **Next** to proceed to the next step.

## Using the Configuration Wizard: Configure event notification

You can enable the system to send notifications to SNMP trap hosts and email addresses when events occur in the system. You can also enable the managed logs feature, which transfers log data to a log-collection system. For more information about the managed logs feature, see “About managed logs” (page 41).

### To change SNMP notification settings

1. Select one of the following Notification Level options:
   - **none** (disabled). All events are excluded from trap notification and traps are disabled.

     However, Critical events and managed-logs events are sent regardless of the notification setting.
   - **Critical**. Notifications are sent for Critical events only.
   - **Error**. Notifications are sent for Error and Critical events only.
   - **Warning**. Notifications are sent for Warning, Error, and Critical events only.
   - **Informational**. Notifications are sent for all events.
2. In the Read community field, enter the SNMP read password for your network. This password is included in traps that are sent. The value is case sensitive and can have a maximum of 31 bytes. It can include any character except for the following: " < >
3. In the Write community field, enter the SNMP write password for your network. The value is case sensitive and can have a maximum of 31 bytes. It can include any character except for the following: " ' < >
4. If SNMP notification is enabled, in the Trap Host Address fields enter the IP addresses of hosts that are configured to receive SNMP traps.

### To change email notification settings

1. If the mail server is not on the local network, make sure that the gateway IP address was set in “Using the Configuration Wizard: Network configuration” (page 49).
2. Select the **Email** tab.
3. In the SMTP Server address field, enter the IP address of the SMTP mail server to use for the email messages.
4. In the Sender Domain field, enter a domain name, which will be 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: \ " : ; < > ( )

   The default is `mydomain.com`. If the domain name is not valid, some email servers will not process the mail.
5. In the Sender Name field, enter a sender name, which will be 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: \ " : ; < > ( ) [ ]

   For example: `Storage-1`.
6. Perform one of the following:
   - To enable email notifications, select the **Enable Email Notifications** check box. This enables the notification level and email address fields.
   - To disable email notifications, clear the **Enable Email Notifications** check box. This disables the notification level and email address fields.
7. If email notification is enabled, select one of the following Notification Level options:
   - **Critical**. Notifications are sent for Critical events only.
   - **Error**. Notifications are sent for Error and Critical events only.
   - **Warning**. Notifications are sent for Warning, Error, and Critical events only.
   - **Informational**. Notifications are sent for all events.
8. 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`.

### To change managed logs settings

1. Select the **Managed Logs** tab.
2. Perform one of the following:
   - To enable managed logs, select the **Enable Managed Logs** check box.
   - To disable managed logs, clear the **Enable Managed Logs** check box.
3. If the managed logs option is enabled, in the Email destination address field, enter the email address of the log-collection system. The email address must use the format `user-name@domain-name` and can have a maximum of 320 bytes. For example: `LogCollector@mydomain.com`.
4. Perform one of the following:
   - 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.
5. Click **Next** to proceed to the next step.

## Using the Configuration Wizard: Port configuration

---

**NOTE:** The Port configuration panel does not appear for systems with SAS controller modules since it does not have SAS host-interface configuration options.

**For AssuredSAN 3004**: Host ports can be configured through the Host Ports Settings panel to use fan-out cables or standard cables (see "Changing host-interface settings" (page 67) for more information).

---

To enable the system to communicate with hosts or with remote systems having FC or iSCSI interfaces, you can configure the system's host-interface options. If the current settings are correct, port configuration is optional.

**For AssuredSAN 4004**: Host ports can be configured as a combination of FC or iSCSI ports. For a 4-port SAS controller module, there are no host-interface options.

**For AssuredSAN 3004**: Host ports can only be configured as either FC or iSCSI ports. For a 2-port SAS controller module, host ports can be configured to use fan-out cables or standard cables.

---

**NOTE:** For information about setting advanced host-port parameters, such as FC port topology, see the CLI Reference Guide.

---

### To configure FC ports

1. Set the Speed option to the proper value to communicate with the host. The speed can be set to **auto**, which auto-negotiates the proper link speed with the host, or to **4-Gbit/s**, **8-Gbit/s**, or **16-Gbit/s**. 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.
2. The FC Connection Mode can be 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. Click **Next** to proceed to the next step.

### To configure iSCSI ports

1. Set the port-specific options:
   - 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.
2. In the Advanced Settings section of the panel, set the options that apply to all iSCSI ports:
   - Enable Authentication) (CHAP). Enables or disables use of Challenge Handshake Authentication Protocol.

     **NOTE:** CHAP records for iSCSI login authentication must be defined if CHAP is enabled. To create CHAP records, see "Configuring CHAP" (page 84).

   - 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.

3. Click **Next** to proceed to the next step.

## Using the Configuration Wizard: Confirm the configuration changes

**NOTE:** For systems with SAS controller modules, this panel appears after the Configure event notification panel since the Port configuration panel is skipped.

Confirm that the changes listed in the wizard panel are correct.

- If they are not correct, click **Previous** to return to previous steps and make necessary changes.
- If they are correct, click **Finish** to apply the settings and finish the wizard. If the changes might disrupt access, confirm the changes.

  When processing is complete, you are prompted to add storage. Click **Yes** to open the Add Disk Group panel. Otherwise, click **No**.

# Changing system information settings

### To change system information settings

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

     The Set System Information panel opens.
2. Set the System Name, System Contact person, System Location, and System Information (description) values. The name is shown in the browser title bar or tab. The name, contact, and location 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. Click **OK**.

# Managing users

The system provides three default users and nine additional users can be created. The default users are “standard users,” which can access one or more of the following standard management interfaces: SMC (WBI), CLI, SMI-S, or FTP. 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 “Changing notification settings” (page 57). For information about the MIB, see “SNMP reference” (page 289).

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 but can only view the settings for other users.

**Table 12 Settings for the default users (v3)**

| User Name | Password | User Type | Roles | Interfaces | Base | Precision | Unit | Temperature | Timeout (minutes) | Locale |
|---|---|---|---|---|---|---|---|---|---|---|
| monitor | !monitor | Standard | monitor | WBI, CLI | Base 10 | 1 | Auto | Celsius | 30 | English |
| manage | !manage | | monitor, manage | WBI, CLI, SMI-S, FTP | | | | | | |
| ftp | !ftp | | monitor, manage | FTP | | | | | | |

**IMPORTANT:** To secure the storage system, set a new password for each default user.

## 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, and one non-alphabetic 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 SMC.
  - **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, which can be used instead of the SMC 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 (1–10) 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 Arabic, Chinese-Simplified, Chinese-Traditional, Dutch, English, French, German, Italian, Japanese, Korean, Portuguese, Russian, and Spanish. The locale determines the character used for the decimal (radix) point, as shown in “Size representations” (page 25).

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** 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 IP address of the host system that will receive SNMP traps.

## Adding, modifying, and deleting users

### To add a new user

1. Perform one of the following:
   - In the Home topic, select **Action > Manage Users**.
   - In the banner, click the user panel and select **Manage Users**.

     The User Management panel opens and shows a table of existing users. For information about using tables, see “Tips for using help” (page 23).
2. Below the table, click **New**.
3. Set the options.
4. Click **Apply**. The user is added and the table is updated.

### To create a user from an existing user

1. Perform one of the following:
   - In the Home topic, select **Action > Manage Users**.
   - In the banner, click the user panel and select **Manage users**.

     The User Management panel opens and shows a table of existing users. For information about using tables, see “Tips for using help” (page 23).
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. Click **Apply**. The user is added and the table is updated.

### To modify a user

1. Perform one of the following:
   - In the Home topic, select **Action > Manage Users**.
   - In the banner, click the user panel and select **Manage users**.

     The User Management panel opens and shows a table of existing users. For information about using tables, see “Tips for using help” (page 23).
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. Click **Apply**. A confirmation panel appears.
5. Click **Yes** to continue. Otherwise, click **No**. If you clicked Yes, the user is modified.

### To delete a user (other than your current user)

1. Perform one of the following:
   - In the Home topic, select **Action > Manage Users**.
   - In the banner, click the user panel and select **Manage users**.

     The User Management panel opens and shows a table of existing users. For information about using tables, see "Tips for using help" (page 23).
2. Select the user to delete.
3. Click **Delete**. A confirmation panel appears.
4. Click **Remove** to continue. Otherwise, click **Cancel**. If you clicked Remove, the user is removed and the table is updated.

## Changing notification settings

You can enable the system to send notifications to SNMP trap hosts and to email addresses when events occur in the system. You can also enable the managed logs feature, which transfers log data to a log-collection system. For more information about the managed logs feature, see "About managed logs" (page 41).

### To change notification settings

1. Open the Notification Settings panel through either method:
   - In the footer, click the events panel and select **Set Up Notifications**.
   - In the Home topic, select **Action > Set Up Notifications**.
2. Change SNMP, email, and managed logs settings, as described in the first three procedures below.
3. Test the notification settings, as described in "To test notification settings" (page 59).

### To change SNMP notification settings

1. Select the **SNMP** tab.
2. If a message near the top of the panel informs you that the SNMP service is disabled, enable it, as described in "Changing system services settings" (page 65).
3. Select one of the following Notification Level options:
   - **none (disabled)**. All events are excluded from trap notification and traps are disabled.

     However, Critical events and managed-logs events are sent regardless of the notification setting.
   - **Critical**. Notifications are sent for Critical events only.
   - **Error**. Notifications are sent for Error and Critical events only.
   - **Warning**. Notifications are sent for Warning, Error, and Critical events only.
   - **Informational**. Notifications are sent for all events.
4. In the Read Community field, enter the SNMP read password for your network. This password is included in traps that are sent. The value is case sensitive and can have a maximum of 31 bytes. It can include any character except for the following: " < >
5. In the Write Community field, enter the SNMP write password for your network. The value is case sensitive and can have a maximum of 31 bytes. It can include any character except for the following: " < >
6. If SNMP notification is enabled, in the Trap Host Address fields, enter the IP addresses of hosts that are configured to receive SNMP traps.
7. Click **Apply**.

### To change email notification settings

1. If the mail server is not on the local network, make sure that the gateway IP address is set in the System IP Network Configuration panel, as described in "Changing network interface settings" (page 66).
2. Select the Email tab.
3. In the SMTP Server address field, enter the IP address of the SMTP mail server to use for the email messages.
4. In the Sender Domain field, enter a domain name, which will be 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: \ " : ; < > ( ).

   The default is `mydomain.com`. If the domain name is not valid, some email servers will not process the mail.
5. In the Sender Name field, enter a sender name, which will be 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: \ " : ; < > ( ) [ ]

   For example: `Storage-1`
6. Set the email notification option:
   - To enable email notifications, select the **Enable Email Notifications** check box. This enables the notification level and email address fields.
   - To disable email notifications, clear the **Enable Email Notifications** check box. This disables the notification level and email address fields.
7. If email notification is enabled, select one of the following Notification Level options:
   - **Critical**. Notifications are sent for Critical events only.
   - **Critical, Error**. Notifications are sent for Error and Critical events only.
   - **Critical, Error, Warning**. Notifications are sent for Warning, Error, and Critical events only.
   - **Critical, Error, Warning, Informational**. Notifications are sent for all events.
8. 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`.
9. Click **Apply**.

### To change managed logs settings

1. Select the **Email** tab and ensure that the SMTP Server Address and Sender Domain options are set, as described above.
2. Select the **Managed Logs** tab.
3. 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.
4. If the managed logs option is enabled, in the Email destination address field, enter the email address of the log-collection system. The email address must use the format *user-name@domain-name* and can have a maximum of 320 bytes. For example: `LogCollector@mydomain.com`.
5. Select one of the following options:
   - To use the 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 the pull mode, clear the **Include logs as an email attachment** check box.
6. Click **Apply**.

### To test notification settings

1. Click **Send Test Event**. A test notification is sent to each configured trap host and email address.
2. Verify that the test notification reached each configured trap host and email address.
3. If the managed logs option is enabled, click **Send Log Test**. A test notification is sent to the log-collection system.
4. Verify that the test notification reached the log-collection system.

## Managing scheduled tasks

You can modify or delete scheduled tasks to create snapshots, reset snapshots, run replications, enable or disable drive spin down (DSD), and copy linear volumes.

**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 SMC. For more information, see the CLI Reference Guide.

### To modify a schedule

1. In the Home topic, select **Action > Manage Schedules**. The Manage Schedules panel opens.
2. Select the schedule to modify. The schedule's settings appear at the bottom of the panel.
3. Modify the settings.
4. Click **Apply**. A confirmation panel appears.
5. Click **Yes** to continue. Otherwise, click **No**. If you clicked Yes, the schedule is modified.
6. Click **OK**.

### To delete a schedule

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 **Apply** to continue. Otherwise, click **No**. If you clicked Apply, the schedule was deleted.
5. Click **OK**.

## Installing a license

A license is required to use the Performance tier, snapshots, replication for virtual storage, and replication for linear storage. A license is also required to use volume copy for linear storage, VDS, VSS, and the Storage Replication Adapter (SRA). You can only provision virtual storage with an upgrade license even though options to provision virtual storage are displayed in the v3 interface. The license is specific to a controller enclosure serial number and firmware version.

If a permanent license is not installed and you want to try these features before buying a permanent license, you can create a one-time temporary license. The temporary license will expire 60 days from the time it is created. After creating a temporary license, if you sign in to the SMC in the last 14 days of the trial period, a message specifies the number of remaining days for the trial period. If you do not install a permanent license before the temporary license expires, you cannot create new items with these features. However, you can continue to use existing items.

After a temporary license is created or a permanent license is installed, the option to create a temporary license remains visible, but not accessible.

## Viewing the status of a licensed feature

1. In the Home topic, select **Action > Install License**. The License Settings panel opens and shows the following information about each licensed feature:
   - Feature. The feature name.
   - Base. One of the following:
     - The number of standard snapshots that users can create without a license.
     - `N/A`. Not applicable.
   - License. One of the following:
     - The number of standard snapshots that the installed license supports.
     - `Enabled`. The feature is enabled.
     - `Disabled`. The feature is disabled.
   - In Use. One of the following:
     - The number of standard snapshots that exist.
     - `N/A`. Not applicable.
   - Max Licensable. One of the following:
     - The number of standard snapshots that the maximum license supports.
     - `N/A`. Not applicable.
   - Expiration. One of the following:
     - `Never`. License is purchased and does not expire.
     - The number of days remaining for a temporary license.
     - `Expired`. The temporary license has expired and cannot be renewed.
     - `Expired/Renewable`. Temporary license has expired and can be renewed.
     - `N/A`. Not applicable.

The panel also shows the licensing serial number and the licensing version number (both required for generating a license).

## Installing a permanent license

1. Verify the following:
   - The license file is saved to a network location that you can access from the SMC.
   - You are signed into the controller enclosure for which the file is generated.
2. In the Home topic, select **Action > Install License**. The License Settings panel opens.
3. On the Permanent License tab, click **Choose File** to locate and select the license file.
4. Click **OK**. The license settings table is updated and, for each feature included in the license, the `Expiration` value changes to `Never` for permanent licenses, and displays the number of days remaining for temporary licenses.

## Creating a temporary license

1. In the Home topic, select **Action > Install License**. The License Settings panel opens.
2. On the **Temporary License** tab, if a temporary license has not already expired, the End User License Agreement appears.
3. Read the license agreement.
4. If you accept the terms of the license agreement, select the check box.
5. Click **OK**. A confirmation panel appears.

- Click **Yes** to start the trial period. Otherwise, click **Cancel**. If you clicked Yes, the license settings table is updated and, for each affected feature, the Expiration value shows the number of days remaining in the trial period. The trial period will expire on the last day. When the trial period expires, the value changes to `Expired`.

# 3 Working in the System topic

## 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.

### 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. For a 2U48 enclosure, each drawer and its disks are depicted from a side view, as you would see the disks when the drawer is open. If installed disks are part of a virtual disk group, linear disk group, or are global spares, unique color codes identify them as such. For information on the specific colors used, see "Color codes" (page 23).

To see more information about an enclosure, drawer, or disks, hover the cursor over an enclosure ear, drawer, or a disk:

| | |
|---|---|
| Enclosure Information | ID, status, vendor, model, disk count, WWN, midplane serial number, revision, health |
| Disk Information | Location, serial number, usage, type, size, status, RPM (spinning disk only), SSD life left, manufacturer, model, revision, power on hours, FDE state (for AssuredSAN 4004 only), FDE lock key (for AssuredSAN 4004 only), job running, sector format, health |
| Drawer Information | ID, WWN, status, health |

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

**NOTE:** Following is more information for selected Disk Information panel items:

- *Power On Hours* refers to the total number of hours that the disk has been powered on since it was manufactured. This value is updated in 30-minute increments.
- For AssuredSAN 4004:
  *FDE State* refers to the FDE state of the disk. For more information about FDE states, see the CLI Reference Guide.
- For AssuredSAN 4004:
  *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, fan modules, 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:

**Table 13 Additional information for rear view of enclosure (v3)**

| | |
|---|---|
| Enclosure | ID, status, vendor, model, disk count, WWN, midplane serial number, revision, health |
| Power supply | Status, vendor, model, serial number, revision, health |
| Fan | Location, status, speed, health |
| Controller module | ID, network-port IP address, description, status, model, serial number, hardware version, system cache memory (MB), hardware revision, health |
| FC host port | Name, type, ID (WWN), status, configured speed, actual speed, topology, health |

**Table 13 Additional information for rear view of enclosure (v3)**

| | |
|---|---|
| iSCSI host port | Name, type, ID (IQN), status, actual speed, IP version, address, gateway, network mask, health |
| SAS host port | Name, type, ID (WWN), status, configured speed, actual speed, cable type, health |
| Network port | Name, mode, IP address, network mask, gateway, health |
| Expansion port | Enclosure ID, controller ID, name, status, health |
| Expansion module (IOM) | ID, description, serial number, hardware revision, health |

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

**For AssuredSAN 3004**: If the system is configured to use fan-out cables, fan-out cable icons appear between the depicted SAS ports. The number of SAS ports that display depends on the configuration.

## 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 information about using tables, see "Tips for using help" (page 23).

For each component, the table shows the following information:

- Health. Shows the health of the component:
  - OK
  - Degraded
  - Fault
  - N/A
  - Unknown
- Type. Shows the component type: enclosure, drawer, 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 drawer, the location is shown in the format *drawer-ID*.
  - 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 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 drawer: its FRU description and ID.
  - For a disk: its type, capacity, and usage.
  - Type is shown as either:
    - `MDL`. Spinning midline SAS disk.
    - `SAS`. Spinning enterprise-class SAS disk.
    - `SSD`. Solid-state SAS disk.
  - Usage is shown as either:
    - `AVAIL`. The disk is available.
    - `SPARE`. The disk is configured as a spare.

  - pool-ID:tier name for disk groups that are part of a virtual pools 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.
  - For AssuredSAN 4004:
    UNUSABLE. The disk cannot be used in a disk group because the system is secured, or the disk is locked to data access, or the disk is from an unsupported vendor.
- 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 drawer:
    - Up. The drawer is present and properly communicating with the expander.
    - Warning. A drawer component is experiencing a problem.
    - Error. The drawer is reporting an error condition.
    - Unknown. The state of the drawer cannot be determined.
    - Unavailable. The drawer is present but cannot communicate with the expander.
    - Not present. The drawer is not installed.
  - 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.
    - 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's 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.

# Managing global spares

You can designate a maximum of 16 global spares for the system. 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 (RAID 1, 5, 6, 10 for virtual disk groups, 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 contains a single disk set, which consists of the disks selected as global spares. The Disk Sets summary includes a row that shows the total space of the disk set and amount of space allocated for spares. Also, a table is located below the row that contains several fields, including the Disks and Size fields. The total space and Size field values reflect the cumulative amount of storage for the selected disks. The Disks field shows the number of spares selected.

Underneath the Disk Sets summary are one or more disk tables depending on how many enclosures your system has. Each table represents an enclosure and all of its disks. To see more information about an enclosure or disks, such as the disk type, capacity, and sector format, hover the cursor over an enclosure ear or disk. The Enclosure Information or Disk Information panel appears. “Viewing pools” (page 86) contains more details about the Disk Information panel.

If installed disks are part of a virtual disk group, linear disk group, or are global spares, unique color codes identify them as such. For information on the specific colors used, see “Color codes” (page 23).

---

**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” (page 26).

---

### To change the system's global spares

1. In the System topic, select **Action > Change Global Spares**. The Change Global Spares panel shows information about available disks in the system. Existing spares are labeled GLOBAL SP.
   - In the Disk Sets summary, the number of white slots in the Disks field shows how many spares you can add. The colored slots show how many disks you have selected to become spares or have already added as spares.
   - In each disk table, which visually represents the disks for an enclosure, only existing global spares and suitable available disks are selectable.
2. Select spares to remove, disks to add as spares, or both.
3. Click **Change**. If the task succeeds, the panel is updated to show which disks are now global spares.

# Changing system services 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.

If a service is disabled, it continues to run but cannot be accessed. To allow specific users to access the SMC (the web browser interface), CLI, FTP, or SMI-S interfaces, see "Managing users" (page 54).

### To change system services settings

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

   The System Services panel opens.
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**, **HTTPS** for increased security, or of both. If you disable both, you will lose access to this interface.
     - Default Management Mode. The default version of the SMC that opens when you access it. Select **v2** for the interface that manages legacy linear storage, or **v3** for the new interface that manages virtual storage.
   - Command Line Interface (CLI). An advanced-user interface that is used to write scripts to manage the system. You can enable use of **SSH** (secure shell) for increased security, **Telnet**, or both.
   - 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 via 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.
   - File Transfer Protocol (FTP). A secondary interface for installing firmware updates, downloading logs, and installing a license.
   - 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.
   - Activity Progress Reporting. Provides access to the activity progress interface via 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. In addition, 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.
3. Click **OK**. If any unsecure interfaces are enabled, a confirmation panel will appear.
4. Click **Yes** to confirm use of unsecure interfaces. Otherwise, click **No**.

# Changing network interface settings

You can change addressing parameters for the network port in each controller module. You can set static IP values or use DHCP. When setting static IP values, you can use either IPv4 or IPv6 format.

In DHCP mode, the system obtains values for the network port IP address, subnet mask, and gateway from a DHCP server if one 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.

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 in the storage system, the following initial values are set and remain set until the system is able to 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: 0.0.0.0

169.254.x.x addresses (including gateway 169.254.0.1) are on a private subnet that is reserved for unconfigured systems and addresses that are not routable. This 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.

△ **CAUTION:** Changing IP settings can cause management hosts to lose access to the storage system.

### To use DHCP to obtain IP values for network ports

1. In the System topic, select **Action > Set Up Network**. The System IP Network Configuration panel opens.
2. Set IP address source to **DHCP** and click **OK**. If the controllers successfully obtain IP values from the DHCP server, the new IP values appear.
3. Record the new addresses.
4. Sign out and try to access the SMC using the new IP addresses.

To set static IP values for network ports:

1. Determine the IP address, subnet mask, and gateway values to use for each network port.
2. In the System topic, select **Action > Set Up Network**. The System IP Network Configuration panel opens.
3. Set IP address source to **manual**.
4. To specify addresses in IPv6 format instead of the default format, IPv4, select the **IPv6** check box. IPv4 uses 32-bit addresses. IPv6 uses 128-bit addresses.

**NOTE:** IPv6 for controller module network ports is not supported in this release.

5. Enter IP address, subnet mask, and gateway values for each controller. You must set a unique IP address for each controller.

   **NOTE:** The following IP addresses are reserved for internal use by the storage system: 192.168.200.253, 192.168.200.254, 172.22.255.253, 172.22.255.254, and 127.0.0.1.

6. Record the IP values you assign.
7. Click **OK**.
8. Sign out and try to access the SMC using the new IP addresses.

# Changing host-interface settings

To enable the system to communicate with hosts or with remote systems having FC or iSCSI interfaces, you can configure the system's host-interface options. If the current settings are correct, port configuration is optional.

**For AssuredSAN 4004**: Host ports can be configured as a combination of FC or iSCSI ports. For a 4-port SAS controller module, there are no host-interface options.

**For AssuredSAN 3004**: Host ports can only be configured as either FC or iSCSI ports. For a 2-port SAS controller module, host ports can be configured to use fan-out cables or standard cables.

**NOTE:** For information about setting `advanced host-port` parameters, such as FC port topology, see the CLI Reference Guide.

### To change FC host interface settings

1. In the System topic, select **Action > Set Up Host Ports**. The Host Ports Settings panel opens.
2. Set the Speed option to the proper value to communicate with the host. The speed can be set to **auto**, which auto-negotiates the proper link speed with the host, or to **4 Gbit/s**, **8 Gbit/s**, or **16 Gbit/s**. 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.
3. The FC Connection Mode can be point-to-point or auto:
   - **point-to-point**: Fibre Channel point-to-point.
   - **auto**: Automatically sets the mode based on the detected connection type.
4. Click **OK**.
5. Click **Apply**. Otherwise, click **Cancel**. If you clicked Apply, the ports are configured.
6. Click **OK**.

### To configure iSCSI ports

1. In the System topic, select **Action > Set Up Host Ports**. The Host Ports Settings panel opens.
2. Set the port-specific options:
   - 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 use of Challenge Handshake Authentication Protocol.

     **NOTE:** CHAP records for iSCSI login authentication must be defined if CHAP is enabled. To create CHAP records, see "Configuring CHAP" (page 84).

   - 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. Click **OK**.
5. Click **Apply**. Otherwise, click **Cancel**. If you clicked Apply, the ports are configured.
6. Click **OK**.

### To change host interface settings for 2-port SAS controller modules (for AssuredSAN 3004 only)

A fan-out cable can connect one port on each of two SAS hosts to one controller port, using two PHY lanes per port. 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 current link speed, cable type, number of PHY lanes expected for the SAS port, and number of PHY lanes active for each SAS port. The number of ports that display depends on the configuration.

**NOTE:** Using fan-out instead of standard cables doubles the number of hosts that can be attached to a single system. It will also halve the maximum bandwidth available to each host, but overall bandwidth available to all hosts is unchanged.

**IMPORTANT:** Changing the fan-out setting will change the logical numbering of controller host ports, which will cause port IDs in mappings between volumes and initiators to be incorrect. Therefore, before changing the fan-out setting, unmap all mappings. After you have changed the fan-out setting and connected the appropriate cables, you can re-create the mappings.

1. In the System topic, select **Action >Set Up Host Ports**. The Host Ports Settings panel opens.
2. To switch to fan-out cables, select the **Use fan-out cables** check box. To switch to standard cables, clear the **Use fan-out cables** check box.
3. Click **OK**.
4. Click **Apply** to continue. Otherwise, click **Cancel**. If you clicked Apply and the task succeeds:
   a. A processing dialog appears and quickly exits.
   b. A message displays that the controllers are restarting.
   c. The Sign-In page appears after the controllers have restarted.
5. Disconnect the existing cables from the controller module SAS ports and host SAS HBA ports.
6. Switch to the standard or fan-out cables by connecting the new cables to the controller module SAS ports and host SAS HBA ports.
7. Log in if you have not already done so.
8. Click the Home topic icon. The Home topic with the SAS port icons appears.
   - If fan-out cables are connected to SAS ports that are configured to use them, fan-out cable icons appear between the depicted SAS ports.
   - If standard cables are connected to SAS ports that are configured to use them, no icons appear.

# 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 Setup 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 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.

### To rescan disk channels

1. Verify that both controllers are operating normally.
2. Perform one of the following:
   - Point to the **System** tab and select **Rescan Disk Channels**.
   - In the System topic, select **Action > Rescan Disk Channels**.

     The Rescan Disk Channels panel opens.
3. Click **Rescan**.

# 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.

**TIP:** 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.

### To 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

You can view the current versions of firmware in controller modules, expansion modules, drawers, and disk drives. You can also install new versions. For information about supported releases for firmware update, see the Release Notes for your product. For information about which controller module will update the other when a controller module is replaced, see "About firmware update" (page 41). For information about how to enable PFU, using the `set advanced-settings` CLI command, see the CLI Reference Guide.

To monitor the progress of a firmware-update operation by using the activity progress interface, see "Using the activity progress interface" (page 74).

## Best practices for firmware update

- In the health panel in the footer, verify that the system health is OK. If the system health is not OK, view the Health Reason value in the health panel in the footer and resolve all problems before you update firmware. For information about the health panel, see "Viewing health information" (page 140).
- Run the `check firmware-upgrade-health` CLI command before upgrading firmware. This command performs a series of health checks to determine whether any conditions exist that need to be resolved before upgrading firmware. Any conditions that are detected are listed with their potential risks. For information about this command, see the CLI Reference Guide.
- If any unwritten cache data is present, firmware update will not proceed. Before you can update firmware, unwritten data must be removed from cache. See information about event 44 in the Event Descriptions Reference Guide and information about the `clear cache` command in the CLI Reference Guide.
- If a disk group is quarantined, resolve the problem that is causing the component to be quarantined before updating firmware. See information about events 172 and 485 in the Event Descriptions Reference Guide.
- 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.

### To prepare to update controller module firmware

1. Follow the best practices in "Best practices for firmware update" (page 71).
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 you start the firmware update.

### To update controller 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. The Update Controller Modules tab shows versions of firmware components that are currently installed in each controller.
2. Click **Browse** and select the firmware file to install.
3. Click **OK**. A panel shows 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 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's enclosure management processor (EMP) to be updated. This typically takes 2.5 minutes for each EMP in a drive enclosure.

If the Storage Controller cannot be updated, the update operation is cancelled. 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 10–20 minutes for the partner controller to be updated.

4. Clear your web browser cache, then sign in to the SMC. If PFU is 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 through the `partner-firmware-upgrade` parameter of the `set advanced-settings` CLI command, 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 and drawer firmware

An expansion enclosure can contain one or two expansion modules. In an enclosure with drawers, each drawer contains two EMPs, which are also referred to as “modules.” Each expansion module and drawer contains an enclosure management processor (EMP). All modules of the same model should run the same firmware version.

Expansion-module and drawer firmware is updated in either of two ways:

- When you update controller-module firmware, all expansion modules and drawers are automatically updated to a compatible firmware version.
- You can update the firmware in each expansion module and drawer by loading a firmware file obtained from the enclosure vendor.

### To prepare to update expansion module and drawer firmware

1. Follow the best practices in “Best practices for firmware update” (page 71).
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.

### To update expansion module and drawer 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 and drawer in the system.
3. Select the expansion modules and/or drawers 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 or drawer might become inoperative. If this occurs, contact technical support. The module or drawer 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 and drawer 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.

### To prepare to update disk-drive firmware

1. Follow the best practices in "Best practices for firmware update" (page 71).
2. Obtain the appropriate firmware file and download it to your computer or network.
3. Read documentation from the disk-drive manufacturer to determine whether the disk drives must be power cycled after firmware update.
4. 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.

### To update disk-drive firmware

- In the banner, click the system panel and select **Update Firmware**.
- In the System topic, select **Action > Update Firmware**.

  The Update Firmware panel opens.

5. Select the **Update Disk Drives** tab. This tab shows information about each disk drive in the system.
6. Select the disk drives to update.
7. Click **File** and select the firmware file to install.
8. 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.
9. 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.

### To use the activity progress interface

1. Enable the Activity Progress Monitor service. See “Changing system services settings” (page 65).
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`* is required and specifies the IP address of a controller network port.
   - `mc=MC-identifier` is an 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` is an 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 14 Activity progress properties and values (v3)**

| 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.<br>• ACTIVE: The operation for this component is currently active and in progress.<br>• OK: The operation for this component completed successfully and is now inactive.<br>• N/A: The operation for this component was not completed because it was not applicable.<br>• ERROR: The operation for this component failed with an error (see code and message). |
| Code | A numeric code indicating the status.<br>• `0`: The operation for this component completed with a “completed successfully” status.<br>• `1`: The operation for this component was not attempted because it is not applicable (the component doesn’t exist or doesn’t need updating).<br>• `2`: The operation is in progress. The other properties will indicate the progress item (message, current, total, percent).<br>• `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 (for AssuredSAN 4004 only)

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
- FDE 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.

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

#### To set or change 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. Enter 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. Re-enter the passphrase.
4. Click **Set**. A dialog box will confirm the passphrase was changed successfully.

### 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 will not be under your physical control.

If the lock keys are cleared while the system is secured, the system will enter the FDE lock-ready state, in preparation for the system being powered down and transported. The disks will still be in the secured, unlocked state. Once the system has been transported and powered back up, the system and disks will both be in the secured, locked state. Set the system's lock key to restore access to data.

#### To clear lock keys

**NOTE:** The FDE tabs are dynamic, and the **Clear All FDE Keys** option is not available until the current passphrase is entered in the Current Passphrase field. (If you do not have a passphrase, the **Clear All FDE Keys** option will not appear. If you have a passphrase but have not entered it, you can view but will be unable to access this option.) If there is no passphrase, set one using the procedure in "Setting the passphrase," above.

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. Click **Clear**. A dialog box displays.
4. Perform one of the following:
   - To clear the keys, click **Yes**.
   - To cancel the request, click **No**.

### Securing the system

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

#### To secure the system

**NOTE:** 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 will not appear. If you have a passphrase but have not entered it, you can view but will be unable to access this option.) If there is no passphrase, set one using the procedure in "Setting the passphrase" (page 75).

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. Click **Secure**. A dialog box displays.
4. Perform one of the following:
   - To secure the system, click **Yes**.
   - To cancel the request, click **No**.

## 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.

#### To repurpose the system

**NOTE:** The FDE tabs are dynamic, and the **Repurpose System** option is not available until the system is secure and all disk groups have been removed from the system.

1. Delete all disk groups in the system. To delete disk groups, see "Removing disk groups" (page 94). Removing disk groups effectively deletes all data on the disks but does not secure erase them.
2. Click the System tab.

3. In the System topic, select **Action > Full Disk Encryption**.

   The Full Disk Encryption panel opens with the **FDE General Configuration** tab selected.
4. Click **Repurpose**. A dialog box displays.
5. Perform one of the following:
   - To repurpose the system, click **Yes**.
   - To cancel the request, click **No**.

## 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, effectively 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.

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

### To repurpose a disk

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 **Repurpose Disks** tab.
3. Select the disk to repurpose.
4. Click **Repurpose**. A dialog box displays.
5. Perform one of the following:
   - To repurpose the selected disk, click **Yes**.
   - To cancel the request, click **No**.

## Setting FDE 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.

### To 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.

# 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 SMC 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 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, 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” (page 133).

### To perform a restart

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 **Yes** to continue. Otherwise, click **No**. If you clicked Yes, a message 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 information shown might be invalid.

### To perform a shut down

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 **Yes** to continue. Otherwise, click **No**. If you clicked Yes, a message describes shutdown activity.

# 4 Working in the Hosts topic

## Viewing hosts

The Hosts topic shows a tabular view of information about initiators, hosts, and host groups that are defined in the system. For information about using tables, see "Tips for using help" (page 23). For more information about hosts, see "About initiators, hosts, and host groups" (page 35). The Hosts topic also enables users to map initiators (see page 113) and view map details (see page 116).

### Hosts table

The hosts table shows the following information. By default, the table shows 10 entries at a time.

- Group. Shows the group name if the initiator is grouped into a host group; otherwise, `-ungrouped-`.
- Host. Shows the host name if the initiator is grouped into a host; otherwise, `-nohost-`.
- Nickname. Shows the nickname 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 profile settings:
  - `Standard`. Default profile.
  - `HP-UX`. The host uses Flat Space Addressing.
- Discovered. Shows `Yes` for a discovered initiator, or `No` for a manually created initiator.
- Mapped. Shows `Yes` for an initiator that is mapped to volumes, or `No` for an initiator that is not mapped.

### 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" (page 116).

# Creating 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.

### To create an initiator

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 the appropriate option:
   - **Standard**. Default profile.
   - **HP-UX**. The host uses Flat Space Addressing.
6. Click **OK**. The initiator is created and the hosts table is updated.

# Modifying an initiator

You can modify manually created initiators.

### To 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 the appropriate option:
   - **Standard**. Default profile.
   - **HP-UX**. The host uses Flat Space Addressing.
5. Click **OK**. The hosts table is updated.

# Deleting 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.

### To delete initiators

1. In the Hosts topic, select 1–1024 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**. The initiators are deleted and the hosts table is updated.

## Adding 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 have the same mappings as all other initiators in the host. This means that the initiator must be mapped with the same access, port, and LUN settings to the same volumes or volume groups.

### To add initiators to a host

1. In the Hosts topic, select 1–128 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. An 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 `-nohost-` to the specified host name.

## Removing 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.

### To remove initiators from hosts:

1. In the Hosts topic, select 1–1024 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 `-nohost-`.

## Removing hosts

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

### To remove hosts

1. In the Hosts topic, select 1–512 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 `-nohost-`.

## Renaming a host

You can rename a host.

### To 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.

# Adding hosts to a host group

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

To add a host to a host group, the host must have the same mappings as all other members of the group. This means that the host must be mapped with the same access, port, and LUN settings to the same volumes or volume groups.

### To add hosts to a host group

1. In the Hosts topic, select 1–256 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 already exist in the system or include the following: " , . < \
4. Click **OK**. For the selected hosts, the Group value changes from `-ungrouped-` to the specified host group name.

# Removing 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. To delete a host group, see “Removing host groups” (page 83).

### To remove hosts from a host group

1. In the Hosts topic, select 1–256 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 `-ungrouped-`.

# Renaming a host group

You can rename a host group.

### To 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.

# Removing host groups

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

### To remove host groups

1. In the Hosts topic, select 1–32 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 `-ungrouped-`.

# 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-interface settings” (page 67).

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” (page 125).

### To 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. 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**.
4. 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.
5. 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: " <
6. 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.
7. Click **Apply** or **OK**. The CHAP records table is updated.

### To delete a CHAP record

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

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

# 5 Working in the Pools topic

## Viewing pools

The Pools topic shows a tabular view of information about the pools and disk groups that are defined in this system. 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.

It also shows information for the disks that each disk group contains. For information about using tables, see “Tips for using tables” (page 22). For more information about pools, see “About SSDs” (page 30). For more information about disk groups, see “About disk groups” (page 26).

### 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.
- Class. Shows the storage type for the pool: virtual or linear.
- Total Size. Shows the storage capacity defined for the pool when it was created.
- 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 that the pool has.

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:

| | |
|---|---|
| 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.<br><br>Linear: Name, serial number, size, available, sector format, owner, health. |

For more information about and to manage the above overcommit, low threshold, mid threshold, and high threshold settings, see “Changing pool settings” (page 95).

### 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.

- 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.
- Class. Shows the storage type for the disk group:
  - `Virtual` (includes read-cache disk groups)
  - `Linear`
- RAID. Shows the RAID level for the disk group.
- Disk Type. 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:
  - CPYBK: The disk group is being used in a copyback operation.
  - DRSC: Disks in the disk group are being scrubbed.
  - EXPD: The linear disk group is being expanded.
  - INIT: The disk group is being initialized.
  - RCON: The disk group is being reconstructed.
  - VDRAIN: The virtual 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.
- 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:

| | |
|---|---|
| Disk Group Information | Virtual: Name, serial number, pool, tier, % of pool, allocated pages, available pages, sector format, health.<br><br>Linear: Name, serial number, pool, owner, chunk size, spares, sector format, health.<br><br>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.

- 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.
  - SAS MDL: Midline SAS.
  - sSAS: SAS SSD.
- 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:

| | |
|---|---|
| Disk Information | Location, serial number, usage, type, size, status, revolutions per minute (spinning disk only), SSD life left, manufacturer, model, firmware revision, power on hours, job status, FDE state (AssuredSAN 4004 only), FDE lock key (AssuredSAN 4004 only), job running, sector format, health. |

**NOTE:** Following is more information for selected Disk Information panel items:

- *Power On Hours* refers to the total number of hours that the disk has been powered on since it was manufactured. This value is updated in 30-minute increments.
- For AssuredSAN 4004:
  *FDE State* refers to the FDE state of the disk. For more information about FDE states, see the CLI Reference Guide.
- For AssuredSAN 4004:
  *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 and 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 type and individual disks and incorporate them into a pool. You cannot create virtual disk groups that contain SSDs without the Performance tier license. 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” (page 26).

## Add Disk Group panel overview

There are three sections that comprise the Add Disk Group panel. The top section provides options for the disk group, such as the type, name, and RAID level of the disk group. The options that appear vary depending on the type of disk group selected.

The middle section contains the disk selection sets summary, which presents cumulative data for the disks selected for the disk group. The amount of disk space (total, available, overhead, and dedicated spares) appears, as do the RAID and disk types that have been selected for the disk group.

The summary also contains the Disks bar, which shows the number of disks selected, and the **Complete** check box. The Disks bar appears for disks intended for use in a RAID configuration, as dedicated spares, or in a read-cache disk group. The **Complete** check box indicates if the minimum number of disks needed for the configuration have been selected. It automatically changes from ☒ to ☑ when the minimum has been selected. For dedicated spares, it is always ☑, since selecting any spares is optional. The options that appear in the middle section vary depending on the type of disk group selected.

In the bottom section are one or more disk tables depending on the number of enclosures that your system has. Each table represents an enclosure and all of its disks. Open check boxes appear on available disks. To see more information about an enclosure or disks, such as the disk type, capacity, and sector format, hover the cursor over an enclosure ear or disk. The Enclosure Information or Disk Information panel appears. “Viewing pools” (page 86) contains more details about the Disk Information panel.

If installed disks are part of a virtual disk group, linear disk group, or are global spares, unique color codes identify them as such. For information on the specific colors used, see “Color codes” (page 23).

## 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 and license installed, virtual disk groups belong to one of the following tiers:

- Enterprise SAS disks: Standard tier.
- Midline SAS disks: Archive tier.
- SAS SSD disks: Requires the Performance tier license to be used in virtual disk groups, which automatically use the Performance tier for SSDs. Does not require the license to be used in read-cache and linear disk groups, which do not use tiers.

**TIP:** All virtual groups in the same tier within a virtual pool should have the same RAID level. This will 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 dequarantined the existing disk group. For information on quarantining and dequaranting disk groups, see the CLI documentation.

## 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:

- Type. When creating a disk group, select **Virtual** to show options for a virtual disk group, **Read Cache** to show options for a read cache disk group, or **Linear** to show options for a linear disk group.
- Name. 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: " , < \
- 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.

    **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 on this command, see the CLI Reference Guide.

- Chunk size (optional, only appears for linear 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

  **NOTE:** For a virtual group, the system will automatically use 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

- 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 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**.
- 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.
- 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.

### 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.
3. If you are creating a linear disk group, select the **RAID** [**number**] or **SPARE** option to determine if you will be selecting disks for the RAID configuration or as dedicated spares for the disk group.
4. Select the disks.
5. Click **Add**.

   If your disk group contains a mix of 512n and 512e disks, a dialog box displays. 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 when you select the pool for it in the pools table.

# Modifying a disk group

You can rename any disk group and assign a different controller to, expand the capacity of, enable the drive spin down (DSD) feature, and set a DSD delay for linear disk groups.

## Virtual disk groups

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

## Linear disk groups

When you choose to add disks to the disk group, three sections are visible in the Modify Disk Group panel. The top section, which appears when you first open the panel, provides options for renaming and assigning a controller to the disk group, enabling DSD, and setting a DSD delay. The middle and bottom sections only appear when you choose to expand the panel to add disks.

The middle section contains the disk selection sets summary, which presents cumulative data for existing disks and dedicated spares for the disk group as well as for currently selected disks. The amount of disk space (total, available, overhead, and dedicated spares) appears, as do the RAID and disk types that have been selected for the disk group. While the RAID level appears, you cannot change it.

The summary also contains the Disks bar, which shows the number of disks selected, and the **Complete** check boxes. The Disks bar appears for disks intended for use in a RAID configuration or as dedicated spares. The RAID **Complete** check box indicates if the minimum number of disks needed for the configuration have been selected. It automatically changes from ☒ to ☑ when the minimum has been selected. For dedicated spares, the check box is always green, since selecting any spares is optional.

In the bottom section are one or more disk tables depending on the number of enclosures that your system has. Each table represents an enclosure and all of its disks. The RAID level for the disks in the disk group appear on the disks. `SPARE` appears on each dedicated spare. Open check boxes appear on available disks. To see more information about an enclosure or disks, such as the disk type, capacity, and sector format, hover the cursor over an enclosure ear or disk. The Enclosure Information or Disk Information panel appears. “Viewing pools” (page 86) contains more details about the Disk Information panel.

If installed disks are part of a virtual disk group, linear disk group, or are global spares, unique color codes identify them as such. For information on the specific colors used, see “Color codes” (page 23).

To see more information about a pool, hover the cursor over the pool in the table. “Viewing pools” (page 86) contains more details about the Pool Information panel.

## Linear disk group expansion

You can expand the capacity of a disk group 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, which becomes available when the expansion is complete. As described in “About RAID levels” (page 28), 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.

When expanding a linear 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” (page 26).

Before expanding a disk group, 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.

**IMPORTANT:** 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.

## Drive spin down

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

### To modify a disk group

1. In the Pools topic, select the pool for the disk group that you are modifying in the pools table. Then, select the disk group 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" (page 86) contains more details about the Pool Information panel that appears.

2. Select **Action > Modify Disk Group**. The Modify Disk Group panel opens.
3. To change the disk group name, replace the existing 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: " , < \
4. In a dual-controller system, to assign a controller to the disk group, choose the controller in 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 proceed to the next step.

5. To expand the disk group:
   a. Select the **Expand?** check box. The Modify Disk Group panel expands and disk tables with the disks for the system appear.
   b. For disk groups with RAID-10 or RAID-50 configurations, choose the number of new sub-groups in the Additional Sub-groups list.
   c. Select additional disks.
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, enter the number of minutes in the Drive Spin Down Delay field. The maximum value is 360 minutes.
8. Click **Modify**.
9. Click **Yes** to continue. Otherwise, click **No**. If you clicked Yes, the disk group modification has started.
10. To close the confirmation panel, click **OK**.

# Removing disk groups

You can remove disk groups. It is possible to 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.

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.

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:** 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.

### To remove a disk group

1. In the Pools topic, select the pool for the disk group(s) that you are deleting in the pools table. Then, select the disk group(s) 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" (page 86) 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 group(s) and their volumes are deleted, the pool for the disk group(s) might be deleted, the disks for the disk group(s) become available, and the Related Disk Groups table is updated.

# Changing dedicated spares

You can add and remove dedicated spares for linear disk groups. Virtual disk groups do not have dedicated spares. Neither do read-cache disk groups.

The Change Disk Group Spares panel consists of two sections. The top section contains the disk sets summary, which presents cumulative data for existing disks and dedicated spares for the disk group as well as for currently selected disks. The amount of disk space (total, available, overhead, and dedicated spares) appears, as do the RAID and disk types for the disk group. The summary also contains the Disks bar, which shows the number of disks selected, and the **Complete** check boxes.

In the bottom section are one or more disk tables depending on the number of enclosures that your system has. Each table represents an enclosure and all of its disks. The RAID level for the disks in the disk group appear on the disks. SPARE appears on each dedicated spare. Open check boxes appear on available disks.

To see more information about an enclosure or disks, such as the disk type, capacity, and sector format, hover the cursor over an enclosure ear or disk. The Enclosure Information or Disk Information panel appears. “Viewing pools” (page 86) contains more details about the Disk Information panel.

If installed disks are part of a virtual disk group, linear disk group, or are global spares, unique color codes identify them as such. For information on the specific colors used, see “Color codes” (page 23).

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” (page 26).

### To change the dedicated spares of a disk group

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 > Change Disk Group Spares**. The Change Disk Group Spares panel opens.
3. To add dedicated spares, select available disks.

   SPARE appears on each selected disk.
4. To remove dedicated spares, select current spares.

   SPARE no longer appears on the selected disk(s).
5. Click **Change**.
6. To close the confirmation panel, click **OK**.

## Creating a volume

You can add volumes to virtual pools and linear disk groups. The Create Virtual Volumes and Create Linear Volumes panels enable you to create virtual and linear volumes. You can access these panels from both the Pools and Volumes topics.

### To create volumes through the Pools topic

1. In the Pools topic, select a pool in the pools table. Then, select a disk group 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” (page 86) contains more details about the Pool Information panel that appears.
2. Select **Action > Create Virtual Volumes**. Depending on the type of disk group that you selected, the Create Virtual Volumes or Create Linear Volumes panel opens.
3. For more information about creating virtual volumes, see “Creating a virtual volume” (page 100). For more information about creating linear volumes, see “Creating a linear volume” (page 102).

## 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, and/or the middle threshold is relatively high, the high threshold may not guarantee 200 GB of reserved space in the pool. The controller will not 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 will be generated to notify the administrator. This value must be less than the Mid Threshold value. The default is 25%.
- Mid Threshold. When this percentage of virtual pool capacity has been used, event 462 will be 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 50%. If the pool is not overcommitted, the event will have Informational severity. If the pool is overcommitted, the event will have Warning severity.
- High Threshold. When this percentage of virtual pool capacity has been used, event 462 will be 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 will have Informational severity. If the pool is overcommitted, the event will have Warning severity and the system will use write-through cache mode until virtual pool usage drops back below this threshold.
- **Enable overcommitment of pools?**. This check box controls whether thin provisioning is enabled, and whether storage-pool capacity may exceed the physical capacity of disks in the system. For information about thin provisioning, see “About thin provisioning” (page 34).

**NOTE:** If you try to disable overcommitment and the total space allocated to thin-provisioned volumes exceeds the physical capacity of their pool, an error will state that there is insufficient free disk space to complete the operation and overcommitment will remain enabled. 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.

To check if the pool is overcommitted, in the Pools topic, display the Pool Information panel by hovering the cursor over the pool in the pools table. In that panel, if the Pool Overcommitted value is `True`, the pool is overcommitted. If the value is `False`, the pool is not overcommitted.

**NOTE:** The above pool settings apply only to virtual pools. They do not affect linear pools.

### To change virtual pool settings

1. In the **Pools** topic, select a virtual pool in the pools table.

   **NOTE:** To see more information about a virtual pool, hover the cursor over the pool in the table. “Viewing pools” (page 86) contains more details about the Pool Information panel that appears.

2. Select **Action > Change Pool Settings**. The Pool Settings panel opens.
3. To change the low and mid thresholds for each pool, enter new values.
4. To enable thin provisioning, select the **Enable overcommitment of pool?** check box.
5. Click **OK**. The changes are saved.

# 6 Working in the Volumes topic

## Viewing volumes

The Volumes topic shows a tabular view of information about volumes, replication sets, snapshots, and snap pools that are defined in the system. For more information about volumes, see “About volumes and volume groups” (page 32). For more information about replication, see “About replicating virtual volumes” (page 118). For more information about snapshots and snap pools, see “About snapshots” (page 37). For information about using tables, see “Tips for using tables” (page 22).

### Volumes table

To see more information about a volume, snapshot, or snap pool, hover the cursor over an item in the volumes table. The Volume Information panel opens with more detailed information about the item. The following table displays the categories of information while descriptions for selected terms follow.

| | |
|---|---|
| Volume Information | Name, type, pool, group, class, size, allocated size, serial number, write policy, read-ahead size, tier affinity, health |

For more information about write policy and read-ahead size, see “Modifying a volume” (page 103).

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, `-ungrouped-`.
- 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), master volume (linear), snap pool (linear), or a snapshot (virtual or linear).
- 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.

**TIP:** When selecting one or more volumes or snapshots in the volumes table, the **Snapshots**, **Maps**, **Replication Sets**, and **Schedules** tabs will be enabled if they have associated information for the selected items. They will be grey and disabled if they do not.

