AssuredSAN Pro 5000 Series Storage Management Guide

P/N 83-00005330-10-01
Revision A
January 2013

Adobe PostScript™

Contents

Figures

Tables

About this guide

This guide provides information about managing an AssuredSAN™ Pro 5000 Series storage system by using its web interface, Storage Management Console.

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, Serial Attached SCSI (SAS), and Ethernet protocols

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*
Installing and using optional host-based software components (CAPI Proxy, VDS Provider, VSS Provider, SES Driver)	AssuredSAN Installing Optional Software for Microsoft Windows® Server
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 Pro 5000 Series Setup Guide
Obtaining and installing a license to use licensed features	AssuredSAN 5000 Series Obtaining and Installing a License
Using the web interface to configure and manage the product	AssuredSAN Pro 5000 Series Storage Management Guide
Using the command-line interface (CLI) to configure and manage the product	AssuredSAN Pro 5000 Series CLI Reference Guide
Event codes and recommended actions	AssuredSAN Pro 5000 Series Event Descriptions Reference Guide
Identifying and installing or replacing field-replaceable units (FRUs)	AssuredSAN Pro 5000 Series FRU Installation and Replacement Guide

* Printed document included in product shipkit.

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

Document conventions and symbols

Table 1 Document conventions

Convention	Element
Blue text	Cross-reference links
Blue, underlined text	Email addresses
Blue, underlined text	Website addresses
Bold text	• Keys that are pressed • Text typed into a GUI element, such as a box • 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 • System output • Code • Commands, their arguments, and argument values
`Monospace, italic` text	• Code variables • Command variables
`Monospace, bold` text	Emphasized 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.

1 Getting started

Storage Management Console 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 Storage Management Console. 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.

Storage Management Console is also called the web-browser interface (WBI).

Topics in this chapter:

System concepts

Paged storage

Paged storage is a method of mapping logical storage requests to physical storage (disks).

The traditional, 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, since it can not easily handle gaps or breaks in the physical storage. This makes it difficult to alter the physical layout after it is established.

In contrast, the paged method inserts a layer of virtualization such that logical host requests are mapped onto "pages" of storage. Each page is then mapped onto either physical storage or traditionally mapped 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 storage-pool component, which is one of up to 16 RAID sets that are grouped into a storage pool. Thus, a paged volume as seen by a host represents a portion of storage in a storage pool. Multiple paged volumes can be created in a storage pool, sharing its resources. This allows for a high level of flexibility, and most efficient use of available physical resources.

Some advantages of using paged storage instead of linear storage are:

- It allows performance to scale as the number of disks in the storage 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.

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

Thin provisioning

Thin provisioning is a paged-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 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 real storage needs grow. The process of expanding the Windows volume is eliminated.

Automated tiered storage

Automated tiered storage (ATS) is a paged-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" zones of data can move to disks with higher performance, lower capacity, and higher costs.
- Infrequently accessed, "cool" zones of data can move to disks with higher capacity, lower performance, and lower costs.

Each storage-pool component, depending on the type of disks it uses, is automatically assigned to one of the following performance tiers:

- Performance—This highest tier uses SAS SSDs, which provide the best performance but also the highest cost and lowest capacity.
- 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 storage pool can have multiple components, each belonging to a different tier, a storage pool can provide multiple tiers of storage.
- The I/O load is automatically balanced between components in a tier.
- Storage-pool components can be added or removed without disrupting I/O. Data in components that are being removed is automatically migrated to other components.

Storage pools

A *storage pool* is comprised of one or more storage-pool components that, as a group, serve up storage pages to volumes. A storage pool can also have spare disks to replace disks that fail in any of its components, and can have an SSD for use as high-speed read cache.

A *storage-pool component* is a RAID set. The RAID level is determined by the type of disks of which the component is comprised. All disks in a component must be the same type (SAS SSD, enterprise SAS, or midline SAS) and have the same capacity. The quantity and type of disks determines which storage tier the disks are suited for and which RAID level to use to create components from those disks. The Performance tier uses RAID-1 components comprised of SAS SSDs; the Standard tier uses RAID-6 components comprised of enterprise SAS disks; the Archive tier uses RAID-6 components comprised of midline SAS disks. For more information about tiers, see Automated tiered storage on page 14.

Each disk has metadata that identifies whether the disk is a member of a component, and identifies other members of that component. This enables a component to be quarantined if disks are not detected at startup.

In a dual-controller system, when a component is created the system automatically assigns ownership to one controller or other, to balance the number of components each controller owns. Typically it does not matter which controller owns a component.

If the owning controller fails, the partner controller assumes temporary ownership of components and resources owned by the failed controller. If a fault-tolerant cabling configuration is used to connect the

controllers to expansion enclosures and hosts, LUNs for both controllers are accessible through the partner controller so I/O to volumes can continue without interruption.

As a user with the manage role, you can use the Add Storage Wizard to provision disks into storage-pool components. For information about how this provisioning works, see Adding and removing storage on page 15. For information about using the wizard, see Using the Add Storage Wizard on page 39.

Adding and removing storage

Adding storage

The Add Storage Wizard provisions disks in selected, properly configured enclosures for use in storage pools, in tiers, as spares, or as SSD read cache. During first-time configuration of a new system, the wizard enables you to quickly provision the storage in all connected enclosures so that you can start creating volumes and mapping them to hosts. Over the life of the system, the wizard enables you to add disks or enclosures to provide additional storage for existing storage pools.

The following rules apply to the Add Storage Wizard:

- In an enclosure, all disks of the same type must have the same capacity.
- For provisioning to start, all disks must be in a good state. If the system detects a bad disk, the wizard will not proceed and you will be alerted to resolve the problem. Spares cannot be used while storage pools are being provisioned.
- A storage-pool component will be constructed with disks that are the same type and have the same capacity and are in the same enclosure; therefore, a component cannot span enclosures.
- Storage-pool components comprised of disks in 24-disk enclosures are created in symmetrical sets that are balanced between the two storage pools. For provisioning to start, there must be enough disks available to create all the components in a set. Components comprised of disks in a 12-disk enclosure can be assigned to either pool.
- If the wizard fails for an enclosure, all changes for that enclosure are discarded.

The wizard requires certain types of disks to be in specific slots. For more information, see the “Supported disk configurations” topic in the Setup Guide for your product.

Removing storage

The Remove Storage Wizard enables you to remove one or more enclosures from the available storage in the system. If disks in an enclosure that will be removed contain data, that data will first be moved (or "drained") to disks in remaining