### Snapshots table

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, select the **Snapshots** tab. The snapshots and all related snapshots appear in the Snapshots table. Then, hover the cursor over the item in the Snapshots table:

| | |
|---|---|
| Snapshot Information | Virtual: Name, serial number, status, status reason, retention priority, snapshot data, unique data, shared data, pool, class, health<br><br>Linear: Name, serial number, status, status reason, snap pool, priority, user priority, snapshot data, unique data, shared data, pool, class, health |

**TIP:** Priority refers to the retention priority for the snapshot, based on the snapshot attributes and the user-defined retention priority for the snapshot type; user priority refers to the user-defined retention priority for the snapshot type; class refers to the storage type: virtual or linear.

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 snap pool is not accessible or is not found.
  - The snapshot is pending.
  - A rollback with modified data is in progress.
- Snap 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).
- Type. Shows one of the following snapshot types:
  - `Standard snapshot`. Snapshot of a standard volume.
  - `Standard snapshot(DRM)`. A temporary standard snapshot created from a replication snapshot for the purpose of doing a test failover for disaster recovery management (DRM).
  - `Replication snapshot`. For a primary or secondary volume, a snapshot that was created by a replication operation but is not a sync point.
  - `Replication snapshot (Replicating)`. For a primary volume, a snapshot that is being replicated to a secondary system.
  - `Replication snapshot (Current sync point)`. For a primary or secondary volume, the latest snapshot that is copy-complete on any secondary system in the replication set.
  - `Replication snapshot (Common sync point)`. For a primary or secondary volume, the latest snapshot that is copy-complete on all secondary systems in the replication set.
  - `Replication snapshot (Old Common sync point)`. For a primary or secondary volume, a common sync point that has been superseded by a new common sync point.
  - `Replication snapshot (Only sync point)`. For a primary or secondary volume, the only snapshot that is copy-complete on any secondary system in the replication set.
  - `Replication snapshot (Queued)`. For a primary volume, a snapshot associated with a replication operation that is waiting for a previous replication operation to complete.
  - `Replication snapshot (Awaiting replicate)`. For a primary volume, a snapshot that is waiting to be replicated to a secondary system.

## Maps table

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" (page 116).

## Replication Sets table

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.

## Schedules table

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. Then, hover the cursor over the item in the Schedules table.

| | |
|---|---|
| Schedule Information | Name, schedule specification, schedule status, next time, task name, task type, task status, task state, error message |

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, a master volume, or a snapshot.
  - `Replicate`. The schedule replicates a virtual replication set to a remote system.

# 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. 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” (page 97) contains more details about the Volume Information panel that appears.

### 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. For the maximum volume size that the system supports, see the system configuration limits topic in the SMC help.

   Volume sizes are aligned to 4-MB boundaries. When a volume is created or expanded, if the resulting size would be less than 4 MB, it will be increased to 4 MB. If the resulting size would be greater than 4 MB, it will be decreased to the nearest 4-MB boundary.
4. Optional: Change the number of volumes to create. See the system configuration limits topic in SMC 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 on the volume tier affinity feature, see “About automated tiered storage” (page 35).
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 will prompt 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 **Yes** to continue. Otherwise, click **No**. If you clicked Yes, 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" (page 97) contains more details about the Volume Information panel that appears.

### 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 SMC 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's pool. For the maximum volume size that the system supports, see the system configuration limits topic in SMC help.

   Volume sizes are aligned to 4-MB boundaries. When a volume is created or expanded, if the resulting size would be less than 4 MB, it will be increased to 4 MB. If the resulting size would be greater than 4 MB, it will be decreased to the nearest 4-MB boundary.
6. Optional: **Enable Snapshots**: If the system is licensed to use Snapshots and you want to create snapshots of this volume, select this check box. This will create the volume as a master volume instead of as a standard volume, and enable the **Snap Pool** option and the **Replication Prepare** check box.
7. Snap Pool. Select either:
   - **Standard Policy**. This option creates a snap pool, whose size is either 20% of the volume size or 5.37 GB, whichever is larger. The recommended minimum size for a snap pool is 50GB.
   - **Snap Pool Size**: Specify the size of the snap pool to create in the disk group and associate it with the new volume. The default size is either 20% of the volume size or 5.37GB, whichever is large. The recommended minimum size for a snap pool is 50 GB.

     You can use any of the following units when specifying the snap pool size: MiB, GiB, TiB, MB, GB, TB.
   - **Attach Pool**. Select an existing snap pool to associate with the new volume.
8. Optional: **Replication Prepare**: If the system is licensed to use remote replication and you want to use this volume as a replication destination, select this check box.
9. 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” (page 33).

---

△ **CAUTION:** Only change the volume cache settings if you fully understand how the host OS, 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 feature” (page 35).

To see more information about a volume, hover the cursor over the volume in the table. “Viewing volumes” (page 97) contains more details about the Volume Information panel that appears.

### 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, enter 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, enter 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-MB boundaries. When a volume is created or expanded, if the resulting size would be less than 4 MB, it will be increased to 4 MB. If the resulting size would be greater than 4 MB, it will be decreased to the nearest 4-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 will overcommit the pool capacity, the system will prompt 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 **Yes** to continue. Otherwise, click **No**. If you clicked Yes, the volumes table is updated.
    b. To close the confirmation panel, click **OK**.

# Adding volumes to a volume group

You can add virtual volumes to a new or existing virtual volume group.

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, port, and LUN 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.

**NOTE:** You cannot add linear volumes to a volume group.

### To add volumes to a volume group

1. In the Volumes topic, select 1–20 volumes to add to a volume group.
2. Select **Action > Add to Volume Group**. The Add to Volume Group panel opens.
3. Perform one of the following:
   - To use an existing volume group, select its name in the Volume Groups list.
   - To create a volume group, enter 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**. For the selected volumes, the Volume Groups value changes from `-ungrouped-` to the specified host group name.

# 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” (page 105).

To see more information about a volume, hover the cursor over the volume in the table. “Viewing volumes” (page 97) contains more details about the Volume Information panel that appears.

### To 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 `-ungrouped-`.

# Renaming a volume group

You can rename a volume group unless it is part of a replication set. Renaming a volume group will delete the volume group and then create one with the new name.

To see more information about a volume, hover the cursor over the volume in the table. “Viewing volumes” (page 97) 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.

### To 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.

# Removing 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" (page 97) contains more details about the Volume Information panel that appears.

### To 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 1–32 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 `-ungrouped-`.

### 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 1–32 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.

# Copying a volume or snapshot

If the system is licensed to use the volume copy feature, you can copy a linear volume or a linear snapshot to a new linear volume through the SMC. You can also copy a virtual base volume or snapshot to a new virtual volume through the CLI, but not through the SMC. For more information about using the CLI to create a copy of a virtual snapshot, see the CLI Reference Guide.

When using a linear snapshot as the source, you can choose whether to include its modified data (data written to the snapshot since it was created). The new volume is completely independent of the source.

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 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 offline.

You can copy a volume immediately or schedule a copy task.

### To copy a linear volume or snapshot

1. In the **Volumes** topic, select a linear 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 enter a different name.
4. Optional: In the Residing On Pool field, change the linear pool in which to create the copy.
5. Optional: If you want to schedule a copy task, perform the following:
   - Select the **Schedule?** check box.
   - 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: 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.
6. Click **OK**. A confirmation panel appears.
7. Click **Yes** to continue. Otherwise, click **No**.
   - If you clicked Yes and the **Schedule?** check box is not selected, the copy operation starts. If you unmounted a snapshot to copy its modified data, wait until processing is complete before you remount it.
   - If you clicked Yes and the **Schedule?** check box is selected, the schedule is created and can be viewed in the Manage Schedules panel, as described in "Managing scheduled tasks" (page 59). If you copy modified data for a snapshot, make a reminder to unmount the snapshot before the scheduled task runs.

## Rolling back a volume

You can replace the data of a source volume or snapshot with the data of a snapshot that was created from it. This feature operates differently depending on the storage technology for the snapshot.

For linear snapshots, you can roll back (revert) the data in a volume to the data that existed when a specified snapshot of that volume was created. You also have the option to include snapshot modified data (data written to the snapshot since it was created). For example, you might want to create a snapshot of a linear volume, mount the snapshot for read and write, and then install new software on the snapshot for testing. If the software installation is successful, you can roll back the linear volume to the contents of the modified snapshot.

△ **CAUTION:** Before rolling back a linear volume, you must unmount it from hosts to avoid data corruption. If you want to include snapshot modified data in the rollback, you must also unmount the snapshot.

△ **CAUTION:** For linear snapshots, if the snap pool runs out of space, the standard volume will change to read-only until the rollback has completed.

△ **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.

For both virtual and linear snapshots, 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 virtual 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 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.

During a rollback for a linear snapshot that includes snapshot modified data, the snapshot must be unmounted and cannot be accessed. Unmounting the snapshot ensures that all data cached by the host is written to the snapshot. If unmounting is not performed at the host level prior to starting the rollback, data may remain in host cache, and thus not be rolled back to the standard volume. As a precaution against inadvertently accessing the snapshot, the system also takes the snapshot offline. The snapshot becomes inaccessible to prevent any data corruption to the standard volume. The snapshot can be remounted once the rollback is complete.

You cannot roll back a volume that is part of a replication set.

To see more information about a volume, hover the cursor over the volume in the table. "Viewing volumes" (page 97) contains more details about the Volume Information panel that appears.

### To roll back a volume

1. Unmount the volume from hosts.
2. If the rollback is for a linear volume and will include snapshot modified data, unmount the snapshot from hosts.
3. In the Volumes topic, select the volume to roll back.
4. Select **Action > Rollback Volume**. The Rollback Volume panel opens and lists snapshots of the volume.
5. Select the snapshot to roll back to.
6. Optional: To include snapshot modified data in the rollback for a linear volume, select the **With Modified Data** check box. Otherwise, the standard volume will contain only the data that existed when the snapshot was created.
7. Click **OK**. A confirmation panel appears.
8. Click **Yes** to continue. Otherwise, click **No**. The rollback starts. You can now remount the volume.

   If you clicked Yes, the rollback starts. You can now remount the volume
9. When the rollback is complete, if you unmounted the snapshot, you can remount it.

# Deleting volumes and snapshots

You can delete volumes and snapshots. You can delete a volume that has no child snapshots. You cannot delete a virtual volume that is part of a replication set.

△ **CAUTION:** Deleting a volume or snapshot removes its mappings and schedules and deletes its data.

**NOTE:** You can only delete a volume with one or more snapshots, or a snapshot with child snapshots, by deleting all of the snapshots or child snapshots 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 Related Snapshots table. "Viewing volumes" (page 97) contains more details about the Volume Information and Snapshot Information panels that appear.

### To 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 1–100 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

If the system is licensed to use snapshots, you can create snapshots of selected virtual or linear volumes, or of virtual snapshots. You can create snapshots immediately or schedule snapshot creation.

**NOTE:** You can create child snapshots of virtual snapshots but not of linear snapshots.

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" (page 97) contains more details about the Volume Information and Snapshot Information panels that appear.

### To 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 1–32. 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: 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 **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” (page 59).

### To create linear snapshots

1. In the Volumes topic, select 1–16 linear volumes (must be exclusively linear, not a combination of both storage types).
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 1–32. 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: 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 **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, as described in "Managing scheduled tasks" (page 59).

## 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 action is not allowed for a replication snapshot.

For virtual snapshots, 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. "Viewing volumes" (page 97) contains more details about the Volume Information and Snapshot Information panels that appear.

### 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:
   - Select the **Schedule** check box.
   - 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:
     - 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**. A confirmation panel appears.

6. Click **Yes** to continue. Otherwise, click **No**. If you clicked Yes:
   - If the **Schedule** check box was not selected, the snapshot is created. You can remount the snapshot.
   - If **Schedule** is selected, the schedule is created and can be viewed in the Manage Schedules panel, as described in "Managing scheduled tasks" (page 59). Make a reminder 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 SMC—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.

### To create a replication set

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 displays.
3. If the selected volume is in a volume group, source options appear.
   - To replicate the selected volume only, select **Single Volume**.
   - 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 or include the following: " , < \
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: Select the **Scheduled** check box to schedule recurring replications.
9. Click **OK**.
10. 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 “Scheduling replications” (page 130).
    - 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 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. You can initiate replications from a replication set's primary system only. For information on scheduling replications, see “Scheduling replications” (page 130).

You can initiate a replication from both the Replications and Volumes topics. For information on how to initiate a replication, see “Initiating replication” (page 129).

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.

# 7 Working in the Mappings topic

## 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. For information about using tables, see “Tips for using tables” (page 22).

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 “Viewing map details” (page 116).

## 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 also applies to hosts and host groups as well as initiators, and 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 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. This behavior is expected by some operating systems, such as Microsoft Windows, which can immediately discover the volume. 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 initiators, you can create an *explicit mapping*. An explicit mapping can use different access mode, LUN, and port settings to allow or prevent access by an initiator 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 group (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 SMC. It will be replaced in the SMC 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.

### To 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 15 Available host groups, hosts, and initiators (v3)**

| 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-nickname* | initiator-ID |

The Available Volume Groups and Volumes table shows one or more of the following rows:

**Table 16 Available volume groups and volumes (v3)**

| 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 |

**NOTE:**

- When you select one or more host groups, hosts, or initiators in the Hosts topic, the item(s) 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 will be displayed.

   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 host(s) and deny access to all other hosts, create explicit map(s) 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 can only be 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 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.

**TIP:** 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**.

# Viewing map details

In the Hosts, Volumes, and Mapping topics, you can see basic information about mappings between hosts and volumes.

### To view additional details

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. For information about using tables, see “Tips for using tables” (page 22).
   - 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

## About replicating virtual volumes

Replication for virtual storage is a licensed feature that 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 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 iSCSI ports, a virtual pool, and a replication license for virtual storage. 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 port-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 CLI documentation. For more information on peer connections, see “Creating a peer connection” (page 125), “Deleting a peer connection” (page 127), and “Modifying a peer connection” (page 127).

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 two internal snapshots for each volume, which are created on both the primary and secondary systems. These snapshots are used internally for replication operations.

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 (write permission is unavailable), rolled back, or modified except through replication. To prevent problems with host systems, which do not handle well volumes whose contents change automatically, the secondary volume also cannot be mapped with read permission.

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. These snapshots also can be used in disaster recovery. For more information on replication sets, see “Creating a replication set from the Replications topic” (page 127), “Creating a replication set from the Volumes topic” (page 111), “Modifying a replication set” (page 129), and “Deleting a replication set” (page 129).

# 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 "Aborting a replication" (page 131), "Initiating replication" (page 129), "Initiating replication from the Volumes topic" (page 112), "Resuming a replication" (page 132), and "Suspending a replication" (page 131).

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, see "Scheduling replications" (page 130).

## Initial replication

The following figure illustrates the internal processes that take place during the initial replication of a single volume.

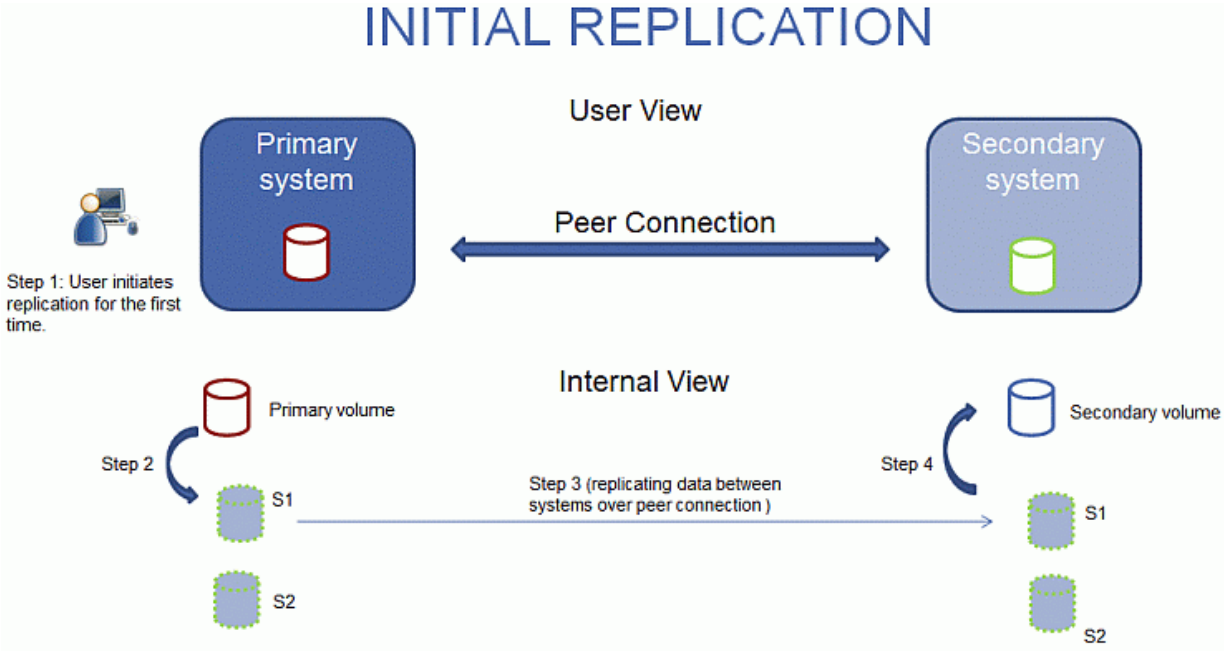



**Figure 1 Replication process for initial replication**

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 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.

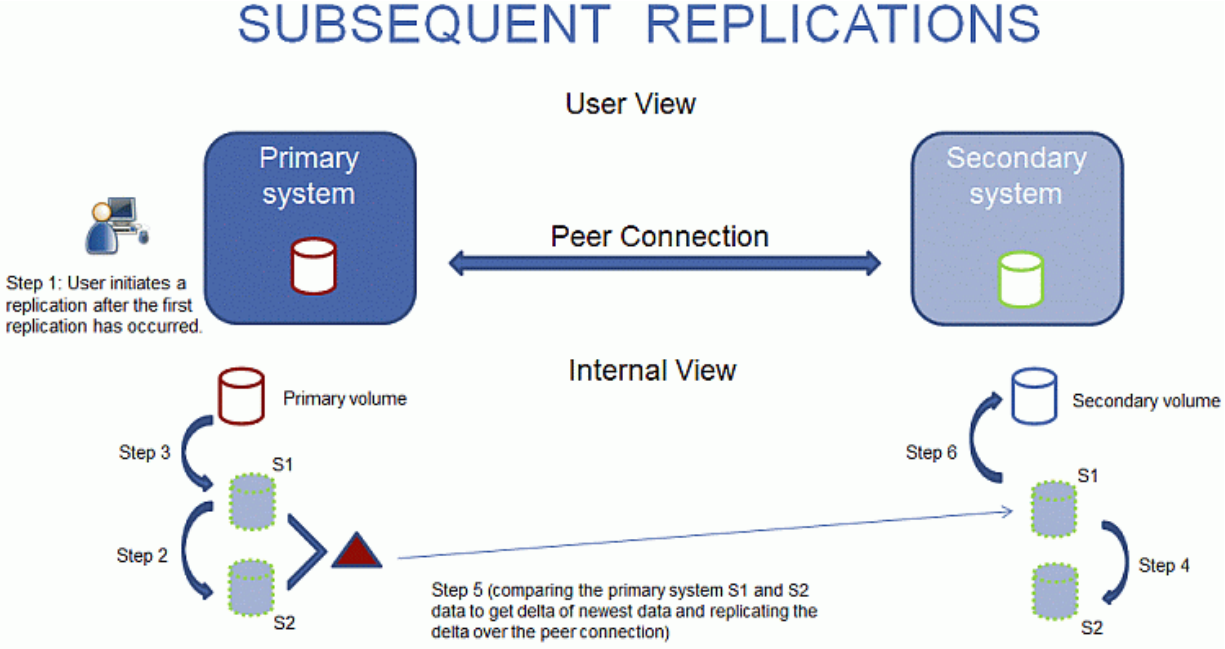



**Figure 2 Replication process for replications subsequent to the initial replication.**

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 do not count against the maximum number of licensed snapshots for the system.

## 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.

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 CLI documentation.

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 CLI documentation.
- 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 CLI documentation.

## 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.

## 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. 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.

#### To temporarily access data at the backup site

1. Create a snapshot of the secondary volume.
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 CLI documentation. 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:

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.

#### To transfer operations from the data center system to the backup system

1. Create a snapshot of the secondary volume, 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.

#### To 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 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.

#### To 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.

## Replication licensing

For information about viewing the status of licensed features in your system, see "Viewing the status of a licensed feature" (page 60).

## Using either linear or virtual replication

You can replicate linear volumes or snapshots by using the linear replication feature accessible through the v2 interface. You can replicate virtual volumes, volume groups, or snapshots by using the virtual replication feature accessible through the v3 interface. Both licensed features share a single license that is valid for both replication technologies. However, you can only use the license for one of the features and cannot alternate between them.

If you are replicating virtual volumes, the system cannot contain any linear replication sets, and vice versa. To move from one replication technology to the other, you must delete all of the replication sets of the current type before being able to configure a replication set of the other one.

If you have previously replicated linear data in AssuredRemote and replicated volumes and snapshots have displayed in the v3 interface, they and associated data will continue to display in the v3 interface as will future linear replicated volumes and snapshots. Information about replication of virtual volumes will not display in the v2 interface.

# Viewing replications

The Replications topic shows a tabular view of information about peer connections and replication sets that are defined in the system. For information about using tables, see “Tips for using tables” (page 22). For more information about replication, see “About replicating virtual volumes” (page 42).

## 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: 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. If the health is not OK, the health reason and recommended action are shown to help you resolve problems.

| | |
|---|---|
| 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.

- 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.

| | |
|---|---|
| Replication Sets | Replication set name and serial number; primary volume or volume group name and serial number; secondary volume or volume group name and serial number; peer connection name; replication schedule name, current run progress, current run start time, current run estimated time to completion, current run transferred data, last success time, last run start time, last run end time, last run transferred data, last run status, and last run error status |

## 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 an IP address of a single available iSCSI host port on the remote system. Only iSCSI host ports are used for the peer connection. FC or SAS ports are not used for peer connections.

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 be licensed to use virtual replication.
- Both systems must have iSCSI ports.
- Each system must have a virtual pool.
- Neither system can have a linear replication set.
- If iSCSI CHAP is configured for the peer connection, the authentication must be valid.

The limit is one peer connection per storage system.

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. (Both systems must be licensed to use the replication feature for virtual storage.) 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.

## 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 below 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 procedure below to set up CHAP. 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.

### 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 address (IP) for the remote system.
4. Click **OK**.
5. 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 displays with errors in red text. Correct the errors, then click **OK**.

### To set up CHAP for a peer connection (using the CLI)

1. If you haven't 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 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 in step 3 through step 5 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 step 3 through step 7 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 without changing the peer connection configurations.

You can only modify a peer connection if there are no replications currently running or suspended from a running state. Abort all running replications and replications suspended from a running state before modifying a peer connection. Also, before modifying your peer connection, suspend your replication set to prevent any scheduled replications from running during the operation. After you have modified the peer connection, you can resume the replication set.

### To 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 displays.
3. Enter a new name for the peer connection or a new address (IP) for the remote system. (You cannot change both.) The name is case sensitive and can have a maximum of 80 bytes. It cannot already exist in the system or include the following: " , < \
4. 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” (page 129).

---

**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.

---

### To 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 SMC—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.

### To create a replication set

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 displays.
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 or include the following: " , < \
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: Select the **Scheduled** check box to schedule recurring replications.
9. Click **OK**.
10. 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 “Scheduling replications” (page 130).
    - 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 the name of a replication set. Volume membership of a replication cannot change for the life of the replication set.

### To 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**.
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 or include the following: " , < \
4. Click **OK**. The name of the replication set is deleted and the Replications Sets table is updated.

# 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 abort replication for that replication set. For more information, see “Aborting a replication” (page 131) or “Suspending a replication” (page 131).

---

**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 CLI documentation.

---

### To 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 replication

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. You can initiate replications from a replication set's primary system only. For information on scheduling replications, see “Scheduling replications” (page 130).

You can initiate a replication from both the Replications and Volumes topics.

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.

### To manually initiate replication

1. In the either the Replications or Volumes topic, select a replication set in the Replication Sets table.
2. Select **Action > Initiate Replication**.
3. Click **OK**. 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`.

## Scheduling replications

After you have created a replication set, you can schedule replication. You can schedule replications from a replication set's primary system only. For more information on replications, see "Initiating replication" (page 129).

**NOTE:** Virtual storage replication tasks are not queued. If a replication task is running and the time comes for that replication task to start again, that task will be skipped, though it will be counted against the schedule's count constraint (if set). Instead of an open-ended schedule, you can specify the number of replications that can occur for the replication task as part of the procedure for scheduling a replication.

### To schedule a replication

1. In the Replications topic, select a replication set in the Replication Sets table.
2. Select **Action > Schedule Replications**. The Schedule Replications panel opens.
3. Select the **Schedule** check box.
4. 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.
5. Optional: If you want the task to run more than once, select the **Schedule** check box.
   - Specify how often the task should repeat. Enter a number and select the appropriate time unit. Replications can recur no less than 60 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.
6. Click **OK**. The schedule is created.

### To manage a replication schedule

1. In the Replications topic, select a replication set in the Replication Sets table.
2. Select **Action > Manage Schedules**.
3. Set the options:
   - 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).
4. 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 60 minutes apart.
   - Either make sure the **End** check box is cleared, which allows the schedule to run without an end date, or select the check box and specify when the schedule should stop 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.
5. Click **OK**. The schedule is modified.

## Aborting a replication

You can abort running or suspended replication operations for a specified replication set, only from its primary system. Aborting a replication for a replication set that is in a `Ready` or `Unsynchronized` state will generate an error.

---

**NOTE:** If you abort 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.

---

### To abort a 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 aborted.

## 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 “Aborting a replication” (page 131) or “Resuming a replication” (page 132).

If replications are attempted during the suspended period (including scheduled replications), the replications will fail.

To suspend a 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 aborted a replication while the replication set was suspended, the aborted replication does not resume.

### To resume a 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`.

# 9 Working in the Performance topic

## 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” (page 40).

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.

### To 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. For information about using tables, see “Tips for using tables” (page 22).
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.

     **TIP:** 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” (page 133).”
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 17 Historical performance graphs (v3)**

| System component | Graph | Description |
|---|---|---|
| Disk, group, pool, tier | Total IOPS | Shows the total number of read and write operations per second since the last sampling time. |
| Disk, group, pool, tier | Read IOPS | Shows the number of read operations per second since the last sampling time. |

**Table 17 Historical performance graphs (v3) (continued)**

| System component | Graph | Description |
|---|---|---|
| Disk, group, pool, tier | Write IOPS | Shows the number of write operations per second since the last sampling time. |
| Disk, group, pool, tier | Data Throughput | Shows the overall rate at which data was read and written since the last sampling time. |
| Disk, group, pool, tier | Read Throughput | Shows the rate at which data was read since the last sampling time. |
| Disk, group, pool, tier | Write Throughput | Shows the rate at which data was written since the last sampling time. |
| Disk, group, pool, tier | Total I/Os | Shows the number of read and write operations since the last sampling time. |
| Disk, group, pool, tier | Number of Reads | Shows the number of read operations since the last sampling time. |
| Disk, group, pool, tier | Number of Writes | Shows the number of write operations since the last sampling time. |
| Disk, group, pool, tier | Data Transferred | Shows the total amount of data read and written since the last sampling time. |
| Disk, group, pool, tier | Data Read | Shows the amount of data read since the last sampling time. |
| Disk, group, pool, tier | Data Written | Shows the amount of data written since the last sampling time. |
| Disk, group | Average Response Time | Shows the average response time for reads and writes since the last sampling time. |
| Disk, group | Average Read Response Time | Shows the average response time for reads since the last sampling time. |
| Disk, group | Average Write Response Time | Shows the average response time for writes since the last sampling time. |
| Disk, group | Average I/O Size | Shows the average size of reads and writes since the last sampling time. |
| Disk, group | Average Read I/O Size | Shows the average size of reads since the last sampling time. |
| Disk, group | Average Write I/O Size | Shows the average size of writes since the last sampling time. |
| Disk, group | Number of Disk Errors | Shows the number of disk errors since the last sampling time. |
| Disk, group | Queue Depth | Shows the 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 | Shows the 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. |
| Tier | Number of Page Moves In | Shows the number of pages moved into this tier from a different tier. |
| Tier | Number of Page Moves Out | Shows the number of pages moved out of this tier to other tiers. |
| Tier | Number of Page Rebalances | Shows the number of pages moved between disk groups in this tier to automatically load balance. |

**Table 17 Historical performance graphs (v3) (continued)**

| System component | Graph | Description |
|---|---|---|
| Tier | Number of Initial Allocations | Shows the 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 | Shows the 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 | Shows the number of 4-MB pages copied from spinning disks to SSD read cache (read flash cache). |
| Tier | Number of Zero-Pages Reclaimed | Shows the 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” (page 40).

You can update historical statistics.

### To update displayed historical statistics

1. Display a historical statistics graph as described in “Viewing performance statistics” (page 133).
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 5–100 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.

   **TIP:** 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.

### To 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.

   **TIP:** 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 quarter hour.

### To 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

## Banner and footer overview

The banner of the SMC v3 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 SMC 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 SMC v3 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 displays. 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 description. It also shows the firmware bundle version for each controller (A and B).

The icon indicates that the panel has a menu. Click anywhere in the panel to display a menu to change system information settings (page 54) and system services settings (page 65), update firmware (page 71), restart or shut down controllers (page 78) and view SSL certificate information (page 138).

## 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 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 controllers" (page 78).

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.

### To 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 SMC and the storage system. The connection information table show the icon that displays for each state.

**Table 18 Connection information (v3)**

| 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 format *year-month-day hour:minutes:seconds*.

Hover the cursor over this panel to display the System Date/Time panel, which shows NTP settings.

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, such as for Daylight Saving Time. You must make such adjustments manually.

### To use manual date and time settings

1. In the banner, click the date/time panel and select **Set Date and Time**. The Set Date and Time panel opens.
2. 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. Click **OK**.

### To 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 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. Click **OK**.

## 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" (page 54).

## 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 (page 57), save log data (page 140), and view system information (page 61).

### 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 SMC, 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.

### To 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 value for your name and phone number can include a maximum of 100 bytes while your email address can include a maximum of 100 characters. All three values can use all characters except the following: " < > \
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

The event panel in the footer shows the numbers of the following types of events that the system has logged:

- 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.

Hover the cursor over 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” (page 142) and change notification settings on “Changing notification settings” (page 57).

## 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 “Changing notification settings” (page 57). For information about using tables, see “Tips for using tables” (page 22).

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.
- 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 Setup 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. For color-code descriptions, see “Color codes” (page 23).

Hover the cursor over a segment to see the storage type and size 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, space used by linear disk groups, and space used by virtual 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 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 needed for internal management of data structures. The terms allocated space and unallocated space have different meanings for the two storage technologies. For virtual storage, allocated space refers to the amount of space that the data written to the pool takes. Unallocated space is the difference between the space designated for all volumes and the allocated space.

For linear storage, allocated space is the space 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 (with the exception of uncommitted space, there are equivalent sections for virtual and linear disk groups if your system has both virtual and linear storage):

- 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 virtual and linear disk groups, both total and by pool
- Reserved. The reserved space for virtual and linear disk groups, both total and by pool
- Allocated. The allocated space for virtual and linear disk groups, both total and by pool
- Unallocated. The unallocated space for virtual and linear 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 I/O 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. For color-code descriptions, see “Color codes” (page 23).

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 I/O 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. For color-code descriptions, see “Color codes” (page 23).

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 and scheduled tasks.

To view past notifications for this SMC session, click the activity panel in the footer and select **Notification History.** For more information, see “Viewing the notification history” (page 144).

# Viewing the notification history

The Notification History panel shows past activity notifications for this SMC 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.

### To 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.

# Part 2: Using WBI v2

Chapters 11-17 describe using the WBI v2 user interface to manage and monitor linear storage.

# 11 Getting started

RAIDar is a web-based application 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 RAIDar. In a dual-controller system, you can access all functions from either controller. If one controller becomes unavailable, you can continue to manage the storage system from the partner controller.

RAIDar is also a web-browser interface (WBI).

There are two user interfaces available for RAIDar. RAIDar v2 is the legacy interface for managing linear storage that you are currently viewing. SMC v3 is the new interface for managing virtual storage. For new installations, SMC v3 is the default management mode. For upgrades, RAIDar v2 is the default management mode. You can change the default management mode or switch to the other mode for the session.

To switch to the user interface that manages linear storage for the session:

- In the URL, replace `v3` with `v2`.

## Configuring and provisioning a new storage system

To configure and provision a storage system for the first time:

1. Configure your web browser to access RAIDar and sign in, as described in "Browser setup" below and ""Signing in and signing out" (page 147)."
2. Set the system date and time, as described in "Changing the system date and time" (page 182).
3. Use the Configuration Wizard to configure other system settings, as described in "Using the Configuration Wizard" (page 169).
4. Use the Provisioning Wizard to create a virtual disk (*vdisk*) containing storage volumes, and optionally to map the volumes to hosts, as described in "Using the Provisioning Wizard" (page 199).
5. Use the Replication Setup Wizard to configure replication for a primary volume to a remote system, as described in "Using the Replication Setup Wizard" (page 274).
6. If you mapped volumes to hosts, verify the mappings by mounting/presenting the volumes from each host and performing simple read/write tests to the volumes.
7. Verify that controller modules and expansion modules have the latest firmware, as described in "Viewing information about the system" (page 235) and "Updating firmware" (page 221).

You can make additional configuration and provisioning changes and view system status, as described in later chapters of this guide.

## Browser setup

- Supported browser versions: Mozilla Firefox 11 and newer; Microsoft Internet Explorer 10 and 11; Google Chrome 17 and newer; Apple Safari 5.1 and newer.
- 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 browser's local-intranet security option to medium or medium-low.
  - Verify that the browser is set to allow cookies at least for the IP addresses of the storage-system network ports.
  - For Internet Explorer, add each controller's network IP address as a trusted site.
  - If RAIDar is configured to use HTTPS, ensure that Internet Explorer is set to use either TLS 1.0, TLS 1.1, or TLS 1.2.

# Signing in and signing out

Multiple users can be signed in to each controller simultaneously.

For each active RAIDar 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 RAIDar session, but all instances of Firefox, Chrome, and Safari share the same RAIDar session.

To sign in:

1. In the web browser's address field, type `https://`*<IP address of a controller network port >* and press **Enter**. The RAIDar Sign In page is displayed. If the Sign In page does not display, verify that you have entered the correct IP address.
2. On the Sign In page, enter the name and password of a configured user. The default user name and password are `manage` and `!manage`. To display the interface in a language other than the user setting, select the language from the Language list.

   Language preferences can be configured for the system and for individual users.
3. Click **Sign In**. If the system is available, the System Overview page is displayed. Otherwise, a message indicates that the system is unavailable.

When you are ready to end your session, sign out as described below. Do not simply close the browser window.

To sign out:

1. Click **Sign Out** near the top of the RAIDar window.
2. In the confirmation panel, click **Sign Out**.

# Tips for signing in and signing out

- Do not include a leading zero in an IP address. For example, enter 10.1.4.33 not 10.1.4.**0**33.
- To switch to the user interface that manages linear storage for the session, when the Sign In page opens, perform the following action:
  - If the v3 version of the Sign In page appears, in the URL, replace `v3` with `v2`.
- Multiple users can be signed in to each controller simultaneously.
- For each active RAIDar 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. Each instance of Internet Explorer can run a separate RAIDar session. However, all instances of Firefox, Chrome, and Safari share the same session.
- End a RAIDar session by clicking the Sign Out link near the top of the RAIDar window. Do not simply close the browser window.

# Tips for using the main window

- The Configuration View panel displays logical and physical components of the storage system. To perform a task, select the component to act on and then either:
  - Right-click to display a context menu and select the task to perform. This is the method that help topics describe.
  - Click a task category in the main panel and select the task to perform.
- The System Status panel shows the system time and how many events of each severity have occurred. To view event details, click a severity icon. For more information see "Viewing the system event log" (page 241).
- Many tables can be sorted by a specific column. To do so, click the column heading to sort low to high. Click again to sort high to low. In tables that allow a task to be performed on multiple items, you can select up to 100 items or clear all selections by toggling the check box in the table's heading row.
- Do not use the browser's Back, Forward, Reload, or Refresh buttons. RAIDar has a single page whose content changes as you perform tasks and automatically updates to show current data.

- A red asterisk (*) identifies a required setting.
- The icon in the upper right corner of the main window shows the status of communication between RAIDar, the Management Controller (MC), and the Storage Controller (SC), as described in the following table.

**Table 19 RAIDar communication status icons (v2)**

| Icon | Meaning |
|---|---|
|  | RAIDar can communicate with the Management Controller, which can communicate with the Storage Controller. |
|  | RAIDar *cannot* communicate with the Management Controller. |
|  | RAIDar can communicate with the Management Controller, which *cannot* communicate with the Storage Controller. |

- Below the communication status icon, a timer shows how long the session can be idle until you are automatically signed out. This timer resets after each action you perform. One minute before automatic sign-out you are prompted to continue using RAIDar.
- If a RAIDar session is active on a controller and the controller is power cycled or is forced offline by the partner controller or certain other events occur, the session might hang. RAIDar might say that it is “Connecting” but stop responding, or the page may become blank with the browser status “Done.” After the controller comes back online, the session will not restart. To continue using RAIDar, close and reopen the browser and start a new RAIDar session.
- Colors that identify how storage space is used are described in “About storage-space color codes” (page 163).
- Icons shown in the Configuration View panel are described in “About Configuration View icons” (page 163).

## Tips for using the help window

- To display help for a component in the Configuration View panel, right-click the component and select Help. To display help for the content in the main panel, click either Help in the menu bar or the help icon in the upper right corner of the panel.
- 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 help window and you can open a new help 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.

# System concepts

## About user accounts

The system provides three default user accounts and allows a maximum of 12 user accounts to be configured. Any account can be modified or removed except you cannot remove the user you are signed in as.

The default user accounts are for general users that can access the SMC (WBI), CLI, FTP, or SMI-S interfaces. You can also create SNMPv3 user accounts that can access the Management Information Base (MIB) or receive trap notifications. SNMPv3 user accounts support SNMPv3 security features such as authentication and encryption. For information about configuring trap notifications, see "Configuring SNMP notification" (page 178). For information about the MIB, see "SNMP reference" (page 289).

General user accounts have these options:

- User Name.
- Password.
- User Roles. Either: Monitor, which lets the user view system settings; or Manage, which lets the user view and change system settings.
- User Type. Identifies the user's experience level: Standard, Advanced, or Diagnostic. This option is informational only and does not affect access to the commands.
- WBI Access. Allows access to the SMC.
- CLI Access. Allows access to the command-line management interface.
- FTP Access. Allows access to the FTP interface, which can be used instead of the SMC to install firmware updates and download logs.
- SMI-S Access. Allows access to the Storage Management Initiative Specification (SMI-S) interface, used for management of the system through your network.
- Base Preference. The base for entry and display of storage-space sizes. In base 2, sizes are shown as powers of 2, using 1024 as a divisor for each magnitude. In base 10, sizes are shown as powers of 10, using 1000 as a divisor for each magnitude. Operating systems usually show volume size in base 2. Disk drives usually show size in base 10. Memory (RAM and ROM) size is always shown in base 2.
- Precision Preference. The number of decimal places (1–10) for display of storage-space sizes.
- Unit Preference. The unit for display of storage-space sizes: Auto, TB, GB, MB. The Auto option lets the system 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, precision is set to 1, and base is set to 10, the size 0.11709 TB is shown as 117.1 GB.
- Temperature Preference. The scale for display of temperature values: Celsius or Fahrenheit.
- Auto Sign Out (minutes). The amount of time that the user's session can be idle before the user is automatically signed out (2–720 minutes).
- Locale. The user's preferred display language, which overrides the system's default display language. Installed language sets include Arabic, Chinese-Simplified, Chinese-Traditional, Dutch, English, French, German, Italian, Japanese, Korean, Portuguese, Russian, and Spanish.

SNMPv3 user accounts have these options:

- User Name.
- Password.
- SNMP User Type. Either: User Access, which allows the user to view the SNMP MIB; or Trap Target, which allows the user to receive SNMP trap notifications. Trap Target uses the IP address set with the Trap Host Address option.
- Authentication Type. Either: MD5 authentication; SHA (Secure Hash Algorithm) authentication; or no authentication. Authentication uses the password set with the Password option.
- Privacy Type. Either: DES (Data Encryption Standard) encryption; AES (Advanced Encryption Standard) encryption; or no encryption. Encryption uses the password set with the Privacy Password option.

- Privacy Password. The encryption password.
- Trap Host Address. The IP address of the host system that will receive SNMP traps.

**Table 20 Settings for default users (v2)**

| Name | Password | Roles | Type | Interfaces enabled | Base | Prec. | Units | Temp. | Auto Sign Out | Locale |
|---|---|---|---|---|---|---|---|---|---|---|
| monitor | !monitor | Monitor | Standard | WBI, CLI | 10 | 1 | Auto | Celsius | 30 min. | English |
| manage | !manage | Monitor, Manage | | WBI, CLI, FTP, SMI-S | | | | | | |
| ftp | !ftp | Monitor, Manage | | FTP | | | | | | |

**NOTE:** To secure the storage system, set a new password for each default user.

## About vdisks

A *vdisk* is a virtual disk that is composed of one or more disks, and has the combined capacity of those disks. The number of disks that a vdisk can contain is determined by its RAID level. All disks in a vdisk must be the same type (SAS SSD), enterprise SAS, or midline SAS). A maximum of 64 vdisks per system can exist.

A vdisk 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 vdisk, regardless of RAID level. For example, the capacity of a vdisk composed of one 500-GB disk and one 750-GB disk is equivalent to a vdisk composed of two 500-GB disks. To maximize capacity, use disks of similar size. For greatest reliability, use disks of the same size and rotational speed.

Each disk has metadata that identifies whether the disk is a member of a vdisk, and identifies other members of that vdisk. This enables disks to be moved to different slots in a system; an entire vdisk to be moved to a different system; and a vdisk to be quarantined if disks are detected missing.

### 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 or vdisk 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 a 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 vdisk contains 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).

△ **CAUTION:** The emulation for 512e disks supports backward-compatibility for many applications and legacy operating systems that do not support 4K native disks. However, older versions of application software, such as virtualization software that resides between the operating system and your storage firmware, may not fully support 512e disk emulation. If not, performance degradation might result. Ensure that you have upgraded to the most recent version of any software that might be affected, and see its documentation for further information.

In a single-controller system, all vdisks are owned by that controller. In a dual-controller system, when a vdisk is created the system automatically assigns the owner to balance the number of vdisks each controller owns; or, you can select the owner. Typically it does not matter which controller owns a vdisk.

In a dual-controller system, when a controller fails, the partner controller assumes temporary ownership of the failed controller's vdisks and resources. If a fault-tolerant cabling configuration is used to connect the controllers to drive enclosures and hosts, both controllers' LUNs are accessible through the partner.

### Chunk size

When you create a vdisk you can use the default chunk size or one that better suits your application. The chunk size is the amount of contiguous data that is written to a disk before moving to the next disk. After a vdisk is created its chunk size cannot be changed. For example, if the host is writing data in 16-KB transfers, that size would be a good choice for random transfers because one host read would generate the read of exactly one disk in the volume. That means if the requests are random-like, then the requests would be spread evenly over all of the disks, which is good for performance. If you have 16-KB accesses from the host and a 64-KB chunk size, then some of the hosts accesses would hit the same disk. Each chunk contains four possible 16-KB groups of data that the host might want to read, which is not an optimal solution. Alternatively, if the host accesses were 128 KB, then each host read would have to access two disks in the vdisk. For random patterns, that ties up twice as many disks.

### Volumes

When you create a vdisk you can also create volumes within it. A volume is a logical subdivision of a vdisk, and can be mapped to controller host ports for access by hosts. The storage system presents only volumes, not vdisks, to hosts.

You can create vdisks with or without volumes by using the Provisioning Wizard, or you can create vdisks manually.

**TIP:** Best practices for creating vdisks include:

- To maximize capacity, use disks of similar size.
- For greatest reliability, use disks of the same size and rotational speed.
- For storage configurations using many disks, create a few vdisks each containing many disks instead of many vdisks each containing a few disks.
- To maximize capacity and disk usage (but not performance), you can create vdisks larger than 2 TB and divide them into multiple volumes each having a capacity of 2 TB or less. This increases the usable capacity of storage configurations by reducing the total number of parity disks required when using parity-protected RAID levels. This differs from using a *volume* larger than 2 TB, which requires specific support by the host operating system, I/O adapter, and application.
- For maximum use of a dual-controller system's resources, each controller should own a similar number of vdisks.
- Set the chunk size to match the transfer block size of the host application.

## About spares

A controller automatically reconstructs a fault-tolerant vdisk (RAID 1, 3, 5, 6, 10, 50) when one or more of its disks fails and a compatible spare disk is available. A compatible disk has enough capacity to replace the failed disk and is the same type (SAS SSD, enterprise SAS, or midline SAS).

There are three types of spares:

- *Dedicated spare*. Reserved for use by a specific vdisk to replace a failed disk. Most secure way to provide spares for vdisks but expensive to reserve a spare for each vdisk.
- *Global spare*. Reserved for use by any fault-tolerant vdisk to replace a failed disk.
- *Dynamic spare*. An available compatible disk that is automatically assigned to replace a failed disk in a fault-tolerant vdisk.

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.

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

### Sparing rules for heterogeneous vdisks

If you upgraded from an earlier release that did not distinguish between enterprise and midline SAS disks, you might have vdisks that contain both types of disks. These are called heterogeneous or mixed vdisks. In the Configuration View panel, the vdisk's RAID-level label includes the suffix `-MIXED`.

For heterogeneous vdisks, the system uses the following logic for global sparing and dynamic sparing. If a vdisk has more than one type of disk in it, the system will look for disks of all types contained in the vdisk. In an effort to migrate heterogeneous vdisks to homogeneous vdisks, the disk type that is most prominent (has the highest number of disks) will be preferred. If all the disk types in a vdisk have the same number of disks, the type that has the smallest capacity disk will be used. If both types have the same capacity disks, enterprise SAS will be the preferred type. Dedicated spares are considered part of a vdisk, so they do not use this logic to choose a preferred disk type since using either type will not change the makeup of the vdisk.

The precedence of spares is as follows:

- Dedicated spares of any type.
- Global spares of preferred type.
- Global spares of non-preferred type.
- Dynamic spares of preferred type (if dynamic sparing is enabled).
- Dynamic spares of non-preferred type (if dynamic sparing is enabled).

## About volumes

A *volume* is a logical subdivision of a vdisk, and can be mapped to controller host ports for access by hosts. A mapped volume provides the storage for a file system partition you create with your operating system or third-party tools. The storage system presents only volumes, not vdisks, to hosts. A maximum of 128 mappable volumes per vdisk can exist.

You can create a vdisk that has one volume or multiple volumes.

- Single-volume vdisks work well in environments that need one large, fault-tolerant storage space for data on one host. A large database accessed by users on a single host that is used only for that application is an example.
- Multiple-volume vdisks work well when you have very large disks and you want to make the most efficient use of disk space for fault tolerance (parity and spares). For example, you could create one 10-TB RAID-5 vdisk and dedicate one spare to the vdisk. This minimizes the amount of disk space allocated to parity and spares compared to the space required if you created five 2-TB RAID-5 vdisks. However, I/O to multiple volumes in the same vdisk can slow system performance.

When you create volumes you can specify their sizes. If the total size of a vdisk's volumes equals the size of the vdisk, you will not have any free space. Without free space, you cannot add or expand volumes. If you need to add or expand a volume in a vdisk without free space, you can delete a volume to create free space. Or, you can expand the vdisk and then either add a volume or expand a volume to use the new free space.

Volume sizes are aligned to 4-MB boundaries. When a volume is created or expanded, if the resulting size would be less than 4 MB it will be increased to 4 MB. If the resulting size would be greater than 4 MB it will be decreased to the nearest 4-MB boundary. The minimum volume size is 4 MB.

You can use a volume's default name or change it to identify the volume's purpose. For example, a volume used to store payroll information can be named Payroll.

You can create vdisks with volumes by using the Provisioning Wizard, or you can create volumes manually.

## About hosts

A *host* identifies an external port that the storage system is attached to. The external port may be a port in an I/O adapter (such as an FC HBA) in a server.

The controllers automatically discover hosts that have sent an `inquiry` command or a `report luns` command to the storage system. Hosts typically do this when they boot up or rescan for devices. When the command from the host occurs, the system saves the host ID. The ID for an FC or SAS host is its WWPN. The ID for an iSCSI host is typically, but not limited to, its IQN. You can also manually create entries for hosts.

You can assign a name to a host to make it easy to recognize for volume mapping. A maximum of 64 names can be assigned.

The Configuration View panel lists hosts by name, or if they are unnamed, by ID.

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 login 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 typically, but not limited to, its IQN. A secret must have 12–16 characters.
- Define CHAP entries in the storage system. If the node name is a host name, then it may be useful to display the hosts that are known to the 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 the CHAP secret(s) in the host iSCSI initiator.
- Establish a new connection to the storage system using CHAP. The host should be able to be displayed 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 login 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.

## About SAS cabling (for AssuredSAN 3004 only)

For systems with a 2-port SAS controller module, host ports can be configured through the WBI or CLI to use fan-out cables or standard cables. A standard cable can connect one port on a SAS host to one controller port, using four PHY lanes per port. A fan-out cable can connect one port on each of two SAS hosts to one controller port, using two PHY lanes per port. Using fan-out cables instead of standard cables doubles the number of hosts that can be attached to a single system. It will also halve the maximum bandwidth available to each host, but overall bandwidth available to all hosts is unchanged. Configuration must be the same for all ports on both controllers, so a mix of standard cables and fan-out cables cannot be used on one system. Use of fan-out cables is enabled by default.

Once you have switched the configuration through the firmware, you can disconnect the existing cables and switch to the other type of cables. For information on how to connect and disconnect cables, refer to your product's Setup Guide.

If you connect a cable that does not match the cable type for the configuration, an event will be logged that indicates a mismatch has occurred. Also, while I/O will occur, half of the PHY lanes for each port will be disabled. The host port properties table accessed through the Rear Graphical tab of the Enclosure Overview panel will reflect that the port is in a degraded state. If a cable mismatch occurs, change the port mode of the system using the Configure Host Interface panel or connect cables of the appropriate type for the configuration.

For more information on checking port properties through the Enclosure Overview panel, see “Viewing information about an enclosure” (page 255).

When configuring the host-interface settings for a 2-port SAS controller module, the current link speed, number of PHY lanes expected for the SAS port, and number of PHY lanes active for each SAS port are displayed. The number of ports that appear depends on the configuration. Changing the host-interface settings interrupts I/O and restarts the storage controllers. For more information on how to configure host ports for use with SAS fan-out cables, see "To change host interface settings for 2-port SAS controller modules (for AssuredSAN 3004 only)" (page 184)

## About volume mapping

Each volume has default host-access settings that are set when the volume is created. These settings are called the *default mapping*. The default mapping applies to any host that has not been explicitly mapped using different settings. *Explicit mappings* for a volume override its default mapping.

Default mapping enables all attached hosts to see a volume using a specified LUN and access permissions set by the administrator. This means that when the volume is first created, all connected hosts can immediately access the volume using the advertised default mapping settings. This behavior is expected by some operating systems, such as Microsoft Windows, which can immediately discover the volume. 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.

You can change a volume's default mapping, 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*. You can apply access privileges to one or more of the host ports on either controller. To maximize performance, map a volume to at least one host port on the controller that owns it. To sustain I/O in the event of controller failure, map to at least one host port on each controller.

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 can only be used once per volume 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.

**TIP:** When an explicit mapping is deleted, the volume's default mapping takes effect. Therefore, it is recommended to use the same LUN for explicit mappings as for the default mapping.

Volume mapping settings are stored in disk metadata. If enough of the disks used by a volume are moved into a different enclosure, the volume's vdisk can be reconstructed and the mapping data is preserved.

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 vdisk 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 volume cache options

You can set options that optimize reads and writes performed for each volume.

### 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. If used incorrectly, you might hinder system performance.

You can change a volume's 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 operation and 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.

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 super-capacitor technology, if the system loses power, data is not lost. For most applications, this is the preferred setting.

If you are doing random access to this volume, leave the write-back cache enabled.

**TIP:** 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

**CAUTION:** 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. Read ahead can be forward (that is, increasing LBAs) or reverse (that is, decreasing LBAs). Increasing the read-ahead cache size can greatly improve performance for multiple sequential read streams. However, increasing read-ahead size will likely decrease random read performance.

- Adaptive. This 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. This is the default.
- Stripe. This option sets the read-ahead size to one stripe. The controllers treat non-RAID and RAID-1 vdisks internally as if they have a stripe size of 512 KB, even though they are not striped.
- Specific size options. These options let you select an amount of data for all accesses.
- Disabled. This 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 managing remote systems

You can add a management object to obtain information from a remote storage system. This allows a local system to track remote systems by their network-port IP addresses and cache their login credentials — the user name and password for a user with the Manage role on that system. The IP address can then be used in commands that need to interact with the remote system.

After a remote system has been added, you can check the connectivity of host ports in the local system to host ports in that remote system. A port in the local system can only link to ports with the same host interface, such as Fibre Channel (FC), in a remote system.

Communication between local and remote systems is an essential part of the remote replication feature.

## About the snapshot feature

Snapshot (AssuredSnap™) is a licensed feature that provides data protection by enabling you to create and save snapshots of a volume. Each snapshot preserves the source volume's data state at the point in time when the snapshot was created. Snapshots can be created manually or by using the task scheduler.

When the first snapshot is taken of a standard volume, the system automatically converts the volume into a *master volume* and reserves additional space for snapshot data. This reserved space, called a *snap pool*, stores pointers to the source volume's data. Each master volume has its own snap pool. 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 snapshot's purpose. Any additional unique data written to a snapshot is also stored in the snap pool.

The following figure shows how the data state of a master volume is preserved in the snap pool by two snapshots taken at different points in time. The dotted line used for the snapshot borders indicates that snapshots are logical volumes, not physical volumes as are master volumes and snap pools.

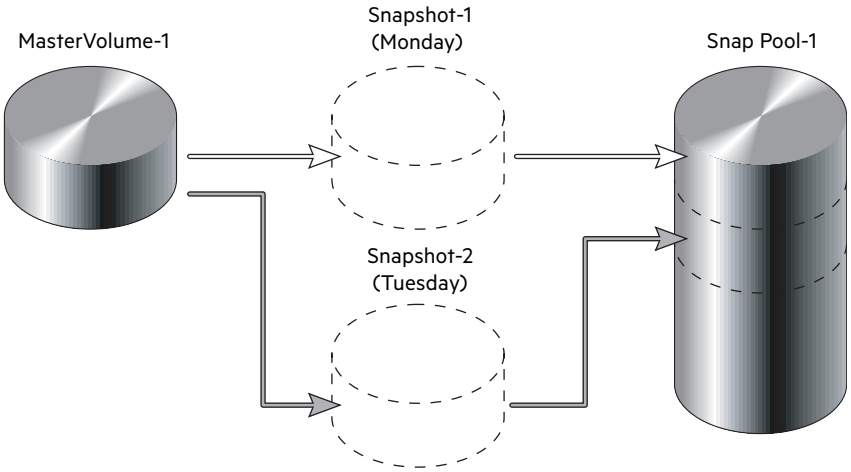



**Figure 3 Relationship between a master volume and its snapshots and snap pool**

The snapshot feature uses the single copy-on-write method to capture only data that has changed. That is, if a block is to be overwritten on the master volume, and a snapshot depends on the existing data in the block being overwritten, the data is copied from the master volume to the snap pool before the data is changed. All snapshots that depend on the older data are able to access it from the same location in the snap pool. This reduces the impact of snapshots when writing to a master volume. In addition, only a single copy-on-write operation is performed on the master volume.

The storage system allows a maximum number of snapshots to be retained, as determined by an installed license. For example, if your license allows four snapshots, when the fifth snapshot is taken an error message informs you that you have reached the maximum number of snapshots allowed on your system. Before you can create a new snapshot you must either delete an existing snapshot, or purchase and install a license that increases the maximum number of snapshots.

The snapshot service has two features for reverting data back to original data:

- Deleting only modified data on a snapshot. For snapshots that have been made accessible as read-write, you can delete just the modified (write) data that was written directly to a snapshot. When the modified data is deleted, the snapshot data reverts to the original data that was snapped. This feature is useful for testing an application, for example. You might want to test some code, which writes data to the snapshot. Rather than having to take another snapshot, you can just delete any write data and start again.
- Rolling back the data in a source volume. The rollback feature enables you to revert the data in a source volume to the data that existed when a specified snapshot was created (preserved data). Alternatively, the rollback can include data that has been modified (write data) on the snapshot since the snapshot was taken. For example, you might want to take a snapshot, mount/present/map that snapshot for read/write, and then install new software on that snapshot for test purposes. If the software installation is successful, you can rollback the master volume to the contents of the modified snapshot (preserved data plus the write data).

The following figure shows the difference between rolling back the master volume to the data that existed when a specified snapshot was created (preserved), and rolling back preserved and modified data.

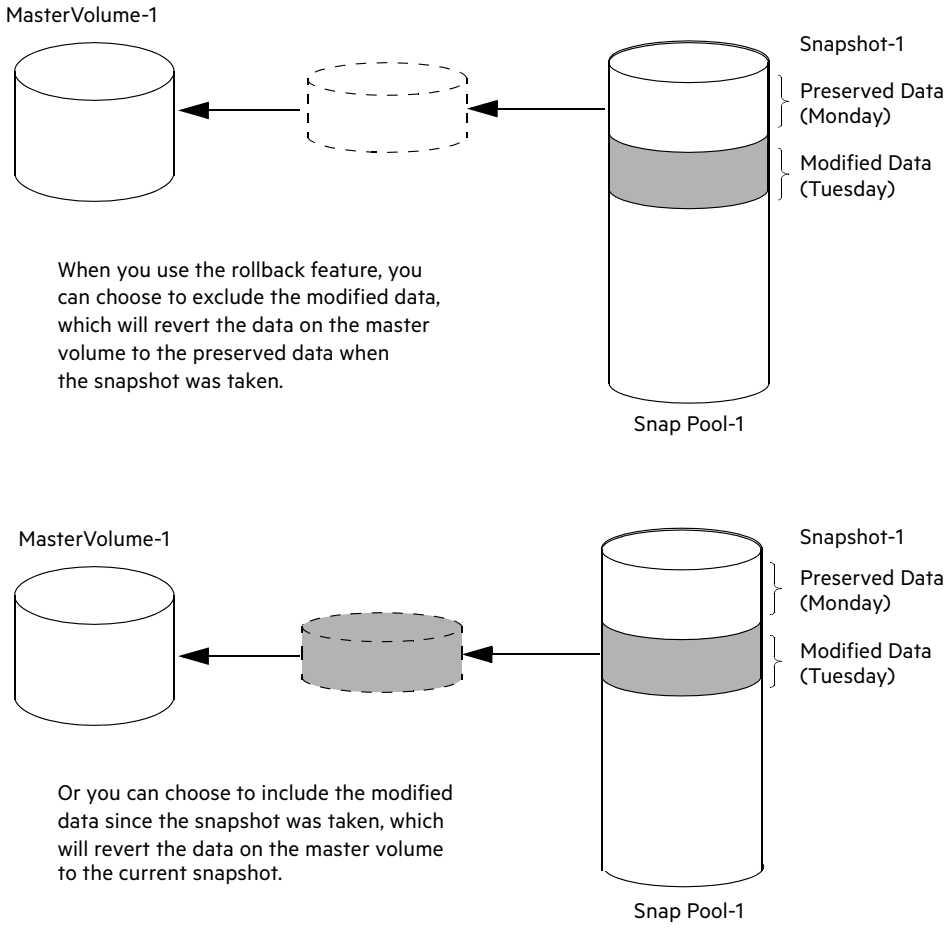



**Figure 4 Rolling back a master volume**

Snapshot operations are I/O-intensive. Every write to a unique location in a master volume after a snapshot is taken will cause an internal read and write operation to occur in order to preserve the snapshot data. If you intend to create snapshots of, create volume copies of, or replicate volumes in a vdisk, ensure that the vdisk contains no more than four master volumes, snap pools, or both. For example: 2 master volumes and 2 snap pools; 3 master volumes and 1 snap pool; 4 master volumes and 0 snap pools.

## About the Volume Copy feature

Volume Copy (AssuredCopy™) is a licensed feature that enables you to copy a volume or a snapshot to a new standard volume.

While a snapshot is a point-in-time logical copy of a volume, the volume copy service creates a complete “physical” copy of a volume within a storage system. It is an exact copy of a source volume as it existed at the time the volume copy operation was initiated, consumes the same amount of space as the source volume, and is independent from an I/O perspective. Volume independence is a key distinction of a volume copy (versus a snapshot, which is a “virtual” copy and dependent on the source volume).

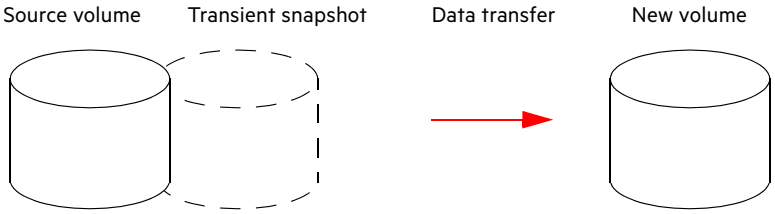
Benefits include:

- Additional data protection. An independent copy of a volume (versus logical copy through snapshot) provides additional data protection against a complete master volume failure. If the source master volume fails, the volume copy can be used to restore the volume to the point in time the volume copy was taken.

- 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 snapshot) 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.

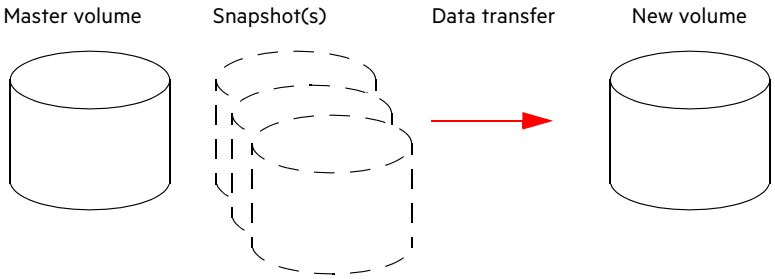
The following figure illustrates how volume copies are created.

**Creating a volume copy from a standard or master volume**




1. Volume copy request is made with a standard volume or a master volume as the source.
2. If the source a standard volume, it is converted to a master volume and a snap pool is created.
3. A new volume is created for the volume copy, and a hidden, transient snapshot is created.
4. Data is transferred from the transient snapshot to the new volume.
5. On completion, the transient volume is deleted and the new volume is a completely independent copy of the master volume, representing the data that was present when the volume copy was started.

**Creating a volume copy from a snapshot**




1. A master volume exists with one or more snapshots associated with it. Snapshots can be in their original state or they can be modified.
2. You can select any snapshot to copy, and you can specify that the modified or unmodified data be copied.
3. On completion, the new volume is a completely independent copy of the snapshot. The snapshot remains, though you can choose to delete it.

**Figure 5 Creating a volume copy from a master volume or a snapshot**

Snapshot operations are I/O-intensive. Every write to a unique location in a master volume after a snapshot is taken will cause an internal read and write operation to occur in order to preserve the snapshot data. If you intend to create snapshots of, create volume copies of, or replicate volumes in a vdisk, ensure that the vdisk contains no more than four master volumes, snap pools, or both. For example: 2 master volumes and 2 snap pools; 3 master volumes and 1 snap pool; 4 master volumes and 0 snap pools.

Guidelines to keep in mind when performing a volume copy include:

- The destination vdisk must be owned by the same controller as the source volume.
- The destination vdisk must have free space that is at least as large as the amount of space allocated to the original volume. A new volume will be created using this free space for the volume copy.
- The destination vdisk does not need to have the same attributes (such as disk type, RAID level) as the volume being copied.

- Once the copy is complete, the new volume will no longer have any ties to the original.
- Volume Copy makes a copy from a snapshot of the source volume. Therefore, the snap pool for the source volume must have sufficient space to store snapshot data when performing this copy.

## About the AssuredRemote replication feature

See "Using AssuredRemote to replicate volumes" (page 267).

## About the VDS and VSS hardware providers

Virtual Disk Service (VDS) enables host-based applications to manage vdisks and volumes. Volume Shadow Copy Service (VSS) enables host-based applications to manage snapshots. A license is required to enable VDS and VSS hardware providers, so hosts can manage vdisks, volumes, and snapshots in the storage system. For more information, see the VDS and VSS hardware provider documentation for your product.

## About the Storage Replication Adapter (SRA)

The SRA is a host-software component installed on a Microsoft Windows Server operating system that allows VMware vCenter Site Recovery Manager software to control certain aspects of the replication feature in storage systems. The presence of the SRA allows the disaster recovery software to automatically coordinate virtual-machine failover and failback between a protected data center and a disaster recovery site. A license is required to enable the SRA.

## About RAID levels

The RAID controllers enable you to set up and manage vdisks, the storage for which may be spread across multiple disks. This is accomplished through firmware resident in the RAID controller. RAID refers to vdisks 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 vdisk fails.

Hosts see each partition of a vdisk, known as a volume, as a single disk. A volume is actually a portion of the storage space on disks behind a RAID controller. The RAID controller firmware makes each volume appear as one very large disk. Depending on the RAID level used for a vdisk, the disk presented to hosts has advantages in fault-tolerance, cost, performance, or a combination of these.

**TIP:** 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

**NOTE:** To create an NRAID, RAID-0, or RAID-3 vdisk, you must use the CLI `create vdisk` command. For more information on this command, see the CLI Reference Guide.

**Table 21 Example applications and RAID levels (v2)**

| 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 |

**Table 21 Example applications and RAID levels (v2)**

| Application | RAID level |
|---|---|
| Very large databases, web server, video on demand | 50 |
| Mission-critical environments that demand high availability and use large sequential workloads | 6 |

**Table 22 RAID level comparison (v2)**

| 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 performance; protects against single disk failure | High redundancy cost overhead: because all data is duplicated, twice 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 sub-vdisks | 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-vdisks | 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 |

**Table 23 Vdisk expansion by RAID level (v2)**

| RAID level | Expansion capability | Maximum disks |
|---|---|---|
| NRAID | Cannot expand. | 1 |
| 0, 3, 5, 6 | You can add 1–4 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-vdisk at a time. The added sub-vdisk must contain the same number of disks as each of the existing sub-vdisks. | 32 |

## About size representations

Parameters such as names of users and volumes have a maximum length in bytes. When encoded in UTF-8, a single character can occupy multiple bytes. Standard US-ASCII characters require 1 byte; most Latin (Western European), Cyrillic, and Arabic characters are encoded with 2 bytes; most Asian characters are 3 bytes.

Operating systems usually show volume size in base 2. Disk drives usually show size in base 10. Memory (RAM and ROM) size is always shown in base 2. In RAIDar, the base for entry and display of storage-space sizes can be set per user or per session. When entering storage-space sizes only, either base-2 or base-10 units can be specified.

**Table 24 Size representations in base 2 and base 10 (v2)**

| Base 2 | | Base 10 | |
|---|---|---|---|
| **Unit** | **Size in bytes** | **Unit** | **Size in bytes** |
| KiB (kibibyte) | 1,024 | KB (kilobyte) | 1,000 |
| MiB (mebibyte) | $1{,}024^2$ | MB (megabyte) | $1{,}000^2$ |
| GiB (gibibyte) | $1{,}024^3$ | GB (gigabyte) | $1{,}000^3$ |
| TiB (tebibyte) | $1{,}024^4$ | TB (terabyte) | $1{,}000^4$ |
| PiB (pebibyte) | $1{,}024^5$ | PB (petabyte) | $1{,}000^5$ |
| EiB (exbibyte) | $1{,}024^6$ | EB (exabyte) | $1{,}000^6$ |

The locale setting determines the character used for the decimal (radix) point, as shown below.

**Table 25 Decimal (radix) point character by locale (v2)**

| Language | Character | Examples |
|---|---|---|
| Arabic, English, Chinese, Japanese, Korean, Russian | Period (.) | 146.81 GB<br>3.0 Gbit/s |
| Dutch, French, German, Italian, Portuguese, Spanish | Comma (,) | 146,81 GB<br>3,0 Gbit/s |

## About the system date and time

You can change the storage system's date and time, which are displayed in the System Status panel. It is important to set the date and time so that entries in system logs and event-notification email messages have correct time stamps.

You can set the date and time manually or configure the system to use Network Time Protocol (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 Coordinated Universal Time (UTC), which provides several options:

- If you want to synchronize the times and logs between storage devices installed in multiple time zones, set all the storage devices to use UTC.
- If you want 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, such as for U.S. daylight savings time. You must make such adjustments manually.

## About storage-space color codes

RAIDar panels use the following color codes to identify how storage space is used.

**Table 26 Storage-space color codes (v2)**

| Area | Color | Meaning |
|---|---|---|
| Overview panels | | Total space |
| | | Available/free space |
| | | Used space |
| | | Reserved/overhead space, used for parity and snap pools, for example |
| Vdisk panels | | Space used by spares |
| | | Wasted space, due to use of mixed disk sizes |

## About Configuration View icons

The Configuration View panel uses the following icons to let you view physical and logical components of the storage system.

**Table 27 Configuration View icons (v2)**

| Icon | Meaning | Icon | Meaning |
|---|---|---|---|
|  | Show all subcomponents |  | Snapshot |
|  | Hide all subcomponents |  | Snap pool |
|  | Show the component's subcomponents |  | Replication-prepared volume |
|  | Hide the component's subcomponents |  | Local primary volume |
|  | Storage system |  | Local secondary volume |
|  | Enclosure |  | Local replication image |
|  | Host/initiator |  | Remote primary volume |
|  | Vdisk |  | Remote secondary volume |
|  | Standard or master volume |  | Remote replication image |

## About disk failure and vdisk reconstruction

Vdisk reconstruction does not require I/O to be stopped, so the vdisk can continue to be used while the Reconstruct utility runs. Vdisk reconstruction starts automatically when all of the following are true:

- One or more disks fail in a fault-tolerant vdisk (RAID 1, 3, 5, 6, 10, or 50)
- The vdisk is still operational
- Compatible spares are available

The storage system automatically uses the spares to reconstruct the vdisk. A compatible spare has a capacity equal to or greater than the smallest disk in the vdisk, has enough capacity to replace a failed disk, and is the same type (SAS SSD, enterprise SAS, or midline SAS) as those disks. If no compatible spares are available, reconstruction does not start automatically. To start reconstruction manually, replace each failed disk and then do one of the following:

- Add each new disk as either a dedicated spare or a global spare. Remember that a global spare might be taken by a different critical vdisk than the one you intended. When a global spare replaces a disk in a vdisk, the global spare's icon in the enclosure view changes to match the other disks in that vdisk.
- Enable the Dynamic Spare Capability option to use the new disks without designating them as spares.
- Change a dedicated spare from a different vdisk to either a global spare or a dedicated spare for the degraded vdisk.

RAID-6 reconstruction behaves as follows:

- During online initialization, if one disk fails, initialization continues and the resulting vdisk will be degraded (FTDN status). After initialization completes, the system can use a compatible spare to reconstruct the vdisk.
- During online initialization, if two disks fail, initialization stops (CRIT status). The system can use two compatible spares to reconstruct the vdisk.
- During vdisk operation, if one disk fails and a compatible spare is available, the system begins to use that spare to reconstruct the vdisk. If a second disk fails during reconstruction, reconstruction continues until it is complete, regardless of whether a second spare is available. If the spare fails during reconstruction, reconstruction stops.
- During vdisk operation, if two disks fail and only one compatible spare is available, the system waits five minutes for a second spare to become available. After five minutes, the system begins to use that spare to reconstruct one disk in the vdisk (referred to as "fail 2, fix 1" mode). If the spare fails during reconstruction, reconstruction stops.
- During vdisk operation, if two disks fail and two compatible spares are available, the system uses both spares to reconstruct the vdisk. If one of the spares fails during reconstruction, reconstruction proceeds in "fail 2, fix 1" mode. If the second spare fails during reconstruction, reconstruction stops.

When a disk fails, its fault LED is illuminated. When a spare is used as a reconstruction target, its activity LED is illuminated. During reconstruction, the fault LED and activity LEDs for all disks in the vdisk blink. For details about LED states, see your product's Setup Guide.

---

**NOTE:** Reconstruction can take hours or days to complete, depending on the vdisk RAID level and size, disk speed, utility priority, and other processes running on the storage system. You can stop reconstruction only by deleting the vdisk.

---

## About data protection in a single-controller storage system

The storage system can operate with a single controller module. Because single-controller mode is not a redundant configuration, this section presents some considerations concerning data protection.

A volume's default caching mode is write back, as opposed to write through. In write-back mode, data is held in controller cache until it is written to disk. In write-through mode, data is written directly 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 target volume's enclosure is powered off without a proper shut down. Data remains in the controller's cache and associated volumes will be missing that data. This can result in data loss or in some cases volume loss.

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

To avoid the possibility of data loss in case the controller fails you can change a volume's caching mode 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 details about caching modes see "About volume cache options" (page 155). To change a volume's caching mode, see "Changing a volume's cache settings" (page 198).

## 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 before any data is lost. The transfer does not remove any data from the logs in the storage system. This feature is disabled by default.

The *log-collection system* is a host computer that is designated to receive the log data transferred from the storage system. Because log data is transferred incrementally, the log-collection system is responsible for integrating the log data for display and analysis.

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/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, SNMP, or SMI-S to the log-collection system, which can then use FTP 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 (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 RAIDar's Save Logs panel or the FTP interface's `get logs` command. 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 panel, see "Saving logs" (page 225). For information about using the FTP interface, see "Using FTP" (page 302).

## About performance monitoring

The storage system samples disk-performance statistics every quarter hour and retains performance data for 6 months. You can view these historical performance statistics to identify disks that are experiencing errors or are performing poorly.

RAIDar displays historical performance statistics in graphs for ease of analysis. You can view historical performance statistics either for a single disk or for all disks in a vdisk. By default, the graphs will show the latest 50 data samples, but you can specify the time period to display. If the specified time period includes more than 50 samples, their data will be aggregated into 50 samples. The graphs show a maximum of 50 samples. Data shown will be up-to-date as of the time it is requested for display, and summary statistics will be updated when a new sample is taken.

Disk-performance graphs include:

- Data Transferred
- Data Throughput
- I/O
- IOPS
- Average Response Time
- Average I/O Size
- Disk Error Counters
- Average Queue Depth

Vdisk-performance graphs include:

- Data Transferred
- Data Throughput
- Average Response Time

You can save historical statistics in CSV format to a file for import into a spreadsheet or other third-party application. You can also reset historical statistics, which clears the retained data and continues to gather new samples.

**NOTE:** RAIDar does not show live statistics. For information about viewing live statistics, see the CLI Reference Guide.

## About firmware update

Controller modules, expansion modules, drawers, 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. The controller-module firmware-update algorithm supports the following scenarios for a dual-controller system:

- 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.

When you update controller firmware, the Partner Firmware Update (PFU) option, which is enabled by default, ensures 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. After, 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 newer firmware version in either controller is transferred to the other controller.

For information about the procedures to update firmware in controller modules, expansion modules, drawers, and disk drives, see “Updating firmware” (page 221). That topic also describes how to use the activity progress interface to view detailed information about the progress of a firmware-update operation.

## About Full Disk Encryption (for AssuredSAN 4004 only)

Full Disk Encryption (FDE) is a method by which you can secure the data residing on the drives. 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 without needing the correct passphrase. Repurposing erases all data and unsecures the system and disks.

FDE operates on a per-system basis, not a per-vdisk basis. To use FDE, all disks in the system must be FDE-capable.

For information about the procedures to change FDE settings, see “Changing FDE settings (for AssuredSAN 4004 only)” (page 188).

# 12 Configuring the system

## Using the Configuration Wizard

The Configuration Wizard helps you initially configure the system or change system configuration settings.

The wizard guides you through the following steps. For each step you can view help by clicking the help icon in the wizard panel. As you complete steps they are highlighted at the bottom of the panel. If you cancel the wizard at any point, no changes are made.

- Change passwords for the default users, providing they still exist
- Configure each controller's network port
- Enable or disable system-management services
- Enter information to identify the system
- Configure event notification
- Configure controller host ports
- Confirm changes and apply them

When you complete this wizard you are given the option to start the Provisioning Wizard to provision storage.

### Starting the wizard

1. In the Configuration View panel, right-click the system and select either **Configuration > Configuration Wizard** or **Wizards > Configuration Wizard**. The wizard panel appears.
2. Click **Next** to continue.

### Changing default passwords

The system provides the default users `manage` and `monitor`.

1. To secure the storage system, set a new password for each default user. 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, and one non-alphabetic character. A password can include printable UTF-8 characters except for the following: a space or ' " , < > \
2. Click **Next** to continue.

### Configuring network ports

You can configure addressing parameters for each controller's network port. You can set static IP values or use DHCP.

In DHCP mode, network port IP address, subnet mask, and gateway values are obtained from a DHCP server if one 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.

Each controller has the following factory-default IP settings:

- 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 is able to 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: 0.0.0.0

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. This 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.

△ **CAUTION:** Changing IP settings can cause management hosts to lose access to the storage system.

### To use DHCP to obtain IP values for network ports

1. Set the IP address source to **DHCP**.
2. Click **Next** to continue.

### To set static IP values for network ports

1. Determine the IP address, subnet mask, and gateway values to use for each controller.
2. Set the IP address source to **manual**.
3. Set the values for each controller. You must set a unique IP address for each network port.

   **NOTE:** The following IP addresses are reserved for internal use by the storage system: 192.168.200.253, 192.168.200.254, 172.22.255.253, 172.22.255.254, and 127.0.0.1

4. Click **Next** to continue.

## Enabling system-management services

You can enable or disable management interfaces to limit the ways in which users and host-based management applications can access the storage system. Network management interfaces operate out-of-band and do not affect host I/O to the system. The network options are:

- Web Browser Interface (WBI). The primary interface for managing the system.
  - You can enable use of HTTPS, HTTP (if lesser security is acceptable), or both. Also, if you choose to disable RAIDar, the change does not take effect until the Configuration Wizard has finished and you have logged in again. If you disable both, you will lose access to this interface.
  - Default Management Mode. The default version of the RAIDar interface that is launched when you point your browser to the address of a controller module network port. Select **v2** for the legacy interface to manage linear storage, or **v3** for the new interface to manage linear and virtual storage.
- Command Line Interface (CLI). An advanced user interface for managing the system. You can enable use of SSH (secure shell) for increased security, Telnet, or both.
- Storage Management Initiative Specification (SMI-S). Used for management of the system through your network. You can enable use of unencrypted or encrypted SMI-S:
  - **Enable**. Selecting this option allows SMI-S clients to communicate with each controller's embedded SMI-S provider via HTTP port 5988. HTTP port 5988 and HTTPS port 5989 cannot be enabled at the same time, so enabling this option will disable port 5989.
  - **Encrypted**. Additionally selecting this option allows SMI-S clients to communicate with each controller's embedded SMI-S provider via HTTPS port 5989. HTTPS port 5989 and HTTP port 5988 cannot be enabled at the same time, so enabling this option will disable port 5988.

- Storage Management Initiative Specification (SMI-S). Used for management of the system through your network. You can enable use of secure (encrypted) or unsecure (unencrypted) SMI-S:
  - Encrypted. This option allows SMI-S clients to communicate with each controller's embedded SMI-S provider via HTTPS port 5989. HTTPS port 5989 and HTTP port 5988 cannot be enabled at the same time, so enabling this option will disable port 5988. This is the default.
  - Unencrypted. This option allows SMI-S clients to communicate with each controller's embedded SMI-S provider via HTTP port 5988. HTTP port 5988 and HTTPS port 5989 cannot be enabled at the same time, so enabling this option will disable port 5989.

  The Storage Management Initiative Specification (SMI-S) is a Storage Networking Industry Association (SNIA) standard that enables interoperable management for storage networks and storage devices. 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.
- File Transfer Protocol (FTP). A secondary interface for installing firmware updates, downloading logs, and installing a license.
- Simple Network Management Protocol (SNMP). Used for 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.
- Activity Progress Reporting. Provides access to the activity progress interface via 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. In addition, when the update operation completes, status is presented indicating either the successful completion, or an error indication if the operation failed.

In-band management interfaces operate through the data path and can slightly reduce I/O performance. The in-band option is:

- In-band SES Capability. Used for in-band monitoring of system status based on SCSI Enclosure Services (SES) data.

If a service is disabled, it cannot be accessed. To allow specific users to access RAIDar, CLI, FTP or SMI-S, see "About user accounts" (page 149).

### To change management interface settings

1. Enable the options that you want to use to manage the storage system, and disable the others. If desired, choose a different default version of RAIDar by selecting a different option.
2. Click **Next** to continue.

## Setting system information

Set the System Name, System Contact person, System Location, and System Information (description) values. Each value can include a maximum of 79 bytes and use any characters except the following: " < > \

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.

Click **Next** to continue.

## Configuring event notification

Configure email addresses and SNMP trap hosts to receive event notifications, and configure the managed logs feature.

1. In the Event Notifications section, set the options:
   - Notification Level. Select the minimum severity for which the system should send notifications: **Critical** (only); **Error** (and Critical); **Warning** (and Error and Critical); **Informational** (all); or **none (Disabled)**.
   - SMTP Server address. The IP address of the SMTP mail server to use for the email messages. If the mail server is not on the local network, make sure that the gateway IP address was set in the network configuration step.
   - Sender Name. The sender name that is joined with an `@` symbol to the domain name to form the “from” address for 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. For example: `Storage-1`. If no sender name is set, a default name is created.
   - Sender Domain. The domain name that is joined with an `@` symbol to the sender name to form the “from” address for 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. For example: `MyDomain.com`. If the domain name is not valid, some email servers will not process the mail.
   - Email Address fields. Up to three email addresses that the system should send notifications to. Email addresses 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`.
2. In the SNMP Configuration section, set the options:
   - Notification Level. Select the minimum severity for which the system should send notifications: **Critical** (only); **Error** (and Critical); **Warning** (and Error and Critical); **Informational** (all); or **none (Disabled)**, which disables SNMP notification. However, Critical events and managed-logs events are sent regardless of the notification setting.
   - Read Community. The SNMP read password for your network. This password is also included in traps that are sent. The value is case sensitive and can have a maximum of 31 bytes. It can include any character except the following: " < >
   - Write Community. The SNMP write password for your network. The value is case sensitive and can have a maximum of 31 bytes. It can include any character except the following: " < >
   - Trap Host Address fields. IP addresses of up to three host systems that are configured to receive SNMP traps.
3. In the Managed Logs Notifications section, set the options:
   - Log Destination. The email address of the log-collection system. The email addresses must use the format *`user-name@domain-name`* and can have a maximum of 320 bytes. For example: `LogCollector@MyDomain.com`.
   - **Include Logs**. When the managed logs feature is enabled, this option activates “push” mode, which automatically attaches system log files to managed-logs email notifications that are sent to the log-collection system.

   **NOTE:** These options configure the managed logs feature but do not enable it, which is done on the Configuration > Advanced Settings > System Utilities panel.
4. Click **Next** to continue.

## Configuring host ports

To enable the system to communicate with hosts or with remote systems having FC or iSCSI interfaces, you can configure the system's host-interface options. If the current settings are correct, port configuration is optional.

**For AssuredSAN 4004**: Host ports can be configured as a combination of FC or iSCSI ports. For a 4-port SAS controller module, there are no host-interface options.

**For AssuredSAN 3004**: Host ports can only be configured as either FC or iSCSI ports. For a 2-port SAS controller module, host ports can be configured to use fan-out cables or standard cables through the Configure Host Interfaces panel. See "Changing host interface settings" (page 182) for more information.

**NOTE:** For information about setting advanced host-port parameters, such as FC port topology, see the CLI Reference Guide.

### To change FC host interface settings

1. Set the Speed option to the proper value to communicate with the host. The speed can be set to **auto**, which auto-negotiates the proper link speed with the host, or to **4Gb**, **8Gb**, or **16Gb** (Gbit/s). 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.
2. The FC Connection Mode can be 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. Click **Next** to continue.

### To change iSCSI host interface settings

1. In the upper section of the panel, set the port-specific options:
   - 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.
   - Link-Local Address. For IPv6, the link-local address that is automatically generated from the MAC address and assigned to the port.

△ **CAUTION:** Changing IP settings can cause data hosts to lose access to the storage system.

2. In the Common Settings for iSCSI section of the panel, set the options that apply to all iSCSI ports:
   - Authentication (CHAP). Enables or disables use of Challenge Handshake Authentication Protocol.

     **NOTE:** CHAP records for iSCSI login authentication must be defined if CHAP is enabled. To create CHAP records, see "Configuring CHAP" (page 218).

   - Jumbo Frames. Enables or disables support for jumbo frames. Allowing for 100 bytes of overhead, a normal frame can contain 1400 bytes whereas a jumbo frame can contain a maximum of 8900 bytes 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.
   - 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.
3. Click **Next** to continue.

### Confirming configuration changes

Confirm that the values listed in the wizard panel are correct.

- If they are not correct, click **Previous** to return to previous steps and make necessary changes.
- If they are correct, click **Finish** to apply the setting changes and finish the wizard.

## Installing a license

A license is required to use Snapshots, Volume Copy, Replication, VDS, VSS, and the Storage Replication Adapter (SRA). The license is specific to a controller enclosure serial number and firmware version.

If a permanent license is not installed and you want to try these features before buying a permanent license, you can create a one-time temporary license. A temporary license will expire 60 days from the time it is created. After creating a temporary license, each time you sign in to RAIDar, a message specifies the number of remaining days for the temporary license. If you do not install a permanent license before the temporary license expires, you cannot create new items with these features. However, you can continue to use existing snapshots.

After a temporary license is created or a permanent license is installed, the option to create a temporary license is no longer displayed.

#### To view information about system licenses

In the Configuration View panel, right-click the system and select **Tools > Install License**.

The System Licenses table shows the following information about licensed features:

- Feature. The name of the licensed feature.
- Base. Either:
  - The number of components that users can create without a license.
  - `N/A`. Not applicable.
- License. Either:
  - The number of user-created components that the installed license supports.
  - `Enabled` or `Disabled`.

- In Use. Either:
  - The number of user-created components that exist.
  - `N/A`. Not applicable.
- Max Licensable. Either:
  - The number of user-created components that the maximum license supports.
  - `N/A`. Not applicable.
- Expiration. One of the following:
  - `Never`. License is purchased and doesn't expire.
  - Number of days remaining for a temporary license.
  - `Expired`. Temporary license has expired and cannot be renewed.
  - `Expired/Renewable`. Temporary license has expired and can be renewed.
  - `N/A`. No license installed.

The panel also shows the licensing serial number (controller enclosure serial number) and licensing version number (controller firmware version), for which a license file must be generated in order to successfully install.

### To create a temporary license

1. In the Configuration View panel, right-click the system and select **Tools > Install License**. If the option to create a temporary license is available, the End User License Agreement appears in the lower portion of the license panel.
2. Read the license agreement.
3. If you accept the terms of the license agreement, select the check box. A confirmation dialog appears.
4. Click **Yes** to start the trial period. The feature's Expiration value shows the number of days remaining in the trial period. The trial period will expire on the last day. When the trial period expires, the value changes to Expired or Expired/Renewable.

### To install a permanent license

1. Ensure that:
   - The license file is saved to a network location that you can access from RAIDar.
   - You are signed into the controller enclosure that the file was generated for.
2. In the Configuration View panel, right-click the system and select **Tools > Install License**.
3. Click **Browse** to locate and select the license file.
4. Click **Install License File**. If installation succeeds, the System Licenses table is updated. The licensing change takes effect immediately. The feature's Expiration value shows `Never` for permanent licenses, and displays the number of days remaining for temporary licenses

# Configuring system services

## Changing management interface settings

You can enable or disable management interfaces to limit the ways in which users and host-based management applications can access the storage system. Network management interfaces operate out-of-band and do not affect host I/O to the system. The network options are:

- Web Browser Interface (WBI). The primary interface for managing the system.
  - You can enable use of HTTP, HTTPS for increased security, or of both. If you disable both, you will lose access to this interface.
  - Default Management Mode. The default version of RAIDar that opens when you access it. Select v2 for the interface that manages legacy linear storage, or v3 for the new interface that manages virtual storage.
- Command Line Interface (CLI). An advanced user interface for managing the system. You can enable use of SSH (secure shell) for increased security, Telnet, or both.
- Storage Management Initiative Specification (SMI-S). Used for management of the system through your network. You can enable use of unencrypted or encrypted SMI-S:
  - Enable. Selecting this option allows SMI-S clients to communicate with each controller's embedded SMI-S provider via HTTP port 5988. HTTP port 5988 and HTTPS port 5989 cannot be enabled at the same time, so enabling this option will disable port 5989.
  - Encrypted. Additionally selecting this option allows SMI-S clients to communicate with each controller's embedded SMI-S provider via HTTPS port 5989. HTTPS port 5989 and HTTP port 5988 cannot be enabled at the same time, so enabling this option will disable port 5988.
- Storage Management Initiative Specification (SMI-S). Used for management of the system through your network. You can enable use of secure (encrypted) or unsecure (unencrypted) SMI-S:
  - Encrypted. This option allows SMI-S clients to communicate with each controller's embedded SMI-S provider via HTTPS port 5989. HTTPS port 5989 and HTTP port 5988 cannot be enabled at the same time, so enabling this option will disable port 5988. This is the default.
  - Unencrypted. This option allows SMI-S clients to communicate with each controller's embedded SMI-S provider via HTTP port 5988. HTTP port 5988 and HTTPS port 5989 cannot be enabled at the same time, so enabling this option will disable port 5989.
- File Transfer Protocol (FTP). A secondary interface for installing firmware updates, downloading logs, and installing a license.
- 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.
- Activity Progress Reporting. Provides access to the activity progress interface via 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. In addition, when the update operation completes, status is presented indicating either the successful completion, or an error indication if the operation failed.

In-band management interfaces operate through the data path and can slightly reduce I/O performance. The in-band option is:

- In-band SES Capability. Used for in-band monitoring of system status based on SCSI Enclosure Services (SES) data.

If a service is disabled, it cannot be accessed. To allow specific users to access RAIDar, CLI, FTP, or SMI-S, see "About user accounts" (page 149).

### To change management interface settings

1. In the Configuration View panel, right-click the system and select **Configuration > Services > Management**.
2. Enable the options that you want to use to manage the storage system, and disable the others.
3. Click **Apply**. If you disabled any options or changed your default management mode setting, a confirmation dialog appears.
4. Click **Yes** to continue. Otherwise, click **No**. If you clicked **Yes**, a processing dialog appears. When processing is complete a success dialog appears.
5. Click **OK**.

## Configuring email notification

You can configure email-notification settings for events and managed logs. For an overview of the managed logs feature, see “About managed logs” (page 165).

### To configure email notification for events

1. In the Configuration View panel, right-click the system and select **Configuration > Services > Email Notification**.
2. In the main panel, set the options:
   - Notification Level. Select the minimum severity for which the system should send notifications: **Critical** (only); **Error** (and Critical); **Warning** (and Error and Critical); **Informational** (all); or **none (Disabled)**. The default is **none**, which disables email notification.
   - SMTP Server address. The IP address of the SMTP mail server to use for the email messages. If the mail server is not on the local network, make sure that the gateway IP address is set in **System Settings > Network Interfaces**.
   - Sender Name. The sender name that is joined with an `@` symbol to the domain name to form the “from” address for 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. The name cannot include a space or: " , < > \\

     For example: `Storage-1`. If no sender name is set, a default name is created.
   - Sender Domain. The domain name that is joined with an `@` symbol to the sender name to form the “from” address for 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. For example: `MyDomain.com`. If the domain name is not valid, some email servers will not process the mail.
   - Email Address fields. Up to three email addresses that the system should send notifications to. Email addresses 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`.
3. Click **Apply**.
4. Send a test message to the configured destinations as described on page 229.

### To configure email notification for managed logs

1. In the Configuration View panel, right-click the system and select **Configuration > Services > Email Notification**.
2. In the main panel, set the options:
   - Log Destination. The email address of the log-collection system. The email addresses must use the format *`user-name@domain-name`* and can have a maximum of 320 bytes. For example: `LogCollector@MyDomain.com`.
   - **Include Logs**. When the managed logs feature is enabled, this option activates “push” mode, which automatically attaches system log files to managed-logs email notifications that are sent to the log-collection system.
3. Click **Apply**.
4. Enable log management as described on page 195.
5. Send a test message to the configured destination as described on page 229.

## Configuring SNMP notification

### To configure SNMP notification of events

1. In the Configuration View panel, right-click the system and select **Configuration > Services > SNMP Notification**.
2. In the main panel, set the options:
   - Notification Level. Select the minimum severity for which the system should send notifications: **Critical** (only); **Error** (and Critical); **Warning** (and Error and Critical); **Informational** (all); or **none (Disabled)**. However, Critical events and managed-logs events are sent regardless of the notification setting.
   - Read Community. The SNMP read password for your network. This password is also included in traps that are sent. The value is case sensitive and can have a maximum of 31 bytes. It can include any character except the following: " < >
     Write Community. The SNMP write password for your network. The value is case sensitive and can have a maximum of 31 bytes. It can include any character except the following: " < >
     Trap Host Address fields. IP addresses of up to three host systems that are configured to receive SNMP traps.
3. Click **Apply**.
4. Optionally, send a test message to the configured destinations as described on page 229.

## Configuring syslog notification

You can set remote syslog notification options to allow events to be logged by the syslog of a specified host computer. Syslog is a protocol for sending event messages across an IP network to a logging server.

### To configure syslog notification of events

1. In the Configuration View panel, right-click the system and select **Configuration > Services > Syslog Notification**.
2. In the main panel, set the options:
   - **Notification Level**. Select the minimum severity for which the system should send notifications: **Critical** (only); **Error** (and Critical); **Warning** (and Error and Critical); **Informational** (all); or **none (Disabled)**, which disables syslog notification.
   - **Syslog Server IP Address**. IP address of the syslog host system.
   - **Syslog Server Port Number**. Port number of the syslog host system.
3. Click **Apply**.
4. Optionally, send a test message to the configured destinations as described in “Testing notifications” (page 229).

# Configuring user accounts

## Adding users

You can create either a general user that can access RAIDar, CLI, FTP or SMI-S interfaces, or an SNMPv3 user that can access the MIB or receive trap notifications. SNMPv3 user accounts support SNMPv3 security features such as authentication and encryption.

### To add a general user

1. In the Configuration View panel, right-click the system and select **Configuration > Users > Add New User**.
2. In the main panel, set the options:
   - 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 must contain 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 " ' , < > \
   - Select **Standard User**.

- User Roles. Select **Monitor** to let the user view system settings, or **Manage** to let the user view and change system settings. You cannot change the roles of user `manage`.
- User Type. Select an option to identify the user's experience level: **Standard**, **Advanced**, or **Diagnostic**. This option is informational only and does not affect access to commands.
- **WBI Access**. Allows access to RAIDar.
- **CLI Access**. Allows access to the command-line management interface.
- **FTP Access**. Allows access to the FTP interface, which can be used instead of RAIDar to install firmware updates and download logs.
- **SMI-S Access**. Allows access to the SMI-S interface, used for management of the system through your network.
- Base Preference. Select the base for entry and display of storage-space sizes, either **Base 10** or **Base 2**. In base 2, sizes are shown as powers of 2, using 1024 as a divisor for each magnitude. In base 10, sizes are shown as powers of 10, using 1000 as a divisor for each magnitude. Operating systems usually show volume size in base 2. Disk drives usually show size in base 10. Memory (RAM and ROM) size is always shown in base 2.

- Precision Preference. Select the number of decimal places (1–10) for display of storage-space sizes.
- Unit Preference. Select a unit for display of storage-space sizes: **Auto**, **TB**, **GB**, **MB**. The Auto option lets the system 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, precision is set to 1, and base is set to 10, the size 0.11709 TB is shown as 117.1 GB.
- Temperature Preference. Specifies the scale to use for temperature values: **Celsius** or **Fahrenheit**.
- Auto Sign Out (minutes). Select the amount of time that the user's session can be idle before the user is automatically signed out (2–720 minutes).
- Locale. The user's preferred display language, which overrides the system's default display language. Installed language sets include Arabic, Chinese-Simplified, Chinese-Traditional, Dutch, English, French, German, Italian, Japanese, Korean, Portuguese, Russian, and Spanish.

3. Click **Add User**.

### To add an SNMPv3 user

1. In the Configuration View panel, right-click the system and select **Configuration > Users > Add New User**.
2. In the main panel, set the options:
   - 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 must contain 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 ' " , < > \
     If the Authentication Type option is set to use authentication, this password is the authentication password and must include at least 8 characters.
   - Select **SNMPv3 User**.
   - SNMP User Type. Select User **Access** to enable the user to view the SNMP MIB, or Trap Target to enable the user to receive SNMP trap notifications. If you select **Trap Target** you must set the Trap Host Address option.
   - Authentication Type. Select whether to use **MD5** or **SHA** authentication, or no authentication (**None**). Authentication uses the user password.
   - Privacy Type. Select whether to use **DES** or **AES** encryption, or no encryption (**none**). To use encryption you must also set the Privacy Password and Authentication Type options.

- Privacy Password. If the Privacy Type option is set to use encryption, specify an encryption password. A password is case sensitive; can have a maximum of 32 bytes; and must include at least 8 characters. It cannot include the following: ' " , < > \
- Trap Host Address. If you set the user type to **Trap Target**, specify the IP address of the host system that will receive SNMP traps.

3. Click **Add User**.

## Modifying users

You can change settings either for a general user that can access RAIDar, CLI, FTP, or SMI-S interfaces, or for an SNMPv3 user.

The system requires at least one CLI user with the Manage role to exist.

### To modify a general user

1. In the Configuration View panel, right-click the system and select **Configuration > Users > Modify User**. A table displays details for each user. For each interface a user can access, a check mark appears in the WBI, CLI, SNMP, FTP, and SMI-S columns.
2. In the main panel, select the user to modify.
3. Set the options:
   - Password. A password is case sensitive and must contain 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 ' " , < > \
   - User Roles. Select **Monitor** to let the user view system settings, or **Manage** to let the user view and change system settings.
   - User Type. Select an option to identify the user's experience level: **Standard**, **Advanced**, or **Diagnostic**. This option is informational only and does not affect access to commands.
   - **WBI Access**. Allows access to RAIDar.
   - **CLI Access**. Allows access to the command-line management interface.
   - **FTP Access**. Allows access to the FTP interface, which can be used instead of RAIDar to install firmware updates and download logs.
   - **SMI-S Access**. Allows access to the SMI-S interface, used for management of the system through your network.
   - Base Preference. Select the base for entry and display of storage-space sizes, either **Base 10** or **Base 2**. In base 2, sizes are shown as powers of 2, using 1024 as a divisor for each magnitude. In base 10, sizes are shown as powers of 10, using 1000 as a divisor for each magnitude. Operating systems usually show volume size in base 2. Disk drives usually show size in base 10. Memory (RAM and ROM) size is always shown in base 2.
   - Precision Preference. Select the number of decimal places (1–10) for display of storage-space sizes.
   - Unit Preference. Select a unit for display of storage-space sizes: **Auto**, **TB**, **GB**, **MB**. The Auto option lets the system 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, precision is set to 1, and base is set to 10, the size 0.11709 TB is shown as 117.1 GB.
   - Temperature Preference. Specifies the scale to use for temperature values: **Celsius** or **Fahrenheit**.
   - Auto Sign Out (minutes). Select the amount of time that the user's session can be idle before the user is automatically signed out (2–720 minutes).
   - Locale. The user's preferred display language, which overrides the system's default display language. Installed language sets include Arabic, Chinese-Simplified, Chinese-Traditional, Dutch, English, French, German, Italian, Japanese, Korean, Portuguese, Russian, and Spanish.
4. Click **Modify User**.

   User changes take effect when the user next signs in.

### To modify an SNMPv3 user

1. In the Configuration View panel, right-click the system and select **Configuration > Users > Modify User**. A table displays details for each user. SNMPv3 users can only access the SNMP interface. The other columns are not applicable.
2. In the main panel, select the user to modify.
3. Set the options:
   - Password. A password is case sensitive and must contain 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 ' " , < > \
     If the Authentication Type option is set to use authentication, this password is the authentication password and must include at least 8 characters.
   - SNMP User Type. Select **User Access** to enable the user to view the SNMP MIB, or Trap Target to enable the user to receive SNMP trap notifications. If you select **Trap Target** you must set the Trap Host Address option.
   - Authentication Type. Select whether to use **MD5** or **SHA** authentication, or no authentication (**None**). Authentication uses the user password.
   - Privacy Type. Select whether to use **DES** or **AES** encryption, or no encryption (**none**). To use encryption you must also set the Privacy Password and Authentication Type options.
   - Privacy Password. If the Privacy Type option 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 you set the user type to **Trap Target**, specify the IP address of the host system that will receive SNMP traps.
4. Click **Modify User**.

   User changes take effect when the user next signs in.

## Removing users

You can remove any user, including the default users. However, the system requires at least one CLI user with the `manage` role to exist. When a user is deleted, any sessions associated with that user name are terminated.

### To remove a user

1. In the Configuration View panel, right-click the system and select **Configuration > Users > Remove User**.
2. In the main panel, select the user to remove.
3. Click **Remove User**. A confirmation dialog appears.
4. Click **Remove** to continue. Otherwise, click **Cancel**. If you clicked **Remove**, a processing dialog appears. When processing is complete, the user is removed from the table.
5. Click **OK**.

# Configuring system settings

## Changing the system date and time

You can enter values manually for the system date and time, or you can set the system to use NTP as explained in "About the system date and time" (page 162).

### To use manual date and time settings

1. In the Configuration View panel, right-click the system and select **Configuration > System Settings > Date, Time**. The date and time options appear.
2. Set the options:
   - Time. Enter the time in the format *hh*:*mm*:*ss*, where *hh* is the hour (0–23), *mm* is the minutes (0–59), and *ss* is the seconds (0–59).
   - Month. Select the month.
   - Day. Enter the day number.
   - Year. Enter the year using four digits.
   - Network Time Protocol (NTP). Select **Disabled**.
3. Click **Apply**.

### To obtain the date and time from an NTP server

1. In the Configuration View panel, right-click the system and select **Configuration > System Settings > Date, Time**. The date and time options appear.
2. Set the options:
   - Network Time Protocol (NTP). Select **Enabled**.
   - NTP Time Zone Offset. Optional. The system's time zone as an offset in hours (-12 through +14) and optionally minutes (0–59) from Coordinated Universal Time (UTC). To specify a positive offset, the '+' is optional. To specify a negative offset, the '-' is required. The hour value can have one or two digits and can omit a leading zero. If the minutes value is specified it must have two digits. If it is omitted, the minutes value is set to 00.
   - NTP Server Address. Optional. If the system should retrieve time values from a specific NTP server, enter the address of an NTP server. If no IP server address is set, the system listens for time messages sent by an NTP server in broadcast mode.
3. Click **Apply**.

## Changing host interface settings

You can configure controller host-interface settings for ports. To enable the system to communicate with hosts you must configure the system's host-interface options.

**For AssuredSAN 4004**: Host ports can be configured as a combination of FC or iSCSI ports. For a system with a 4-port SAS controller module, there are no host-interface options.

**For AssuredSAN 3004**: Host ports can only be configured as either FC or iSCSI ports. For a system with a 2-port SAS controller module, host ports can be configured to use fan-out cables or standard cables.

---

**NOTE:** For information about setting advanced host-port parameters, such as FC port topology, see the CLI Reference Guide.

---

### To change FC host interface settings

1. In the Configuration View panel, right-click the system and select **Configuration > System Settings > Host Interfaces**.
2. Set the Speed option to the proper value to communicate with the host. The speed can be set to **auto**, which auto-negotiates the proper link speed with the host, or to **4Gb**, **8Gb**, or **16Gb** (Gbit/s). 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.
3. The FC Connection Mode can be point-to-point or auto:
   - point-to-point: Fibre Channel point-to-point.
   - auto: Automatically sets the mode based on the detected connection type.
4. Click **Apply**.

### To change iSCSI host interface settings

1. In the Configuration View panel, right-click the system and select **Configuration > System Settings > Host Interfaces**.
2. In the upper section of the panel, set the port-specific options:
   - 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.
   - Link-Local Address. For IPv6, the link-local address that is automatically generated from the MAC address and assigned to the port.

   △ **CAUTION:** Changing IP settings can cause data hosts to lose access to the storage system.

3. In the Common Settings for iSCSI section of the panel, set the options that apply to all iSCSI ports:
   - Authentication (CHAP). Enables or disables use of Challenge Handshake Authentication Protocol.

     **NOTE:** CHAP records for iSCSI login authentication must be defined if CHAP is enabled. To create CHAP records, see "Configuring CHAP" (page 218).

   - 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.

- 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.

4. Click **Apply**.

### To change host interface settings for 2-port SAS controller modules (for AssuredSAN 3004 only)

**NOTE:** A fan-out cable can connect one port on each of two SAS hosts to one controller port, using two PHY lanes per port. 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 Configure Host Interface panel displays the current link speed, cable type, number of PHY lanes expected for the SAS port, and number of PHY lanes active for each SAS port. The number of ports that display depends on the configuration.Using fan-out instead of standard cables doubles the number of hosts that can be attached to a single system. It will also halve the maximum bandwidth available to each host, but overall bandwidth available to all hosts is unchanged.

**IMPORTANT:** Changing the fan-out setting will change the logical numbering of controller host ports, which will cause port IDs in mappings between volumes and initiators to be incorrect. Therefore, before changing the fan-out setting, unmap all mappings. After you have changed the fan-out setting and connected the appropriate cables, you can re-create the mappings.

1. In the Configuration View panel, right-click the system and select **Configuration > System Settings > Host Interfaces**.
2. To switch to fan-out cables, select the **Use fan-out cables** check box. To switch to standard cables, clear the **Use fan-out cables** check box.
3. Click **Apply**.
4. Click **Apply** to continue. Otherwise, click **Cancel**. If you clicked Apply and the task succeeds:
   a. A processing dialog appears and quickly exits.
   b. A message displays that the controllers are restarting.
   c. The Sign In page appears after the controllers have restarted.
5. Disconnect the existing cables from the controller module SAS ports and host SAS HBA ports.
6. Switch to the standard or fan-out cables by connecting the new cables to the controller module SAS ports and host SAS HBA ports.
7. Login in if you have not already done so.
8. In the Configuration View panel, right-click an enclosure and select View > Overview > Rear Graphical.
   - If fan-out cables are connected to SAS ports that are configured to use them, fan-out cable icons appear between the depicted SAS ports.
   - If standard cables are connected to SAS ports that are configured to use them, no icons appear.

## Changing network interface settings

You can configure addressing parameters for each controller's network port. You can set static IP values or use DHCP.

In DHCP mode, network port IP address, subnet mask, and gateway values are obtained from a DHCP server if one 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.

Each controller has the following factory-default IP settings:

- DHCP: disabled
- 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 is able to 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: 0.0.0.0

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. This 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.

△ **CAUTION:** Changing IP settings can cause management hosts to lose access to the storage system.

### To use DHCP to obtain IP values for network ports

1. In the Configuration View panel, right-click the system and select **Configuration > System Settings > Network Interfaces**.
2. Set the IP address source to **DHCP**.
3. Click **Apply**. If the controllers successfully obtain IP values from the DHCP server, the new IP values are displayed.
4. Record the new addresses.
5. Sign out and access RAIDar using the new IP addresses.

### To set static IP values for network ports

1. Determine the IP address, subnet mask, and gateway values to use for each controller.
2. In the Configuration View panel, right-click the system and select **Configuration > System Settings > Network Interfaces**.
3. Set the IP address source to **manual**.
4. Set the values for each controller. You must set a unique IP address for each network port.

   **NOTE:** The following IP addresses are reserved for internal use by the storage system: 192.168.200.253, 192.168.200.254, 172.22.255.253, 172.22.255.254, and 127.0.0.1

5. Record the IP values you assign.
6. Click **Apply**.
7. Sign out and access RAIDar using the new IP addresses.

## Setting system information

### To set system information

1. In the Configuration View panel, right-click the system and select **Configuration > System Settings > System Information**.
2. In the main panel, set the **System Name**, **System Contact person**, **System Location**, and **System Information (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. Click **Apply**.

# Configuring advanced settings

## Changing disk settings

### 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.

#### To change the SMART setting

1. In the Configuration View panel, right-click the system and select **Configuration > 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.
   - **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**.

### Configuring dynamic spares

The dynamic spares feature lets you use all of your disks in fault-tolerant vdisks 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 vdisk. A compatible disk has enough capacity to replace the failed disk and is the same type (SAS SSD, enterprise SAS, or midline SAS). If a dedicated spare, global 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.

#### To change the dynamic spares setting

1. In the Configuration View panel, right-click the system and select **Configuration > Advanced Settings > Disk**.
2. Either select (enable) or clear (disable) the **Dynamic Spare Capability** option.
3. Click **Apply**.

## Configuring drive spin down for available disks and global spares

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 disks and global spares, and 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 all disks" (page 187). To configure DSD for a vdisk, see "Configuring drive spin down for a vdisk" (page 197).

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.

### To configure DSD for available disks and global spares

1. In the Configuration View panel, right-click the local system and select **Configuration > Advanced Settings > Disk**.
2. Set the options:
   - Either select (enable) or clear (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 1–360 minutes.
3. Click **Apply**. When processing is complete a success dialog appears.
4. Click **OK**.

## Scheduling drive spin down for all disks

For all 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 a vdisk, see "Configuring drive spin down for a vdisk" (page 197). To configure DSD for available disks and global spares, see "Configuring drive spin down for available disks and global spares" (page 187).

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.

### To schedule DSD for all disks

1. In the Configuration View panel, right-click the local system and select **Configuration > 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**.

### Configuring the EMP polling rate

You can change the frequency interval at which the storage system polls each attached enclosure's EMP for status changes. 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.

#### To change the EMP polling rate

1. In the Configuration View panel, right-click the system and select **Configuration > 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.
3. Click **Apply**.

## Changing FDE settings (for AssuredSAN 4004 only)

In the Full Disk Encryption Settings 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
- FDE 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.

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

#### To set or change the passphrase

1. In the Configuration View panel, right-click the system and select **Configuration > Advanced Settings > Full Disk Encryption** and select the **FDE General Configuration** tab.
2. Enter a passphrase in the **Passphrase** field. A passphrase is case sensitive and can include 8–32 printable UTF-8 characters. It cannot include the following: ' " , < > \
3. Re-enter the passphrase.
4. Click **Set**. A dialog box will confirm the passphrase was changed successfully.

## 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 will not be under your physical control.

If the lock keys are cleared while the system is secured, the system will enter the FDE lock-ready state, in preparation for the system being powered down and transported. The disks will still be in the secured, unlocked state. Once the system has been transported and powered back up, the system and disks will both be in the secured, locked state. Set the system's lock key to restore access to data.

### To clear lock keys

**NOTE:** The FDE panels are dynamic, and the Clear All FDE Keys option is not available until the current passphrase is entered in the **Current Passphrase** field. If there is no passphrase, set one using the procedure in "Setting the passphrase" (page 188).

1. In the Configuration View panel, right-click the system and select **Configuration > Advanced Settings > Full Disk Encryption** and select the **FDE General Configuration** tab.
2. Enter the passphrase in the **Current Passphrase** field.
3. Click **Clear**. A dialog box appears.
4. Do one of the following:
   - To clear the keys, click **Yes**.
   - To cancel the request, click **No**.

## Securing the system

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

### To secure the system

**NOTE:** The FDE panels are dynamic, and the Secure option is not available until the current passphrase is entered in the **Current Passphrase** field. If there is no passphrase, set one using the procedure in "Setting the passphrase" (page 188).

1. In the Configuration View panel, right-click the system and select **Configuration > Advanced Settings > Full Disk Encryption** and select the **FDE General Configuration** tab.
2. Enter the passphrase in the **Current Passphrase** field.
3. Click **Secure**.
4. Do one of the following:
   - To secure the system, click **Yes**.
   - To cancel the request, click **No**.

## Repurposing the system (for AssuredSAN 4004 only)

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.

**NOTE:** If you want to repurpose more than one disk and the drive spin down (DSD) feature is enabled, disable DSD before repurposing the disks. You can re-enable it after the disks are repurposed. For information about disabling and enabling DSD, see "Configuring drive spin down for available disks and global spares" (page 187).

### To repurpose the system

**NOTE:** The FDE panels are dynamic, and the Repurpose System option is not available until the system is secure and all vdisks have been removed from the system.

1. Delete all vdisks in the system. To delete vdisks, see "Deleting vdisks" (page 203). Deleting vdisks effectively deletes all data on the disks but does not secure erase them.
2. In the Configuration View panel, right-click the system and select **Configuration > Advanced Settings > Full Disk Encryption** and select the **FDE General Configuration** tab.
3. Click **Repurpose**. A dialog box displays.
4. Do one of the following:
   - To repurpose the system, click **Yes**.
   - To cancel the request, click **No**.

## Repurposing disks (for AssuredSAN 4004 only)

You can repurpose a disk that is no longer part of a vdisk. Repurposing a disk resets the encryption key on the disk, effectively 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.

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

### To repurpose a disk

1. In the Configuration View panel, right-click the system and select **Configuration > Advanced Settings > Full Disk Encryption** and select the **Repurpose Disks** tab.
2. Select the disk to repurpose.
3. Click **Repurpose**. A dialog box displays.
4. Do one of the following:
   - To repurpose the selected disk, click **Yes**.
   - To cancel the request, click **No**.

## Setting FDE import lock key IDs (for AssuredSAN 4004 only)

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.

### To set or change the import passphrase

1. In the Configuration View panel, right-click the system and select **Configuration > Advanced Settings > Full Disk Encryption** and select the **Set Import Lock Key ID** tab.
2. In the **Passphrase** field, enter the passphrase associated with the displayed lock key.
3. Re-enter the passphrase.
4. Click **Import Passphrase**. A dialog box will confirm the passphrase was changed successfully.

## Changing system cache settings

### 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.

### To change the synchronize-cache mode

1. In the Configuration View panel, right-click the system and select **Configuration > Advanced Settings > Cache**.
2. Set the Sync Cache Mode option to either:
   - **Immediate**. Good status is returned immediately and cache content is unchanged.
   - **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 vdisks). Use Not Ready unless the system is used in a VMware environment or a service technician asks you to change it to work around a host driver problem.

### To change the missing LUN response

1. In the Configuration View panel, right-click the system and select **Configuration > 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.
3. Click **Apply**.

## Controlling host access to the system's write-back cache setting

You can prevent hosts from using `SCSI MODE SELECT` commands to change the system's write-back cache setting. Some operating systems disable write cache. If host control of write-back cache is disabled, the host cannot modify the cache setting.

This option is useful in some environments where the host disables the system's write-back cache, resulting in degraded performance.

### To change host access to the write-back cache setting

1. In the Configuration View panel, right-click the system and select **Configuration > Advanced Settings > Cache**.
2. Either select (enable) or clear (disable) the **Host Control of Write-Back Cache** option.
3. Click **Apply**.

## Changing the controllers' cache redundancy mode

In a dual-controller system's default redundancy/operating mode, Active-Active ULP, data for volumes configured to use write-back cache is automatically mirrored between the two controllers. Cache redundancy has a slight impact on performance but provides fault tolerance. You can disable cache redundancy, which permits independent cache operation for each controller. This is called independent cache performance mode (ICPM).

The advantage of ICPM is that the two controllers can achieve very high write bandwidth and still use write-back caching. User data is still safely stored in nonvolatile RAM, with backup power provided by super-capacitors should a power failure occur. This feature is useful for high-performance applications that do not require a fault-tolerant environment for operation. That is, where speed is more important than the possibility of data loss due to a drive fault prior to a write completion.

The disadvantage of ICPM is that if a controller fails, the other controller will not be able to fail over (that is, take over I/O processing for the failed controller). If a controller experiences a complete hardware failure, and needs to be replaced, then user data in its write-back cache will be lost.

**CAUTION:** Data might be compromised if a RAID controller failure occurs after it has accepted write data, but before that data has reached the disk drives. Do not use ICPM in an environment that requires fault tolerance.

**NOTE:** You cannot enable ICPM if the Partner Firmware Update (PFU) feature or single-controller mode is enabled.

### To change the controllers' cache redundancy mode

1. In the Configuration View panel, right-click the system and select **Configuration > Advanced Settings > Cache**.
2. Either select (enable) or clear (disable) the **Independent Cache Performance Mode** option. In Single Controller mode this option is grayed out.
3. Click **Apply**. For the change to take effect, you must restart both Storage Controllers.

### Changing auto-write-through cache triggers and behaviors

You can set conditions that cause ("trigger") a controller to change the cache mode from write-back to write-through, as described in "About volume cache options" (page 155). You can also specify actions for the system to take when write-through caching is triggered.

#### To change auto-write-through cache triggers and behaviors

1. In the Configuration View panel, right-click the system and select **Configuration > Advanced Settings > Cache**.
2. In the Auto-Write Through Cache Trigger Conditions section, either select (enable) or clear (disable) the options:
   - **Controller Failure**. Changes to write-through if a controller fails. 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.
   - **CompactFlash**. Changes to write-through if CompactFlash memory is not detected during POST, fails during POST, or fails while the controller is under operation.
   - **Power Supply Failure**. Changes to write-through if a power supply unit fails.
   - **Fan Failure**. Changes to write-through if a cooling fan fails.
   - **Overtemperature Failure**. Forces a controller shutdown if a temperature is detected that exceeds system threshold limits.
3. In the Auto-Write Through Cache Behaviors section, either select (enable) or clear (disable) the options:
   - **Revert when Trigger Condition Clears**. Changes back to write-back caching after the trigger condition is cleared.
   - **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 continue using its current caching mode for better performance. In Single Controller mode this option is grayed out.
4. Click **Apply**.

## Configuring partner firmware update

In a dual-controller system in which partner firmware update is enabled, 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.

#### To change the partner firmware update setting

1. In the Configuration View panel, right-click the system and select **Configuration > Advanced Settings > Firmware**.
2. Either select (enable) or clear (disable) the **Partner Firmware Update** option.
3. Click **Apply**.

## Configuring system utilities

### Configuring background scrub for vdisks

You can enable or disable whether the system continuously analyzes disks in vdisks to find and fix disk errors. This command will fix parity mismatches for RAID 3, 5, 6, and 50; mirror mismatches for RAID 1 and 10; and media errors for all RAID levels.

You can use a vdisk while it is being scrubbed. Background vdisk 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 vdisk being scrubbed. A vdisk scrub may be in process on multiple vdisks at once. A new vdisk will first be scrubbed 20 minutes after creation. After a vdisk is scrubbed, scrub will start again after the interval specified by the Vdisk 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 vdisk scrub is recommended.

**TIP:** If you choose to disable background vdisk scrub, you can still scrub a selected vdisk by using **Tools > Media Scrub Vdisk** (page 231).

### To configure background scrub for vdisks

1. In the Configuration View panel, right-click the system and select **Configuration > Advanced Settings > System Utilities**.
2. Set the options:
   - Either select (enable) or clear (disable) the **Vdisk Scrub** option.
   - Set the Vdisk Scrub Interval (hours) option, which is the interval between background vdisk scrub finishing and starting again, from 0–360 hours.
3. Click **Apply**.

## Configuring background scrub for disks not in vdisks

You can enable or disable whether the system continuously analyzes disks that are not in vdisks 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.

### To configure background scrub for disks not in vdisks

1. In the Configuration View panel, right-click the system and select **Configuration > Advanced Settings > System Utilities**.
2. Either select (enable) or clear (disable) the **Disk Scrub** option.
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.

### To change the utility priority

1. In the Configuration View panel, right-click the system and select **Configuration > 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.
   - **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/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” (page 165).

#### To enable or disable managed logs

1. In the Configuration View panel, right-click the system and select **Configuration > Advanced Settings > System Utilities**.
2. Either select (enable) or clear (disable) the **Managed Logs** option.
3. Click **Apply**.

# Configuring remote systems

## Adding a remote system

You can add a management object to obtain information from a remote storage system. This allows a local system to track remote systems by their network-port IP addresses and cache their login credentials. The IP address can then be used in commands that need to interact with the remote system.

#### To add a remote system

1. In the Configuration View panel, either:
   - Right-click the local system and select **Configuration > Remote System > Add Remote System**.
   - Right-click a remote system and select **Configuration > Add Remote System**.
2. In the main panel set the options:
   - IP address. IP address of a network port on the remote system.
   - User Name. User name of a user with a Manage role on the remote system.
   - Password. Password for that user.
3. Click **Create Remote System**. If the task succeeds, the new remote system appears in the Configuration View panel.

## Deleting remote systems

You can delete the management objects for remote systems.

After establishing replication to a remote system, if you choose to delete the remote system you can safely do so without affecting replications. However, because the remote system’s name and IP address will no longer appear in user interfaces, record this information before deleting the remote system so that you can access it at a later time, such as to delete old replication images or for disaster recovery.

#### To delete remote systems

1. In the Configuration View panel, either:
   - Right-click the local system and select **Configuration > Remote System > Delete Remote System**.
   - Right-click a remote system and select **Configuration > Delete Remote System**.
2. In the main panel, select the remote systems to remove. To select or clear all remote systems, toggle the check box in the heading row.
3. Click **Delete Remote System(s)**. A confirmation dialog appears.
4. Click **Delete** to continue. Otherwise, click **Cancel**. If you clicked **Delete**, a processing dialog appears. If the task succeeds, the System Overview panel and a success dialog appear.
5. Click **OK**. As processing completes, the deleted items are removed from the Configuration View panel.

# Configuring a vdisk

## Managing dedicated spares

You can assign a maximum of four available disks to a fault-tolerant vdisk (RAID 1, 3, 5, 6, 10, 50) for use as spares by that vdisk only. A spare must be the same type (SAS SSD, enterprise SAS, or midline SAS) as other disks in the vdisk, and have sufficient capacity to replace the smallest disk in the vdisk.

Vdisks 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). To identify the sector format for a disk, in the Configuration View panel, right-click an enclosure and select **View > Overview**. Select a disk and click the **Properties** tab to view the disk properties, including its sector format (512n or 512e).

---

**NOTE:** If you upgraded from an earlier release that did not distinguish between enterprise and midline SAS disks, you might have vdisks that contain both types of disks. For such a vdisk, whose RAID-level label has the suffix `-MIXED` in the Configuration View panel, you can designate either or both types of disks to be spares.

---

If a disk in the vdisk fails, a dedicated spare is automatically used to reconstruct the vdisk. A fault-tolerant vdisk other than RAID-6 becomes Critical when one disk fails. A RAID-6 vdisk becomes Degraded when one disk fails and Critical when two disks fail. After the vdisk's parity or mirror data is completely written to the spare, the vdisk returns to fault-tolerant status. For RAID-50 vdisks, if more than one sub-vdisk becomes critical, reconstruction and use of assigned spares occur in the order sub-vdisks are numbered.

### To change a vdisk's spares

1. In the Configuration View panel, right-click a vdisk and select **Configuration > Manage Dedicated Spares**. The main panel shows information about the selected vdisk, its spares, and all disks in the system. Existing spares are labeled SPARE.
   - In the Disk Sets table, the number of white slots in the Disks column of the SPARE row shows how many spares you can add to the vdisk.
   - In the Graphical or Tabular view, only existing spares and suitable available disks are selectable.
2. Select spares to remove, disks to add as spares, or both. To add a spare, select its check box. To remove a spare, clear its check box.
3. Click **Modify Spares**. If the vdisk and spares contain a mix of 512n and 512e disks, a dialog box displays.
4. Perform one of the following:
   - To change the vdisk's spares, click **Yes**.
   - To cancel the request, click **No**.

   If the task succeeds, the panel is updated to show which disks are now spares for the vdisk.

## Changing a vdisk's name

### To change a vdisk's name

1. In the Configuration View panel, right-click a vdisk and select **Configuration > Modify Vdisk Name**. The main panel shows the vdisk's name.
2. Enter a new name. A vdisk name is case sensitive and can have a maximum of 32 bytes. It cannot already exist in the system or include the following: ' " , < \
3. Click **Modify Name**. The new name appears in the Configuration View panel.

## Changing a vdisk's owner

Each vdisk is owned by one of the controllers, A or B, known as the *preferred owner*. Typically, you should not need to change vdisk ownership.

When a controller fails, the partner controller assumes temporary ownership of the failed controller's vdisks and resources, becoming the *current owner*. If the system uses a fault-tolerant cabling configuration, both controllers' LUNs are accessible through the partner.

---

△ **CAUTION:**

- Before changing the owning controller for a vdisk, you must stop host I/O to the vdisk's volumes.
- Because a volume and its snap pool must be in vdisks owned by the same controller, if an ownership change will cause volumes and their snap pools to be owned by different controllers, the volumes will not be able to access their snap pools.

---

Changing the owner of a vdisk does not affect the mappings volumes in that vdisk.

### To change a vdisk's owner

1. In the Configuration View panel, right-click a vdisk and select **Configuration > Modify Vdisk Owner**. The main panel shows the vdisk's owner.
2. Select a new owner.
3. Click **Modify Owner**. A confirmation dialog appears.
4. Click **Yes** to continue. Otherwise, click **No**. If you clicked Yes, a processing dialog appears. When processing is complete a success dialog appears.
5. Click **OK**.

# Configuring drive spin down for a vdisk

The drive spin down (DSD) feature monitors disk activity within system enclosures and spins down inactive disks to conserve energy. For a specific vdisk, you can enable or disable DSD and set the period of inactivity after which the vdisk's disks and dedicated spares automatically spin down.

To configure a time period to suspend and resume DSD for all vdisks, see "Scheduling drive spin down for all disks" (page 187). To configure DSD for available disks and global spares, see "Configuring drive spin down for available disks and global spares" (page 187).

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 vdisk has started spinning down, the vdisk spins up again.

### To configure DSD for a vdisk

1. In the Configuration View panel, right-click a vdisk and select **Configuration > Configure Vdisk Drive Spin Down**.
2. Set the options:
   - Either select (enable) or clear (disable) the **Enable Drive Spin Down** option.
   - Set the Drive Spin Down Delay (minutes) option, which is the period of inactivity after which the vdisk's disks and dedicated spares automatically spin down, from 1–360 minutes.
3. Click **Apply**. When processing is complete a success dialog appears.
4. Click **OK**.

# Configuring a volume

## Changing a volume's name

### To change a volume's name

1. In the Configuration View panel, right-click a volume and select **Configuration > Modify Volume Name**.
2. Enter a new name. A volume name is case sensitive and can have a maximum of 32 bytes. It cannot already exist in a vdisk or include the following: ' " , < \
3. Click **Modify Name**. The new name appears in the Configuration View panel.

## Changing a volume's cache settings

For explanations of volume cache options, see "About volume cache options" (page 155).

**CAUTION:**

- Only disable write-back caching if you fully understand how the host operating system, application, and adapter move data. If used incorrectly, you might hinder system performance.
- Only change read-ahead cache and cache optimization mode settings if you fully understand how the host operating system, application, and adapter move data so that you can adjust the settings accordingly.

### To change a volume's cache settings

1. In the Configuration View panel, right-click a volume and select **Configuration > Modify Volume Cache Settings**.
2. In the main panel, set the volume cache options:
   - Write Policy. Select Write-back or Write-through.
   - Write Optimization. Select Standard or No-mirror.
   - Read Ahead Size. Select Disabled, Adaptive, Stripe, or a specific size (512KB, 1MB, 2MB, 4MB, 8MB, 16MB, or 32MB).
3. Click **Modify Cache Settings**.

# Configuring a snapshot

## Changing a snapshot's name

### To change a snapshot's name

1. In the Configuration View panel, right-click a snapshot and select **Configuration > Modify Snapshot Name**.
2. Enter a new name. A snapshot name is case sensitive and can have a maximum of 32 bytes. It cannot already exist in a vdisk or include the following: ' " , < \
3. Click **Modify Name**. A message indicates whether the task succeeded or failed.
4. Click **OK**. The new name appears in the Configuration View panel.

# Configuring a snap pool

## Changing a snap pool's name

### To change a snap pool's name

1. In the Configuration View panel, right-click a snap pool and select **Configuration > Modify Snap Pool Name**.
2. Enter a new name. A snap pool name is case sensitive and can have a maximum of 32 bytes. It cannot already exist in a vdisk or include the following: ' " , < \
3. Click **Modify Name**. The new name appears in the Configuration View panel.

# 13 Provisioning the system

## Using the Provisioning Wizard

The Provisioning Wizard helps you create a vdisk with volumes and to map the volumes to hosts. Before using this wizard, read documentation for your product to learn about vdisks, volumes, and mapping. Then plan the vdisks and volumes you want to create and the default mapping settings you want to use.

The wizard guides you through the following steps. For each step you can view help by clicking the help icon in the wizard panel. As you complete steps they are highlighted at the bottom of the panel. If you cancel the wizard at any point, no changes are made.

- Specify a name and RAID level for the vdisk
- Select disks to use in the vdisk
- Specify the number and size of volumes to create in the vdisk
- Specify the default mapping for access to the volume by hosts
- Confirm changes and apply them

**NOTE:** To create an NRAID, RAID-0, or RAID-3 vdisk, you must use the CLI `create vdisk` command. For more information on this command, see the CLI Reference Guide.

### Starting the wizard

1. In the Configuration View panel, right-click the system and select either **Provisioning > Provisioning Wizard** or **Wizards > Provisioning Wizard**. The wizard panel appears.
2. Click **Next** to continue.

### Specifying the vdisk name and RAID level

A *vdisk* is a virtual disk that is composed of one or more disks, and has the combined capacity of those disks. The number of disks that a vdisk can contain is determined by its RAID level. When you create a vdisk, all its disks must be the same type: either SAS SSD, enterprise SAS, or midline SAS.

A vdisk can contain different models of disks, and disks with different capacities. If you mix disks with different capacities, the smallest disk determines the logical capacity of all other disks in the vdisk, regardless of RAID level. For example, the capacity of a vdisk composed of one 500-GB disk and one 750-GB disk is equivalent to a vdisk composed of two 500-GB disks. To maximize capacity, use disks of similar size. For greatest reliability, use disks of the same size and rotational speed.

In a single-controller system, all vdisks are owned by that controller. In a dual-controller system, when a vdisk is created the system automatically assigns the owner to balance the number of vdisks each controller owns; or, you can select the owner. Typically it doesn't matter which controller owns a vdisk.

In a dual-controller system, when a controller fails, the partner controller assumes temporary ownership of the failed controller's vdisks and resources. If the system uses a fault-tolerant cabling configuration, both controllers' LUNs are accessible through the partner.

When you create a vdisk you can also create volumes within it. A volume is a logical subdivision of a vdisk, and can be mapped to controller host ports for access by hosts. The storage system presents only volumes, not vdisks, to hosts.

### To create a vdisk

1. Set the options:
   - Vdisk name. This field is populated with a default name, which you can change. A vdisk name is case sensitive and can have a maximum of 32 bytes. It cannot already exist in the system or include the following: " , < \
   - Assign to. If the system is operating in Active-Active ULP mode, optionally select a controller to be the preferred owner for the vdisk. Auto automatically assigns the owner to load-balance vdisks between controllers. If the system is operating in Single Controller mode, the Assign to setting is ignored and the system automatically load-balances vdisks in anticipation of the insertion of a second controller in the future.
   - RAID level. Select a RAID level for the vdisk. Each RAID level requires a minimum number of disks, so the number of available disks determines which RAID-level options are selectable. The default, with at least three available disks, is RAID 5.
   - Number of sub-vdisks. For a RAID-10 or RAID-50 vdisk, optionally change the number of sub-vdisks that the vdisk should contain.
   - Chunk size. For RAID 5, 6, 10, or 50, optionally set the amount of contiguous data that is written to a vdisk member before moving to the next member of the vdisk. For RAID 50, this option sets the chunk size of each RAID-5 sub-vdisk. The chunk size of the RAID-50 vdisk is calculated as: *configured-chunk-size* x (*subvdisk-members* - 1). For RAID 1, chunk size has no meaning and is therefore disabled.
2. Click **Next** to continue.

## Selecting disks

Select disks to include in the vdisk. The Disk Selection Sets table has one row for each sub-vdisk in a RAID-10 or RAID-50 vdisk, or a single row for a vdisk having another RAID level. The table also has a SPARE row where you can assign dedicated spares to the vdisk. In each row, the Disks field shows how many disks you can, and have, assigned. As you select disks, the table shows the amount of storage space in the vdisk. For descriptions of storage-space color codes, see “About storage-space color codes” (page 163).

The Tabular tab shows all available disks in all enclosures in a table, displaying Health, Name, Type, State, Size, Enclosure, Serial Number, and Status. The Graphical tab shows disk information graphically, displaying the state for each disk (VDISK, AVAIL, SPARE, VIRTUAL POOL). Only available disks can be selected. Disks you select are highlighted and color-coded to match the rows in the Disk Selection Sets table. Based on the type of disk you select first (SAS SSD, enterprise SAS, or midline SAS), only available disks of that type become selectable. Disks of different types cannot be mixed in a vdisk.

---

**NOTE:** The VIRTUAL POOL label on disks in the Tabular tab view indicates the state of disks used in the virtual storage system.

---

### To select disks and spares

1. Select disks to populate each vdisk row. When you have selected enough disks, a check mark appears in the table’s Complete field.
2. Optionally select up to four dedicated spares for the vdisk.
3. Click **Next** to continue.

## Defining volumes

A *volume* is a logical subdivision of a vdisk and can be mapped to controller host ports for access by hosts. A mapped volume provides the storage for a file system partition you create with your operating system or third-party tools. The storage system presents only volumes, not vdisks, to hosts.

You can create multiple volumes with the same base name, size, and default mapping settings. If you choose to define volumes in this step, you will define their mapping settings in the next step.

### To define volumes

1. Set the options:
   - Number of volumes to create. Specify the number of volumes to create. If you do not want to create volumes, enter **0**. After changing the value, press **Tab**.
   - Volume size. Specify the size of each volume. The default size is the total capacity of the vdisk divided by the number of volumes.
   - Base name for volumes. Specify the base name for the volumes. A volume name is case sensitive and can have a maximum of 16 bytes. It cannot already exist in a vdisk or include the following: " , < \
2. Click **Next** to continue.

## Setting the default mapping

You can optionally specify *default mapping* settings to control whether and how hosts will be able to access the vdisk's volumes. These settings include:

- A logical unit number (LUN), used to identify a mapped volume to hosts. Both controllers share one set of LUNs. Each LUN can be assigned as the default LUN for only one volume in the storage system. For example, if LUN 5 is the default for Volume1, LUN5 cannot be the default LUN for any other volume.
- The level of access — read-write, read-only, or no access — that hosts will have to each volume. When a mapping specifies no access, the volume is *masked*.
- Controller host ports through which hosts will be able to access each volume. To maximize performance, it is recommended to map a volume to at least one host port on the controller that the volume's vdisk is assigned to. To sustain I/O in the event of controller failure, it is recommended to map to at least one host port on each controller.

After a volume is created you can change its default mapping, and create, modify, or delete explicit mappings. An *explicit mapping* overrides the volume's default mapping for a specific host.

---

**NOTE:** When mapping a volume to a host using the Linux ext3 file system, specify read-write access. Otherwise, the file system will be unable to mount/present/map the volume and will report an error such as "unknown partition table."

---

### To specify the default mapping

1. Select **Map**.
2. Set the starting LUN for the volumes. If this LUN is available, it will be assigned to the first volume and the next available LUNs in sequence will be assigned to any remaining volumes.
3. In the enclosure view or list, select controller host ports through which attached hosts can access each volume.
4. Select the access level that hosts will have to each volume: **read-write**, **read-only**, or **no-access** (masked).
5. Click **Next** to continue.

### To proceed without specifying a default mapping

1. Do not select **Map**.
2. Click **Next** to continue.

## Confirming vdisk settings

Confirm that the values listed in the wizard panel are correct.

- If they are not correct, click **Previous** to return to previous steps and make necessary changes.
- If they are correct, click **Finish** to apply the setting changes and finish the wizard.

# Creating a vdisk

Before creating a vdisk, consider some basics, such as the RAID level and the type, capacity, and sector format of the disks. When selecting disks for the vdisk, you can view the disk type and capacity. To identify the sector format for a disk, in the Configuration View panel, right-click an enclosure and select **View > Overview**. Select a disk and click the Properties tab to view the disk properties, including its sector format (512n or 512e). Vdisks 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).

---

**NOTE:** To create an NRAID, RAID-0, or RAID-3 vdisk, you must use the CLI `create vdisk` command. For more information on this command, see the CLI Reference Guide.

---

### To create a vdisk

1. In the Configuration View panel, right-click the system or **Vdisks** and then select **Provisioning > Create Vdisk**.
2. In the main panel set the options:
   - Vdisk name. Optionally change the default name for the vdisk. A vdisk name is case sensitive and can have a maximum of 32 bytes. It cannot already exist in the system or include the following: " , < \
   - Assign to. If the system is operating in Active-Active ULP mode, optionally select a controller to be the preferred owner for the vdisk. The default, Auto, automatically assigns the owner to load-balance vdisks between controllers. If the system is operating in Single Controller mode, the Assign to setting is ignored and the system automatically load-balances vdisks in anticipation of the insertion of a second controller in the future.
   - RAID Level. Select a RAID level for the vdisk. Each RAID level requires a minimum number of disks, so the number of available disks determines which RAID-level options are selectable.
   - Number of Sub-vdisks. For a RAID-10 or RAID-50 vdisk, optionally change the number of sub-vdisks that the vdisk should contain.
   - Chunk size. For RAID 5, 6, 10, or 50, optionally set the amount of contiguous data that is written to a vdisk member before moving to the next member of the vdisk. For RAID 50, this option sets the chunk size of each RAID-5 sub-vdisk. The chunk size of the RAID-50 vdisk is calculated as: *configured-chunk-size* x (*subvdisk-members* - 1). ForRAID 1, chunk size has no meaning and is therefore disabled. The default size is `512KB`.
   - Online Initialization. If you select (enable) this option, you can use the vdisk while it is initializing but because the verify method is used to initialize the vdisk, initialization takes more time. If you clear (disable) this option, you must wait for initialization to complete before using the vdisk, but initialization takes less time. Online initialization is fault tolerant.
3. Select disks to include in the vdisk. The Disk Selection Sets table has one row for each sub-vdisk in a RAID-10 or RAID-50 vdisk, or a single row for a vdisk having another RAID level. The table also has a SPARE row where you can assign dedicated spares to the vdisk. In each row, the Disks field shows how many disks you can, and have, assigned. As you select disks, the table shows the amount of storage space in the vdisk. For descriptions of storage-space color codes, see “About storage-space color codes” (page 163). The Tabular tab shows all available disks in all enclosures in a table, displaying Health, Name, Type, State, Size, Enclosure, Serial Number, and Status. The Graphical tab shows disk information graphically, displaying the state for each disk (VDISK, AVAIL, SPARE). Only available disks can be selected. Disks you select are highlighted and color-coded to match the rows in the Disk Selection Sets table. Based on the type of disk you select first (SAS SSD, enterprise SAS, or midline SAS), only available disks of that type become selectable. Disks of different types cannot be mixed in a vdisk.

To select disks and spares:

- Select disks to populate each vdisk row. When you have selected enough disks, a check mark appears in the table's Complete field.
- Optionally select up to four dedicated spares for the vdisk.

4. Click **Create Vdisk**. If the task succeeds, the new vdisk appears in the Configuration View panel. If the vdisk contains a mix of 512n and 512e disks, a dialog box displays.
5. Perform one of the following:
   - To create the vdisk, click **Yes**.
   - To cancel the request, click **No**.

   If the task succeeds, the new vdisk appears in the Configuration View panel.

# Deleting vdisks

**CAUTION:** Deleting a vdisk removes all of its volumes and their data.

### To delete vdisks

1. Verify that hosts are not accessing volumes in the vdisks that you want to delete.
2. In the Configuration View panel, either:
   - Right-click the system or **Vdisks** and then select **Provisioning > Delete Vdisks**.
   - Right-click a vdisk and select **Provisioning > Delete Vdisk**.
3. In the main panel, select the vdisks to delete. To select or clear all vdisks, toggle the check box in the heading row.
4. Click **Delete Vdisk(s)**. A confirmation dialog appears.
5. Click **Delete** to continue. Otherwise, click **Cancel**. If you clicked Delete, a processing dialog appears. If the task succeeds, an overview panel and a success dialog appear.
6. Click **OK**. As processing completes, the deleted items are removed from the Configuration View panel.

# Managing global spares

You can designate a maximum of 16 global spares for the system. If a disk in any fault-tolerant vdisk (RAID 1, 3, 5, 6, 10, 50) fails, a global spare is automatically used to reconstruct the vdisk. At least one vdisk must exist before you can add a global spare. A spare must have sufficient capacity to replace the smallest disk in an existing vdisk.

The vdisk remains in critical status until the parity or mirror data is completely written to the spare, at which time the vdisk returns to fault-tolerant status. For RAID-50 vdisks, if more than one sub-vdisk becomes critical, reconstruction and use of spares occur in the order sub-vdisks are numbered.

To illuminate a locator LED for a disk, select the disk and click **Turn On LEDs**. To turn off locator LEDs for a disk, click **Turn Off LEDs**.

**NOTE:** Vdisks 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). If a global spare has a different sector format than the disks in a vdisk, an event will appear when the system chooses the spare after a disk in the vdisk fails. For more information about vdisks, see "About vdisks" (page 150).

### To change the system's global spares

1. In the Configuration View panel, right-click the system and select **Provisioning > Manage Global Spares**. The main panel shows information about available disks in the system. Existing spares are labeled GLOBAL SP.
   - In the Disk Sets table, the number of white slots in the Disks field shows how many spares you can add.
   - In the Graphical or Tabular view, only existing global spares and suitable available disks are selectable.
2. Select spares to remove, disks to add as spares, or both.
3. Click **Modify Spares**. If the task succeeds, the panel is updated to show which disks are now global spares.

## Creating a volume set

In a vdisk that has sufficient free space, you can create multiple volumes with the same base name and size. Optionally, you can specify a default mapping for the volumes. Otherwise, they will be created unmapped.

Volume sizes are aligned to 4-MB boundaries. When a volume is created or expanded, if the resulting size would be less than 4 MB it will be increased to 4 MB. If the resulting size would be greater than 4 MB it will be decreased to the nearest 4-MB boundary.

### To create a volume set

1. In the Configuration View panel, right-click a vdisk and select **Provisioning > Create Volume Set**.
2. In the main panel, set the options:
   - Volume Set Base-name. This field is populated with a default base name for the volumes, which you can change. The volume names will consist of the base name and a number that increments from 0000. If a name in the series is already in use, the next name in the series is assigned. For example, for a two-volume set starting with Volume0000, if Volume0001 already exists, the second volume is named Volume0002. A base name is case sensitive and can have a maximum of 16 bytes. It cannot include the following: " , < \
   - Total Volumes. Specify the number of volumes to create. Volumes are created up to the maximum number supported per vdisk.
   - Size. Optionally change the volume size. The default size is the total space divided by the number of volumes.
   - Map. Select this option to specify a default mapping for the volumes:
     - Access. Select the access level that hosts will have to the volumes.
     - LUN. If the access level is set to read-write or read-only, set a LUN for the first volume. The next available LUN is assigned to the next volume mapped through the same ports. If a LUN to be assigned to a volume is already in use, that volume and any subsequent volumes are not mapped.
     - In the enclosure view or list, select controller host ports through which attached hosts can access the volumes.
3. Click **Apply**. If the task succeeds, the new volumes appear in the Configuration View panel.

## Creating a volume

You can add a volume to a vdisk that has sufficient free space, and define default mapping settings.

Volume sizes are aligned to 4-MB boundaries. When a volume is created or expanded, if the resulting size would be less than 4 MB it will be increased to 4 MB. If the resulting size would be greater than 4 MB it will be decreased to the nearest 4-MB boundary.

**NOTE:** In rare cases, a large amount of I/O can cause a snap pool that is too small to fill quickly. This can result in all snapshots being deleted due to the snap pool running out of space. Create snap pools of at least 50 GB to avoid this situation.

### To create a volume in a vdisk

1. In the Configuration View panel, right-click a vdisk and select **Provisioning > Create Volume**.
2. In the main panel, set the options:
   - Volume name. This field is populated with a default name, which you can change. A volume name is case sensitive and can have a maximum of 32 bytes. It cannot already exist in a vdisk or include the following: " , < \
   - Size. Optionally change the default size, which is all free space in the vdisk.
   - Enable Snapshots. If the system is licensed to use Snapshots and you want to create snapshots of this volume, select this option. This specifies to create the volume as a master volume instead of as a standard volume, and enables the Snap Pool and Replication Prepare options.
   - Snap Pool. Select either:
     - Standard Policy. This option creates a snap pool named `spvolume-name` whose size is either 20% of the volume size or 5.37 GB, whichever is larger. The recommended minimum size for a snap pool is 50 GB.
     - Reserve Size. Specify the size of the snap pool to create in the vdisk and associate with the new volume. The default size is either 20% of the volume size or 5.37 GB, whichever is larger. The recommended minimum size for a snap pool is 50 GB.
     - Attach Pool. Select an existing snap pool to associate with the new volume.
   - Replication Prepare. If the system is licensed to use remote replication and you want to use this volume as a replication destination, select this option. Selecting this option disables the Map option.
   - Map. Select this option to change the default mapping for the volume:
     - Access. Select the access level that hosts will have to the volume.
     - LUN. If the access level is set to read-write or read-only, set a LUN for the volume.
     - In the enclosure view or list, select controller host ports through which attached hosts can access the volume.
3. Click **Apply**. If the task succeeds, the new volume appears in the Configuration View panel. If you specified an option to create a snap pool, the new snap pool also appears in that panel.

## Deleting volumes

You can use the Delete Volumes panel to delete standard and master volumes.

△ **CAUTION:** Deleting a volume removes its mappings and schedules and deletes its data.

### To delete volumes

1. Verify that hosts are not accessing the volumes that you want to delete.
2. In the Configuration View panel, either:
   - Right-click the system or **Vdisks** or a vdisk and then select **Provisioning > Delete Volumes**.
   - Right-click a volume and select **Provisioning > Delete Volume**.
3. In the main panel, select the volumes to delete. To select up to 100 volumes or clear all selections, toggle the check box in the heading row.
4. Click **Delete Volume(s)**.
5. Click **Delete** to continue. Otherwise, click **Cancel**. If you clicked **Delete**, a processing dialog appears. If the task succeeds, an overview panel and a success dialog appear.
6. Click **OK**. As processing completes, the deleted items are removed from the Configuration View panel.

**NOTE:** The system might be unable to delete a large number of volumes in a single operation. If you specified to delete a large number of volumes, verify that all were deleted. If some of the specified volumes remain, repeat the deletion on those volumes.

## Changing default mapping for multiple volumes

For all volumes in all vdisks or a selected vdisk, you can change the default access to those volumes by all hosts. When multiple volumes are selected, LUN values are sequentially assigned starting with a LUN value that you specify. For example, if the starting LUN value is 1 for 30 selected volumes, the first volume's mapping is assigned LUN 1 and so forth, and the last volume's mapping is assigned LUN 30. For LUN assignment to succeed, ensure that no value in the sequence is already in use.

**CAUTION:** Volume mapping changes take effect immediately. Make changes that limit access to volumes when the volumes are not in use. Before changing a volume's LUN, be sure to unmount/unpresent/unmap the volume.

**NOTE:** You cannot map the secondary volume of a replication set.

**TIP:** When mapping a volume to a host using the Linux ext3 file system, specify read-write access. Otherwise, the file system will be unable to mount/present/map the volume and will report an error such as "unknown partition table."

### To change default mapping for multiple volumes

1. In the Configuration View panel, right-click **Vdisks** or a vdisk and then select **Provisioning > Map Volume Defaults**. In the main panel, a table shows all the volumes for the selected vdisk.
2. In the table, select the volumes to change. To select up to 100 volumes or clear all selections, toggle the check box in the heading row.
3. Either:
   - Map the volumes to all hosts by setting a starting LUN, selecting ports, and setting access to **read-only** or **read-write**.
   - Mask the volumes from all hosts by setting a starting LUN, selecting ports, and setting access to **no-access**. Setting the default mapping to **no-access** will result in the LUN mapping being removed.
4. Click **Apply**. A message specifies whether the change succeeded or failed.
5. Click **OK**.

## Explicitly mapping multiple volumes

For all volumes in all vdisks or a selected vdisk, you can change access to those volumes by a specific host. When multiple volumes are selected, LUN values are sequentially assigned starting with a LUN value that you specify. For example, if the starting LUN value is 1 for 30 selected volumes, the first volume's mapping is assigned LUN 1 and so forth, and the last volume's mapping is assigned LUN 30. For LUN assignment to succeed, ensure that no value in the sequence is already in use. When specifying access through specific ports, the ports and host must be the same type (for example, FC or SAS).

**CAUTION:** Volume mapping changes take effect immediately. Make changes that limit access to volumes when the volumes are not in use. Before changing a volume's LUN, be sure to unmount/unpresent/unmap the volume.

**NOTE:** You cannot map the secondary volume of a replication set.

**TIP:** When mapping a volume to a host using the Linux ext3 file system, specify read-write access. Otherwise, the file system will be unable to mount/present/map the volume and will report an error such as “unknown partition table.”

### To explicitly map multiple volumes

1. In the Configuration View panel, right-click **Vdisks** or a vdisk and then select **Provisioning > Map Volumes**. In the main panel, a table shows all the volumes for the selected vdisk.
2. In the table, select the volumes to change. To select up to 100 volumes or clear all selections, toggle the check box in the heading row.
3. In the Hosts table, select the host to change access for.
4. Either:
   - Map the volumes to the host by setting a starting LUN, selecting ports, and setting access to **read-only** or **read-write**.
   - Mask the volumes from the host by setting a starting LUN, selecting ports, and setting access to **no-access**.
5. Click **Apply**.
6. Click **Yes** to continue. Otherwise, click No. If you clicked Yes, mapping changes begin. A message specifies whether the change succeeded or failed.

## Changing a volume’s default mapping

**CAUTION:** Volume mapping changes take effect immediately. Make changes that limit access to volumes when the volumes are not in use. Be sure to unmount/unpresent/unmap a volume before changing the volume’s LUN.

**NOTE:** You cannot map the secondary volume of a replication set.

**TIP:** When mapping a volume to a host using the Linux ext3 file system, specify read-write access. Otherwise, the file system will be unable to mount/present/map the volume and will report an error such as “unknown partition table.”

### To view the default mapping

In the Configuration View panel, right-click a volume and select **Provisioning > Default Mapping**. The main panel shows the volume’s default mapping:

- Ports. Controller host ports through which the volume is mapped to the host.
- LUN. Volume identifier presented to the host.
- Access. Volume access type: read-write, read-only, no-access (masked), or not-mapped.

### To modify the default mapping

1. Select **Map**.
2. Set the LUN and select the ports and access type. Setting the default mapping to **no-access** will result in the LUN mapping being removed.
3. Click **Apply**. A message specifies whether the change succeeded or failed.
4. Click **OK**. Each mapping that uses the default settings is updated.

### To delete the default mapping

1. Clear **Map**.
2. Click **Apply**. A message specifies whether the change succeeded or failed.
3. Click **OK**.
4. Click **Yes** to continue. Otherwise, click **No**. If you clicked Yes, mapping changes begin. A message specifies whether the change succeeded or failed. Each mapping that uses the default settings is updated.

## Changing a volume's explicit mappings

**CAUTION:** Volume mapping changes take effect immediately. Make changes that limit access to volumes when the volumes are not in use. Be sure to unmount/unpresent/unmap a volume before changing the volume's LUN.

**NOTE:** You cannot map the secondary volume of a replication set.

**TIP:** When mapping a volume to a host using the Linux ext3 file system, specify read-write access. Otherwise, the file system will be unable to mount/present/map the volume and will report an error such as "unknown partition table."

### To view volume mappings

In the Configuration View panel, right-click a volume and select **Provisioning > Explicit Mappings**. The main panel shows the following information about the volume's mappings:

- Type. Explicit or Default. Settings for an explicit mapping override the default mapping.
- Host ID. WWPN or IQN.
- Host Name. User-defined nickname for the host.
- Ports. Controller host ports through which the volume is mapped to the host.
- LUN. Volume identifier presented to the host.
- Access. Volume access type: read-write, read-only, no-access (masked), or not-mapped.

### To create an explicit mapping

1. In the Maps for Volume table, select a host.
2. Select **Map**.
3. Set the LUN and select the ports and access type.
4. Click **Apply**. A message specifies whether the change succeeded or failed.
5. Click **OK**. The mapping becomes Explicit with the new settings.

### To modify an explicit mapping

1. In the Maps for Volume table, select the Explicit mapping to change.
2. Set the LUN and select the ports and access type.
3. Click **Apply**. A message specifies whether the change succeeded or failed.
4. Click **OK**. The mapping settings are updated.

### To delete an explicit mapping

1. In the Maps for Volume table, select the Explicit mapping to delete.
2. Clear **Map**.
3. Click **Apply**. A message specifies whether the change succeeded or failed.
4. Click **OK**. The mapping returns to the Default mapping.

## Unmapping volumes

You can delete all of the default and explicit mappings for multiple volumes.

**CAUTION:** Volume mapping changes take effect immediately. Make changes that limit access to volumes when the volumes are not in use. Before changing a volume's LUN, be sure to unmount/unpresent/unmap the volume.

### To unmap volumes

1. In the Configuration View panel, right-click **Vdisks** or a vdisk and then select **Provisioning > Unmap Volumes**. In the main panel, a table shows all the volumes for the selected vdisk.
2. In the table, select the volumes to unmap. To select up to 100 items or clear all selections, toggle the check box in the heading row.
3. Click **Unmap Volume(s)**. A message specifies whether the change succeeded or failed.
4. Click **OK**. Default and explicit mappings are deleted and the volumes' access type changes to not-mapped.

## Expanding a volume

You can expand a standard volume if its vdisk has free space and sufficient resources. Because volume expansion does not require I/O to be stopped, the volume can continue to be used during expansion.

Volume sizes are aligned to 4-MB boundaries. When a volume is created or expanded, if the resulting size would be less than 4 MB it will be increased to 4 MB. If the resulting size would be greater than 4 MB it will be decreased to the nearest 4-MB boundary.

**NOTE:** This command is not supported for master volumes.

### To expand a volume

1. In the Configuration View panel, right-click a standard volume and select **Tools > Expand Volume**.
2. In the main panel, specify the amount of free space to add to the volume.
3. Click **Expand Volume**. If the specified value exceeds the amount of free space in the vdisk, a dialog lets you expand the volume to the limit of free space in the vdisk. If the task succeeds, the volume's size is updated in the Configuration View panel.

# Creating multiple snapshots

If the system is licensed to use Snapshots, you can select multiple volumes and immediately create a snapshot of each volume.

The first time a snapshot is created of a standard volume, the volume is converted to a master volume and a snap pool is created in the volume's vdisk. The snap pool's size is either 20% of the volume size or 5.37 GB, whichever is larger. The recommended minimum size for a snap pool is 50 GB. Before creating or scheduling snapshots, verify that the vdisk has enough free space to contain the snap pool.

### To create snapshots of multiple volumes

1. In the Configuration View panel, right-click the system or **Vdisks** or a vdisk and then select **Provisioning > Create Multiple Snapshots**.
2. In the main panel, select each volume to take a snapshot of. To select up to 100 volumes or clear all selections, toggle the check box in the heading row.
3. Click **Create Snapshots**. If the task succeeds, the snapshots appear in the Configuration View panel.

# Creating a snapshot

If the system is licensed to use Snapshots, you can create a snapshot now or schedule the snapshot task.

The first time a snapshot is created of a standard volume, the volume is converted to a master volume and a snap pool is created in the volume's vdisk. The snap pool's size is either 20% of the volume size or 5.37 GB, whichever is larger. The recommended minimum size for a snap pool is 50 GB. Before creating or scheduling snapshots, verify that the vdisk has enough free space to contain the snap pool.

### To create a snapshot now

1. In the Configuration View panel, right-click a volume and select **Provisioning > Create Snapshot**.
2. In the main panel, select **Now**.
3. Optionally change the default name for the snapshot. A snapshot name is case sensitive and can have a maximum of 32 bytes. It cannot already exist in a vdisk or include the following: " , < \
4. Click **Create Snapshot**. If the task succeeds, the snapshot appears in the Configuration View panel.

### To schedule a create snapshot task

1. In the Configuration View panel, right-click a volume and select **Provisioning > Create Snapshot**.
2. In the main panel, select **Scheduled**.
3. Set the options:
   - Snapshot prefix. Optionally change the default prefix to identify snapshots created by this task. The prefix is case sensitive and can have a maximum of 26 bytes. It cannot already exist in a vdisk or include the following: " , < \ Automatically created snapshots are named *prefix*_s*n*, where *n* starts at 001.
   - Snapshots to Retain. Select the number of snapshots to retain. 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 volume's oldest snapshot is unmapped, reset, and renamed to the next name in the sequence.
   - Start Schedule. 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.
     - Date must use the format *yyyy-mm-dd*.
     - 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.

- Recurrence. Specify either One Time, which schedules a single instance, or the interval at which the task should run. Set the interval to at least two minutes. For better performance if this task will run under heavy I/O conditions or on more than three volumes, set the retention count and the schedule interval to similar values. For example if the retention count is 10 then the interval should be set to 10 minutes.
- Time Constraint. Specify either No Time Constraint, which allows the schedule to run at any time, or a time range within which the task should run.
- Date Constraint. Specify either No Date Constraint, which allows the schedule to run on any day, or days when the task should run. Ensure that this constraint includes the Start Schedule date.
- End Schedule. Specify either Continuous, which allows the schedule to run without an end date, or when the task should stop running.

4. Click **Schedule Snapshots**. If processing succeeds, the schedule is saved and can be viewed in the overview panel for the volume or system.

# Deleting snapshots

You can use the Delete Snapshots panel to delete standard and replication snapshots.

When you delete a snapshot, all data uniquely associated with that snapshot is deleted and associated space in the snap pool is freed for use. Snapshots can be deleted in any order, irrespective of the order in which they were created.

△ **CAUTION:** Deleting a snapshot removes its mappings and schedules and deletes its data.

△ **CAUTION:** If a replication snapshot's type is shown as a "sync point" for its replication set, consider carefully whether you want to delete that snapshot. If you delete the current sync point, then if a replication-set failure occurs, a prior sync point will be used. If you delete the only sync point then the next replication will require a full sync to be performed (*all* data to be re-replicated from the primary volume to a secondary volume).

### To delete snapshots

1. Verify that hosts are not accessing the snapshots that you want to delete.
2. In the Configuration View panel, right-click either the system or a vdisk or a master volume or a primary volume or a secondary volume or a snapshot or a replication image and then select **Provisioning > Delete Snapshot**.
3. In the main panel, select the snapshots to delete.
4. Click **Delete Snapshot(s)**.
5. Click **OK** to continue. Otherwise, click **Cancel**. If you clicked OK, a processing dialog appears. If the task succeeds, an overview panel and a success dialog appear.
6. Click **OK**. As processing completes, the deleted items are removed from the Configuration View panel.

# Resetting a snapshot

If the system is licensed to use Snapshots, 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's name and mapping settings are not changed. The snapshot data is stored in the source volume's snap pool. This task is not allowed for a replication snapshot.

**CAUTION:** To avoid data corruption, before resetting a snapshot it must be unmounted/unpresented/unmapped from hosts.

You can reset a snapshot now or schedule the reset task.

### To reset a snapshot now

1. Unmount/unpresent/unmap the snapshot from hosts.
2. In the Configuration View panel, right-click a snapshot and select **Provisioning > Reset Snapshot**.
3. In the main panel, select **Now**.
4. Click **Reset Snapshot**. A confirmation dialog appears.
5. Click **Yes** to continue. Otherwise, click **No**. If you clicked Yes, a processing dialog appears. When processing is complete a success dialog appears.
6. Click **OK**.
7. Optionally, remount/re-present/remap the snapshot.

### To schedule a reset snapshot task

1. In the Configuration View panel, right-click a snapshot and select **Provisioning > Reset Snapshot**.
2. In the main panel, select **Scheduled**.
3. Set the options:
   - Start Schedule. 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.
     - Date must use the format *yyyy-mm-dd*.
     - 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.
   - Recurrence. Specify either One Time, which schedules a single instance, or the interval at which the task should run. Set the interval to at least 2 minutes.
   - Time Constraint. Specify either No Time Constraint, which allows the schedule to run at any time, or a time range within which the task should run.
   - Date Constraint. Specify either No Date Constraint, which allows the schedule to run on any day, or days when the task should run. Ensure that this constraint includes the Start Schedule date.
   - End Schedule. Specify either Continuous, which allows the schedule to run without an end date, or when the task should stop running.
4. Click **Reset Snapshot**. If the task succeeded, the schedule is saved and can be viewed in the overview panel for the snapshot or system.
5. Make a reminder to unmount/unpresent/unmap the snapshot before the scheduled task runs.

# Creating a volume copy

If the system is licensed to use Volume Copy, you can copy a volume or a snapshot to a new standard volume. The destination volume must be in a vdisk owned by the same controller as the source volume. If the source volume is a snapshot, you can choose whether to include its modified data (data written to the snapshot since it was created). The destination volume is completely independent of the source volume.

The first time a volume copy is created of a standard volume, the volume is converted to a master volume and a snap pool is created in the volume's vdisk. The snap pool's size is either 20% of the volume size or 5.37 GB, whichever is larger. The recommended minimum size for a snap pool is 50 GB. Before creating or scheduling copies, verify that the vdisk has enough free space to contain the snap pool.

For a master volume, the volume copy creates a transient snapshot, copies the data from the snapshot, and deletes the snapshot when the copy is complete. For a snapshot, the volume copy 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/presented/mapped and I/O is occurring to it.

To ensure the integrity of a copy of a master volume, unmount/unpresent/unmap the volume or at minimum perform a system cache flush and refrain from writing to the volume. Since the system cache flush is not natively supported on all operating systems, it is recommended to unmount/unpresent/unmap temporarily. The volume copy is for all data on the disk at the time of the request, so if there is data in the operating-system cache, that will not be copied over. Unmounting/unpresenting/unmapping the volume forces the cache flush from the operating system. After the volume copy has started, it is safe to remount/re-present/remap the volume and/or resume I/O.

To ensure the integrity of a copy of a snapshot with modified data, unmount/unpresent/unmap the snapshot or perform a system cache flush. The snapshot will not be available for read or write access until the volume copy is complete, at which time you can remount/re-present/remap the snapshot. If modified write data is not to be included in the copy, then you may safely leave the snapshot mounted/presented/mapped. During a volume copy using snapshot modified data, the system takes the snapshot offline, as shown by the Snapshot Overview panel.

The volume copy's progress is shown in the Volume Overview panel.

You can create a volume copy now or schedule the copy task.

### To create a volume copy now

1. In the Configuration View panel, right-click a volume and select **Provisioning > Create Volume Copy**.
2. In the main panel, select **Now**.
3. Set the options:
   - New Volume Name. Optionally change the default name for the destination volume. A volume name is case sensitive and can have a maximum of 32 bytes. It cannot already exist in a vdisk or include the following: " , < \
   - Residing On Vdisk. Optionally change the destination vdisk.
   - **With Modified Data**. If the source volume is a snapshot, select this option to include the snapshot's modified data in the copy. Otherwise, the copy will contain only the data that existed when the snapshot was created.
4. Click **Copy the Volume**. A confirmation dialog appears.
5. Click **Yes** to continue. Otherwise, click **No**. If you clicked Yes and With Modified Data is selected and the snapshot has modified data, a second confirmation dialog appears.
6. Click **Yes** to continue. Otherwise, click **No**. If you clicked Yes, the volume copy operation starts. While the operation is in progress, the destination volume is offline and its type is shown as "standard*". If you unmounted/unpresented/unmapped a snapshot to copy its modified data, *wait* until processing is complete before you remount/re-present/remap it. If the task succeeds, the destination volume's type becomes standard and the volume appears in the Configuration View panel.
7. Optionally map the volume to hosts.

### To schedule a volume copy task

1. In the Configuration View panel, right-click a volume and select **Provisioning > Create Volume Copy**.
2. In the main panel, select **Scheduled**.
3. Set the options:
   - New Volume Prefix. Optionally change the default prefix to identify volumes created by this task. The prefix is case sensitive and can have a maximum of 26 bytes. It cannot include the following: " , < \
     Automatically created volumes are named *prefix_cn*, where *n* starts at 001.
   - Residing On Vdisk. Optionally change the destination vdisk.
   - **With Modified Data**. If the source volume is a snapshot, select this option to include the snapshot's modified data in the copy. Otherwise, the copy will contain only the data that existed when the snapshot was created.
   - Start Schedule. 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.
     - Date must use the format *yyyy-mm-dd*.
     - 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.
   - Recurrence. Specify interval at which the task should run. Set the interval to at least 2 minutes. The default is 1 minute.
   - Time Constraint. Specify a time range within which the task should run.
   - Date Constraint. Specify days when the task should run. Ensure that this constraint includes the Start Schedule date.
   - End Schedule. Specify when the task should stop running.
4. Click **Schedule Volume Copy**. If the task succeeded, the schedule is saved and can be viewed in the overview panel for the volume or system.
5. If you will copy snapshot modified data, make a reminder to unmount/unpresent/unmap the snapshot before the scheduled task runs.

## Aborting a volume copy

If the system is licensed to use Volume Copy, you can cancel an in-progress volume copy operation. When the cancellation is complete, the destination volume is deleted.

### To abort a volume copy

1. In the Configuration View panel, right-click the destination volume and then select **Provisioning > Abort Volume Copy**. The Volume Overview panel shows the operation's progress.
2. Click **Abort Volume Copy**. A message confirms that the operation has been aborted.
3. Click **OK**. The destination volume is removed from the Configuration View panel.

# Rolling back a volume

You can roll back (revert) the data in a volume to the data that existed when a specified snapshot was created. You also have the option of including its modified data (data written to the snapshot since it was created). For example, you might want to take a snapshot, mount/present/map it for read/write, and then install new software on the snapshot for testing. If the software installation is successful, you can roll back the volume to the contents of the modified snapshot.

△ **CAUTION:**

- Before rolling back a volume you must unmount/unpresent/unmap it from data hosts to avoid data corruption. If you want to include snapshot modified data in the roll back, you must also unmount/unpresent/unmap the snapshot.
- If the snap pool runs out of space, the master volume will change to read only until the rollback has completed.
- Whenever you perform a roll back, the data that existed on the volume is replaced by the data on the snapshot. That is, all data on the volume written since the snapshot was taken is lost. As a precaution, take a snapshot of the volume before starting a roll back.

Only one roll back is allowed on the same volume at one time. Additional roll backs are queued until the current roll back is complete. However, after the roll back is requested, the volume is available for use as if the roll back has already completed.

During a roll back operation using snapshot modified data, the snapshot must be unmounted/unpresented/unmapped and cannot be accessed. Unmounting/unpresenting/unmapping the snapshot ensures that all data cached by the host is written to the snapshot. If unmounting/unpresenting/unmapping is not performed at the host level prior to starting the roll back, data may remain in host cache, and thus not be rolled back to the master volume. As a precaution against inadvertently accessing the snapshot, the system also takes the snapshot offline, as shown by the Snapshot Overview panel. The snapshot becomes inaccessible in order to prevent any data corruption to the master volume. The snapshot can be remounted/re-presented/remapped once the roll back is complete.

### To roll back a volume

1. Unmount/unpresent/unmap the volume from hosts.
2. If the roll back will include snapshot modified data, unmount/unpresent/unmap the snapshot from hosts.
3. In the Configuration View panel, right-click a volume and select **Provisioning > Roll Back Volume**.
4. In the main panel, set the options:
   - For Volume. The name of the volume to roll back.
   - From Snapshot Volume. Enter the name of the snapshot to roll back to.
   - **With Modified Data**. Select this option to include the snapshot's modified data in the roll back. Otherwise, the master volume will contain only the data that existed when the snapshot was created.
5. Click **Roll Back Volume**. The roll back starts. You can now remount/re-present/remap the volume.
6. When the roll back is complete, if you unmounted/unpresented/unmapped the snapshot you can remount/re-present/remap it.

# Creating a snap pool

Before you can convert a standard volume to a master volume or create a master volume for snapshots, a snap pool must exist. A snap pool and its associated master volumes can be in different vdisks, but must be owned by the same controller.

### To create a snap pool

1. In the Configuration View panel, right-click a vdisk and select **Provisioning > Create Snap Pool**.
2. In the main panel set the options:
   - Snap Pool name. Optionally change the default name for the snap pool. A snap pool name is case sensitive and can have a maximum of 32 bytes. It cannot already exist in the system or include the following: " , < \
   - Size. Optionally change the default size, which is all free space in the vdisk. Although a snap pool can be as small as 5.37 GB, the recommended minimum size is 50 GB.
3. Click **Create Snap Pool**. If the task succeeds, the new snap pool appears in the Configuration View panel.

# Deleting snap pools

Before you can delete a snap pool you must delete any associated snapshots, and either delete the associated master volume or convert the master volume to a standard volume.

### To delete snap pools

1. Verify that no master volume or snapshots are associated with the snap pool.
2. In the Configuration View panel, either:
   - Right-click the local system or **Vdisks** or a vdisk and select **Provisioning > Delete Snap Pools**.
   - Right-click a snap pool and select **Provisioning > Delete Snap Pool**.
3. In the main panel, select the snap pools to delete.
4. Click **Delete Snap Pool(s)**.
5. Click **Delete** to continue. Otherwise, click **Cancel**. If you clicked Delete, a processing dialog appears. If the task succeeds, an overview panel and a success dialog appear.
6. Click **OK**. As processing completes, the deleted items are removed from the Configuration View panel.

# Adding a host

### To add a host

1. Determine the host's WWPN or IQN.
2. In the Configuration View panel, right-click the system or **Hosts** and then select **Provisioning > Add Host**.
3. In the main panel set the options:
   - Host ID (WWN/IQN). Enter the host's WWPN or IQN. A WWPN value can include a colon between each pair of digits but the colons will be discarded.
   - Host Name. This field is populated with a default name, which you can change to a name that helps you easily identify the host. For example, `FileServer_1`. An host name is case sensitive and can have a maximum of 32 bytes. It cannot already exist in the system or include the following: " , . < \
   - Profile.
     - Standard: Default profile.
     - HP-UX: The host uses Flat Space Addressing.
4. Click **Add Host**. If the task succeeds, the new host appears in the Configuration View panel.

# Removing hosts

### To remove hosts

1. Verify that the hosts you want to remove are not accessing volumes.
2. In the Configuration View panel, either:
   - Right-click the system or **Hosts** and then select **Provisioning > Remove Hosts**.
   - Right-click a host and select **Provisioning > Remove Host**.
3. In the main panel, select the hosts to remove. To select or clear all items, toggle the check box in the heading row.
4. Click **Remove Host(s)**. A confirmation dialog appears.
5. Click **Remove** to continue. Otherwise, click **Cancel**. If you clicked Remove, a processing dialog appears. If the task succeeds, an overview panel and a success dialog appear.
6. Click **OK**. As processing completes, the deleted items are removed from the Configuration View panel.

# Changing a host's name or profile

### To change a host's name or profile

1. In the Configuration View panel, right-click a host and select **Provisioning > Rename Host**.
2. Enter a new name that helps you easily identify the host. For example, FileServer_1. An host name is case sensitive and can have a maximum of 32 bytes. It cannot already exist in the system or include the following: " , . < \
3. Optionally, change the host profile:
   - Standard: Default profile.
   - HP-UX: The host uses Flat Space Addressing.
4. Click **Modify Name**. A confirmation dialog appears.
5. Click **Yes** to continue. Otherwise, click **No**. If you clicked Yes, a message indicates whether the task succeeded or failed.
6. Click **OK**.

# Changing host mappings

For each volume that is mapped to the selected host, you can create, modify, and delete explicit mappings. To change a volume's default mapping, see "Changing a volume's default mapping" (page 207).

**CAUTION:** Volume mapping changes take effect immediately. Make changes that limit access to volumes when the volumes are not in use. Be sure to unmount/unpresent/unmap a volume before changing the volume's LUN.

**NOTE:** You cannot map the secondary volume of a replication set.

**TIP:** When mapping a volume to a host using the Linux ext3 file system, specify read-write access. Otherwise, the file system will be unable to mount/present/map the volume and will report an error such as "unknown partition table."

### To view host mappings

In the Configuration View panel, right-click a host and select **Provisioning > Manage Host Mappings**. The main panel shows the following information about volumes mapped to the host:

- Type. Explicit or Default. Settings for an explicit mapping override the default mapping.
- Name. Volume name.
- Serial Number. Volume serial number.
- Ports. Controller host ports through which the volume is mapped to the host.
- LUN. Volume identifier presented to the host.
- Access. Volume access type: read-write, read-only, no-access (masked), or not-mapped.

### To create an explicit mapping

1. In the Maps for Host table, select the Default mapping to override.
2. Select **Map**.
3. Set the LUN and select the ports and access type.
4. Click **Apply**. A message specifies whether the change succeeded or failed.
5. Click **OK**. The mapping becomes Explicit with the new settings.

### To modify an explicit mapping

1. In the Maps for Host table, select the Explicit mapping to change.
2. Set the LUN and select the ports and access type.
3. Click **Apply**. A message specifies whether the change succeeded or failed.
4. Click **OK**. The mapping settings are updated.

### To delete an explicit mapping

1. In the Maps for Host table, select the Explicit mapping to delete.
2. Clear **Map**.
3. Click **Apply**. A message specifies whether the change succeeded or failed.
4. Click **OK**. The mapping returns to the Default mapping.

## 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 entries must exist on each device. Each CHAP entry 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 storage system, the host is the initiator and the storage system 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 hosts, see “Changing host interface settings” (page 182).

### To add or modify a CHAP entry

1. In the Configuration View panel, right-click **Hosts** or a specific host and then select **Provisioning > Configure CHAP**. If any CHAP entries exist, a table shows them by node name.
2. Optionally, select an entry whose name you want to change to create a new entry. The entry’s values appear in the option fields.

3. Set the options:
   - Node Name (IQN). The initiator name, typically in IQN format.
   - Secret. The secret that the target uses 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: " <
   - Name, if mutual CHAP. Optional. For mutual CHAP only. Specifies the target name, typically in IQN format. The value is case sensitive and can include a maximum of 223 bytes. To find a controller iSCSI port's IQN, select the controller enclosure, view the Enclosure Overview panel (page 255), select the Rear Graphical tab, select an iSCSI port, and view the Target ID field.
   - Secret, if mutual CHAP. Optional. For mutual CHAP only. Specifies the secret that the initiator uses 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's secret is shared by both controllers.
4. Click **Add/Modify Entry**. If the task succeeds, the new or modified entry appears in the CHAP entries table.

### To delete a CHAP entry

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

1. In the Configuration View panel, right-click **Hosts** or a specific host and then select **Provisioning > Configure CHAP**. If any CHAP entries exist, a table shows them by node name.
2. Select the entry to delete.
3. Click **Delete Entry**. If the task succeeds, the entry is removed from the CHAP entries table.

## Modifying a schedule

### To modify a schedule

1. In the Configuration View panel, right-click the system or a volume or a snapshot and select **Provisioning > Modify Schedule**. In the main panel, a table shows each schedule.
2. In the table, select the schedule to modify. For information about schedule status values, see "Schedule properties" (page 250).
3. Set the options:
   - Snapshot Prefix. Optionally change the default prefix to identify snapshots created by this task. The prefix is case sensitive and can have a maximum of 26 bytes. It cannot include the following: " , < \
   - Snapshots to Retain. Select the number of snapshots to retain. 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 volume's oldest snapshot is unmapped, reset, and renamed to the next name in the sequence.
   - Start Schedule. 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.
     - Date must use the format *yyyy-mm-dd*.
     - 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.
   - Recurrence. Specify interval at which the task should run. Select either One Time or how often the task should occur. If the task is recurrent, select Minutes, Hours, Days, Weeks, Months, or Years from the list. If One Time is selected, no further options are available and the task will occur only on the date and time specified in Start Schedule.

- For a snapshot schedule, set the interval to at least 2 minutes. For better performance if this task will run under heavy I/O conditions or on more than three volumes, set the retention count and the interval to similar values. For example if the retention count is 10 then set the interval to 10 minutes.
- For a volume-copy or reset-snapshot schedule, set the interval to at least 2 minutes.
- For a replication schedule, set the interval to at least 30 minutes.

- Time Constraint. Specify a time range within which the task should run. Select either No Time Constraint or times between which the task will run.
  - If No Time Constraint is selected, the task will run whenever scheduled.
  - If a set of times is specified, the task can only occur during that period of time.
- Date Constraint. Specify days when the task should run. Ensure that this constraint includes the Start Schedule date. Select No Date Constraint, Any, or a specific time.
  - If No Date Constraint is selected, the task will occur whenever scheduled.
  - For Any, select a type of day (any day, weekday, weekend day, or specific day of the week) and a year, month, or specific month. For example, if you select Any Weekday of June, the task can occur only on weekdays in June.
  - For a specific time, select a type of day (any day, weekday, weekend day, or specific day of the week), a number, and a year, month, or specific month. For example, if you select Sunday number 3 of January, the task can occur only on the 3rd Sunday of January.
- End Schedule. Specify when the task should stop running. Select Continuous, Date, or End After.
  - If Continuous is selected, the task will never end.
  - If a date and time is specified, the task will not run as scheduled after that date.
  - If End After is selected, the task will end after the running the number of times you specify. For example, if you enter 5, the task will run only 5 times.

4. Click **Modify Schedule**.
5. Click **Yes** to continue. Otherwise, click **No**. If you clicked Yes, a processing dialog appears. When processing is complete a success dialog appears.
6. Click **OK**.

## Deleting schedules

If a component has a scheduled task that you no longer want to occur, you can delete the schedule. When a component is deleted, its schedules are also deleted.

### To delete task schedules

1. In the Configuration View panel, right-click the system or a volume or a snapshot and select **Provisioning > Delete Schedule**.
2. In the main panel, select the schedule to remove.
3. Click **Delete Schedule**. A confirmation dialog appears.
4. Click **Yes** to continue. Otherwise, click **No**. If you clicked **Yes**, a processing dialog appears. If the task succeeds, the schedules are removed from the table and from the Configuration View panel. When processing is complete a success dialog appears.
5. Click **OK**.

# 14 Using system tools

## Updating firmware

You can view the current versions of firmware in controller modules, expansion modules, drawers, and disks, and install new versions.

To monitor the progress of a firmware-update operation by using the activity progress interface, see “Using the activity progress interface” (page 224).

**TIP:** 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.

**IMPORTANT:**

- Run the `check firmware-upgrade-health` CLI command before upgrading firmware. This command performs a series of health checks to determine whether any conditions exist that need to be resolved before upgrading firmware. Any conditions that are detected are listed with their potential risks. For information about this command, see the CLI Reference Guide.
- If a vdisk is quarantined, resolve the problem that is causing the vdisk to be quarantined before updating firmware. See information about events 172 and 485 in the Event Descriptions Reference Guide, and “Removing a vdisk from quarantine” (page 231).
- If any unwritten cache data is present, firmware update will not proceed. Before you can update firmware, unwritten data must be removed from cache. See information about event 44 in the Event Descriptions Reference Guide and information about the `clear cache` command in the CLI Reference Guide.
- If the system’s health is Fault, firmware update will not proceed. Before you can update firmware, you must resolve the problem specified by the Health Reason value on the System Overview panel (page 235).

### Updating controller-module firmware

A controller enclosure can contain one or two controller modules. In a dual-controller system, both controllers should run the same firmware versions. Storage systems in a replication set must 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.

If you have a dual-controller system and the Partner Firmware Update (PFU) option is enabled, when you update one controller the system automatically updates the partner controller. If PFU is disabled, after updating firmware on one controller you must log into the partner controller’s IP address and perform this firmware update on that controller also. For information about how to disable or re-enable PFU, using the `set advanced-settings` CLI command, see the CLI Reference Guide.

For best results, the storage system should be in a healthy state before starting firmware update.

**NOTE:** For information about supported releases for firmware update, see the product’s Release Notes.

### To update controller-module firmware

1. Obtain the appropriate firmware file and download it to your computer or network.
2. If the storage system has a single controller, stop I/O to vdisks before starting the firmware update.
3. In the Configuration View panel, right-click the system and select **Tools > Update Firmware**. The table titled Current Controller Versions shows the currently installed versions.
4. Click the button and browse for the firmware file to install.
5. Click **Install Controller-Module Firmware File**. A dialog box shows 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 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 attached enclosures, allow additional time for each expansion module's enclosure management processor (EMP) to be updated. This typically takes 2.5 minutes for each EMP in a drive enclosure.

   If the Storage Controller cannot be updated, the update operation is cancelled. 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 Management Controller will restart. Until the restart is complete, the RAIDar Sign In page will say that the system is currently unavailable. When this message is cleared, you may sign in.

   If PFU is enabled, allow 10–20 minutes for the partner controller to be updated.
6. Clear your web browser's cache, then sign in to RAIDar. 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:** After firmware update has completed on both controllers, 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 and drawer firmware

A drive enclosure can contain one or two expansion modules. Each expansion module contains an enclosure management processor (EMP). In an enclosure with drawers, each drawer contains two EMPs, which are also referred to as "modules." All modules of the same product model should run the same firmware version.

Expansion-module and drawer firmware is updated in either of two ways:

- When you update controller-module firmware, all expansion-module and drawer EMPs are automatically updated to a compatible firmware version.
- You can update the firmware in each expansion-module and drawer EMP by loading a firmware file obtained from the enclosure vendor.

### To update expansion-module and drawer firmware

1. Obtain the appropriate firmware file and download it to your computer or network.
2. If the storage system has a single controller, stop I/O to vdisks before starting the firmware update.
3. In the Configuration View panel, right-click the system and select **Tools > Update Firmware**. The table titled Current Versions of All Expansion Modules (EMPs) shows the currently installed versions.
4. Select the modules and/or drawers to update.
5. Click the button and browse for the firmware file to install.
6. Click **Install Expansion-Module Firmware File**. 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 or drawer might become inoperative. If this occurs, contact technical support. The module's FRU 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.
7. Verify that each updated module and drawer has the correct firmware version.

## Updating disk firmware

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

Firmware update is supported for all disks, including FDE-capable disks (for AssuredSAN 4004 only).

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.

### To update disk firmware

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. 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.
4. In the Configuration View panel, right-click the system and select **Tools > Update Firmware**. The table titled Current Versions (Revisions) of All Disk Drives shows the currently installed versions.
5. Select the disks to update.
6. Click **Browse** and select the firmware file to install.
7. Click **Install Disk Firmware File**. A dialog box shows firmware-update progress.

   △ **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 occurs, contact technical support.

   It typically takes several minutes for the firmware to load. Wait for a message that the update has completed.
8. If the updated disks must be power cycled:
   a. Shut down both controllers. See "Restarting or shutting down controllers" (page 228).
   b. Power cycle all enclosures as described in your product's Setup Guide.
9. Verify that each disk has the correct firmware revision.

## Using the activity progress interface

The activity progress interface reports whether a firmware update operation is active and shows the progress through each step of the operation. When the update operation completes, status is presented that either indicates successful completion or indicates an error if the operation failed.

When the interface is enabled it is accessible at all times, except when an MC is restarting. The interface is accessed through an HTTP-based query to a specified MC or to both MCs. The content is presented in a unified way so that activity in both MCs in a dual-controller system can be accessed simultaneously.

Use of this interface will not interfere in any way with firmware update performed via RAIDar or FTP.

### To access the activity progress interface

1. Enable the Activity Progress Monitor service. See "Changing management interface settings" (page 176).
2. In a new tab in your web browser, enter a URL of the form:

   `http://`*`controller-address`*`:8081/cgi-bin/content.cgi?mc=`*`MC-identifier`*`&refresh=true`

   where:
   - *`controller-address`* is required and specifies the IP address of a controller network port.
   - `mc=`*`MC-identifier`* is an 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` is an 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.

### Activity progress output

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

**Table 28 Activity progress properties and values (v2)**

| 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.<br>• ACTIVE: The operation for this component is currently active and in progress.<br>• OK: The operation for this component completed successfully and is now inactive.<br>• N/A: The operation for this component was not completed because it was not applicable.<br>• ERROR: The operation for this component failed with an error (see code and message). |

**Table 28 Activity progress properties and values (v2)**

| Property | Value |
|---|---|
| Code | A numeric code indicating the status.<br>• 0: The operation for this component completed with a “completed successfully” status.<br>• 1: The operation for this component was not attempted because it is not applicable (the component doesn’t exist or doesn’t need updating).<br>• 2: The operation is in progress. The other properties will indicate the progress item (message, current, total, percent).<br>• 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. |

# Saving logs

To help service personnel diagnose a system problem, you might be asked to provide system log data. Using RAIDar, you can save log data to a compressed zip file. The file will contain the following data:

- 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

**NOTE:** The controllers share one memory buffer for gathering log data and for loading firmware. Do not try to perform more than one save-logs operation at a time, or to perform a firmware-update operation while performing a save-logs operation.

### To save logs

1. In the Configuration View panel, right-click the system and select **Tools > Save Logs**.
2. In the main panel:
   a. Enter your name, email address, and phone number so support personnel will know who provided the log data. Each value can include a maximum of 100 bytes, using all characters except the following: " < > \
   b. Enter comments that describe the problem and specify the date and time when the problem occurred. This information helps service personnel when they analyze the log data. Each comment can include a maximum of 500 bytes, using all characters except the following: " < > \
3. Click **Save Logs**.

**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.

Log data is collected, which takes several minutes.

4. When prompted to open or save the file, click **Save**.
   - If you are using Firefox and have a download directory set, the file `store.zip` is saved there.
   - 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:** Because the file is compressed, you must uncompress it before you can view the files it contains. To examine diagnostic data, first view `store_yyyy_mm_dd__hh_mm_ss.logs`.

# Resetting a host port

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 (channels).

For FC, you can reset a single port. For an FC host port configured to use FC-AL (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 (either the first and second ports or the third and fourth ports). Resetting a SAS host port issues a `COMINIT/COMRESET` sequence and might reset other ports.

### To reset a host port

1. In the Configuration View panel, right-click the system and select **Tools > Reset Host Port**.
2. Select the port or port pair to reset.
3. Click **Reset Host Port**.

# Rescanning disk channels

A rescan forces a rediscovery of disks and enclosures in the storage system. If both Storage Controllers are online and able to communicate with both expansion modules in each connected enclosure, rescan rebuilds the internal SAS layout information, reassigns enclosure IDs of attached enclosures based on controller A's enclosure cabling order, and ensures that the enclosures are displayed in the proper order. A manual rescan temporarily pauses all I/O processes, then resumes normal operation. It can take up to two minutes for the enclosure IDs to be corrected. For further cabling information, refer to your product's Setup Guide.

A manual rescan may be needed after system power-up to display enclosures in the proper order. Whenever you replace a drive chassis or controller chassis, perform a manual rescan to force fresh discovery of all drive enclosures connected to the controller enclosure.

A manual rescan is not needed after inserting or removing 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.

### To rescan disk channels

1. Verify that both controllers are operating normally.
2. In the Configuration View panel, right-click the system and select **Tools > Rescan Disk Channels**.
3. Click **Rescan**.

# Restoring system defaults

If the system is not working properly and you cannot determine why, you can restore its default configuration settings. You then can reconfigure the settings that are necessary to use the system.

To restore defaults, use the CLI's `restore defaults` command, as described in the CLI Reference Guide.

# Clearing disk metadata

**CAUTION:**

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

Each disk in a vdisk has metadata that identifies the owning vdisk, the other members of the vdisk, and the last time data was written to the vdisk. The following situations cause a disk to become a *leftover*:

- Vdisk members' 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.

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

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

If spares are available, and the health of the vdisk is Degraded, the vdisk 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 How Used state to AVAIL, making the disk available for use in a new vdisk or as a spare.

If spares are not available to begin reconstruction, or reconstruction has not completed, keep the leftover disk so that you'll 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.

### To clear metadata from leftover disks

1. In the Configuration View panel, right-click the system and then select **Tools > Clear Disk Metadata**.
2. In the main panel, select leftover disks to clear metadata from. To select or clear all leftover disks, toggle the check box in the heading row.
3. Click **Clear Metadata**. A confirmation dialog appears.
4. Click **Continue** to continue. Otherwise, click **Cancel**. If you clicked Continue, a processing dialog appears. If the task succeeds, a success dialog appears.
5. Click **OK**.

# Restarting or shutting down controllers

You can restart the processors in a controller module when RAIDar informs you that you have changed a configuration setting that requires restarting or when the controller is not working properly. Shut down the processors in a controller module before you remove it from an enclosure, or before you power off its enclosure for maintenance, repair, or a move.

A restart can be performed on either the Storage Controller processor or the Management Controller processor. A shut down affects both processors.

## Restarting

If you restart a Storage Controller, it attempts to shut down with a proper failover sequence, which includes stopping all I/O operations and flushing the write cache to disk, and then the Storage Controller restarts. Restarting a Storage Controller restarts the corresponding Management Controller.

If you restart a Management Controller, communication with it is lost until it successfully restarts. If the restart fails, the partner Management Controller remains active with full ownership of operations and configuration information.

△ **CAUTION:** If you restart both Storage Controllers, both Management Controllers will also be restarted so all users will lose access to the system and its data until the restart is complete.

**NOTE:** When a Storage Controller is restarted, live performance statistics that it recorded will be reset. Historical performance statistics are not affected. In a dual-controller system, disk statistics may be reduced but will not be reset to zero, because disk statistics are summed between the two controllers. For more information, see help for commands that show statistics.

### To perform a restart

1. In the Configuration View panel, right-click the local system and select **Tools > Shut Down or Restart Controller**.
2. In the main panel, set the options:
   - Operation. Select **Restart**.
   - Controller Type. Select the type of controller processor to restart: **Management** or **Storage**.
   - Controller. Select the controller to restart: **A**, **B**, or **Both**.
3. Click **Restart now**. A confirmation dialog appears.
4. Click **Yes** to continue. Otherwise, click **No**. If you clicked Yes, a second confirmation dialog appears.
5. Click **Yes** to continue. Otherwise, click **No**. If you clicked Yes, a message describes restart activity.

## Shutting down

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 the Storage Controller in both controller modules is shut down, hosts cannot access the system's data. Perform a shut down before removing a controller module or powering down the system.

△ **CAUTION:** You can continue to use the CLI when either or both Storage Controllers are shut down, but information shown might be invalid.

### To perform a shut down

1. In the Configuration View panel, right-click the local system and select **Tools > Shut Down or Restart Controller**.
2. In the main panel, set the options:
   - Operation. Select **Shut down**.
   - Controller. Select the controller to shut down: **A**, **B**, or **Both**.
3. Click **Shut down now**. A confirmation dialog appears.
4. Click **Yes** to continue. Otherwise, click **No**. If you clicked Yes, a second confirmation dialog appears.
5. Click **Yes** to continue. Otherwise, click **No**. If you clicked Yes, a message describes shutdown activity.

## Testing notifications

You can send test messages to verify that email, SNMP, and/or syslog settings are properly configured for destinations to receive event notifications and managed-logs notifications.

For event notification, the email, SNMP, or syslog settings must include a notification level other than "none (disabled)." For managed-logs notification, the managed logs feature must be configured and enabled. For an overview of the log-management feature, see "About managed logs" (page 165).

### To test event notification

1. In the Configuration View panel, right-click the local system and select **Tools > Test Event Notifications and Managed Logs**.
2. Under the Test Event Notifications heading, click **Send Event**. If the task succeeds, verify that the test message reached the destinations.

### To test managed-logs notification

1. In the Configuration View panel, right-click the local system and select **Tools > Test Event Notifications and Managed Logs**.
2. Under the Test Managed Logs Notifications heading, click **Send Managed Logs**. If the task succeeds, verify that the test message reached the destination.

## Expanding a vdisk

You can expand the capacity of a vdisk by adding disks to it, up to the maximum number of disks that the storage system supports. Host I/O to the vdisk can continue while the expansion proceeds. You can then create or expand a volume to use the new free space, which becomes available when the expansion is complete. You can expand only one vdisk at a time. As described in "About RAID levels" (page 160), the RAID level determines whether the vdisk can be expanded and the maximum number of disks the vdisk can have. This task cannot be performed on an NRAID or RAID-1 vdisk.

Vdisks 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). To identify the sector format for a disk, in the Configuration View panel, right-click an enclosure and select **View > Overview**. Select a disk and click the **Properties** tab to view the disk properties, including its sector format (512n or 512e). Vdisks support a mix of 512n and 512e disks.

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

**IMPORTANT:** Expansion can take hours or days to complete, depending on the vdisk'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 vdisk.

### Before expanding a vdisk

Back up the vdisk's data so that if you need to stop expansion and delete the vdisk, you can move the data into a new, larger vdisk.

### To expand a vdisk

1. In the Configuration View panel, right-click a vdisk and select **Tools > Expand Vdisk**. Information appears about the selected vdisk and all disks in the system.
   - In the Disk Selection Sets table, the number of white slots in the vdisk's Disks field shows how many disks you can add to the vdisk.
   - In the enclosure view or list, only suitable available disks are selectable.
2. Select disks to add.
3. Click **Expand Vdisk**. If your vdisk contains a mix of 512n and 512e disks, a warning dialog box displays.
4. Perform one of the following:
   - Click **Yes** to continue.
   - To cancel the request, click **No**.

   If you clicked Yes or your vdisk does not contain a mix of 512n and 512e disks, a processing dialog appears.
5. Click **OK**. The expansion's progress is shown in the **View > Overview** panel.

## Verifying a vdisk

If you suspect that a fault-tolerant (mirror or parity) vdisk has a problem, run the Verify utility to check the vdisk's integrity. For example, if the storage system was operating outside the normal temperature range, verify its vdisks. The Verify utility analyzes the selected vdisk 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 mirror mismatches for RAID 1 and 10. This task can be performed only on a vdisk whose status is FTOL (fault tolerant and online). It cannot be performed for NRAID or RAID 0.

**TIP:** Media Scrub Vdisk (page 231) operates similarly to Verify Vdisk but can find and fix media errors for any RAID level, including NRAID and RAID 0.

Verification can last over an hour, depending on the size of the vdisk, the utility priority, and the amount of I/O activity. You can use a vdisk 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 vdisk is going bad. For information about identifying a failing disk, use the SMART option (see "Configuring SMART" (page 186).

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 it over.

### To verify a vdisk

1. In the Configuration View panel, right-click a fault-tolerant vdisk and select **Tools > Verify Vdisk**.
2. Click **Start Verify Utility**. A message confirms that verification has started.
3. Click **OK**. The panel shows the verification's progress.

### To abort vdisk verification

1. In the Configuration View panel, right-click a fault-tolerant vdisk and select **Tools > Verify Vdisk**.
2. Click **Abort Verify Utility**. A message confirms that verification has been aborted.
3. Click **OK**.

# Scrubbing a vdisk

The system-level Vdisk Scrub option (see “Configuring background scrub for vdisks” (page 193)) automatically checks all vdisks for disk defects. If this option is disabled, you can still perform a scrub on a selected vdisk. Scrub analyzes a vdisk to find and fix disk errors. It will fix parity mismatches for RAID 3, 5, 6, and 50; mirror mismatches for RAID 1 and 10; and media errors for all RAID levels.

Scrub can last over an hour, depending on the size of the vdisk, the utility priority, and the amount of I/O activity. However, a “foreground” scrub performed by Media Scrub Vdisk is typically faster than a background scrub performed by Vdisk Scrub. You can use a vdisk 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.

### To scrub a vdisk

1. In the Configuration View panel, right-click a vdisk and select **Tools > Media Scrub Vdisk**.
2. Click **Start Media Scrub Utility**. A message confirms that the scrub has started.
3. Click **OK**. The panel shows the scrub’s progress.

### To abort a vdisk scrub

1. In the Configuration View panel, right-click a vdisk and select **Tools > Media Scrub Vdisk**.

   **NOTE:** If the vdisk is being scrubbed but the Abort Media Scrub Utility button is grayed out, a background scrub is in progress. To stop the background scrub, disable the Vdisk Scrub option as described in “Configuring background scrub for vdisks” (page 193).

2. Click **Abort Media Scrub Utility**. A message confirms that the scrub has been aborted.
3. Click **OK**.

# Removing a vdisk from quarantine

△ **CAUTION:** Carefully read this topic to determine whether to use the Dequarantine Vdisk panel to manually remove a vdisk from quarantine. The Dequarantine Vdisk 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 vdisk is manually dequarantined and does not have enough disks to continue operation, its status will change to OFFL and its data may or may not be recoverable through use of the `trust` command. It is recommended that you contact technical support for assistance in determining if the recovery procedure that makes use of the Dequarantine Vdisk panel and the `trust` command is applicable to your situation and for assistance in performing it. Also, see the help for the `trust` command.

To continue operation (that is, not go to quarantined status), a RAID-3 or RAID-5 vdisk can have only one inaccessible disk; a RAID-6 vdisk can have only one or two inaccessible disks; a RAID-10 or RAID-50 vdisk can have only one inaccessible disk per sub-vdisk. For example, a 16-disk RAID-10 vdisk can remain online (critical) with 8 inaccessible disks if one disk per mirror is inaccessible.

The system will automatically quarantine a vdisk having a fault-tolerant RAID level if one or more of its disks becomes inaccessible, or to prevent invalid (“stale”) data that may exist in the controller from being written to the vdisk. 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 vdisk to prevent invalid data from being written to the vdisk. 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 vdisk 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 vdisk will be automatically dequarantined if the inaccessible disks come online and the vdisk status becomes FTOL (fault tolerant and online), or if after 60 seconds the vdisk status is QTCR or QTDN.
- During system operation, a vdisk loses redundancy plus one more disk. For example, three disks are inaccessible in a RAID-6 vdisk or two disks are inaccessible for other fault-tolerant RAID levels. The vdisk will be automatically dequarantined if after 60 seconds the vdisk status is FTOL, FTDN, or CRIT.

Quarantine isolates the vdisk from host access and prevents the system from changing the vdisk status to OFFL (offline). The number of inaccessible disks determines the quarantine status, from least to most severe:

- QTDN (quarantined with a down disk): The RAID-6 vdisk has one inaccessible disk. The vdisk is fault tolerant but degraded. If the inaccessible disks come online or if after 60 seconds from being quarantined the vdisk is QTCR or QTDN, the vdisk is automatically dequarantined.
- QTCR (quarantined critical): The vdisk is critical with at least one inaccessible disk. For example, two disks are inaccessible in a RAID-6 vdisk 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 vdisk is QTCR or QTDN, the vdisk is automatically dequarantined.
- QTOF (quarantined offline): The vdisk is offline with multiple inaccessible disks causing user data to be incomplete, or is an NRAID or RAID-0 vdisk.

When a vdisk 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 vdisk's volumes and volumes in other vdisks, quarantine may temporarily impact operation of those other volumes. For example, if the quarantined vdisk contains the snap pool used for snapshot, volume-copy, or replication operations, quarantine may temporarily cause the associated master volume to go offline. A volume-copy or replication operation can also be disrupted if an associated volume (snap pool, source volume, or destination volume) goes offline. Depending on the operation, the length of the outage, and the settings associated with the operation, the operation may automatically resume when the vdisk is dequarantined or may require manual intervention. A vdisk can remain quarantined indefinitely without risk of data loss.

A vdisk is dequarantined when it is brought back online, which can occur in three ways:

- If the inaccessible disks come online, making the vdisk FTOL, the vdisk is automatically dequarantined.
- If after 60 seconds from being quarantined the vdisk is QTCR or QTDN, the vdisk is automatically dequarantined. The inaccessible disks are marked as failed and the vdisk status changes to CRIT (critical) or FTDN (fault tolerant with a down disk). If the inaccessible disks later come online, they are marked as LEFTOVR (leftover).
- The dequarantine command is used to manually dequarantine the vdisk. If the inaccessible disks later come online, they are marked as LEFTOVR (leftover). If event 485 was logged, use the dequarantine command only as specified by the event's recommended-action text to avoid data corruption or loss.

A quarantined vdisk 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 vdisk power up. Check that all enclosures have restarted after a power failure. If these problems are found and then fixed, the vdisk recovers and no data is lost.

If the inaccessible disks cannot be restored (for example, they failed), and the vdisk'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 vdisk becomes quarantined. When the disk is found, the vdisk is dequarantined and reconstruction starts. If reconstruction was in process, it continues where it left off.

---

**NOTE:** The only tasks allowed for a quarantined vdisk are Dequarantine Vdisk and Delete Vdisk. If you delete a quarantined vdisk and its inaccessible disks later come online, the vdisk will reappear as quarantined or offline and you must delete it again (to clear those disks).

---

### To remove a vdisk from quarantine (if specified by the recommended action for event 172 or 485)

1. In the Configuration View panel, right-click a quarantined vdisk and select **Tools > Dequarantine Vdisk**.
2. Click **Dequarantine Vdisk**. Depending on the number of disks that remain active in the vdisk, its health might change to Degraded (RAID 6 only) and its status changes to FTOL, CRIT, or FTDN. For status descriptions, see "Vdisk properties" (page 244).

## Expanding a snap pool

By default, snap pools are configured to automatically expand when they become 90% full.

However, if a snap pool's policy is *not* set to Auto Expand and the snap pool is running out of free space, you can manually expand the snap pool.

For expansion to succeed, the vdisk must have free space and sufficient resources. Because expansion does not require I/O to be stopped, the snap pool can continue to be used during expansion.

### To expand a snap pool

1. In the Configuration View panel, right-click a snap pool and select **Tools > Expand Snap Pool**.
2. In the main panel, specify the amount of free space to add to the snap pool.
3. Click **Expand Snap Pool**. A message indicates whether the task succeeded or failed.
4. Click **OK**. If the task succeeds, the snap pool's size is updated in the Configuration View panel.

## Checking links to a remote system

After a remote system has been added, you can check the connectivity between host ports in the local system and the remote system. A host port in the local system can only link to other host ports with the same host interface, such as Fibre Channel (FC), in a remote system. When you check links, this panel will show this information for each linked host port in the local system:

- The link type
- The ID of the port in the local system
- The ID of each accessible port in the remote system

If a host port is not shown then either:

- It is not linked
- Its link type is not supported by both systems

### To check links to a remote system

1. In the Configuration View panel, right-click a remote system and select **Tools > Check Remote System Link**.
2. Click **Check Links**.

## Checking local system links

You can check the connectivity between host ports in both controllers in the local system. A host port can only link to other ports with the same host interface. When you check links, this panel will show this information for each linked host port in both controllers:

- The link type
- The port ID
- The ID of each linked port in the local system

### To check links in the local system

1. In the Configuration View panel, right-click the local system and select **Tools > Check Local System Link**.
2. Click **Check Links**.

# Resetting or saving historical disk-performance statistics

## Resetting historical disk-performance statistics

You can reset (clear) all historical performance statistics for all disks. When you reset historical statistics, an event will be logged and new data samples will continue to be stored every quarter hour.

### To reset historical disk performance statistics

1. In the Configuration View panel, right-click the local system and select **Tools > Reset or Save Disk Performance Statistics**.
2. In the main panel, under the Reset Disk Performance Statistics heading, click **Reset**. A confirmation dialog appears.
3. Click **Yes** to continue. Otherwise, click **No**. If you clicked Yes, a processing dialog appears. When processing is complete a success dialog appears.
4. Click **OK**.

## Saving historical disk-performance statistics

You can download historical disk-performance statistics for all disks in the storage system. This task 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 CLI Reference Guide.

```
"sample-time","durable-id","serial-number","number-of-ios", ...
"2012-01-18 01:00:00","disk_1.1","PLV2W1XE","2467917", ...
"2012-01-18 01:15:00","disk_1.1","PLV2W1XE","2360042", ...
...
```

### To save historical disk-performance statistics

1. In the Configuration View panel, right-click the local system and select **Tools > Reset or Save Disk Performance Statistics**.
2. In the main panel, under the Save Disk Performance Statistics heading, specify start and end dates and times to define the range of performance data to retrieve.
3. Click **Save**.

> **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 Reset or Save Disk Performance Statistics panel and retry the save operation.

4. When prompted to open or save the file, click **Save**.
   - If you are using Firefox 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.

# 15 Viewing system status

## Viewing information about the system

In the Configuration View panel, right-click the system and select **View > Overview**. The System Overview table shows:

- Health.
  - OK
  - Degraded
  - Fault
  - N/A
  - Unknown
- Component. System, Enclosures, Disks, Vdisks, Volumes, Schedules, Configuration Limits, Versions, Snap Pools, Snapshots, Licensed Features.
- Count.
- Capacity.
- Storage Space. For descriptions of storage-space color codes, see "About storage-space color codes" (page 163).

Select a component to see more information about it.

---

**NOTE:** If the system is not working properly and you cannot determine why, you can restore its default configuration settings. You then can reconfigure the settings that are necessary to use the system. To restore defaults, in the CLI, use the `restore defaults` command, as described in the CLI Reference Guide.

---

## System properties

When you select System in the System Overview table, two tables display information about the system.

The System Information table shows:

- Health.
  - OK
  - Degraded
  - Fault
  - N/A
  - Unknown
- Health Reason. If the system's health is not OK, its Health Reason specifies that a subcomponent is unhealthy. In the System Overview table, notice which other components are unhealthy and view their properties as described in the following sections.
- System Name. User-defined system name.
- System Contact. User-defined system contact.
- System Location. User-defined system location.
- System Information. User-defined description of the system.
- Vendor Name.
- Product ID.
- Product Brand.
- SCSI Vendor ID.
- SCSI Product ID.
- Supported Locales. Languages supported by the system.

- FDE Security Status (for AssuredSAN 4004 only).
  - Not Secured: The disk is not secured.
  - Unknown: The FDE state is unknown.
  - Not FDE Capable: The disk is not FDE-capable.
  - Secured, Unlocked: The system is secured and the disk is unlocked.
  - Secured, Locked: The system is secured and the disk is locked to data access, preventing its use.
  - FDE Protocol Failure: A temporary state that can occur while the system is securing the disk.

The System Redundancy table shows:

- Controller Redundancy Mode.
- Controller Redundancy Status.
- Controller A Status.
- Controller B Status.

## Enclosure properties

When you select Enclosures in the System Overview table, a table displays the following information for each enclosure:

- Health.
   OK
   Degraded
   Fault
   N/A
   Unknown

  If an enclosure's health is not OK, select it in the Configuration View panel to view details about it.
- Enclosure ID.
- Enclosure WWN.
- Vendor.
- Model.
- Number of Disks. The number of disks installed in the enclosure.

## Disk properties

When you select Disks in the System Overview table, a table shows:

- Health.
   OK
   Degraded
   Fault
   N/A
   Unknown

  If a disk's health is not OK, select it in the Configuration View panel to view details about it.
- Enclosure ID.
- Slot. The number of the slot the disk resides in.
- Serial Number.
- Vendor.
- Model.
- Revision.
- Type.

- SAS: Enterprise SAS.
- SAS MDL: Midline SAS.
- sSAS: SAS SSD

- How Used

  Two values are listed together: the first is How Used and the second is Current Job. For example, for a disk used in a vdisk (VDISK) that is being scrubbed (VRSC), VDISKVRSC displays.

  - How Used
    - AVAIL: Available.
    - FAILED: The disk is unusable and must be replaced. Reasons for this status include: excessive media errors; SMART error; disk hardware failure; unsupported disk.
    - GLOBAL SP: Global spare.
    - LEFTOVR: Leftover.
    - UNUSABLE: The disk cannot be used in a vdisk because the system is secured and the disk is not FDE-capable, or because the disk is locked to data access (for AssuredSAN 4004 only).
    - VDISK: Used in a vdisk.
    - VDISK SP: Spare assigned to a vdisk.
  - Current Job
    - DRSC: Disks in the vdisk are being scrubbed.
    - EXPD: The vdisk is being expanded.
    - INIT: The vdisk is being initialized.
    - RCON: The vdisk is being reconstructed.
    - VRFY: The vdisk is being verified.
    - VRSC: The vdisk is being scrubbed.

- Status.
  - 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.
  - Error: The disk is present but is 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.
- Size. Total size of the disk.
- FDE State (for AssuredSAN 4004 only).
  - Not Secured: The disk is not secured.
  - Unknown: The FDE state is unknown.
  - Not FDE-Capable: The disk is not FDE-capable.
  - Secured, Unlocked: The system is secured and the disk is unlocked.
  - Secured, Locked: The system is secured and the disk is locked to data access, preventing its use.
  - FDE Protocol Failure: A temporary state that can occur while the system is securing the disk.

If there are no disks in the system, the table displays no data.

## Vdisk properties

When you select Vdisks in the System Overview table, a table displays the following information for each vdisk:

- Health.

  OK

  Degraded

  Fault

  N/A

  Unknown

  If a vdisk's health is not OK, select it in the Configuration View panel to view details about it.
- Name. Vdisk name.
- Size. Total size of the vdisk.
- Free. Amount of free space remaining on the vdisk.
- RAID. RAID level.
- Status.
  - CRIT: Critical. The vdisk is online but isn't fault tolerant because some of its disks are down.
  - DMGD: Damaged. The vdisk is online and fault tolerant, but some of its disks are damaged.
  - FTDN: Fault tolerant with down disks. The vdisk is online and fault tolerant, but some of its disks are down.
  - FTOL: Fault tolerant and online.
  - MSNG: Missing. The vdisk is online and fault tolerant, but some of its disks are missing.
  - OFFL: Offline. Either the vdisk is using offline initialization, or its disks are down and data may be lost.
  - QTCR: Quarantined critical. The vdisk is critical with at least one inaccessible disk. For example, two disks are inaccessible in a RAID-6 vdisk 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 vdisk is QTCR or QTDN, the vdisk is automatically dequarantined.
  - QTDN: Quarantined with a down disk. The RAID-6 vdisk has one inaccessible disk. The vdisk is fault tolerant but degraded. If the inaccessible disks come online or if after 60 seconds from being quarantined the vdisk is QTCR or QTDN, the vdisk is automatically dequarantined.
  - QTOF: Quarantined offline. The vdisk is offline with multiple inaccessible disks causing user data to be incomplete, or is an NRAID or RAID-0 vdisk.
  - STOP: The vdisk is stopped.
  - UNKN: Unknown.
  - UP: Up. The vdisk is online and does not have fault-tolerant attributes
- Disk Type.
  - SAS: Enterprise SAS.
  - SAS MDL: Midline SAS.
  - sSAS: SAS SSD.

---

**NOTE:** In the Configuration View panel, if a vdisk contains more than one type of disk, its RAID-level label includes the suffix `-MIXED`.

---

If no vdisks exist, the table displays no data.

## Virtual Storage properties

When you select Virtual Storage in the System Overview table, the amount of storage created and managed through the user interface of the RAIDar virtual storage system displays in the Capacity column. For more information, see the explanation below the System Overview table or click the WBIv3 link to access the user interface.

## Volume properties

When you select Volumes in the System Overview table, a table displays the following information for each volume:

- Name.
- Serial Number.
- Size. Total size of the volume.
- Vdisk Name. The name of the vdisk the volume resides on.

If no volumes exist, the table displays no data.

## Schedule properties

When you select Schedules in the System Overview table, a table displays the following information for each schedule:

- Schedule Name.
- Schedule Specification. The start day and time of the schedule.
- Status. Schedule status.
  - Uninitialized: Schedule is not yet ready to run.
  - Ready: Schedule is ready to run.
  - Suspended: Schedule is suspended.
  - Expired: Schedule has expired.
  - Invalid: Schedule is invalid.
  - Deleted: Schedule has been deleted.
- Next Time. The next time the task is scheduled to run.
- Task Type. Type of task assigned to run.
- Status. Task status.
  - Uninitialized: Task is not yet ready to run.
  - Ready: Task is ready to run.
  - Active: Task is running.
  - Error: Task has an error.
  - Invalid: Task is invalid.
  - Complete: Task is complete.
  - Deleted: Task has been deleted.
- Task State. Specific information about task type.

When you select a schedule, two tables display: the Schedule Details table and the Task Details table.

The Schedule Details table displays specifics about the schedule:

- Schedule Name.
- Schedule Specification. The start day and time of the schedule.
- Status.
  - Uninitialized: Schedule is not yet ready to run.
  - Ready: Schedule is ready to run.
  - Suspended: Schedule is suspended.

    - Expired: Schedule has expired.
    - Invalid: Schedule is invalid.
    - Deleted: Schedule has been deleted.
- Next Time. The next time the task is scheduled to run.

The Task Details table displays specifics about the task for the selected schedule:

- Task Name.
- Task Type. Type of task assigned to run.
- Status.
    - Uninitialized: Task is not yet ready to run.
    - Ready: Task is ready to run.
    - Active: Task is running.
    - Error: Task has an error.
    - Invalid: Task is invalid.
    - Complete: Task is complete.
    - Deleted: Task has been deleted.
- Task State. Specific information about task type.

When you select a task of type TakeSnapshot, a third table displays. The Retained Set table shows the name and serial number of each snapshot that the task has created and that is being retained.

If no schedules exist, the table displays no data.

To modify or delete scheduled tasks to suspend (disable) and resume (re-enable) DSD, use the Advanced Settings Disk panel. See “Scheduling drive spin down for all disks” (page 187).

## Configuration limits

When you select Configuration Limits in the System Overview table, a table shows the Maximum Vdisks, Maximum Volumes, Maximum LUNs, Maximum Disks, and Number of Host Ports that the system supports. For a summary of the physical and logical limits of the storage system, see the system configuration limits topic in RAIDar help.

## Version properties

When you select Versions in the System Overview table, a table shows the versions of firmware and hardware in each controller module.

- Storage Controller CPU Type.
- Bundle Version.
- Build Date.
- Storage Controller Code Version.
- Storage Controller Code Baselevel.
- Memory Controller FPGA Code Version.
- Storage Controller Loader Code Version.
- CAPI Version.
- Management Controller Code Version.
- Management Controller Loader Code Version.
- Expander Controller Code Version.
- CPLD Code Version.
- Hardware Version.
- Host Interface Module Version.

- Host Interface Module Model.
- Backplane Type.
- Host Interface Hardware (Chip) Version.
- Disk Interface Hardware (Chip) Version.
- SC Boot Memory Reference Code.

### Snap-pool properties

When you select Snap Pools in the System Overview table, a table shows each snap pool's name, serial number, size, free space, master volumes, snapshots, and vdisk name.

If no snap pools exist, the table displays no data.

### Snapshot properties

When you select Snapshots in the System Overview table, a table shows each snapshot's name; serial number; source volume; snap-pool name; amounts of snap data, unique data, and shared data; and vdisk name.

- Snap data is 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).
- Unique data is the amount of data that has been written to the snapshot since the last snapshot was taken. If the snapshot has not been written or is deleted, this value is zero bytes.
- Shared data is the amount of data that is potentially shared with other snapshots and the associated amount of space that will be freed if the snapshot is deleted. This represents the amount of data written directly to the snapshot. It also includes data copied from the source volume to the storage area for the oldest snapshot, since that snapshot does not share data with any other snapshot. For a snapshot that is not the oldest, if the modified data is deleted or if it had never been written to, this value is zero bytes.

If no snapshots exist, the table displays no data.

## Viewing the system event log

In the Configuration View panel, right-click the system and select **View > Event Log**. The System Events panel shows the 100 most recent events that have been logged by either controller. All events are logged, regardless of event-notification settings. Click the buttons above the table to view all events, or only critical, warning, or informational events.

The event log table shows the following information:

- Severity.

  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 status for a condition that caused an event to be logged that is now resolved.
- Time. Date and time when the event occurred, shown as *year-month-day hour:minutes:seconds*. Time stamps have one-second granularity.
- Event ID. An identifier for the event. The prefix A or B identifies the controller that logged the event.
- Code. An event code that helps you and support personnel diagnose problems. For event-code descriptions and recommended actions, see the Event Descriptions Reference Guide.
- Message. Brief information about the event. Click the message to show or hide additional information and recommended actions.

**NOTE:** If you are having a problem with the system or a vdisk, check the event log before calling technical support. Event messages might enable you to resolve the problem.

When reviewing events, do the following:

1. For any critical, error, or warning events, click the message to view additional information and recommended actions. This information also appears in the Event Descriptions Reference Guide.

   Identify the primary events and any that might be the cause of the primary event. For example, an over-temperature event could cause a disk failure.
2. View the event log and locate other critical/error/warning events in the sequence for the controller that reported the event.

   Repeat this step for the other controller if necessary.
3. Review the events that occurred before and after the primary event.

   During this review you are looking for any events that might indicate the cause of the critical/error/warning event. You are also looking for events that resulted from the critical/error/warning event, known as secondary events.
4. Review the events following the primary and secondary events.

   You are looking for any actions that might have already been taken to resolve the problems reported by the events.

## Viewing information about all vdisks

In the Configuration View panel, right-click **Vdisks** and select **View > Overview**. The Vdisks Overview table shows:

- Health.
  - OK
  - Degraded
  - Fault
  - N/A
  - Unknown
- Component.
- Count. Number of components.
- Capacity. Total capacity of the component.
- Storage Space. Amount of space on the component. For descriptions of storage-space color codes, see “About storage-space color codes” (page 163).

The Vdisks table shows more information about each vdisk.

- Health.
- Name. Vdisk name.
- Size. Total storage space in the vdisk.
- Free. Available space in the vdisk.
- RAID. RAID level of the vdisk and all of its volumes.
- Status.
  - CRIT: Critical. The vdisk is online but isn’t fault tolerant because some of its disks are down.
  - DMGD: Damaged. The vdisk is online and fault tolerant, but some of its disks are damaged.
  - FTDN: Fault tolerant with a down disk. The vdisk is online and fault tolerant, but some of its disks are down.
  - FTOL: Fault tolerant and online.
  - MSNG: Missing. The vdisk is online and fault tolerant, but some of its disks are missing.
  - OFFL: Offline. Either the vdisk is using offline initialization, or its disks are down and data may be lost.

    - QTCR: Quarantined critical. The vdisk is critical with at least one inaccessible disk. For example, two disks are inaccessible in a RAID-6 vdisk 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 vdisk is QTCR or QTDN, the vdisk is automatically dequarantined.
    - QTDN: Quarantined with a down disk. The RAID-6 vdisk has one inaccessible disk. The vdisk is fault tolerant but degraded. If the inaccessible disks come online or if after 60 seconds from being quarantined the vdisk is QTCR or QTDN, the vdisk is automatically dequarantined.
    - QTOF: Quarantined offline. The vdisk is offline with multiple inaccessible disks causing user data to be incomplete, or is an NRAID or RAID-0 vdisk.
    - STOP: The vdisk is stopped.
    - UNKN: Unknown.
    - UP: Up. The vdisk is online and does not have fault-tolerant attributes.
- Disk Type.
    - SAS: Enterprise SAS.
    - SAS MDL: Midline SAS.
    - sSAS: SAS SSD.
- Preferred Owner. Controller that owns the vdisk and its volumes during normal operation.
- Current Owner. Either the preferred owner during normal operation or the partner controller when the preferred owner is offline.
- Disks. Quantity of disks in the vdisk.
- Spares. Quantity of dedicated spares in the vdisk.

## Viewing information about a vdisk

In the Configuration View panel, right-click a vdisk and select **View > Overview**. The Vdisks Overview table shows:

- Health.
   OK
   Degraded
   Fault
   N/A
   Unknown
- Component. Vdisk, disks, volumes.
- Count.
- Capacity.
- Storage Space. For descriptions of storage-space color codes, see “About storage-space color codes” (page 163).

Select a component to see more information about it. When the Vdisk component is selected, you can view properties or historical performance statistics.

---

**NOTE:** Failure of a disk in the vdisk causes the Vdisk and Disks components to have Degraded health. Because tables displayed when the Disks component is selected exclude failed disks, those tables will show fewer disks than the Disk component’s Count value.

---

## Vdisk properties

When you select Vdisk in the Vdisk Overview table and click the **Properties** tab, the Properties for *Vdisk* table shows:

- Health.
  - OK
  - Degraded
  - Fault
  - N/A
  - Unknown
- Health Reason. If Health is not OK, this field shows the reason for the health state.
- Health Recommendation. If Health is not OK, this field shows recommended actions to take to resolve the health issue.
- Name. Vdisk name.
- Size. Total storage space in the vdisk.
- Free. Available space in the vdisk.
- Current Owner. Either the preferred owner during normal operation or the partner controller when the preferred owner is offline.
- Preferred Owner. Controller that owns the vdisk and its volumes during normal operation.
- Serial Number. Vdisk serial number.
- RAID. RAID level of the vdisk and all of its volumes.
- Disks. Quantity of disks in the vdisk.
- Spares. Quantity of dedicated spares in the vdisk.
- Chunk Size.
  - For RAID levels except NRAID, RAID 1, and RAID 50, the configured chunk size for the vdisk.
  - For NRAID and RAID 1, chunk size has no meaning and is therefore shown as not applicable (N/A).
  - For RAID 50, the vdisk chunk size calculated as: *configured-chunk-size* x (*subvdisk-members* - 1). For a vdisk configured to use 32-KB chunk size and 4-disk sub-vdisks, the value would be `96k` (32KB x 3).
- Created. Date and time when the vdisk was created.
- Minimum Disk Size. Capacity of the smallest disk in the vdisk.
- Status.
  - CRIT: Critical. The vdisk is online but isn't fault tolerant because some of its disks are down.
  - DMGD: Damaged. The vdisk is online and fault tolerant, but some of its disks are damaged.
  - FTDN: Fault tolerant with a down disk. The vdisk is online and fault tolerant, but some of its disks are down.
  - FTOL: Fault tolerant and online.
  - MSNG: Missing. The vdisk is online and fault tolerant, but some of its disks are missing.
  - OFFL: Offline. Either the vdisk is using offline initialization, or its disks are down and data may be lost.
  - QTCR: Quarantined critical. The vdisk is critical with at least one inaccessible disk. For example, two disks are inaccessible in a RAID-6 vdisk 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 vdisk is QTCR or QTDN, the vdisk is automatically dequarantined.
  - QTDN: Quarantined with a down disk. The RAID-6 vdisk has one inaccessible disk. The vdisk is fault tolerant but degraded. If the inaccessible disks come online or if after 60 seconds from being quarantined the vdisk is QTCR or QTDN, the vdisk is automatically dequarantined.
  - QTOF: Quarantined offline. The vdisk is offline with multiple inaccessible disks causing user data to be incomplete, or is an NRAID or RAID-0 vdisk.
  - STOP: The vdisk is stopped.

    - UNKN: Unknown.
    - UP: Up. The vdisk is online and does not have fault-tolerant attributes.
- Current Job. If a utility is running on the vdisk, this field shows the utility's name and progress.
    - Disk Scrub: Disks in the vdisk are being scrubbed.
    - Expand: The vdisk is being expanded.
    - Initialize: The vdisk is being initialized.
    - Media Scrub: The vdisk is being scrubbed.
    - Reconstruct: The vdisk is being reconstructed.
    - Verify: The vdisk is being verified.
    - Virtual Drain: The virtual disk group is being drained.
    - Virtual Prepare: The virtual disk group is being prepared.
- Active Drive Spin Down Enable. Shows whether drive spin down is enabled or disabled for this vdisk.
- Sector Format.
    - 512n (512-byte native sector size).
    - 512e (512-byte emulated sector size).

A second table displays information about unhealthy components. If all components are healthy, this table displays the text, "There is no data for your selection."

---

**NOTE:** In the Configuration View panel, if a vdisk contains more than one type of disk, its RAID-level label includes the suffix `-MIXED`.

---

## Vdisk performance

When you select Vdisk in the Vdisk Overview table and click the **Performance** tab, the Performance Statistics panel shows three graphs of historical performance statistics for the vdisk: Data Transferred, Data Throughput, and Average Response Time. Data samples are taken every quarter hour and the graphs represent up to 50 samples.

To specify a time range of samples to display, set the start and end values and click **Update**. The system determines whether the number of samples in the time range exceeds the number of samples that can be displayed (50), requiring aggregation. To determine this, the system divides the number of samples in the specified time range by 50, giving a quotient and a remainder. If the quotient is 1, the 50 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 50 so all 4 samples are displayed.
- Example 2: A 15-hour range includes 60 samples. 60 divided by 50 gives a quotient of 1 and a remainder of 10. Therefore, the newest 50 samples will be displayed and the oldest 10 samples will be excluded.
- Example 3: A 30-hour range includes 120 samples. 120 divided by 50 gives a quotient of 2 and a remainder of 20. Therefore, each two newest samples will be aggregated into one sample for display and the oldest 20 samples will be excluded.

If aggregation is required, the system aggregates samples for each disk in the vdisk (as described in "Disk performance" (page 259)) and then aggregates the resulting values as follows:

- For a count statistic such as data transferred, the aggregated values are added to produce the value of the aggregated sample.
- For a rate statistic such as data throughput, the aggregated values are added and then are divided by their combined interval (seconds per sample multiplied by the number of samples).

The system will change the time settings to match the times of the oldest and newest samples displayed. The graphs are updated each time you click either the Performance tab or the Update button.

- For the vdisk, the Data Transferred graph shows the amounts of data read and written and the combined total over the sampling time period. The base unit is bytes.
- For the vdisk, the Data Throughput graph shows the rates at which data are read and written and the combined total over the sampling time period. The base unit is bytes per second.
- For each disk in the vdisk, the Average Response Time graph shows the average response times for reads and writes over the sampling time period. The base unit is microseconds. To view the graph's legend, which identifies the color-coding for each disk, select **Show Legend**.

**TIP:** If you specify a time range, it is recommended to specify a range of 12 hours or less.

To view performance data for an individual disk, use the Enclosure Overview panel (page 255). To view live (non-historical) performance statistics for one more vdisks, in the CLI use the `show vdisk-statistics` command.

**NOTE:** Values for the amount of data transferred and for data throughput appear to be much higher in historical output than in live output. This is caused by a difference in the way that historical and live values are calculated.

Live values are calculated based on the vdisk as viewed from the controller cache perspective. In the live statistics, performance numbers are obtained by accounting for when data is written from cache to disk or is read from disk to cache.

Historical data is obtained by using the summation of the disk statistics for the disks in the vdisk. The historical vdisk data shows transfers to and from the disks in the vdisk that include the overhead of any RAID transfers as well as any host activity.

Because I/Os from the RAID engine are included, values for the historical data appear higher than the numbers for the live data.

## Disk properties

When you select Disks in the Vdisk Overview table, a Disk Sets table and enclosure view appear. The Disk Sets table shows:

- Total Space. Total storage space in the vdisk, followed by a color-coded measure of how the space is used.
- Type. For RAID 10 or RAID 50, the sub-vdisk that the disk is in; for other RAID levels, the disk's RAID level; or SPARE.
- Disk Type.
  - SAS: Enterprise SAS.
  - SAS MDL: Midline SAS.
  - sSAS: SAS SSD.
- Disks. Quantity of disks in the vdisk or sub-vdisk.
- Size. Total capacity of the disks in the vdisk or sub-vdisk.

The enclosure view has two tabs. The Tabular tab shows:

- Health.
   OK
   Degraded
   Fault
   N/A (if the disk is spun down)
   Unknown

  If the disk's health is not OK, view health details in the Enclosure Overview panel (page 255).
- Name. System-defined disk name using the format Disk-*enclosure-number.disk-slot-number*.

- Type.
  - SAS: Enterprise SAS.
  - SAS MDL: Midline SAS.
  - sSAS: SAS SSD.
- State. Shows how the disk is used:
  - AVAIL: Available
  - FAILED: The disk is unusable and must be replaced. Reasons for this status include: excessive media errors; SMART error; disk hardware failure; unsupported disk.
  - GLOBAL SP: Global spare
  - LEFTOVR: Leftover
  - UNUSABLE: The disk cannot be used in a vdisk because the system is secured and the disk is not FDE-capable, or because the disk is locked to data access.
  - VDISK: Used in a vdisk.
  - VDISK SP: Spare assigned to a vdisk.

  This also shows any job running on the disk:
  - DRSC: The disk is being scrubbed
  - EXPD: The vdisk is being expanded
  - INIT: The vdisk is being initialized
  - RCON: The vdisk is being reconstructed
  - VRFY: The vdisk is being verified
  - VRSC: The vdisk is being scrubbed
- Size. Disk capacity.
- Enclosure. Name of the enclosure containing the disk.
- Serial Number. Disk serial number.
- Status. Up (operational) or Not Present.

The Graphical tab shows the locations of the vdisk's disks in system enclosures and each disk's Health and State. If a disk belongs to the virtual storage system, "VIRTUAL POOL" will appear on it.

## Volume properties

When you select Volumes in the Vdisk Overview table, the Volumes table shows:

- Name. Volume name.
- Serial Number. Volume serial number.
- Size. Volume size.
- Vdisk Name. The name of the vdisk containing the volume.

## Snap-pool properties

When you select Snap Pools in the Vdisk Overview table, the Snap Pools table shows:

- The snap pool's name, serial number, size, and free space.
- The quantity of master volumes and snapshots associated with the snap pool.
- The name of the vdisk containing the snap pool.

# Viewing information about a volume

In the Configuration View panel, right-click a volume and select **View > Overview**. The Volume Overview table shows:

- Component. Volume, Maps, or Schedules.
- Count. The quantity of mappings for the volume.
- Capacity. The capacity of the volume.
- Storage Space. The space usage of the volume. For descriptions of storage-space color codes, see “About storage-space color codes” (page 163).
- Replication Addresses. The quantity of replication addresses for the volume.
- Replication Images. The quantity of replication images for the volume.

Select a component to see more information about it.

## Volume properties

When you select Volume in the Volume Overview table, the Properties for *Volume* table shows:

- Vdisk Name. Name of the vdisk that the volume is in.
- Name. Volume name.
- Size. Volume size.
- Preferred Owner. Controller that owns the vdisk and its volumes during normal operation.
- Current Owner. Either the preferred owner during normal operation or the partner controller when the preferred owner is offline.
- Serial Number. Volume serial number.
- Cache Write Policy. Write-back or Write-through. See “Using write-back or write-through caching” (page 155).
- Read Ahead Size. See “Optimizing read-ahead caching” (page 156).
- Type. Standard volume, master volume, or snapshot.
- Progress. If the volume is being created by a volume-copy operation, the percent complete.
- Health. OK, Degraded, Fault, or Unknown.

  Health Reason. If Health is not OK, this field shows the reason for the health state.
- Health Recommendation. If Health is not OK, this field shows the recommended actions to take to resolve the health issue.

For a *local* primary or secondary volume, the Replication Properties for Volume table shows:

- Name. Replication volume name.
- Serial Number. Replication volume serial number.
- Status. Replication volume status:
  - Initializing: The initial (full) replication to the volume is in progress.
  - Online: The volume is online and is consistent with the last replicated image.
  - Inconsistent: The volume is online but is in an inconsistent state. A full replication is required to initialize it.
  - Replicating: The volume is online and replication is in progress.
  - Replicate-delay: The volume is online but the in-progress replication has been temporarily delayed. A retry is occurring.
  - Suspended: The volume is online but the in-progress replication has been suspended.
  - Offline: The volume cannot be accessed or is unusable due to an error.
  - Establishing proxy: The volume is establishing a proxy connection to a remote volume. This will occur when a detached secondary volume is reattached and is re-establishing a connection with the primary system in preparation for replication.
  - Detached: The volume is detached for removal.

- Status-Reason. More information about the status value, or N/A for Online status.
- Monitor. Replication volume monitoring status:
  - OK: Communication to the remote volume is successfully occurring on the FC or iSCSI network.
  - Failed: Communication to the remote volume has failed because of an FC or iSCSI network issue or because the remote volume has gone offline.
- Location. Local or Remote.
- Primary Volume Name. Primary volume name. If the replication set has a primary-volume conflict, all associated primary volumes are displayed.
- Primary Volume Serial Number. Primary volume serial number. If the replication set has a primary-volume conflict, all associated primary volumes are displayed.
- Primary Volume Status. Primary volume status: Online, Offline, Conflict, or N/A.
- Maximum Number of Queued Images. Number of replication images to consider when determining the next image to replicate. Used only if the On Collision parameter is set to Oldest.
- Maximum Retry Time (Seconds). Amount of time in seconds that the replication volume should retry a replication operation on any specific image when errors occur. Used only if the On Error parameter is set to Retry.
- On Error. Error policy to invoke when errors occur during the replication process: Retry or Suspend.
- Link Type. Type of ports used to link the primary and secondary volumes: FC or iSCSI.
- On Collision. Collision policy used to determine the next image to replicate when multiple replication images are queued: Newest or Oldest.
- Monitor Interval. Interval in seconds at which the primary volume should query the secondary volume.
- Priority. Priority of the replication process on the replication volume: Low, Medium, or High.
- Connection Status.
  - Not Attempted. Communication has not been attempted to the remote volume.
  - Online. The volumes in the replication set have a valid connection but communication is not currently active.
  - Active. Communication is currently active to the remote volume.
  - Offline. No connection is available to the remote system.
- Connection Time. Date and time of the last communication with the remote volume, or N/A.

## Mapping properties

When you select Maps in the Volume Overview table, the Maps for *Volume* table shows:

- Type. Explicit or Default. Settings for an explicit mapping override the default mapping.
- Host ID. WWPN or IQN.
- Host Name. User-defined nickname for the host.
- Ports. Controller host ports through which the volume is mapped to the host.
- LUN. Volume identifier presented to the host.
- Access. Volume access type: read-write, read-only, no-access (masked), or not-mapped.

## Schedule properties

If any schedules exist for this volume, when you select the Schedules component, the Schedules table shows each schedule's name, specification, status, next run time, task type, task status, and task state. For the selected schedule, two tables appear.

The Schedule Details table shows:

- Schedule Name. Schedule name.
- Schedule Specification. The schedule's start time and recurrence or constraint settings.
- Status.
  - Uninitialized: Schedule is not yet ready to run.
  - Ready: Schedule is ready to run.
  - Suspended: Schedule is suspended.
  - Expired: Schedule has expired.
  - Invalid: Schedule is invalid.
  - Deleted: Schedule has been deleted.
- Next Time. The next time the associated task will run.

The Task Details table shows different properties depending on the task type. Properties shown for all task types are:

- Task Name. Task name.
- Task Type. ReplicateVolume, ResetSnapshot, TakeSnapshot, or VolumeCopy.
- Status.
  - Uninitialized: Task is not yet ready to run.
  - Ready: Task is ready to run.
  - Active: Task is running.
  - Error: Task has an error.
  - Invalid: Task is invalid.
  - Complete: Task is complete.
  - Deleted: Task has been deleted.
- Task State. Current step of task processing. Steps vary by task type.
- Source Volume. Name of the volume to snap, copy, or replicate.
- Source Volume Serial. Source volume serial number.
- Destination Vdisk. Name of the destination vdisk for a volume copy.
- Destination Vdisk Serial. Destination vdisk serial number.
- Prefix. Label that identifies snapshots, volume copies, or replication images created by this task.
- Count. Number of snapshots to retain with this prefix. When a new snapshot exceeds this limit, the oldest snapshot with the same prefix is deleted.
- Last Created. Name of the last snapshot, volume copy, or replication image created by the task.
- Last Used Snapshot. For a task whose replication mode is last-snapshot, the name of the last snapshot used for replication.
- Snapshot Name. Name of the snapshot to reset.
- Snapshot Serial. Snapshot serial number.
- Mode. Replication mode:
  - new-snapshot: Replicate a new snapshot of the primary volume.
  - last-snapshot: Replicate the most recent existing snapshot of the primary volume.

For a TakeSnapshot task, the Retained Set table shows the name and serial number of each snapshot that the task has taken and is retaining.

## Replication addresses

If any remote port addresses are associated with this volume, when you select the Replication Addresses component, the Replication Addresses table shows:

- Connected Ports.
  - For a remote primary or secondary volume, this field shows the IDs of up to two hosts ports in the local system that are connected to the remote system. If two ports are connected but only one is shown, this indicates that a problem is preventing half the available bandwidth from being used.
  - For a local primary or secondary volume, this field shows N/A.
- Remote Address. The address of each host port in the remote system through which the volume is accessible.

## Replication images

If any replication images exist for this volume, when you select the Replication Images component, the Replication Images table shows information about each image. For the selected image, the Replication Images table shows:

- Image Serial Number. Replication image serial number.
- Image Name. User-defined name assigned to the primary replication image.
- Snapshot Serial Number. Replication snapshot serial number associated with the image. The replication snapshot is associated with the replication volume specified in the request.
- Snapshot Name. Replication snapshot name associated with the image. For a secondary replication image, this value is not filled in until the replication is completed.
- Creation Date/Time. Date and time when the replication image was created on the replication volume.

# Viewing information about a snapshot

In the Configuration View panel, right-click a snapshot and select **View > Overview**. The Snapshot Overview table shows:

- The capacity and space usage of the snapshot
- The quantity of mappings for the snapshot
- The quantity of task schedules for the snapshot

For descriptions of storage-space color codes, see “About storage-space color codes” (page 163).

Select a component to see more information about it.

## Snapshot properties

When you select the Snapshot component, the Properties for Snapshot table shows:

- Name and serial number of the pool containing the snapshot
- Snapshot name, creation date/time, status, and status reason
- Source volume name
- Parent volume name
- Base volume name
- Number of snapshots and snapshots in the tree
- Snap pool name
- Amounts of total, unique, and shared data associated with the snapshot
  - Snap Data. 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).
  - UniqueData. The amount of data that has been written to the snapshot since the last snapshot was taken. If the snapshot has not been written or is deleted, this value is zero bytes.

    - SharedData. The amount of data that is potentially shared with other snapshots and the associated amount of space that will be freed if the snapshot is deleted. This represents the amount of data written directly to the snapshot. It also includes data copied from the source volume to the storage area for the oldest snapshot, since that snapshot does not share data with any other snapshot. For a snapshot that is not the oldest, if the modified data is deleted or if it had never been written to, this value is zero bytes.
- Default and user-specified retention priorities for this type of snapshot
- Type.
    - Standard snapshot: Snapshot of a master volume that consumes a snapshot license.
    - Standard snapshot (DRM): A temporary standard snapshot created from a replication snapshot for the purpose of doing a test failover for disaster recovery management (DRM).
    - Replication snapshot: For a primary or secondary volume, a snapshot that was created by a replication operation but is not a sync point.
    - Replication snapshot (Replicating): For a primary volume, a snapshot that is being replicated to a secondary system.
    - Replication snapshot (Current sync point): For a primary or secondary volume, the latest snapshot that is copy-complete on any secondary system in the replication set.
    - Replication snapshot (Common sync point): For a primary or secondary volume, the latest snapshot that is copy-complete on all secondary systems in the replication set.
    - Replication snapshot (Old Common sync point): For a primary or secondary volume, a common sync point that has been superseded by a new common sync point.
    - Replication snapshot (Only sync point): For a primary or secondary volume, the only snapshot that is copy-complete on any secondary system in the replication set.
    - Replication snapshot (Queued): For a primary volume, a snapshot associated with a replication operation that is waiting for a previous replication operation to complete.
    - Replication snapshot (Awaiting replicate): For a primary volume, a snapshot that is waiting to be replicated to a secondary system.

## Mapping properties

When you select the Maps component, the Maps for *Volume* table shows:

- Type. Explicit or Default. Settings for an explicit mapping override the default mapping.
- Host ID. WWPN or IQN.
- Host Name. User-defined nickname for the host.
- Ports. Controller host ports through which the volume is mapped to the host.
- LUN. Volume identifier presented to the host.
- Access. Volume access type: read-write, read-only, no-access (masked), or not-mapped.

## Schedule properties

If any schedules exist for the snapshot, when you select the Schedules component, the Schedules table shows information about each schedule. For the selected schedule, the Schedule Details table shows:

- Schedule Name.
- Schedule Specification.
- Schedule Status.
- Next Time.
- Task Type.
- Task Status.
- Task State.
- Source Volume.

- Source Volume Serial.
- Prefix.
- Count.
- Last Created.

# Viewing information about a snap pool

In the Configuration View panel, right-click a snap pool and select **View > Overview**. The Snap Pool Overview table shows:

- The capacity and space usage of the snap pool
- The quantity of volumes using the snap pool
- The quantity of snapshots in the snap pool

For descriptions of storage-space color codes, see "About storage-space color codes" (page 163).

---

**NOTE:** The process of freeing space associated with deleted snapshots occurs more slowly when the system is operating write-through cache mode than in write-back cache mode. Therefore, there will be a delay between deleting the snapshots and when their used space is shown as available space in the Snap Pool Overview panel.

---

Select a component to see more information about it.

## Snap pool properties

When you select the Snap Pool component, two tables appear. The first table shows the snap pool's name, serial number, size (total capacity), vdisk name, and free space, the number of snapshots in the snap pool, and its status. The status values are:

- Available: The snap pool is available for use.
- Offline: The snap pool is not available for use, as in the case where its disks are not present.
- Corrupt: The snap pool's data integrity has been compromised. The snap pool can no longer be used.

The second table shows the snap pool's threshold values and associated policies. Three thresholds are defined:

- Warning: The snap pool is moderately full. When this threshold is reached, an event is generated to alert the administrator.
- Error: The snap pool is nearly full and unless corrective action is taken, snapshot data loss is probable. When this threshold is reached, an event is generated to alert the administrator and the associated snap-pool policy is triggered.
- Critical: The snap pool is 98% full and data loss is imminent. When this threshold is reached, an event is generated to alert the administrator and the associated snap-pool policy is triggered.

The following policies are defined:

- Auto Expand: Automatically expand the snap pool by the indicated expansion-size value. This is the default policy for the Error threshold.

  If the snap pool's space usage reaches the percentage specified by its error threshold, the system will log Warning event 230 and will try to automatically expand the snap pool by the snap pool's expansion-size value. If the snap pool cannot be expanded because there is not enough available space in its vdisk, the system will log Warning event 444 and will automatically delete the oldest snapshot that is not a current sync point.
- Delete Oldest Snapshot: Delete the oldest snapshot.
- Delete Snapshots: Delete all snapshots. This is the default policy for the Critical threshold.
- Halt Writes: Halt writes to all master volumes and snapshots associated with the snap pool.

- Notify Only: Generates an event to notify the administrator. This is the only policy for the Warning threshold.
- No Change: Take no action.

---

**NOTE:** The policies Delete Oldest Snapshot and Delete Snapshots do not apply business logic to the delete decision and may delete snapshots that are mounted/presented/mapped or modified. You may set retention priorities for a snap pool as a way of suggesting that some snapshots are more important than others, but these priorities do not ensure any specific snapshot is protected.

---

For details about setting snap-pool thresholds and policies, see the CLI Reference Guide.

### Volume properties

When you select the Client Volumes component, a table shows the name, serial number, size, vdisk name, and vdisk serial number for each volume using the snap pool.

### Snapshot properties

When you select the Resident Snapshots component, a table shows each snapshot's name; serial number; amounts of snap data, unique data, and shared data; and status (Available or Unavailable).

- Snap data is 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).
- Unique data is the amount of data that has been written to the snapshot since the last snapshot was taken. If the snapshot has not been written or is deleted, this value is zero bytes.
- Shared data is the amount of data that is potentially shared with other snapshots and the associated amount of space that will be freed if the snapshot is deleted. This represents the amount of data written directly to the snapshot. It also includes data copied from the source volume to the storage area for the oldest snapshot, since that snapshot does not share data with any other snapshot. For a snapshot that is not the oldest, if the modified data is deleted or if it had never been written to, this value is zero bytes.

## Viewing information about all hosts

In the Configuration View panel, right-click **Hosts** and select **View > Overview**. The Hosts table shows the quantity of hosts configured in the system.

For each host, the Hosts Overview table shows the following details:

- Host ID. WWPN or IQN.
- Name. User-defined nickname for the host.
- Discovered. If the host was discovered and its entry was automatically created, Yes. If the host entry was manually created, No.
- Mapped. If volumes are mapped to the host, Yes. Otherwise, No.
- Profile.
  - Standard: Default profile.
  - HP-UX: The host uses Flat Space Addressing.
- Host Type.
  - If the host was discovered and its entry was automatically created, its host-interface type.
  - If the host entry was manually created: Undefined.

# Viewing information about a host

In the Configuration View panel, right-click a host and select **View > Overview**. The Host Overview table shows:

- Host properties
- The quantity of mappings for the host

Select a component to see more information about it.

## Host properties

When you select Host in the Host Overview table, the Properties for `Host` table shows:

- Host ID. WWPN or IQN.
- Name. User-defined nickname for the host.
- Discovered. If the host was discovered and its entry was automatically created, Yes. If the host entry was manually created, No.
- Mapped. If volumes are mapped to the host, Yes. Otherwise, No.
- Profile.
  - Standard: Default profile.
  - HP-UX: The host uses Flat Space Addressing.
- Host Type.
  - If the host was discovered and its entry was automatically created, its host-interface type.
  - If the host entry was manually created: Undefined.

## Mapping properties

When you select Maps in the Host Overview table, the Maps for `Host` table shows:

- Type. Explicit or Default. Settings for an explicit mapping override the default mapping.
- Name. Volume name.
- Serial Number. Volume serial number.
- Ports. Controller host ports through which the volume is mapped to the host.
- LUN. Volume identifier presented to the host.
- Access. Volume access type: read-write, read-only, no-access (masked), or not-mapped.

# Viewing information about an enclosure

In the Configuration View panel, right-click an enclosure and select **View > Overview**. You can view information about the enclosure and its components in a front or rear graphical view, or in a front or rear tabular view.

- Front Graphical. Shows a graphical view of the front of each enclosure and its drawers and disks.
- Front Tabular. Shows a tabular view of each enclosure and its drawers and disks.
- Rear Graphical. Shows a graphical view of components at the rear of the enclosure.
- Rear Tabular. Shows a tabular view of components at the rear of the enclosure.

Tabular views are initially sorted by the Name property.

In any of these views, select a component to see more information about it. Components vary by enclosure model. If any components are unhealthy, a table at the bottom of the panel identifies them. When a disk is selected, you can view properties or historical performance statistics.

## Enclosure properties

When you select an enclosure, a table shows:

- Health.
   OK
   Degraded
   Fault
   N/A
   Unknown
- Health Reason. If Health is not OK, this field shows the reason for the health state.
- Health Recommendation. If Health is not OK, this field shows recommended actions to take to resolve the health issue.
- Status.
- Enclosure ID.
- Vendor.
- Model.
- Number of Disks. The number of disks installed in the enclosure.
- Enclosure WWN.
- Midplane Serial Number.
- Part Number.
- Manufacturing Date.
- Manufacturing Location.
- Revision.
- EMP A Revision. Firmware revision of the Enclosure Management Processor in controller module A's Expander Controller.
- EMP B Revision. Firmware revision of the Enclosure Management Processor in controller module B's Expander Controller.
- EMP A Bus ID.
- EMP B Bus ID.
- EMP A Target ID.
- EMP B Target ID.
- Midplane Type.
- Enclosure Power (watts).
- PCIe 2-Capable. Shows whether the enclosure is capable of using PCIe version 2.

## Drawer properties

For a 2U48 enclosure, each drawer and its disks are depicted from a side view, as you would see the disks when the drawer is open. For a more detailed view of the physical layout of disks in a 2U48 enclosure drawer, see the Setup Guide for your system.

When you select a drawer, a table shows:

- Health.
  - OK
  - Degraded
  - Fault
  - N/A
  - Unknown
- Health Reason. If Health is not OK, this field shows the reason for the health state.
- Health Recommendation. If Health is not OK, this field shows recommended actions to take to resolve the health issue.
- Status.
- Drawer ID.
- Drawer WWN.
- EMP A Revision. Firmware revision of the drawer's Enclosure Management Processor for controller module A's Expander Controller.
- EMP B Revision. Firmware revision of the drawer's Enclosure Management Processor for controller module B's Expander Controller.
- EMP A Bus ID.
- EMP B Bus ID.
- EMP A Target ID.
- EMP B Target ID.

## Disk properties

When you select a disk and click the **Properties** tab, a table shows:

- Health.
  - OK
  - Degraded
  - Fault
  - N/A (if the disk is spun down)
  - Unknown
- Health Reason. If Health is not OK, this field shows the reason for the health state.
- Health Recommendation. If Health is not OK, this field shows recommended actions to take to resolve the health issue.
- Status.
  - 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.
  - Error: The disk is present but is 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.

    For an SSD, the Front Tabular view also shows the percentage of disk life remaining from 100% to 0%. When the value decreases to 20%, event 502 is logged with Informational severity. Event 502 is logged again with Warning severity when the value decreases to 5%, 2%, and 0%.
- Enclosure ID.
- Slot.
- How Used.
    - AVAIL: Available.
    - FAILED: The disk is unusable and must be replaced. Reasons for this status include: excessive media errors; SMART error; disk hardware failure; unsupported disk.
    - GLOBAL SP: Global spare.
    - LEFTOVR: Leftover.
    - UNUSABLE: The disk cannot be used in a vdisk because the system is secured and the disk is not FDE-capable, or because the disk is locked to data access (for AssuredSAN 4004 only).
    - VDISK: Used in a vdisk.
    - VDISK SP: Spare assigned to a vdisk.
- Type.
    - SAS: Enterprise SAS.
    - SAS MDL: Midline SAS.
    - sSAS: SAS SSD.
- Vendor.
- Model.
- Size.
- Speed (kr/min).
- Transfer Rate. The data transfer rate in Gbit/s. Some 6-Gbit/s disks might not consistently support a 6-Gbit/s transfer rate. If this happens, the controller automatically adjusts transfers to those disks to 3 Gbit/s, increasing reliability and reducing error messages with little impact on system performance. This rate adjustment persists until the controller is restarted or power-cycled.
- Revision. Disk firmware revision number.
- Serial Number.
- Current Job.
    - DRSC: Disks in the vdisk are being scrubbed.
    - EXPD: The vdisk is being expanded.
    - INIT: The vdisk is being initialized.
    - RCON: The vdisk is being reconstructed.
    - VRFY: The vdisk is being verified.
    - VRSC: The vdisk is being scrubbed.
- SMART. Shows whether Self-Monitoring Analysis and Reporting Technology is enabled. For more information, see “Configuring SMART” (page 186).
- Current Owner. For the disk’s vdisk, either the preferred owner during normal operation or the partner controller when the preferred owner is offline.
- Drive Spin Down Count. How many times the disk has been spun down.
- Power On Hours. The total number of hours that the disk has been powered on since it was manufactured. This value is stored in disk metadata and is updated in 30-minute increments.

- Sector Format.
  - 512n (512-byte native sector size).
  - 512e (512-byte emulated sector size).
- SSD Life Remaining.
  - For an SSD this property shows the percentage of disk life remaining, represented by a color-coded bar graph:

    | Life remaining | Bar color | Disk health |
    |---|---|---|
    | 100–20% | | OK |
    | 19–5% | | OK |
    | 4–1% | | Degraded |
    | 0% | (No bar) | Critical or Fault |

    When the value decreases to 20%, event 502 is logged with Informational severity. Event 502 is logged again with Warning severity when the value decreases to 5%, 2%, and 0%.
  - For a non-SSD this property shows N/A.
- FDE State (for AssuredSAN 4004 only).
  - Not Secured: The disk is not secured.
  - Unknown: The FDE state is unknown.
  - Not FDE-Capable: The disk is not FDE-capable.
  - Secured, Unlocked: The system is secured and the disk is unlocked.
  - Secured, Locked: The system is secured and the disk is locked to data access, preventing its use.
  - FDE Protocol Failure: A temporary state that can occur while the system is securing the disk.

## Disk performance

When you select a disk and click the **Performance** tab, a table shows eight graphs of historical performance statistics for the disk. Data samples are taken every quarter hour and the graphs represent up to 50 samples. By default, the graphs show the newest 50 samples.

To specify a time range of samples to display, set the start and end values and click **Update**. The system determines whether the number of samples in the time range exceeds the number of samples that can be displayed (50), requiring aggregation. To determine this, the system divides the number of samples in the specified time range by 50, giving a quotient and a remainder. If the quotient is 1, the 50 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 50 so all 4 samples are displayed.
- Example 2: A 15-hour range includes 60 samples. 60 divided by 50 gives a quotient of 1 and a remainder of 10. Therefore, the newest 50 samples will be displayed and the oldest 10 samples will be excluded.
- Example 3: A 30-hour range includes 120 samples. 120 divided by 50 gives a quotient of 2 and a remainder of 20. Therefore, each two newest samples will be aggregated into one sample for display and the oldest 20 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/s.

- 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.

The system will change the time settings to match the times of the oldest and newest samples displayed. The graphs are updated each time you click either the Performance tab or the Update button.

- Data Transferred. Shows the amounts of data read and written and the combined total over the sampling time period. The base unit is bytes.
- Data Throughput. Shows the rates at which data are read and written and the combined total over the sampling time period. The base unit is bytes/s.
- I/O. Shows the numbers of reads and writes and the combined total over the sampling time period.
- IOPS. Shows numbers of reads and writes per second and the combined total over the sampling time period.
- Average Response Time. Shows the average response times for reads and writes and the combined average over the sampling time period. The base unit is microseconds.
- Average I/O Size. Shows the average sizes of reads and writes and the combined average over the sampling time period. The base unit is bytes.
- Disk Error Counters. Shows the number of disk errors over the sampling time period.
- Average Queue Depth. Shows the average number of pending I/O operations that are being serviced over the sampling time period. This value represents periods of activity only and excludes periods of inactivity.

**TIP:** If you specify a time range, it is recommended to specify a range of 12 hours or less.

To view summary performance data for a vdisk, use the Vdisk Overview panel as described on page 243. To view live (non-historical) performance statistics for one or more disks, in the CLI use the `show disk-statistics` command.

## Power supply properties

When you select a power supply, a table shows:

- Health.
  - OK
  - Degraded
  - Fault
  - N/A
  - Unknown
- Health Reason. If Health is not OK, this field shows the reason for the health state.
- Health Recommendation. If Health is not OK, this field shows recommended actions to take to resolve the health issue.
- Status.
- Model.
- Vendor.
- Location.
- Serial Number.
- Revision.
- Part Number.
- Manufacturing Date.
- Manufacturing Location.

## Fan properties

In a 4U56 enclosure when you select a fan, a table shows:

- Health.
  - OK
  - Degraded
  - Fault
  - N/A
  - Unknown
- Health Reason. If Health is not OK, this field shows the reason for the health state.
- Health Recommendation. If Health is not OK, this field shows recommended actions to take to resolve the health issue.
- Status.
- Location.
- Speed.
- Serial Number.
- Firmware Version.
- Hardware Version.

## Controller module properties

When you select a controller module, a table shows:

- Health.
  - OK
  - Degraded
  - Fault
  - N/A
  - Unknown
- Health Reason. If Health is not OK, this field shows the reason for the health state.
- Health Recommendation. If Health is not OK, this field shows recommended actions to take to resolve the health issue.
- Status.
- Controller ID.
- Description.
- CPLD Version.
- Storage Controller Code Version.
- Model.
- Storage Controller CPU Type.
- Serial Number.
- Part Number.
- Position.
- Hardware Version.
- Revision.
- System Cache Memory (MB).
- Manufacturing Date.
- Manufacturing Location.

## Controller module: network port properties

When you select a network port, a table shows:

- Health.
  - OK
  - Degraded
  - Fault
  - N/A
  - Unknown
- Health Reason. If Health is not OK, this field shows the reason for the health state.
- MAC Address.
- Addressing Mode.
- IP Address.
- Gateway.
- Subnet Mask.

## Controller module: FC host port properties

When you select an FC host port, a table shows:

- Health.
  - OK
  - Degraded
  - Fault
  - N/A
  - Unknown
- Health Reason. If Health is not OK, this field shows the reason for the health state.
- Status.
  - Up: The port is cabled and has an I/O link.
  - Warning: Not all of the port's 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.
- Ports. The port ID, which is the controller ID and port number.
- Media.
  - FC(L): Fibre Channel-Arbitrated Loop (public or private).
  - FC(P): Fibre Channel Point-to-Point.
  - FC(-): Fibre Channel disconnected.
- Target ID. The port WWN.
- Configured Speed. Auto, 4Gb, 8Gb, or 16Gb (Gbit/s).
- Actual Speed. Actual link speed in Gbit/s, or blank if not applicable.
- Configured Topology.
  - PTP: Fibre Channel Point-to-Point.
  - Loop: Fibre Channel-Arbitrated Loop (public or private).
- Primary Loop ID. Primary loop ID, or blank if not applicable.

- SFP Status.
  - OK
  - Not present: No SFP is inserted in this port.
  - Not compatible: The SFP in this port is not qualified for use in this system. When this condition is detected, event 464 is logged.
  - Incorrect protocol: The SFP protocol does not match the port protocol. When this condition is detected, event 464 is logged.
- Part Number. The SFP part number.
- Supported Speeds. The link speeds that the SFP supports, in Gbit/s.

## Controller module: iSCSI host port properties

When you select an iSCSI host port, a table shows:

- Health.

   OK

   Degraded

   Fault

   N/A

   Unknown
- Health Reason. If Health is not OK, this field shows the reason for the health state.
- Status.
  - Up: The port is cabled and has an I/O link.
  - Warning: Not all of the port's 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.
- Ports. The port ID, which is the controller ID and port number.
- Media. iSCSI.
- Target ID. The port IQN.
- Configured Speed. Auto: the link speed is auto-negotiated.
- Actual Speed. Actual link speed in Gbit/s, or blank if not applicable.
- IP Version. The IP version: IPv4 or IPv6.
- MAC. The port's MAC address.
- IP Address. For IPv4 or IPv6, assigned port IP address.
- Netmask. For IPv4, subnet mask for assigned port IP address.
- Gateway. For IPv4, gateway for assigned port IP address.
- Default Router. For IPv6, default router for assigned port IP address.
- Link-Local Address. For IPv6, the link-local address that is automatically generated from the MAC address and assigned to the port.
- SFP Status.
  - OK
  - Not present: No SFP is inserted in this port.
  - Not compatible: The SFP in this port is not qualified for use in this system. When this condition is detected, event 464 is logged.
  - Incorrect protocol: The SFP protocol does not match the port protocol. When this condition is detected, event 464 is logged.

- 10G Compliance. The SFP's 10G compliance code, if supported.
- Cable Length. The link length (in meters) that is supported by the SFP while operating in compliance with applicable standards for the cable type, or 0 if this information is not provided by the SFP manufacturer.
- Cable Technology. Shows whether the SFP supports active or passive cable technology, or N/A if this information is not provided by the SFP manufacturer.
- Ethernet Compliance. The SFP's Ethernet compliance code, if supported.
- Part Number. The SFP part number.

## Controller module: SAS host port properties

**For AssuredSAN 3004**: The SAS fan-out cable capability is only applicable to systems with a 2-port SAS controller module. If fan-out cables are connected to SAS ports that are configured to use them, fan-out cable icons appear between the depicted SAS ports. The number of SAS ports that display depends on the configuration.

When you select a SAS host port, a table shows:

- Health.
  - OK
  - Degraded
  - Fault
  - N/A
  - Unknown
- Health Reason. If Health is not OK, this field shows the reason for the health state.
- Health Recommendation. If Health is not OK, this field shows recommended actions to take to resolve the health issue.
- Status.
  - Up: The port is cabled and has an I/O link.
  - Warning: Not all of the port's 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.
- Ports. The port ID, which is the controller ID and port number.
- Media. SAS.
- Target ID. The port WWN.
- Configured Speed. Blank: not applicable for SAS.
- Actual Speed. Auto: the link speed is auto-negotiated.
- Lanes Expected. The expected number of PHY lanes in the SAS port.
- Active Lanes. The number of active lanes in the SAS port. If the port is connected and fewer lanes are active than are expected, the port status will change to Warning, the health will change to Degraded, and event 354 will be logged. If the port is disconnected, the value will be 0.
- Num Ports Per Connector. The number of host ports per controller host-port connector. This reflects whether the system is set to use fan-out SAS cables or standard SAS cables. (for AssuredSAN 3004 only).
  - 1: The system is set to use standard SAS cables.
  - 2: The system is set to use fan-out SAS cables.

## Controller module: expansion port properties

When you select an expansion (Out) port, a table shows:

- Health.
  - OK
  - Degraded
  - Fault
  - N/A
  - Unknown
- Health Reason. If Health is not OK, this field shows the reason for the health state.
- Health Recommendation. If Health is not OK, this field shows recommended actions to take to resolve the health issue.
- Status.
- Name.

## Controller module: CompactFlash properties

When you select a CompactFlash card in the Rear Tabular view, a table shows:

- Health.
  - OK
  - Degraded
  - Fault
  - N/A
  - Unknown
- Health Reason. If Health is not OK, this field shows the reason for the health state.
- Health Recommendation. If Health is not OK, this field shows recommended actions to take to resolve the health issue.
- Status.
- Cache Flush.
  - Enabled: If the controller loses power, it will automatically write cache data to the CompactFlash card. Cache flush is normally enabled, but is temporarily disabled during controller shut down.
  - Disabled: Cache flush is disabled.

## Drive enclosure: I/O module properties

When you select an I/O module, a table shows:

- Health.
  - OK
  - Degraded
  - Fault
  - N/A
  - Unknown
- Health Reason. If Health is not OK, this field shows the reason for the health state.
- Status.
- Controller ID.

## I/O module: In port properties

When you select an In port, a table shows:

- Health.
  - OK
  - Degraded
  - Fault
  - N/A
  - Unknown
- Health Reason. If Health is not OK, this field shows the reason for the health state.
- Health Recommendation. If Health is not OK, this field shows recommended actions to take to resolve the health issue.
- Status.
- Name.

## I/O module: Out port properties

When you select an Out port, a table shows:

- Health.
  - OK
  - Degraded
  - Fault
  - N/A
  - Unknown
- Health Reason. If Health is not OK, this field shows the reason for the health state.
- Health Recommendation. If Health is not OK, this field shows recommended actions to take to resolve the health issue.
- Status.
- Name.

# Viewing information about a remote system

In the Configuration View panel, right-click a remote system and select **View > Overview**. The System Information table shows:

- The username and network-port IP addresses that are configured on the local system to access the remote system. The configured password is not shown.
- Information such as the system name, location, and status that is read from the remote system.

To sign in to the remote system, click one of its IP address links.

# 16 Using AssuredRemote to replicate volumes

## About the AssuredRemote replication feature

AssuredRemote™ is a licensed feature for disaster recovery. This feature performs asynchronous (batch) replication of block-level data from a volume on a local storage system to a volume that can be on the same system or on a second, independent system. This second system can be located at the same site as the first system or at a different site.

A typical replication configuration involves these physical and logical components:

- A host connected to a local storage system, which is networked via FC or iSCSI ports to a remote storage system as described in installation documentation.
- *Remote system*. A management object on the local system that enables the MCs in the local system and in the remote system to communicate and exchange data.
- *Replication set*. Associated master volumes that are enabled for replication and that typically reside in two physically or geographically separate storage systems. These volumes are also called replication volumes.
- *Primary volume*. The volume that is the source of data in a replication set and that can be mapped to hosts. For disaster recovery purposes, if the primary volume goes offline, a secondary volume can be designated as the primary volume. The primary volume exists in a primary vdisk in the primary system.
- *Secondary volume*. The volume that is the destination for data in a replication set and that is not accessible to hosts. For disaster recovery purposes, if the primary volume goes offline, a secondary volume can be designated as the primary volume. The secondary volume exists in a secondary vdisk in a secondary system.
- *Replication snapshot*. A special type of snapshot that preserves the state of data of a replication set's primary volume as it existed when the snapshot was created. For a primary volume, the replication process creates a replication snapshot on both the primary system and, when the replication of primary-volume data to the secondary volume is complete, on the secondary system. Replication snapshots are unmappable and are not counted toward a license limit, although they are counted toward the system's maximum number of volumes. A replication snapshot can be exported to a regular, licensed snapshot.
- *Replication image*. A conceptual term for replication snapshots that have the same image ID in the primary and secondary systems. These synchronized snapshots contain identical data and can be used for disaster recovery.

### Replication process overview

As a simplified overview of the remote-replication process, it can be configured to provide a single point-in-time replication of volume data or a periodic delta-update replication of volume data.

The periodic-update process has multiple steps. At each step, matching snapshots are created: in the primary system, a replication snapshot is created of the primary volume's current data. This snapshot is then used to copy new (delta) data from the primary volume to the secondary volume. Then in the secondary system, a matching snapshot is created for the updated secondary volume. This pair of matching snapshots establishes a replication sync point and these sync points are used to continue the replication process.

The following figure illustrates three replication sets in use by two hosts:

- The host in New York is mapped to and updates the Finance volume. This volume is replicated to the system in Munich.

- The host in Munich is mapped to and updates the Sales and Engineering volumes. The Sales volume is replicated from System 2 to System 3 in the Munich data center. The Engineering volume is replicated from System 3 in Munich to System 1 in New York.

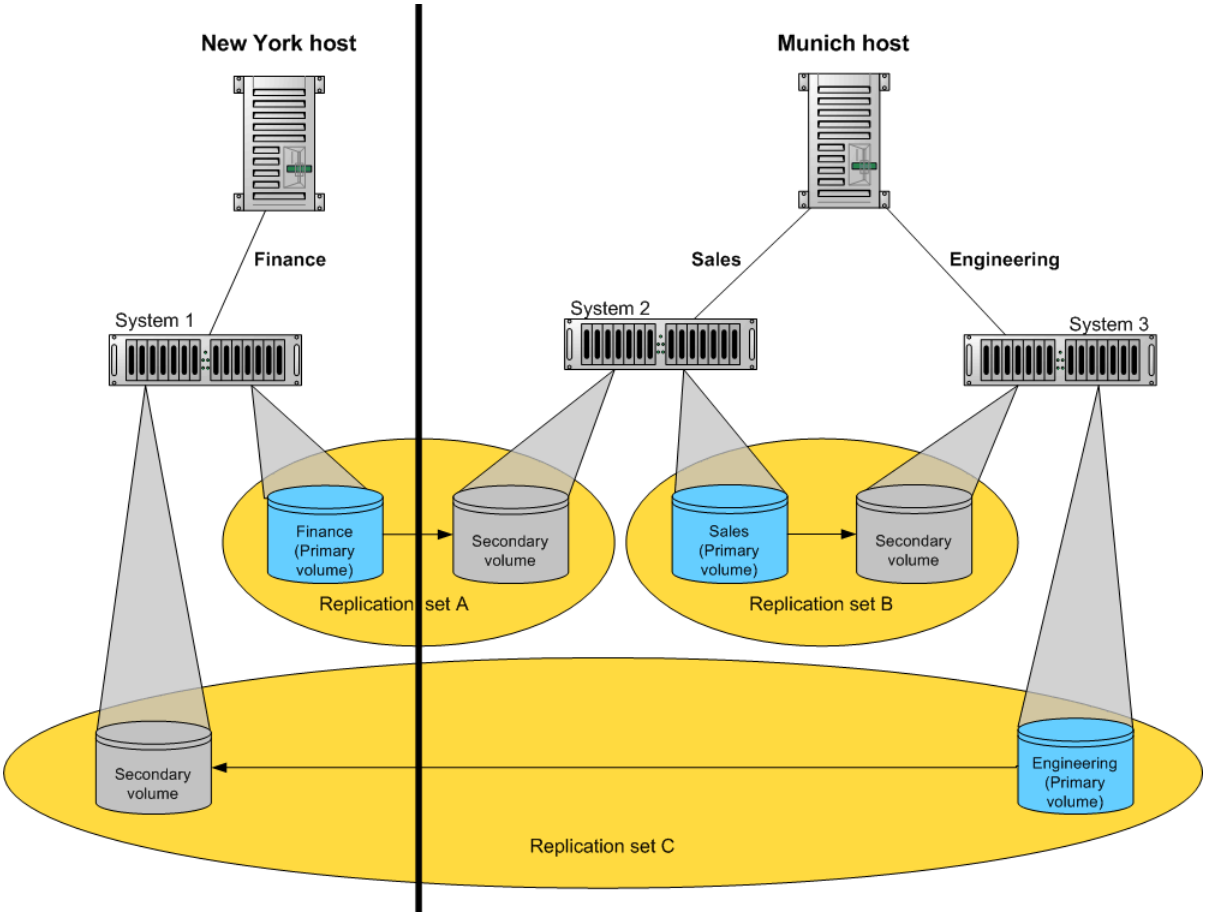



**Figure 6 Intersite and intrasite replication sets**

Remote replication uses snapshot functionality to track the data to be replicated and to determine the differences in data updated on the master volume, minimizing the amount of data to be transferred.

In order to perform a replication, a snapshot of the primary volume is taken, creating a point-in-time image of the data. This point-in-time image is then replicated to the secondary volume by copying the data represented by the snapshot using a transport medium such as TCP/IP (iSCSI) or Fibre Channel. The first replication copies all data from the primary volume to the secondary volume. Subsequent replications use sparse snapshots. A sparse snapshot stores only those blocks that are different from an already existing full copy of the data.

Replication snapshots are retained for both the primary volume and the secondary volume. When a matching pair of snapshots is retained for both volumes, the matching snapshots are referred to as *replication sync points*. The two snapshots (one on each volume) are used together as a synchronization reference point, minimizing the amount of data to transfer. The two snapshots in a replication sync point are assigned the same *image ID*, which uniquely identifies that the data in those snapshots are from the same point-in-time image and are block-for-block identical.

When a replication snapshot is created from a standard snapshot, while that snapshot remains present the replication snapshot's total data represented is zero bytes. This behavior occurs because the snapshot data remains associated with the standard snapshot and there is no data specifically associated with the replication snapshot. If the standard snapshot is deleted, its data becomes associated with (is preserved by) the replication snapshot and the replication snapshot's size changes to reflect the size of the deleted snapshot.

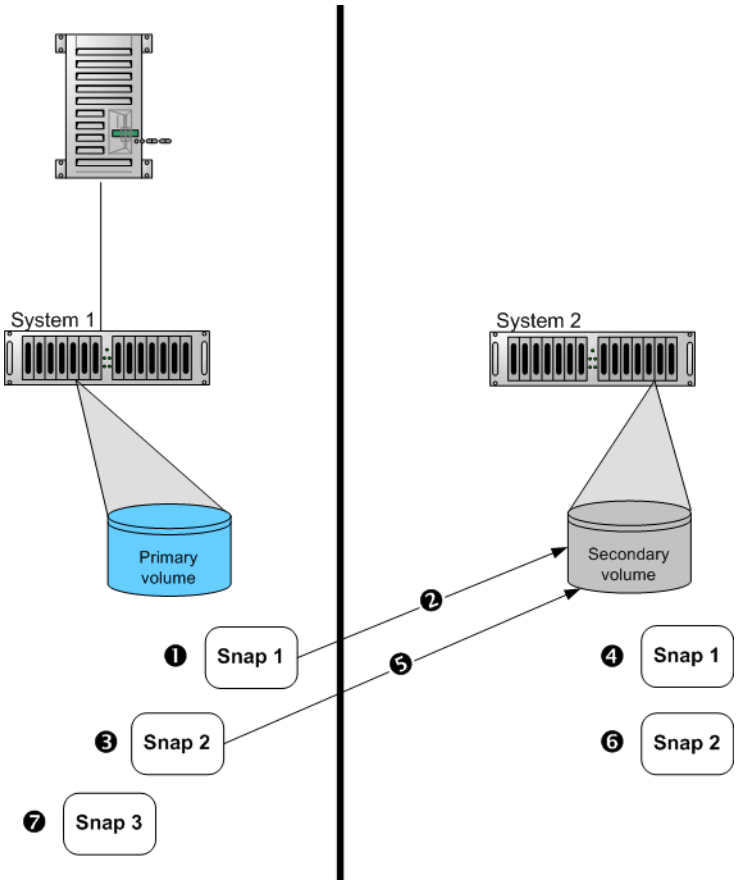
An added benefit of using snapshots for replication is that these snapshots can be kept and restored later in the event of a non-hardware failure, such as virus attack. Since the replication source is a snapshot, any writes performed on the primary volume after the snapshot is taken are not replicated by that task. This gives you more control over what is contained in each replication image.

**NOTE:** Because replication is not synchronous (continuous), data in a secondary volume is only as current as the last replication that completed successfully. Replications can be performed manually or scheduled.

**NOTE:** Snapshot operations are I/O-intensive. Every write to a unique location in a master volume after a snapshot is taken will cause an internal read and write operation to occur in order to preserve the snapshot data. If you intend to create snapshots of, create volume copies of, or replicate volumes in a vdisk, ensure that the vdisk contains no more than four master volumes, snap pools, or both. For example: 2 master volumes and 2 snap pools; 3 master volumes and 1 snap pool; 4 master volumes and 0 snap pools.

## Replication actions

The following figure illustrates actions that occur during a series of replications from System 1 to System 2.




1. Take initial snapshot and initiate replication.
2. Initial replication consists of a full data copy.
3. Take second snapshot and request replication. This can be taken while the initial replication is in progress.
4. Snapshot taken on secondary volume. This is the first replication sync point.
5. When the initial replication is complete, the second replication automatically starts. Only the data changed since Snap 1 is replicated.
6. Second snapshot taken on secondary volume. This is the second sync point.
7. Other snapshots can be taken and replication initiated on the primary volume while replication is in progress. These snapshots are queued waiting for prior replications to complete. These replication snapshots will not become sync points until their replications are complete.

**Figure 7 Actions that occur during a series of replications**

The figure above illustrates initial, delta, and queued replications:

- Initial replication: When the first replication is initiated, a snapshot of the primary volume is taken and every block of data is then copied to the secondary volume. When the copy is complete, the first snapshot is taken on the secondary volume, creating the first sync point. This sync point can be used to determine the delta data from that sync point to a later snapshot. Actions 1–4 are the initial replication.
- Delta replications: Delta data is the “list” of 64-KB blocks that differs between the last snapshot replicated and the next snapshot to be replicated. This delta data is then replicated from the replication snapshot on the primary volume to the secondary volume. Once the initial replication has completed, all future replications for that replication set will be delta replications so long as sync points are maintained. Action 5 is a delta replication.

- Queued replications: New replications can be initiated while other replication snapshots are in the process of being replicated. This enables you to take snapshots at specific intervals while other replications are ongoing. Note that a replication that is initiated while another to the same secondary volume is ongoing will be queued, and will not begin to transfer data until the prior one completes. In action 3, Snap 2 is queued while Snap 1 is being replicated. In action 7, Snap 3 is queued while Snap 2 is being replicated.

An in-progress replication can be suspended, either manually by a user or automatically if a network error occurs. If you want the replication to continue, you must manually resume it. If you want to cancel the replication, you can abort it.

**IMPORTANT:** For a replication to begin, the controller that owns the secondary volume must have a link to the controller that owns the primary volume. This link must be of the type specified by the link-type parameter supplied during replication set creation or modification. If all links to the controller that owns the primary volume fail, but links remain between its partner controller and the controller that owns the secondary volume, replications currently in progress or queued may continue, but their progress may not be reported correctly. If the controller that owns the secondary volume loses all links to both controllers of the primary system, then the replications will suspend and progress will be updated appropriately. Links from the partner controller of the controller that owns the secondary volumes are not considered for use. Replications that enter the suspended state must be resumed manually.

## Performing initial replication locally or remotely

When you set up replication for a volume, you specify to use a secondary volume in a vdisk in either the local (primary) system or a remote (secondary) system. Local replication is allowed only if the primary and secondary volumes are in vdisks owned by different controllers.

- If the speed of the initial replication is most important, replicate locally. In the local system, specify a vdisk owned by a different controller than the one that owns the primary volume's vdisk in the same system.

  After replication is set up, you can perform the initial replication and then physically move the vdisk containing the secondary volume and its snap pool into a remote system. Moving a vdisk involves using RAIDar to detach the secondary volume and stop its vdisk, removing the vdisk's disks or enclosure, transporting the disks or enclosure to the remote location, inserting the disks or enclosure into the remote system, and using RAIDar to restart the vdisk and reattach the secondary volume. If the secondary volume's snap pool is in a different vdisk then that vdisk must also be stopped, moved, and restarted.
- If ease of setup is most important, replicate remotely. Specify a vdisk owned by either controller in a remote system. After replication is set up, you can start replication.
- A third method is to physically co-locate the primary and secondary systems, set up and perform the initial replication, and then move the secondary system to the remote site. Ensure that the local system can communicate over the network with the remote system at its new location.

In either case, you must specify the link type to be used for replication between the primary and secondary systems and you cannot change this setting for the life of the replication set.

You can only select a vdisk that has enough available space for replication. For details, see the following topic.

## Criteria for selecting a vdisk to contain a secondary volume

When setting up replication for a volume that will become the primary volume in a replication set, you have the option to select an existing vdisk in which to create the secondary volume.

The vdisk-selection option only lists vdisks that have sufficient available space for replication, and that do not contain a volume with a conflicting name (*rprimary-volume-name*) or a snap pool with a conflicting name (*sprprimary-volume-name*). The system calculates the required space for the secondary volume (the reserve size) and its snap pool as follows:

- The snap-pool size will be either 20% of the primary volume's size or 5.37GB, whichever is larger.
- The reserve size is calculated as follows:
  - If the primary volume and the snap pool are each less than 500 GB, the reserve will be the same size as the primary volume.
  - If the primary volume is larger than 500 GB, the reserve size will be the maximum, 500 GB.
  - If the snap pool is larger than 500 GB, the reserve will be the same size as the snap pool.
- The required space in the vdisk is calculated as follows:
  - If the combined size of the primary volume and the reserve is less than the combined size of the primary volume and the snap pool, the required space is the combined size of the primary volume and the snap pool.
  - If the combined size of the primary volume and the reserve is larger than the combined size of the primary volume and the snap pool, the required space is the combined size of the primary volume and the reserve.

The following table shows examples of how much available space a vdisk must have in order to be shown by the vdisk option. If you want to replicate a volume whose size is not shown, you can use the above calculations to determine how much available space the secondary vdisk must have.

**Table 29 Available space required for a vdisk to be selectable to contain a secondary volume (v2)**

| Primary volume size (GB) | Available space required in vdisk (GB) | Primary volume size (GB) | Available space required in vdisk (GB) | Primary volume size (GB) | Available space required in vdisk (GB) |
|---|---|---|---|---|---|
| 100 | 200 | 1100 | 1600 | 2100 | 2600 |
| 200 | 400 | 1200 | 1700 | 2200 | 2700 |
| 300 | 600 | 1300 | 1800 | 2300 | 2800 |
| 400 | 800 | 1400 | 1900 | 2400 | 2900 |
| 500 | 1000 | 1500 | 2000 | 2500 | 3000 |
| 600 | 1100 | 1600 | 2100 | 2600 | 3120 |
| 700 | 1200 | 1700 | 2200 | 2700 | 3240 |
| 800 | 1300 | 1800 | 2300 | 2800 | 3360 |
| 900 | 1400 | 1900 | 2400 | 2900 | 3480 |
| 1000 | 1500 | 2000 | 2500 | 3000 | 3600 |

## Remote replication disaster recovery

Replication can continue in the event of system faults such as:

- Temporary communication failure. Remote replication will retry replication operations according to user-configured policies.
- Controller failure. In a dual-controller system, failover will occur and the surviving controller will take over replication processing until controller recovery occurs.
- Disk or power supply failure.

If a disaster causes the primary volume to become inaccessible, you can set the secondary volume to be the primary volume so that volume can be mapped to hosts. Disaster recovery requires user intervention because decisions must be made based on the data content of replication volumes and their snapshots.

1. Synchronize the secondary volume to a replication snapshot, preferably a replication sync point. Any data written to the primary volume since the last-completed replication will not be available.

2. After synchronization, set the secondary volume to be the new primary volume.
3. Map the new primary volume to hosts, as was the original primary volume.

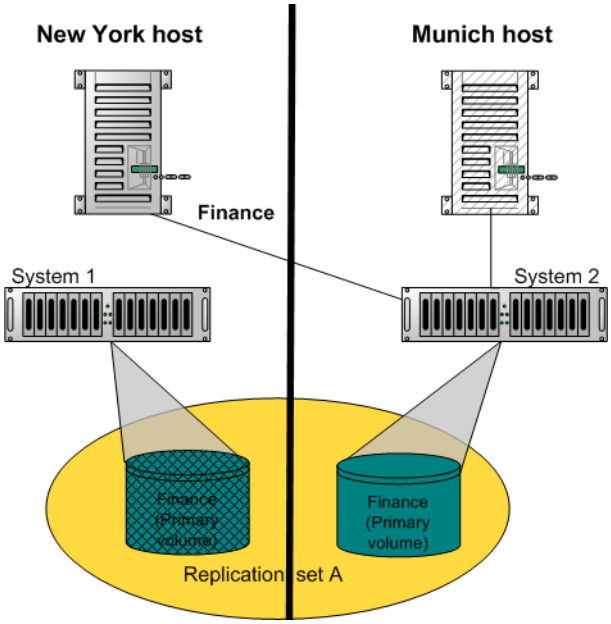



**Figure 8 Example of primary-volume failure**

If the original primary volume becomes accessible, you can set it to be the primary volume again as described in the following process overview:

1. Take a snapshot of the original primary volume. This preserves the volume's current data state for later comparison with the new primary volume.
2. Remove the volume's mappings.
3. Set the original primary volume to be a secondary volume.
4. Replicate any data written to the new primary volume to the original primary volume (now a secondary volume). This can be done as one or more replications. On the final replication, halt host access to the primary volume to ensure that all data has been transferred to the secondary volume.
5. Set the secondary volume (the original primary volume) to be the new primary volume.
6. You can now mount/present/map the snapshot taken in step 1 and compare it with the new primary volume to identify any data discrepancies and try to recover any data from the snapshot that would otherwise be lost. For example, you could use host file-system tools to find any files modified since a certain time, or for a database you could export any differing records from the snapshot and re-enter them into the current database.

For details, see the procedure to change the primary volume back to the original primary volume in "Changing the primary volume for a replication set" (page 284).

## Remote replication licensing

The AssuredRemote and AssuredSnap features are separately licensed. AssuredRemote can operate without AssuredSnap being enabled. However, to get the most out of AssuredRemote, it is recommended to enable both features. Normally, replication snapshots are not accessible to hosts. However, if AssuredSnap is enabled, a replication snapshot can be exported for use as a standard snapshot and will count toward the snapshot license limit.

## Related topics

- "Installing a license" (page 174)
- Adding (page 195) or deleting (page 195) a remote system
- "Checking links to a remote system" (page 233)
- "Using the Replication Setup Wizard" (page 274)
- Replicating a volume (page 276) or a snapshot (page 279)
- Detaching (page 280) and reattaching (page 283) a secondary volume
- Stopping (page 281) and restarting (page 282) a vdisk
- Suspending (page 280), resuming (page 280), or aborting (page 280) a replication
- "Exporting a replication image to a snapshot" (page 283)
- "Changing the primary volume for a replication set" (page 284)
- "Viewing replication properties, addresses, and images for a volume" (page 285)
- "Viewing information about a replication image" (page 288)
- "Viewing information about a remote primary or secondary volume" (page 287)

# Using the Replication Setup Wizard

If the system is licensed to use remote replication, you can use the Replication Setup Wizard to prepare to replicate an existing volume to another vdisk in the local system or to a remote system. Before using this wizard, read the documentation for your product to learn about replication. Then plan the storage systems, replication mode, and volumes you want to use for the replication.

The wizard guides you through the following steps. For each step you can view help by clicking the help icon in the wizard panel. As you complete steps they are highlighted at the bottom of the panel. If you cancel the wizard at any point, no changes are made.

- Select the primary volume, which is an existing volume or snapshot to replicate.
- Specify whether the replication mode will be local or remote. If the replication will be to a remote system that has not already been added to the local system, you can add it. To do so, you must know the user name and password of a user with the Manage role on that system and the system's IP address.
- Specify the secondary volume. You can select an existing replication-prepared volume or specify to create a volume in an existing vdisk that has sufficient available space for the replicated data.
- Confirm changes and apply them.

**IMPORTANT:** Before starting this procedure, if you intend to use CHAP to authenticate iSCSI login requests between the local system and a remote system, do the following:

- Create a one-way CHAP record on each system. On the local system, the CHAP record must refer to the node name of the remote system. On the remote system, the CHAP record must refer to the node name of the local system. Both records must use the same secret. (Mutual CHAP is not used between storage systems. CHAP records' mutual fields can be set but are not used.) To create a CHAP record, see "Configuring CHAP" (page 218).
- After the CHAP records are created, enable CHAP on the primary system, the secondary system, or both. To enable CHAP, see "Changing host interface settings" (page 182).

If both records don't exist or don't use the same secret, replication-set creation will fail.

**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.

## Starting the wizard

1. In the Configuration View panel, right-click the system and select **Wizards > Replication Setup Wizard**. The wizard panel appears.
2. Click **Next** to continue.

## Selecting the primary volume

Select the volume whose data you want to replicate. If the volume has at least one snapshot, you can select a snapshot to be the replication source.

### To select the primary volume

1. Set the options:
   - Select the vdisk that contains the volume to replicate. Only vdisks that contain at least one volume are listed for selection.
   - Select the volume to replicate. Only volumes that are not already part of a replication set are listed for selection.
2. Click **Next** to continue.

## Selecting the replication mode

Select the replication mode, which specifies whether the replication destination is in the local system or a remote system. If you want to replicate to a remote system that hasn't already been added to the local system, you can add it. Local replication is allowed only if the primary and secondary volumes are in vdisks owned by different controllers.

### To replicate within the local system

1. Select **Local Replication**.
2. Although it is recommended to check host-port links between controllers in the local system, if you already know the status of links you can clear the **Check Links** check box to skip this task.
3. Click **Next** to continue. If Check Links is selected and there are no links between the controllers, a message appears, and only vdisks and volumes that are owned by the same controller as the primary volume will appear in the next step.

### To replicate to a remote system

1. Select **Remote Replication**.
2. In the Remote System list, look for the remote system that you want to use.
   - If you find the system, select it and continue with step 5.
   - If you don't find it, add it as described in step 3.
3. To add a remote system, in the Add new Remote System area:
   a. Enter the IP address of a network port on the remote system.
   b. Enter the user name of a user with a Manage role on the remote system.
   c. Enter that user's password.
   d. Click **Add Remote System**. If task succeeds, the new remote system appears in the Remote System list and is selected.
4. Although it is recommended to check host-port links between the two systems, this can take up to 3 minutes, so if you already know the status of links you can clear the **Check Links** check box to skip this task.
5. Click **Next** to continue. If Check Links is selected and there are no links to the remote system, a message appears and you cannot proceed. For an AssuredSAN 4004 CNC system, if only one link type is up, only that link type will appear in the next step.

## Selecting the secondary volume

Specify the secondary volume. You can either select an existing vdisk in which to create the secondary volume, or select an existing replication-prepared volume to be the secondary volume.

### To specify the secondary volume

1. Either:
   - Select **Create new volume on vdisk** and select an existing vdisk in which to create the secondary volume. For an explanation of the criteria that determines which vdisks are listed for selection, see "Criteria for selecting a vdisk to contain a secondary volume" (page 271).
   - Select **Use existing replication-prepared volume** and select an existing replication-prepared volume to be the secondary volume. Only replication-prepared volumes that are exactly the same size in blocks as the primary volume are listed for selection.
2. Select the link type used between the two systems.
3. Click **Next** to continue.

## Confirming replication settings

Confirm that the values listed in the wizard panel are correct.

- If they are not correct, click **Previous** to return to previous steps and make necessary changes.
- If they are correct, click **Finish** to apply the setting changes and finish the wizard.

# Replicating a volume

If the system is licensed to use remote replication, you can create a replication set that uses the selected volume as the primary volume, and to immediately start or schedule replication. The primary volume can be a standard volume or a master volume.

To create a replication set you must select a secondary system and a secondary vdisk or volume. The secondary system can be the local system, or a remote system added by using the Add Remote System panel. When using RAIDar it is recommended to select a secondary vdisk and let the secondary volume be created automatically, instead of selecting an existing secondary volume. For a secondary (replication-prepared) volume to be available for selection, it must be exactly the same size in blocks as the primary volume, and that is difficult to ensure, especially with maximum-size volumes.

You can select the local system if you intend to create the replication set on the local system and then physically move the secondary vdisk's disks (or enclosure) to a remote system. Otherwise, select a remote system for which you've already added a management object on the local system. Local replication is allowed only if the primary and secondary volumes are in vdisks owned by different controllers.

**TIP:** A best practice is to schedule no more than three volumes to start replicating at the same time, and for those replications to recur no less than 60 minutes apart. If you schedule more replications to start at the same time, or schedule replications to start more frequently, some scheduled replications may not have time to complete.

**IMPORTANT:** Before starting this procedure, if you intend to use CHAP to authenticate iSCSI login requests between the local system and a remote system, do the following:

- Create a one-way CHAP record on each system. On the local system, the CHAP record must refer to the node name of the remote system. On the remote system, the CHAP record must refer to the node name of the local system. Both records must use the same secret. (Mutual CHAP is not used between storage systems. CHAP records' mutual fields can be set but are not used.) To create a CHAP record, see "Configuring CHAP" (page 218).
- After the CHAP records are created, enable CHAP on the primary system, the secondary system, or both. To enable CHAP, see "Changing host interface settings" (page 182).

If both records don't exist or don't use the same secret, replication-set creation will fail.

**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.

**NOTE:** If replication requests are sent to a secondary system whose temporary replication license has expired, the requests are queued but are not processed, and the secondary system reports event 472. If this condition occurs, check for this event in the event log, event-notification emails, and SNMP traps. To continue using replication, purchase a permanent replication license.

### To create a replication set and optionally start or schedule replication

1. In the Configuration View panel, right-click a volume and select **Provisioning** > **Replicate Volume**.
2. In the main panel, set the destination options:
   - Secondary System. Select a storage system to replicate the volume to.
   - Secondary Volume. Select either an existing vdisk in which to create the secondary volume, or an existing replication-prepared volume to be the secondary volume. For an explanation of the criteria that determines which vdisks are listed for selection, see "Criteria for selecting a vdisk to contain a secondary volume" (page 271).
3. Select the link type used between the two systems.
4. If you want to start replication now:
   a. Select the **Initiate Replication** and **Now** options.
   b. Optionally change the default replication image name. A name is case sensitive and can have a maximum of 32 bytes. It cannot already exist in a vdisk or include the following: " , < \
   c. Continue with step 7.
5. If you want to schedule replication:
   a. Select the **Initiate Replication** and **Scheduled** options.
   b. Set the options:
      - Replication image prefix. Optionally change the default prefix to identify images created by this schedule. The prefix is case sensitive and can have a maximum of 26 bytes. It cannot already exist in a vdisk or include the following: " , < \
      - Replication Mode. Specifies whether to replicate a new snapshot of the volume to the remote system, or to replicate the last (most recent existing) snapshot of the volume to the remote system.

- Replication images to Retain. Select the number of replication images to retain for both the primary volume and the secondary volume. When the task runs, the retention count is compared with the number of existing replication images:
  - Whether the retention count has been reached or not, a new replication image is created.
  - If the retention count has been reached, the volume's oldest replication image that was created by this schedule and is neither being replicated, nor a current sync point, nor a queued snapshot, is deleted.
  - If there is more than one queued snapshot, only the oldest queued snapshot is retained. It is retained to serve as the source for the next scheduled replication to create a replication image from.
- Start Schedule. 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. Date must use the format *yyyy-mm-dd*. 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.
- Recurrence. Specify either One Time, which schedules a single instance, or the interval at which the schedule should run.
- Time Constraint. Specify either No Time Constraint, which allows the schedule to run at any time, or a time range within which the schedule should run.
- Date Constraint. Specify either No Date Constraint, which allows the schedule to run on any day, or days when the schedule should run. Ensure that this constraint includes the Start Schedule date.
- End Schedule. Specify either Continuous, which allows the schedule to run without an end date, or when the schedule should stop running.

**c.** Continue with step 7.

6. If you do not want to start or schedule replication, clear the **Initiate Replication** check box. The replication set will still be created and you can replicate the volume at a later time.
7. Click **Apply**. Within a couple of minutes, the replication set is created and the following changes occur in the Configuration View panel:
   - Under the primary vdisk:
     - The selected primary volume changes to a master volume, and is designated as a Primary Volume.
     - If the secondary volume is on a remote system, the secondary volume appears under the primary volume.
     - If a replication was performed, under both the primary volume and the secondary volume a replication image appears.
     - If not already present, the primary volume's snap pool appears.
   - Under the secondary vdisk:
     - The secondary volume appears.
     - If the primary volume is on a remote system, the primary volume appears under the secondary volume.
     - If a replication was performed, under both the primary volume and the secondary volume a replication image appears.
     - If not already present, the secondary volume's snap pool appears.

# Replicating a snapshot

If the system is licensed to use remote replication, you can replicate an existing, primary snapshot that is mapped to a host. You can only replicate a snapshot of a volume that is already part of a replication set.

If the selected snapshot hasn't already been replicated to a secondary volume, each replication volume in the replication set is requested to replicate the snapshot data. Only snapshot preserved data is replicated. Snapshot modified data is not replicated.

### To replicate a snapshot

1. In the Configuration View panel, right-click a snapshot and select **Provisioning > Replicate Snapshot**.
2. In the main panel, optionally change the default replication image name. A name is case sensitive and can have a maximum of 32 bytes. It cannot already exist in a vdisk or include the following: " , < \
3. Click **Initiate Replication**. A message indicates whether the task succeeded or failed.
4. Click **OK**. After a few seconds, in the Configuration View panel, under both the primary volume and the secondary volume, a replication image appears.

# Removing replication from a volume

If the system is licensed to use remote replication and you no longer want to replicate a volume, you can remove its replication set. When a replication set is removed:

- A rollback is automatically performed to the latest available snapshot on the secondary volume to ensure that data is consistent.
- Replication volumes associated with the replication set are converted to master volumes.
- Any replication images associated with the replication volumes are converted to standard snapshots. Snapshots are converted regardless of the number of snapshots allowed by the system's license.
- There is no longer a relationship between the volumes or their snapshots in the two vdisks.

### To remove replication from a volume

1. In the Configuration View panel, right-click a local primary volume and select **Provisioning > Remove Replication Set**.
2. In the main panel, click **Remove Replication Set**. A confirmation dialog appears.
3. Click **Remove** to continue. Otherwise, click **Cancel**. If you clicked Remove, a processing dialog appears. A message indicates whether the task succeeded or failed.
4. Click **OK**. If the task succeeded, the following changes occur in the Configuration View panel:
   - Under the primary vdisk:
     - The primary volume's designation is changed from Primary Volume to Volume
     - The secondary volume is removed
     - Any replication images are replaced by snapshots
   - Under the secondary vdisk:
     - The secondary volume's designation is changed from Secondary Volume to Volume
     - The primary volume is removed
     - Any replication images are replaced by snapshots

**NOTE:** Normally, if you want to remove a replication set you must select its primary volume. However, if the primary volume is inaccessible, you can set the secondary volume to be the primary volume (as described in "Changing the primary volume for a replication set" (page 284)) and then perform a Remove Replication Set operation.

## Suspending a replication

If the system is licensed to use remote replication, you can suspend the current replication operation for a selected a replication volume. You must perform this task on the system that owns the secondary volume. Once suspended, the replication must be resumed or aborted to allow the replication volume to resume normal operation.

### To suspend replication

1. In the Configuration View panel, right-click a local replication volume and select **Provisioning > Suspend Replication**.
2. In the main panel, click **Suspend Replication**. A message indicates whether the task succeeded or failed.
3. Click **OK**.

## Resuming a suspended replication

If the system is licensed to use remote replication, you can resume a suspended replication operation for a selected replication volume. You must perform this task on the system that owns the secondary volume.

### To resume replication

1. In the Configuration View panel, right-click a local replication volume and select **Resume Replication**.
2. In the main panel, click **Resume Replication**. A message indicates whether the task succeeded or failed.
3. Click **OK**.

## Aborting replication

If the system is licensed to use remote replication, you can abort the current replication operation for the selected replication volume. The current replication may be running or suspended. You must perform this task on the system that owns the secondary volume.

### To abort replication

1. In the Configuration View panel, right-click a local replication volume and select **Provisioning > Abort Replication**.
2. In the main panel, click **Abort Replication**. A message indicates whether the task succeeded or failed.
3. Click **OK**.

## Detaching a secondary volume

When using the replication feature, if you chose to create a replication set's primary and secondary volumes in the primary system, you can perform the initial replication and then physically move the secondary volume's vdisk into the secondary system.

The process to move a secondary volume is:

1. In the system where the secondary volume resides:
   a. Detach the secondary volume.
   b. If the secondary volume's vdisk contains other secondary volumes, detach those volumes.
   c. Stop the secondary volume's vdisk. For details see "Stopping a vdisk" (page 281).
   d. If the secondary volumes' snap pools are in other vdisks, stop those vdisks.
   e. Move the vdisks into the secondary system. This system must support the link type that the replication set is configured to use. For example, if the replication set's link type is configured to use FC links, the secondary system must have FC ports.
2. In the secondary system:
   a. Start the snap pools' vdisks. For details see "Starting a vdisk" (page 282).
   b. Start the secondary volumes' vdisks.
   c. Reattach the secondary volumes. For details see "Reattaching a secondary volume" (page 283).

Detached volumes remain associated with their replication sets but are not updated with replication data or with replication control information.

**NOTE:**

- It is recommended that the vdisk that you are moving contains only secondary volumes and their snap pools. You are allowed to move other volumes along with secondary volumes and their snap pools, but be sure that you are doing so intentionally.
- If you intend to move a vdisk's enclosure and you want to allow I/O to continue to the other enclosures, it is best if it is at the end of the chain of connected enclosures. If the enclosure is in the middle of the chain, the enclosures must be cabled with no single point of failure, so that removing the enclosure does not prevent communication between other enclosures.

### To detach a secondary volume

1. In the Configuration View panel, right-click the secondary volume and select **Provisioning > Detach Replication Volume**.
2. In the main panel, click **Detach Replication Volume**. A message indicates whether the task succeeded or failed.
3. Click **OK**. When a volume is detached its status is shown as Detached.

## Stopping a vdisk

Stopping a vdisk is part of the process for moving a secondary volume from a primary system into a secondary system. The process to move a secondary volume is:

1. In the system where the secondary volume resides:
   a. Detach the secondary volume. For details see "Detaching a secondary volume" (page 280).
   b. If the secondary volume's vdisk contains other secondary volumes, detach those volumes.
   c. Stop the secondary volume's vdisk.
   d. If the secondary volumes' snap pools are in other vdisks, stop those vdisks.
   e. Move the vdisks into the secondary system. This system must support the link type that the replication set is configured to use. For example, if the replication set's link type is configured to use FC links, the secondary system must have FC ports.
2. In the secondary system:
   a. Start the snap pools' vdisks. For details see "Starting a vdisk" (page 282).
   b. Start the secondary volumes' vdisks.
   c. Reattach the secondary volumes. For details see "Reattaching a secondary volume" (page 283).

Before stopping a vdisk, ensure that all secondary volumes that it contains are detached. When a vdisk is stopped:

- The volumes in the vdisk become inaccessible to hosts.
- Its cached data is flushed to disk.
- Removing its disks will not cause the system to report errors or to attempt reconstruction.

**NOTE:** You cannot stop a vdisk that contains a primary volume.

**NOTE:** If a secondary volume and its snap pool are in different vdisks, you cannot stop the snap pool's vdisk until you stop the secondary volume's vdisk.

### To stop a vdisk

1. In the Configuration View panel, right-click the vdisk and select **Provisioning > Stop Vdisk**.
2. In the main panel, click **Stop Vdisk**. A confirmation prompt appears.
3. Click **Yes** to continue. Otherwise, click **No**. If you clicked **Yes**, the stop operation begins. A message indicates whether the task succeeded or failed. If the stop operation succeeds, the vdisk's health is shown as `Unknown`, its status is shown as `STOP`, and its subcomponents are no longer displayed in the Configuration View panel.
4. If the stop operation succeeded for the secondary volume's vdisk and for its snap pool's vdisk (if applicable), you can move the disks into the remote system.

## Starting a vdisk

Starting a vdisk is part of the process for moving a secondary volume from a primary system into a secondary system. The process to move a secondary volume is:

1. In the system where the secondary volume resides:
   a. Detach the secondary volume. For details see "Detaching a secondary volume" (page 280).
   b. If the secondary volume's vdisk contains other secondary volumes, detach those volumes.
   c. Stop the secondary volume's vdisk. For details see "Stopping a vdisk" (page 281).
   d. If the secondary volumes' snap pools are in other vdisks, stop those vdisks.
   e. Move the vdisks into the secondary system. This system must support the link type that the replication set is configured to use. For example, if the replication set's link type is configured to use FC links, the secondary system must have FC ports.
2. In the secondary system:
   a. Start the snap pools' vdisks.
   b. Start the secondary volumes' vdisks.
   c. Reattach the secondary volumes. For details see "Reattaching a secondary volume" (page 283).

### To start a vdisk

1. In the Configuration View panel, right-click a stopped vdisk and select **Provisioning > Start Vdisk**.
2. In the main panel, click **Start Vdisk**. A message indicates whether the task succeeded or failed.

---

**NOTE:** If the replication set was deleted while the secondary volume's vdisk was stopped, restarting the vdisk will make the set partially reappear. To clean up this remnant, reattach the secondary volume, set it to be the primary volume (by using the Set Replication Primary Volume panel on page 284), and then delete the replication set again.

---

# Reattaching a secondary volume

Reattaching a secondary volume is the last part of the process for moving a secondary volume from a primary system into a secondary system. The process to move a secondary volume is:

1. In the system where the secondary volume resides:
   a. Detach the secondary volume. For details see “Detaching a secondary volume” (page 280).
   b. If the secondary volume’s vdisk contains other secondary volumes, detach those volumes.
   c. Stop the secondary volume’s vdisk. For details see “Stopping a vdisk” (page 281).
   d. If the secondary volumes’ snap pools are in other vdisks, stop those vdisks.
   e. Move the vdisks into the secondary system. This system must support the link type that the replication set is configured to use. For example, if the replication set’s link type is configured to use FC links, the secondary system must have FC ports.
2. In the secondary system:
   a. Start the snap pools’ vdisks. For details see “Starting a vdisk” (page 282).
   b. Start the secondary volumes’ vdisks.
   c. Reattach the secondary volumes.

### To reattach a secondary volume

1. In the Configuration View panel, right-click the secondary volume and select **Provisioning > Reattach Replication Volume**.
2. In the main panel, click **Reattach Replication Volume**. A confirmation dialog appears.
3. Click **Yes** to continue. Otherwise, click **No**. If you clicked **Yes**, a message indicates whether the task succeeded or failed.
4. Click **OK**. In a few seconds, the following changes occur in the Configuration View panel:
   - If the task succeeds, the secondary volume’s status changes to “Establishing proxy” while it is establishing the connection to the remote (primary) system in preparation for replication. Then the status changes to Online. The replication set is ready to resume replication operations.
   - If the reattach operation fails and says it is unable to get the primary volume’s link type, the vdisk that contains the secondary volume may not have completed its startup activities. Wait approximately one minute for these activities to complete, then retry the operation. If this message continues to occur, check the event log to better understand the condition and for an indication of how to correct it.

**NOTE:** If the secondary system does not support the link type that the replication set is configured to use, the secondary volume will be attached with the wrong link type. To fix this, repeat process steps 1 and 2 above to move the secondary volume into a system that supports the required link type.

# Exporting a replication image to a snapshot

If the system is licensed to use remote replication, you can export a replication image to a new standard snapshot. For example, you could export a replication image from a secondary volume for use on the remote system. The standard snapshot will reside in the same snap pool, take a snapshot license, and be independent of the primary replication image, which can continue to be used as a sync point. The standard snapshot can be used like any other standard snapshot, and changes to it will not affect the replication image.

The standard snapshot is subject to the snap pool’s deletion policies. If the snap pool reaches its critical threshold, the snapshot may be deleted, even if it is mapped. If you want to preserve the standard snapshot’s data, you can create a standard volume from the snapshot. See “Creating a volume copy” (page 213).

**NOTE:** The export task will not succeed if the resulting snapshot would exceed license limits.

### To export a replication image to a snapshot

1. In the Configuration View panel, right-click a replication image and select **Provisioning > Export Snapshot**.
2. In the main panel, optionally change the default name for the snapshot. A snapshot name is case sensitive and can have a maximum of 32 bytes. It cannot already exist in a vdisk or include the following: " , < \
3. Click **Export Snapshot**. A message specifies whether the task succeeded or failed.
4. Click **OK**. If the task succeeds, in the Configuration View panel the snapshot appears under the secondary volume on the remote system.

## Changing the primary volume for a replication set

If a replication set's primary system goes offline, and the secondary volume is in a remote system, you can set the secondary volume to be the primary volume so hosts can access that volume and the replicated data it contains.

When the secondary volume becomes the primary volume, it only retains the replication images that the primary volume had and deletes any images that the primary volume did not have. Because the secondary volume may not have successfully replicated all the images associated with the primary volume, the secondary volume might have a subset of the primary volume's images.

If the primary system comes back online, you can set its volume to be the primary volume again.

The following procedures apply to a replication set in which the primary and secondary volume are in separate storage systems. To change the primary volume for a replication set in which both volumes are in the same system (local replication), use the CLI `set replication-primary-volume` command.

### To change the secondary volume of a replication set to be its primary volume

1. On the secondary system, in the Configuration View panel, right-click the secondary volume and select **Provisioning > Set Replication Primary Volume**.
2. In the main panel, select the primary volume in the list.
3. Click **Set Replication Primary Volume**. In the Configuration View panel, the volume's designation changes from Secondary Volume to Primary Volume.

**NOTE:** The offline primary volume remains designated a Primary Volume.

### To change the primary volume of a replication set back to its original primary volume

1. On the primary system:
   a. Create a standard snapshot (page 210) to preserve the primary volume's current data state.
   b. Remove all mappings from the original primary volume: in the Configuration View panel, right-click the original primary volume, select **Provisioning > Explicit Mappings**, record the mappings, and remove them. Then select **Provisioning > Default Mapping**, record the mapping, and remove it.
   c. Select **Provisioning > Set Replication Primary Volume**.
   d. In the main panel, in the Primary Volume list select the primary volume that is in the secondary system.
   e. Click **Set Replication Primary Volume**. In the Configuration View panel, the original primary volume is designated a Secondary Volume.

2. On the secondary system:
   a. Replicate the primary volume (page 276) to the secondary volume that is in the primary system to synchronize their data at the last valid common sync point. This will replicate any data changes made in the secondary volume back to the original primary volume. Let the replication operation complete.

      **NOTE:** An administrator can mount/present/map this snapshot and the snapshot taken in step 1 and compare them to verify any discrepancies.

   b. Remove all mappings from the primary volume: in the Configuration View panel, right-click the primary volume, select **Provisioning > Explicit Mappings**, record the mappings, and remove them. Then select **Provisioning > Default Mapping**, record the mapping, and remove it.
3. On the primary system:
   a. In the Configuration View panel, right-click the secondary volume and select **Provisioning > Set Replication Primary Volume**.
   b. In the main panel, in the Primary Volume list select the original primary volume.
   c. Click **Set Replication Primary Volume**. In the Configuration View panel, the original primary volume is designated a Primary Volume. (The replication set now has a primary volume in each system.)
   d. Re-create the mappings for the primary volume: in the Configuration View panel, right-click the primary volume, select **Provisioning > Default Mapping**, and re-create the default mapping that you recorded. Then select **Provisioning > Explicit Mappings** and re-create the explicit mappings that you recorded.
4. On the secondary system:
   a. In the Configuration View panel, right-click the primary volume and select **Provisioning > Set Replication Primary Volume**.
   b. In the main panel, in the Primary Volume list select the original primary volume.
   c. Click **Set Replication Primary Volume**. The replication set once again has its primary volume in the primary system, and its secondary volume in the secondary system.

# Viewing replication properties, addresses, and images for a volume

In the Configuration View panel, right-click a volume and select **View > Overview**. The Volume Overview table shows:

- As described in "Viewing information about a volume" (page 248): the capacity and space usage of the volume; the quantity of mappings for the volume; and the quantity of task schedules for the volume
- The quantity of replication addresses for the volume
- The quantity of replication images for the volume

For descriptions of storage-space color codes, see "About storage-space color codes" (page 163).

Select a component to see more information about it.

## Replication properties

For a *local* primary or secondary volume, the Replication Properties for *Volume* table shows:

- Name. Replication volume name.
- Serial Number. Replication volume serial number.
- Status. Replication volume status:
  - Initializing: The initial (full) replication to the volume is in progress.
  - Online: The volume is online and is consistent with the last replicated image.
  - Inconsistent: The volume is online but is in an inconsistent state. A full replication is required to initialize it.
  - Replicating: The volume is online and replication is in progress.

    - Replicate-delay: The volume is online but the in-progress replication has been temporarily delayed. A retry is occurring.
    - Suspended: The volume is online but the in-progress replication has been suspended.
    - Offline: The volume cannot be accessed or is unusable due to an error.
    - Establishing proxy: The volume is establishing a proxy connection to a remote volume. This will occur when a detached secondary volume is reattached and is re-establishing a connection with the primary system in preparation for replication.
    - Detached: The volume is detached for removal.
- Status-Reason. More information about the status value, or N/A for Online status.
- Monitor. Replication volume monitoring status:
    - OK: Communication to the remote volume is successfully occurring on the FC or iSCSI network.
    - Failed: Communication to the remote volume has failed because of an FC or iSCSI network issue or because the remote volume has gone offline.
- Location. Local or Remote.
- Primary Volume Name. Primary volume name. If the replication set has a primary-volume conflict, all associated primary volumes are displayed.
- Primary Volume Serial Number. Primary volume serial number. If the replication set has a primary-volume conflict, all associated primary volumes are displayed.
- Primary Volume Status. Primary volume status: Online, Offline, Conflict, or N/A.
- Maximum Number of Queued Images. Number of replication images to consider when determining the next image to replicate. Used only if the On Collision parameter is set to Oldest.
- Maximum Retry Time (Seconds). Amount of time in seconds that the replication volume should retry a replication operation on any specific image when errors occur. Used only if the On Error parameter is set to Retry.
- On Error. Error policy to invoke when errors occur during the replication process: Retry or Suspend.
- Link Type. Type of ports used to link the primary and secondary volumes: FC or iSCSI.
- On Collision. Collision policy used to determine the next image to replicate when multiple replication images are queued: Newest or Oldest.
- Monitor Interval. Interval in seconds at which the primary volume should query the secondary volume.
- Priority. Priority of the replication process on the replication volume: Low, Medium, or High.
- Connection Status.
    - Not Attempted. Communication has not been attempted to the remote volume.
    - Online. The volumes in the replication set have a valid connection but communication is not currently active.
    - Active. Communication is currently active to the remote volume.
    - Offline. No connection is available to the remote system.
- Connection Time. Date and time of the last communication with the remote volume, or N/A.

## Replication addresses

If any remote port addresses are associated with this volume, when you select the Replication Addresses component, the Replication Addresses table shows:

- Connected Ports.
    - For a remote primary or secondary volume, this field shows the IDs of up to two hosts ports in the local system that are connected to the remote system. If two ports are connected but only one is shown, this indicates that a problem is preventing half the available bandwidth from being used.
    - For a local primary or secondary volume, this field shows N/A.
- Remote Address. The address of each host port in the remote system through which the volume is accessible.

## Replication images

If any replication images exist for this volume, when you select the Replication Images component, the Replication Images table shows information about each image. For the selected image, the Replication Images table shows:

- Image Serial Number. Replication image serial number.
- Image Name. User-defined name assigned to the primary replication image.
- Snapshot Serial Number. Replication snapshot serial number associated with the image. The replication snapshot is associated with the replication volume specified in the request.
- Snapshot Name. Replication snapshot name associated with the image. For a secondary replication image, this value is not filled in until the replication is completed.
- Creation Date/Time. Date and time when the replication image was created on the replication volume.

# Viewing information about a remote primary or secondary volume

In the Configuration View panel, right-click a *remote* primary or secondary volume and select **View > Overview**. The Replication Volume Overview table shows:

- Replication properties for the volume
- The quantity of replication addresses for the volume
- The quantity of replication images for the volume

Select a component to see more information about it.

## Replication properties

When you select the Replication component a table shows the volume's replication properties, including the volume's name, serial number, status, status reason, monitor status, and location (local or remote); primary volume name, serial number, and status; maximum number of queued images, maximum retry time, error policy, link type, collision policy, monitor interval, and priority; and connection status and last connection date/time.

## Replication addresses

When you select the Replication Addresses component a table shows:

- Connected Ports.
  - For a remote primary or secondary volume, this field shows the ID of the port in the local system that is being used for communication with the remote system. To determine this, the system first probes all host ports on the controller that owns the replication set to find communication paths to a remote address. After all host ports are probed, if at least one path is found, the IDs of host ports found are shown and the probing stops. If no path is found, the system will repeat this process on the partner controller. If no path is found, N/A is shown.
  - For a local primary or secondary volume, this field shows N/A.
- Remote Address. The address of each host port in the remote system through which the volume is accessible.

## Replication image properties

When you select the Replication Images component a table shows replication image details including the image serial number and name, snapshot serial number and name, and image creation date/time.

# Viewing information about a replication image

In the Configuration View panel, right-click a replication image and select **View > Overview**. The Replication Image Overview table shows:

- Replication status properties
- Primary volume snapshot properties
- Secondary volume snapshot properties

Select a component to see more information about it.

## Replication status properties

When you select the Status component a table shows the status, progress, start date/time, date/time of last update, date/time the replication was suspended, estimated completion time, elapsed or total replication time (including any suspension time). The panel also shows the replication image's serial number.

## Primary-volume snapshot properties

If the snapshot is on the local system, when you select the Primary Volume Snapshot component a table shows the:

- Name and serial number of the pool containing the snapshot
- Snapshot name, creation date/time, status, and status reason
- Source volume name
- Parent volume name
- Base volume name
- Number of snapshots and snapshots in the tree
- Snap pool name
- Amounts of total, unique, and shared data associated with the snapshot
- Default and user-specified retention priorities for this type of snapshot
- Snapshot type

If the snapshot is on a remote system, when you select the Primary Volume Snapshot component a table shows the snapshot serial number and creation date/time.

## Secondary volume snapshot properties

If the snapshot is on the local system, when you select the Secondary Volume Snapshot component a table shows the:

- Name and serial number of the pool containing the snapshot
- Snapshot name, creation date/time, status, and status reason
- Source volume name
- Parent volume name
- Base volume name
- Number of snapshots and snapshots in the tree
- Snap pool name
- Amounts of total, unique, and shared data associated with the snapshot
- Default and user-specified retention priorities for this type of snapshot
- Snapshot type

If the snapshot is on a remote system, when you select the Secondary Volume Snapshot component a table shows the snapshot serial number and creation date/time.

# A SNMP reference

This appendix describes the Simple Network Management Protocol (SNMP) capabilities that AssuredSAN storage systems support. This includes standard MIB-II, the FibreAlliance SNMP Management Information Base (MIB) version 2.2 objects, and enterprise traps.

AssuredSAN 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

AssuredSAN 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`) is based on the vendor name followed by ".2." and the identifier for the particular product model. For example, the object identifier for AssuredSAN storage systems is 1.3.6.1.4.1.11.2.347. 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, `dhtraps.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 WBI.

The text of the trap MIB is included at the end of this appendix.

# 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 WBI. The statistics section is not implemented.

The following table lists the MIB objects, their descriptions and the value set in a AssuredSAN storage system. 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 | 0220 |
| `UNumber` | Number of connectivity units present | 1 |
| `SystemURL` | Top-level URL of the 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`) |

**Table 30 FA MIB 2.2 objects, descriptions, and values (continued)**

| Object | Description | Value |
|---|---|---|
| **connUnitTable** | **Includes the following objects as specified by the FA MIB2.2 Spec** | |
| 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 |
| connUnitConfiguration ChangeTime | Same as configurationChangeTime | Same as configurationChangeTime |
| 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 |

**Table 30 FA MIB 2.2 objects, descriptions, and values (continued)**

| Object | Description | Value |
|---|---|---|
| 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 |
| connUnitEventFilter | Defines the event severity that will be logged by this connectivity unit. Settable only through WBI. | 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 |
| **connUnitRevsTable** | **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 connUnitRevsTable” (page 296) |
| 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 connUnitRevsTable” (page 296) |
| **connUnitSensorTable** | **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 connUnitSensorTable” (page 297) |
| connUnitSensorName | Display string containing textual identification of the sensor intended primarily for operator use | See “External details for connUnitSensorTable” (page 297) |
| 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 |

**Table 30 FA MIB 2.2 objects, descriptions, and values (continued)**

| Object | Description | Value |
|---|---|---|
| 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 connUnitSensorTable” (page 297) |
| connUnitSensor Characteristic | Characteristics being monitored by this sensor | See “External details for connUnitSensorTable” (page 297) |
| **connUnitPortTable** | **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 |
| 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) |
| connUnitPortTransmitter Type | 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<br><br>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 |

**Table 30 FA MIB 2.2 objects, descriptions, and values (continued)**

| Object | Description | Value |
|---|---|---|
| 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 connUnitPortTable" (page 298) |
| connUnitPortPhysical Number | Port number represented on the hardware | Port number represented on the hardware |
| connUnitPortStatObject | Not supported | 0 (No statistics available) |
| **connUnitEventTable** | **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 |
| connUnitREventTime | Real time when the event occurred, in the following format:<br>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 |
| connUnitLinkTable | Not supported | N/A |
| connUnitPortStatFabric Table | Not supported | N/A |
| connUnitPortStatSCSITable | Not supported | N/A |
| connUnitPortStatLANTable | Not supported | N/A |
| **SNMP TRAPS** | **The following SNMP traps are supported** | |
| trapMaxClients | Maximum number of trap clients | 1 |
| 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 |

**Table 30 FA MIB 2.2 objects, descriptions, and values (continued)**

| Object | Description | Value |
|---|---|---|
| trapRegTable | 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)<br>WRITE: Not supported |
| **Enterprise-specific fields** | **Includes the following objects** | |
| cpqSiSysSerialNum | System serial number | For example, 3CL8Y40991 |
| cpqSiSysProductId | System product ID | For example, 481321-001 |
| cpqSiProductName | System product name | For example, DH4824 |
| cpqHoMibStatusArray | An array of MIB status structures. Octets 0–3 in block 0 are reserved for systems management and serve as an aggregate of the other MIBs. | Octet 0: 0.<br>Octet 1 (overall status):<br>0 = Not available;<br>1 = Unknown/other;<br>2 = OK/normal;<br>3 = Degraded/warning;<br>4 = Failed/critical<br>Octet 2 (system flags):<br>9 = device is not a server and web-based management is enabled<br>Octet 3 (device type):<br>14 = enclosure<br>For example, 00.02.09.14 (hex) |
| cpqHoGUID | Globally unique identifier formed from the product ID and serial number | For example, 4813213CL8Y40991 |

# External details for certain FA MIB 2.2 objects

Tables in this section specify values for certain objects described in Table 30.

## External details for connUnitRevsTable

**Table 31 connUnitRevsTable index and description values**

| connUnitRevsIndex | connUnitRevsDescription |
|---|---|
| 1 | CPU Type for Storage Controller (Controller A) |
| 2 | Bundle revision for Controller (Controller A) |
| 3 | Build date for Storage Controller (Controller A) |
| 4 | Code revision for Storage Controller (Controller A) |
| 5 | Code baselevel for Storage Controller (Controller A) |
| 6 | FPGA code revision for Memory Controller (Controller A) |
| 7 | Loader code revision for Storage Controller (Controller A) |
| 8 | CAPI revision (Controller A) |
| 9 | Code revision for Management Controller (Controller A) |
| 10 | Loader code revision for Management Controller (Controller A) |
| 11 | Code revision for 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 interface hardware (chip) revision (Controller A) |
| 18 | Disk interface hardware (chip) revision (Controller A) |
| 19 | CPU Type for Storage Controller (Controller B) |
| 20 | Bundle revision for Controller (Controller B) |
| 21 | Build date for Storage Controller (Controller B) |
| 22 | Code revision for Storage Controller (Controller B) |
| 23 | Code baselevel for Storage Controller (Controller B) |
| 24 | FPGA code revision for Memory Controller (Controller B) |
| 25 | Loader code revision for Storage Controller (Controller B) |
| 26 | CAPI revision (Controller B) |
| 27 | Code revision for Management Controller (Controller B) |
| 28 | Loader code revision for Management Controller (Controller B) |
| 29 | Code revision for 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) |

**Table 31 connUnitRevsTable index and description values (continued)**

| connUnitRevsIndex | connUnitRevsDescription |
|---|---|
| 35 | Host interface hardware (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 Controller Temperature (Controller A) | board(8) | temperature(3) |
| 10 | Memory Controller Temperature (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) |
| 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) |

**Table 32 connUnitSensorTable index, name, type, and characteristic values (continued)**

| connUnitSensorIndex | connUnitSensorName | connUnitSensorType | connUnitSensor Characteristic |
|---|---|---|---|
| 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 |
|---|---|
| 1 | Host Port 1 (Controller A) |
| 2 | Host Port 2 (Controller B) |
| 3 | Host Port 1 (Controller A) |
| 4 | Host Port 2 (Controller B) |

# Configuring SNMP event notification in WBI

1. Verify that the storage system's SNMP service is enabled. See "Changing management interface settings" (page 176).
2. Configure and enable SNMP traps. See "Configuring SNMP notification" (page 178).
3. Optionally, configure a user account to receive SNMP traps. See "Configuring user accounts" (page 178).

# SNMP management

You can manage storage devices using SNMP with a network management system such as HPE OpenView, HPE System Insight Manager (SIM), or HPE Instant Support Enterprise Edition (ISEE). See their documentation for information about loading MIBs, configuring events, and viewing and setting group objects.

In order to view and set system group objects, SNMP must be enabled in the storage system. See "Changing management interface settings" (page 176). 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 "Configuring user accounts" (page 178). The same users, security protocols, and passwords must be configured in the network management system.

# Enterprise trap MIB

The following pages show the source for the enterprise traps MIB, `dhtraps.mib`. This MIB defines the content of the SNMP traps that AssuredSAN storage systems generate.

```
-- ------------------------------------------------------
-- Dot Hill Low Cost Array MIB for SNMP Traps
--
-- $Revision: 11692 $
--
-- Copyright 2005 Dot Hill Systems Corp.
-- All rights reserved. Use is subject to license terms.
--
-- ------------------------------------------------------

DHTRAPS-MIB
-- Last edit date: Nov 11th, 2005
DEFINITIONS ::= BEGIN
  IMPORTS
    enterprises
        FROM RFC1155-SMI
    TRAP-TYPE
        FROM RFC-1215
    connUnitEventId, connUnitEventType, connUnitEventDescr
        FROM FCMGMT-MIB;


    --Textual conventions for this MIB

-------------------------------------------------------------------------
    -- formerly Box Hill
    dothill    OBJECT IDENTIFIER ::= { enterprises 347 }


-- Related traps

    dhEventInfoTrap TRAP-TYPE
        ENTERPRISE dothill
        VARIABLES { connUnitEventId,
                    connUnitEventType,
                    connUnitEventDescr }
        DESCRIPTION
            "An event has been generated by the storage array.
            Recommended severity level (for filtering): info"

        -- Trap annotations are as follows:
        --#TYPE "Informational storage event"
        --#SUMMARY "Informational storage event # %d, type %d, description: %s"
        --#ARGUMENTS {0,1,2}
        --#SEVERITY INFORMATIONAL
        --#TIMEINDEX 6
        ::= 1
```

```
dhEventWarningTrap TRAP-TYPE
    ENTERPRISE dothill
    VARIABLES { connUnitEventId,
                connUnitEventType,
                connUnitEventDescr }
    DESCRIPTION
        "An event has been generated by the storage array.
        Recommended severity level (for filtering): warning"

    -- Trap annotations are as follows:
    --#TYPE "Warning storage event"
    --#SUMMARY "Warning storage event # %d, type %d, description: %s"
    --#ARGUMENTS {0,1,2}
    --#SEVERITY MINOR
    --#TIMEINDEX 6
    ::= 2

dhEventErrorTrap TRAP-TYPE
    ENTERPRISE dothill
    VARIABLES { connUnitEventId,
                connUnitEventType,
                connUnitEventDescr }
    DESCRIPTION
        "An event has been generated by the storage array.
        Recommended severity level (for filtering): error"

    -- Trap annotations are as follows:
    --#TYPE "Error storage event"
    --#SUMMARY "Error storage event # %d, type %d, description: %s"
    --#ARGUMENTS {0,1,2}
    --#SEVERITY MAJOR
    --#TIMEINDEX 6
    ::= 3

dhEventCriticalTrap TRAP-TYPE
    ENTERPRISE dothill
    VARIABLES { connUnitEventId,
                connUnitEventType,
                connUnitEventDescr }
    DESCRIPTION
        "An event has been generated by the storage array.
        Recommended severity level (for filtering): critical"

    -- Trap annotations are as follows:
    --#TYPE "Critical storage event"
    --#SUMMARY "Critical storage event # %d, type %d, description: %s"
    --#ARGUMENTS {0,1,2}
```

```
        --#SEVERITY CRITICAL
        --#TIMEINDEX 6
        ::= 4

END
```

# B Using FTP

Although the WBI is the preferred interface for downloading log data and historical disk-performance statistics, updating firmware, installing a license, and installing a security certificate, you can also use FTP to do these tasks.

**IMPORTANT:** 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 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 client. A GUI-based FTP client might not work.

### To download system logs

1. In the WBI, prepare to use FTP:
   a. Determine the network-port IP addresses of the system's controllers. See "Changing network interface settings" (page 66).
   b. Verify that the system's FTP service is enabled. See "Changing management interface settings" (page 176).
   c. Verify that the user you will log in as has permission to use the FTP interface. See "Modifying users" (page 180).
2. Open a Command Prompt (Windows) or a terminal window (UNIX) and navigate to the destination directory for the log file.
3. Enter:

   **ftp** *controller-network-address*

   For example:

   **ftp 10.1.0.9**
4. Log in as a user that has permission to use the FTP interface.
5. Enter:

   **get logs** *filename*.**zip**

   where *filename* is the file that will contain the logs. It is recommended to choose a filename that identifies the system, controller, and date.

   For example:

   **get logs Storage2_A_20120126.zip**

   Wait for the message `Operation Complete` to appear.
6. Quit the FTP session.
7. If the problem to diagnose seems specific to user-interface behavior, repeat step 3 through step 6 on the partner controller to collect its unique MC log data.

**NOTE:** You must uncompress a zip file before you can view the files it contains. To examine diagnostic data, first view `store_yyyy_mm_dd__hh_mm_ss.logs`.

## 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 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" (page 165).

Use a command-line-based FTP client. A GUI-based FTP client might not work.

### To transfer log data to a log-collection system

1. In the WBI, prepare to use FTP:
   a. Determine the network-port IP addresses of the system's controllers. See "Changing network interface settings" (page 185).
   b. Verify that the system's FTP service is enabled. See "Changing management interface settings" (page 176).
   c. Verify that the user you will log in as has permission to use the FTP interface. See "Modifying users" (page 180).
2. On the log-collection system, open a Command Prompt (Windows) or a terminal window (UNIX) and navigate to the destination directory for the log file.
3. Enter:

   **`ftp`** *`controller-network-address`*

   For example:

   **`ftp 10.1.0.9`**
4. Log in as a user that has permission to use the FTP 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 will contain the transferred data. It is recommended to choose a filename that identifies the system, controller, log type, and date.

   For example:

   **`get managed-logs:scdebug Storage2-A_scdebug_2011_08_22.zip`**

   Wait for the message `Operation Complete` to appear.
6. Quit the FTP session.

**NOTE:** You must uncompress a zip file before you can view the files it contains.

# Downloading historical disk-performance statistics

You can access the storage system's FTP 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 CLI Reference 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 client. A GUI-based FTP client might not work.

### To retrieve historical disk-performance statistics

1. In the WBI, prepare to use FTP:
   a. Determine the network-port IP addresses of the system's controllers. See "Changing network interface settings" (page 185).
   b. Verify that the system's FTP service is enabled. See "Changing management interface settings" (page 176).
   c. Verify that the user you will log in as has permission to use the FTP interface. See "Modifying users" (page 180).
2. Open a Command Prompt (Windows) or a terminal window (UNIX) and navigate to the destination directory for the log file.
3. Enter:

   **ftp** *controller-network-address*

   For example:

   **ftp 10.1.0.9**
4. Log in as a user that has permission to use the FTP interface.
5. Enter:

   **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* is the file that will contain the data. It is recommended to choose a filename that identifies the system, controller, and date.

   For example:

   **get perf:start.2012-01-26.12:00.PM.end.2012-01-26.23:00.PM Storage2_A_20120126.csv**

   Wait for the message `Operation Complete` to appear.
6. Quit the FTP session.

# Updating firmware

You can update the versions of firmware in controller modules, expansion modules (in drive enclosures), and disks.

**TIP:** 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.

**IMPORTANT:**

- If a disk group is quarantined, resolve the problem that is causing the disk group to be quarantined before updating firmware. See information about events 172 and 485 in the Event Descriptions Reference Guide, and "Removing a vdisk from quarantine" (page 231).
- If any unwritten cache data is present, firmware update will not proceed. Before you can update firmware, unwritten data must be removed from cache. See information about event 44 in the Event Descriptions Reference Guide and information about the `clear cache` command in the CLI Reference Guide.
- If the system's health is Fault, firmware update will not proceed. Before you can update firmware, you must resolve the problem specified by the Health Reason value on the System Overview panel (page 235).

## Updating controller-module firmware

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

If you have a dual-controller system and the Partner Firmware Update (PFU) option is enabled, when you update one controller the system automatically updates the partner controller. If PFU is disabled, after updating firmware on one controller you must log into the partner controller's IP address and perform this firmware update on that controller also.

For best results, the storage system should be in a healthy state before starting firmware update.

**NOTE:** For information about supported releases for firmware update, see the product's Release Notes.

### To update controller-module firmware

1. Obtain the appropriate firmware file and download it to your computer or network.
2. In the WBI, prepare to use FTP:
   a. Determine the network-port IP addresses of the system's controllers.
   b. Verify that the system's FTP service is enabled.
   c. Verify that the user you will log in as has permission to use the FTP interface.
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 navigate to the directory containing the firmware file to load.
5. Enter:

   **`ftp`** *`controller-network-address`*

   For example:

   **`ftp 10.1.0.9`**
6. Log in as an FTP user.

7. Enter:

   **put** *firmware-file* **flash**

   For example:

   **put T230R01-01.bin 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 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 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 expansion module's enclosure management processor (EMP) to be updated. This typically takes 2.5 minutes for each EMP in a drive enclosure.

   **NOTE:** If you are using a Windows FTP client, during firmware update a client-side FTP application issue can cause the FTP session to be aborted. If this issue persists try using the WBI to perform the update, use another client, or use another FTP application.

   If the Storage Controller cannot be updated, the update operation is cancelled. If the FTP prompt does not return, quit the FTP 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 message `Operation Complete` is printed, the FTP session returns to the `ftp>` prompt, and the FTP session to the local MC is closed.

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

8. Quit the FTP session.
9. Clear your web browser's cache, then sign in to the WBI. 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:** After firmware update has completed on both controllers, 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 and drawer firmware

A drive enclosure can contain one or two expansion modules. Each expansion module contains an enclosure management processor (EMP). In an enclosure with drawers, each drawer contains two EMPs, which are also referred to as "modules." All modules of the same product model should run the same firmware version.

Expansion-module and drawer firmware is updated in either of two ways:

- When you update controller-module firmware, all expansion-module and drawer EMPs are automatically updated to a compatible firmware version.
- You can update the firmware in each expansion-module and drawer EMP by loading a firmware file obtained from the enclosure vendor.

You can specify to update all expansion modules or only specific expansion modules. If you specify to update all expansion modules and the system contains more than one type of enclosure, the update will be attempted on all enclosures in the system. The update will only succeed for enclosures whose type matches the file, and will fail for enclosures of other types.

### To update expansion-module and drawer firmware

1. Obtain the appropriate firmware file and download it to your computer or network.
2. If you want to update all expansion modules, continue with the next step. Otherwise, in the WBI, 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's 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. It is recommended to perform update tasks consistently through one controller to avoid confusion.
3. In the WBI, prepare to use FTP:
   a. Determine the network-port IP addresses of the system's controllers.
   b. Verify that the system's FTP service is enabled.
   c. Verify that the user you will log in as has permission to use the FTP interface.
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 navigate to the directory containing the firmware file to load.
6. Enter:

   **ftp** *controller-network-address*

   For example:

   **ftp 10.1.0.9**
7. Log in as an FTP user.
8. Either:
   - To update all expansion modules, enter:

     **put** *firmware-file* **encl**
   - To update specific expansion modules, enter:

     **put** *firmware-file* **encl:***EMP-bus-ID***:***EMP-target-ID*

     For example:

     **put S110R01.bin encl:1:63**

   **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 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.

### To 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 WBI, 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 WBI, prepare to use FTP:
   a. Determine the network-port IP addresses of the system's controllers.
   b. Verify that the system's FTP service is enabled.
   c. Verify that the user you will log in as has permission to use the FTP interface.
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.

### To update disk firmware

1. Open a Command Prompt (Windows) or a terminal window (UNIX) and navigate to the directory containing the firmware file to load.
2. Enter:

   **ftp** *controller-network-address*

   For example:

   **ftp 10.1.0.9**
3. Log in as an FTP user.
4. Either:
   - To update all disks of the type that the firmware applies to, enter:

     **put** *firmware-file* **disk**
   - To update specific disks, enter:

     **put** *firmware-file* **disk:***enclosure-ID***:***slot-number*

     For example:

     **put** *firmware-file* **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 occurs, contact technical support.

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

**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.

5. If you are updating specific disks, repeat step 4 for each remaining disk to update.
6. Quit the FTP session.
7. If the updated disks must be power cycled:
   a. Shut down both controllers by using the WBI.
   b. Power cycle all enclosures as described in your product's Setup Guide.
8. Verify that each disk has the correct firmware revision.

# Installing a license file

1. Ensure that the license file is saved to a network location that the storage system can access.
2. Open a Command Prompt (Windows) or a terminal window (UNIX) and navigate to the directory containing the license file to load.
3. Log in to the controller enclosure that the file was generated for:

   **ftp** *controller-network-address*

   For example:

   **ftp 10.1.0.9**
4. Log in as an FTP user.
5. Enter:

   **put** *license-file* **license**

   For example:

   **put certificate.txt license**

   A message confirms whether installation succeeded or failed. If installation succeeds, licensing changes take effect immediately.

# 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 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.

### To install a security certificate

1. In the WBI, prepare to use FTP:
   a. Determine the network-port IP addresses of the system's controllers. See "Changing network interface settings" (page 185).
   b. Verify that the system's FTP service is enabled. See "Changing management interface settings" (page 176).
   c. Verify that the user you will log in as has permission to use the FTP interface. See "Modifying users" (page 180).
2. Open a Command Prompt (Windows) or a terminal window (UNIX) and navigate to the directory that contains the certificate files.

3. Enter:

   **ftp** *controller-network-address*

   For example:

   **ftp 10.1.0.9**
4. Log in as a user that has permission to use the FTP interface.
5. Enter:

   **put** *certificate-file-name* **cert-file**

   where *certificate-file-name* is the name of the certificate file for your specific system.
6. Enter:

   **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.

# 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's FTP 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 WBI, prepare to use FTP:
   a. Determine the network-port IP addresses of the system's controllers. See "Changing network interface settings" (page 66).
   b. Verify that the system's FTP service is enabled. See "Changing system services settings" (page 65).
   c. Verify that the user you will log in as has permission to use the FTP interface. See "To modify a user" (page 56).
2. Open a Command Prompt (Windows) or a terminal window (UNIX) and navigate to the destination directory for the log file.
3. Enter:

   **ftp** *controller-network-address*

   For example:

   **ftp 10.1.0.9**
4. Log in as a user that has permission to use the FTP interface.
5. Enter:

   **get logs:heatmap** *filename.csv*

   where: *filename* is the file that will contain the data.

   For example:

   **get logs:heatmap IO_density.csv**

   Wait for the message `Operation Complete` to appear.
6. Quit the FTP session.

# C 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.

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. SMI-enabled management clients such as HPE SIM or HPE Storage Essentials can perform storage management tasks such as monitoring, configuring or event-management. 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 Target Ports subprofile
- SAS Target Ports subprofile
- iSCSI Target Ports subprofile
- 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
- DMTF Device Tray profile (if disk drawers exist)
- Thin Provisioning profile
- Pools from Volumes profile

The embedded SMI-S provider supports:

- HTTP/HTTPS using SSL encryption on the default port 5989, or standard HTTP/HTTPS 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, AssuredSAN storage systems), and provides the CIMOM with information about them. In theory, providers for multiple types of devices (for example, AssuredSAN 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 CMPI (Common Management Protocol Interface) provider and uses this interface. To reduce the memory footprint, a third-party package called CIMPLE (www.simplewbem.org) is used. For more information on SFCB go to http://sourceforge.net/projects/sblim/files/sblim-sfcb.

# About the AssuredSAN SMI-S provider

The GL105 provider is a SMI-S 1.5 provider which passes CTP 1.5 tests. Full provisioning is supported. CTP results can be found at http://www.snia.org/ctp/conformingproviders/dothill.html.

The AssuredSAN 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.

AssuredSAN CNC and SAS systems are supported.The classes for Dot Hill are `DHS_XXX`. The device namespace for Dot Hill is `/root/dhs`.

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/dhs`
- 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 array systems. It provides a high-level overview of the array system. |
| Block Services package | Defines a standard expression of existing storage capacity, the assignment of capacity to Storage Pools, and allocation of capacity to be used by external devices or applications. |
| Physical Package package | Models information about a storage system's physical package and optionally about internal sub-packages. |
| Health package | Defines the general mechanisms used in expressing health in SMI-S. |
| Server profile | Defines the capabilities of a CIM object manager based on the communication mechanisms that it supports. |
| FC Target Ports profile | Models the Fibre Channel-specific aspects of a target storage system. |
| SAS Target Ports subprofile | Models the SAS-specific aspects of a target storage system. |
| iSCSI Target Ports subprofile | Models the iSCSI-specific aspects of a target storage system. |
| Access Points subprofile | Provides addresses of remote access points for management services. |
| 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. |
| 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. |

**Table 34 Supported SMI-S profiles (continued)**

| Profile/subprofile/package | Description |
|---|---|
| DMTF Device Tray profile | Models enclosure drawers and their relationship to the disks & sensors. Also, enables service personnel to flash the LEDs on the drawers and stop and start the drawers using SMI-S. |
| Thin Provisioning profile | Specializes the Block Services Package to add support for thin provisioning of volumes.<br>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" (page 317).

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 Table 35 pertain to FRU assemblies and certain FRU components.

**Table 35 CIM Alert indication events**

| FRU/Event category | Corresponding SMI-S class | Operational status values that would trigger alert conditions |
|---|---|---|
| Controller | DHS_Controller | Down, Not Installed, OK |
| Hard Disk Drive | DHS_DiskDrive | Unknown, Missing, Error, Degraded, OK |
| Fan | DHS_PSUFan | Error, Stopped, OK |
| Power Supply | DHS_PSU | Unknown, Error, Other, Stressed, Degraded, OK |
| Temperature Sensor | DHS_OverallTempSensor | Unknown, Error, Other, Non-Recoverable Error, Degraded, OK |
| Battery/Super Cap | DHS_SuperCap | Unknown, Error, OK |
| FC Port | DHS_FCPort | Stopped, OK |

**Table 35 CIM Alert indication events**

| FRU/Event category | Corresponding SMI-S class | Operational status values that would trigger alert conditions |
|---|---|---|
| SAS Port | DHS_SASTargetPort | Stopped, OK |
| iSCSI Port | DHS_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_InstCreation WHERE SourceInstance ISA CIM_StoragePool`<br>Send life cycle indication when a vdisk is created or deleted. | Both |
| Block Services | `SELECT * FROM CIM_InstCreation WHERE SourceInstance ISA CIM_StorageVolume`<br>Send life cycle indication when a volume is created or deleted. | Both |
| Block Services | `SELECT * FROM CIM_InstModification WHERE SourceInstance ISA CIM_LogicalDevice`<br>Send life cycle indication when disk drive (or any logical device) status changes. | Both |
| Copy Services | `SELECT * FROM CIM_InstModification WHERE SourceInstance ISA CIM_StorageSynchronized AND SourceInstance.SyncState <> PreviousInstance.SyncState`<br>Send life cycle indication when the snapshot synchronization state changes. | CQL |
| Disk Drive Lite | `SELECT * FROM CIM_InstCreation WHERE SourceInstance ISA CIM_DiskDrive`<br>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`<br>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`<br>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`<br>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`<br>Send life cycle indication when a LUN is created, deleted, or modified. | Both |

**Table 36 Life cycle indications (continued)**

| Profile or subprofile | Element description and name | WQL or CQL |
|---|---|---|
| Multiple Computer System | `SELECT * FROM CIM_InstCreation WHERE SourceInstance ISA CIM_ComputerSystem`<br>Send life cycle indication when a controller is powered on or off. | Both |
| Multiple Computer System | `SELECT * FROM CIM_InstModification WHERE SourceInstance ISA CIM_ComputerSystem AND SourceInstance.OperationalStatus <> PreviousInstance.OperationalStatus`<br>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`<br>Send life cycle indication when the controller active-active configuration changes. | WQL |
| Target Ports | `SELECT * FROM CIM_InstCreation WHERE SourceInstance ISA CIM_FCPort`<br>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`<br>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, which is the recommended protocol for SMI-S.
- The SMI-S interface is enabled for the `manage` user.

Table 37 lists the CLI commands relevant to the SMI-S protocol:

**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 |

### To configure the SMI-S interface for other users:

1. Log in as `manage`
2. If the user does not already exist, create one using this command:

   `create user role manage` *`username`*
3. Type this command:

   `set user` *`username`* `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. For more information about the managed logs feature, see "About managed logs" (page 165).

To set up SMI-S to listen for managed logs notifications:

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.

## Testing SMI-S

Use an SMI-S certified client for SMI-S 1.5. Dot Hill has clients such as HPE SIM and HPE Storage Essentials. Other common clients are 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 provides solutions to common SMI-S problems.

**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 protocol smis 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 users" (page 178) 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. | Install wbemcli on a Linux system by typing: `apt-get install wbemcli`<br>Type: `wbemcli -nl -t -noverify ein 'https://manage:!manage@:5989/root/dhs:cim_computersystem'` |
| SMI-S is not responding to client requests. | SMI-S configuration may have become corrupted. | Use the CLI command `reset smis-configuration`. Refer to the CLI Reference Guide for further information. |

# D 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” (page 165).

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.

## 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, SNMP traps, or SMI-S 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 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” (page 303).

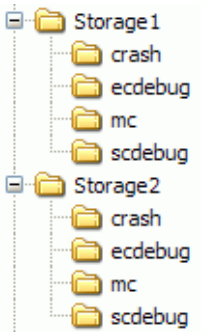
## Log-file details

- 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 interface to get the log and save it into the `scdebug` subdirectory of the `Storage2` directory.

# Glossary

| | |
|---|---|
| **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. |
| **2U48** | An enclosure that is two rack units in height and can contain 48 disks. |
| **4U56** | An enclosure that is four rack units in height and can contain 56 disks. |
| **Additional Sense Code/Additional Sense Code Qualifier** | See ASC/ASCQ. |
| **Advanced Encryption Standard** | *See* AES. |
| **AES** | Advanced Encryption Standard. A specification for the encryption of data using a symmetric-key algorithm. |
| **Air Management Sled** | *See* AMS. |
| **Air Management Solution** | *See* AMS. |
| **allocated page** | A page of storage-pool space that has been allocated to a volume to store data. |
| **allocation rate** | The rate, in pages per minute, at which a pool is allocating pages to its volumes because they need more space to store data. |
| **ALUA** | Asymmetric Logical Unit Access. |
| **AMS** | For a 2U12 or 2U24 enclosure, Air Management Sled. A drive blank designed to fill an empty disk slot in an enclosure to maintain optimum airflow through the chassis.<br>For a 2U48 enclosure, Air Management Solution. A plastic insert designed to fill an empty disk bay (four disk slots) within a drawer to maintain optimum airflow through the chassis. |
| **array** | *See* storage system. |
| **ASC/ASCQ** | Additional Sense Code/Additional Sense Code Qualifier. Information on sense data returned by a SCSI device. |
| **ATS** | Automated tiered storage. A paged-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. |
| **automated tiered storage** | *See* ATS. |
| **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, and 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** | For virtual storage, a volume that is not a snapshot of any other volume, and is the root of a snapshot tree. |
| **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 sheetmetal housing of an enclosure. |
| **child volume** | For virtual storage, the snapshot of a parent volume in a snapshot tree. |

| | |
|---|---|
| **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. |
| **CIM Query Language** | *See* CQL. |
| **CIMOM** | Common Information Model Object Manager. A component in CIM that handles the interactions between management applications and providers. |
| **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. |
| **comma separated values** | *See* CSV. |
| **Common Information Model** | *See* CIM. |
| **Common Information Model Object Manager** | *See* CIMOM. |
| **compatible disk** | A disk that can be used to replace a failed member disk of a disk group because it both has enough capacity and is of the same type (enterprise SAS, for example) as the disk that failed. *See also* available disk, dedicated spare, dynamic spare, and global spare. |
| **complex programmable logic device** | *See* CPLD. |
| **Configuration Application Programming Interface** | *See* CAPI. |
| **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 nonvolatile memory (CompactFlash); host, expansion, network, and service ports; and midplane connectivity. |
| **converged network controller** | *See* CNC. |
| **Coordinated Universal Time** | *See* UTC. |
| **CPLD** | Complex programmable logic device. An electronic component used to build reconfigurable digital circuits. It can replace large numbers of logic gates. |
| **CQL** | CIM Query Language. |
| **CRC** | Cyclic Redundancy Check. A mathematical algorithm that, when implemented in software or hardware, can be used to detect errors in data. |
| **CSV** | Comma separated values. A format to store tabular data in plain-text form. |
| **Cyclic Redundancy Check** | *See* CRC. |
| **DAS** | Direct Attached Storage. A dedicated storage device that connects directly to a host without the use of a switch. |
| **Data Encryption Standard** | *See* DES. |
| **deallocation rate** | The rate, in pages per minute, at which a 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, and 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 and masking. |
| **DES** | Data Encryption Standard. An algorithm for the encryption of electronic data. |
| **DHCP** | Dynamic Host Configuration Protocol. A network configuration protocol for hosts on IP networks. |
| **Direct Attached Storage** | *See* DAS. |
| **disk group** | A set of disk drives that is configured to use a specific RAID type and provides storage capacity for a pool. *See also* linear disk group and virtual disk group. |
| **Distributed Management Task Force** | *See* DMTF. |
| **DMTF** | Distributed Management Task Force. An industry organization that develops and maintains standards for system management. |
| **drain** | For virtual storage, the automatic movement of active volume data from a disk group to other disk-group members within the same pool. |
| **drawer** | In a 2U48 enclosure, one of three FRUs that each holds up to 16 disks. In a 4U56 enclosure, one of two FRUs that each holds 28 disks. |
| **drive enclosure** | *See* expansion enclosure. *See also* JBOD. |
| **drive spin down** | *See* DSD. |
| **DRM** | Disaster recovery management. Storage-system firmware features that, when the Site Replication Adapter (SRA) feature is enabled, support the use of VMware's Site Recovery Manager to automate disaster-recovery failover and failback tasks. *See also* SRA. |
| **DSD** | Drive spin down. A power-saving feature that monitors disk activity in the storage system and spins down inactive disks based on user-selectable policies. Drive spin down is not applicable to disks in virtual pools. |
| **dual-port disk** | A disk that is connected to both controllers so it has two data paths, achieving fault tolerance. |
| **Dynamic Host Configuration Protocol** | *See* DHCP. |
| **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, and global spare. |
| **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, MC, and SC. |
| **EMP** | Enclosure management processor. An EC 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. |
| **enclosure management processor** | *See* EMP. |
| **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* JBOD. |
| **expansion module** | A FRU that contains the following subsystems and devices: a SAS expander and EC 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 and 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* recovery. |
| **fan module** | The fan FRU used in 4U56 enclosures. There are two in each enclosure, separate from the PSUs. |
| **FC** | Fibre Channel interface protocol. |
| **FC-AL** | Fibre Channel Arbitrated Loop. The FC topology in which devices are connected in a one-way loop. |
| **FDE (for AssuredSAN 4004 only)** | Full disk encryption. A method by which you can secure the data residing on a system. *See also* lock key, passphrase, repurpose, and SED. |
| **Fibre Channel Arbitrated Loop** | *See* FC-AL. |
| **field-programmable gate array** | *See* FPGA. |
| **FPGA** | Field-programmable gate array. An integrated circuit designed to be configured after manufacturing. |
| **FRU** | Field-replaceable unit. A part that can be removed and replaced by the user or support technician without having to send the product to a repair facility. |
| **full disk encryption (for AssuredSAN 4004 only)** | *See* FDE. |
| **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, and dynamic spare. |
| **HBA** | Host bus adapter. A device that facilitates I/O processing and physical connectivity between a host and the storage system. |
| **host** | (v3) A user-defined group of initiators that represents a server or switch.<br>(v2) An external port that the storage system is attached to. The external port may be a port in an I/O adapter in a server, or a port in a network switch. Product interfaces use the terms host and initiator interchangeably. |
| **host bus adapter** | *See* HBA. |
| **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. |
| **image ID** | For linear replication, a globally unique serial number that identifies the point-in-time image source for a volume. All volumes that have identical image IDs have identical data content, whether they be snapshots or stand-alone volumes. |
| **initiator** | (v3) 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.<br>(v2) *See* host. |
| **I/O Manager** | A MIB-specific term for a controller module. |
| **I/O module** | *See* IOM. |
| **IOM** | Input/output module. An IOM can be either a controller module or an expansion module. |
| **IQN** | iSCSI Qualified Name. |
| **iSCSI** | Internet SCSI interface protocol. |
| **iSNS** | Internet Storage Name Service. |
| **JBOD** | “Just a bunch of disks.” *See* drive enclosure. |
| **large form factor** | *See* LFF. |
| **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** | A set of disk drives that is configured to use a specific RAID type. The number of disks that a 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** | 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 (for AssuredSAN 4004 only)** | A system-generated value that manages the encryption and decryption of data on FDE-capable disks. *See also* FDE and passphrase. |
| **logical block address** | *See* LBA. |
| **Logical Unit Number** | *See* LUN. |
| **loop** | *See* FC-AL. |
| **Loop Initialization Primitive** | *See* LIP. |
| **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. |
| **Management Information Base** | *See* MIB. |
| **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, and masking. |
| **masking** | A volume-mapping setting that specifies no access to that volume by hosts. *See also* default mapping and explicit mapping. |
| **master volume** | For linear storage, a volume that is enabled for snapshots and has an associated snap pool. |
| **MC** | Management Controller. A processor (located in a controller module) that is responsible for human-computer interfaces, such as the WBI, and computer-computer interfaces, such as SNMP, and interacts with the Storage Controller. *See also* EC and SC. |
| **Media Access Control Address** | *See* MAC address. |
| **metadata** | Data in the first sectors of a disk drive that stores all 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. |
| **mount** | To enable access to a volume from a host OS. *See also* host, map/mapping, and volume. |

| | |
|---|---|
| **network port** | The Ethernet port on a controller module through which its Management Controller is connected to the network. |
| **network time protocol** | *See* NTP. |
| **NTP** | Network time protocol. |
| **object identifier** | *See* OID. |
| **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 volumes exceeds the physical capacity of the storage system. |
| **page** | For virtual storage, 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** | For virtual storage, a 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 (for AssuredSAN 4004 only)** | A user-created password that allows users to manage lock keys in an FDE-capable system. *See also* FDE and lock key. |
| **PCBA** | Printed circuit board assembly. |
| **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 connection between devices in a SAS network that enables transmission of data. |
| **physical layer** | *See* PHY. |
| **point-to-point** | Fibre Channel Point-to-Point topology in which two ports are directly connected. |
| **pool** | *See* linear pool and virtual pool. |
| **POST** | Power-on self test. Tests that run immediately after a device is powered on. |
| **Power-On Self Test** | *See* POST. |
| **power supply unit** | *See* PSU. |
| **primary system** | For virtual replication, the storage system that contains a replication set's primary volume. *See also* replication set, secondary system. |
| **primary volume** | For linear replication, the volume that is the source of data in a replication set and that can be mapped to hosts. For disaster recovery purposes, if the primary volume goes offline, a secondary volume can be designated as the primary volume. The primary volume exists in a primary disk group in the primary (or local) storage system. |
| **primary volume** | For virtual replication, the source volume in a replication set. This volume's data will be replicated to the secondary volume in the secondary system. See also replication set, secondary volume. |
| **proxy volume** | A virtual volume in the local system that represents a volume in a remote system. Proxy volumes are used internally by the controllers to perform actions such as transferring replication data. |
| **PSU** | Power supply unit. The power supply FRU. |

| | |
|---|---|
| **quick rebuild** | A feature for virtual storage 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. |
| **read cache** | For virtual storage, a special disk group using SSDs that can be added to a 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* failover. |
| **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 (linear storage only) or iSCSI links. The capability to replicate volumes is a licensed feature. |
| **replication image** | For linear storage, a conceptual term for replication snapshots that have the same image ID in primary and secondary systems. These synchronized snapshots contain identical data and can be used for disaster recovery. |
| **replication-prepared volume** | For linear storage, a volume created for the purpose of being the secondary volume in a replication set. Replication-prepared volumes are automatically created by the Replication Setup Wizard, or they can be created in the CLI or the WBI. |
| **replication set** | For linear replication, associated primary and secondary volumes that are enabled for replication and that typically reside in two physically or geographically separate storage systems. *See* primary volume and secondary volume. |
| **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 and secondary volume. |
| **replication snapshot** | For linear storage, a special type of snapshot, created by the replication feature, that preserves the state of data of a replication set's primary volume as it existed when the snapshot was created. For a primary volume, the replication process creates a replication snapshot on both the primary system and, when the replication of primary-volume data to the secondary volume is complete, on the secondary system. Replication snapshots are unmappable and are not counted toward a license limit, although they are counted toward the system's maximum number of volumes. A replication snapshot can be exported to a regular, licensed snapshot. *See also* replication sync point. |
| **replication sync point** | For linear storage, the state of a replication snapshot whose corresponding primary or secondary snapshot exists and contains identical data. For a replication set, four types of sync points are identified: the only replication snapshot that is copy-complete on any secondary system is the “only sync point”; the latest replication snapshot that is copy-complete on any secondary system is the “current sync point”; the latest replication snapshot that is copy-complete on all secondary systems is the “common sync point”; a common sync point that has been superseded by a new common sync point is an “old common sync point.” |
| **repurpose (for AssuredSAN 4004 only)** | 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 and passphrase. |
| **RFC** | Read flash cache. *See* read cache. |
| **SAS** | Serial Attached SCSI interface protocol or disk-drive architecture. |
| **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 and MC. |

| | |
|---|---|
| **SCSI Enclosure Services** | *See* SES. |
| **secondary system** | The storage system that contains a replication set's secondary volume. *See also* replication set, primary system. |
| **secondary volume** | For linear replication, the volume that is the destination for data in a replication set and that is not accessible to hosts. For disaster recovery purposes, if the primary volume goes offline, a secondary volume can be designated as the primary volume. The secondary volume exists in a secondary disk group in a secondary (or remote) storage system.<br>The contents of a secondary volume are in a constant state of flux and are not in a consistent state while a replication is in process. Only snapshots that are associated with a secondary volume are data consistent. |
| **secondary volume** | For virtual replication, the volume on the remote peer system that represent the copy created and maintained by a replication set. Certain operations on this volume are restricted but it may be snapped at any time to create writable volumes. *See also* primary volume, replication set. |
| **secret** | For use with CHAP, a password that is shared between an initiator and a target to enable authentication. |
| **secure hash algorithm** | *See* SHA. |
| **secure shell** | *See* SSH. |
| **Secure Sockets Layer** | *See* SSL. |
| **SED (for AssuredSAN 4004 only)** | 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. |
| **Self-Monitoring Analysis and Reporting Technology** | *See* SMART. |
| **serial electrically erasable programmable ROM** | *See* SEEPROM. |
| **Service Location Protocol** | *See* SLP. |
| **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. A type of disk drive. |
| **SHA** | Secure Hash Algorithm. A cryptographic hash function. |
| **SLP** | Service Location Protocol. Enables computers and other devices to find services in a local area network without prior configuration. |
| **Small Footprint CIM Broker** | *See* SFCB. |
| **small form factor** | *See* SFF. |
| **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. |
| **SMI-S** | Storage Management Initiative - Specification. The SNIA standard that enables interoperable management of storage networks and storage devices.<br>The interpretation of CIM for storage. It provides a consistent definition and structure of data, using object-oriented techniques. |
| **snap pool** | For linear storage, a volume that stores data that is specific to snapshots of an associated master volume, including copy-on-write data and data written explicitly to the snapshots. A snap pool cannot be mapped. |

| | |
|---|---|
| **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. The capability to create snapshots is a licensed feature (AssuredSnap). Snapshots that can be mapped to hosts are counted against the snapshot-license 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, and 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. |
| **sparse snapshot** | A type of point-in-time copy that preserves the state of data at an instant in time by storing only those blocks that are different from an already existing full copy of the data. |
| **SRA** | Storage Replication Adapter. A host-based software component that allows VMware's Site Recovery Manager to manage the storage-system firmware's disaster recovery management (DRM) features, automating disaster-recovery failover and failback tasks. The SRA uses the CLI XML API to control the storage system. *See also* DRM. |
| **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 Management Initiative - Specification** | *See* SMI-S. |
| **Storage Networking Industry Association** | *See* SNIA. |
| **storage system** | A controller enclosure with at least one connected drive 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. |
| **thin provisioning** | A 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** | For virtual storage, a homogeneous set of disk drives, typically of the same capacity and performance level, that comprise one or more 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:<br>• Performance, which uses SAS SSDs (high speed).<br>• Standard, which uses enterprise-class spinning SAS disks (lower speed, higher capacity)<br>• Archive, which uses midline spinning SAS disks (low speed, high capacity). |
| **tier migration** | For virtual storage, the automatic movement of blocks of data, associated with a single volume, between tiers based on the access patterns that are detected for the data on that volume. |
| **tray** | *See* enclosure. |
| **UCS Transformation Format - 8-bit** | *See* UTF-8. |

| | |
|---|---|
| **ULP** | Unified LUN Presentation. A RAID controller feature that enables a host system to access mapped volumes through any controller host port. ULP incorporates Asymmetric Logical Unit Access (ALUA) extensions. |
| **undercommitted** | The amount of storage capacity that is allocated to volumes is less than the physical capacity of the storage system. |
| **Unified LUN Presentation** | *See* ULP. |
| **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. |
| **UTC** | Coordinated Universal Time. The primary time standard by which the world regulates clocks and time. It replaces Greenwich Mean 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 CLI and WBI interfaces. |
| **v2** | The legacy interface for managing linear storage. This is the default for a system that has been upgraded from a previous release. |
| **v3** | The new interface for managing virtual and linear storage. This is the default for a new installation. |
| **vdisk** | A virtual disk comprising the capacity of one or more disks. The number of disks that a vdisk can contain is determined by its RAID level. *See* linear disk group. |
| **vdisk spare** | *See* dedicated spare. |
| **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** | *See* vdisk. |
| **virtual disk group** | A set of disk drives that is configured to use a specific RAID type. The number of disks that a disk group can contain is determined by its RAID level. A virtual disk group can use RAID 1, 5, 6, or 10. A virtual disk group can be added to a new or existing virtual pool. *See also* virtual pool. |
| **virtual pool** | For virtual storage, 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 create volume copies is a licensed feature (AssuredCopy) that makes use of snapshot functionality. |
| **volume group** | A user-defined group of volumes for ease of management, such as for mapping operations. |
| **WBEM** | Web-Based Enterprise Management. A set of management and internet standard technologies developed to unify the management of enterprise computing environments. |
| **web-based interface/web-browser interface** | *See* WBI. |
| **WBI** | Web-browser interface, called Storage Management Console. The primary interface for managing the system. A user can enable the use of HTTP, HTTPS for increased security, or both. |
| **Web-Based Enterprise Management** | *See* WBEM. |
| **World Wide Name** | *See* WWN. |
| **World Wide Node Name** | *See* WWNN. |
| **World Wide Port Name** | *See* WWPN. |
| **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. |

# Index

## D



## E

## F



## G



## H

## I

## S

## T

## U



## V

## W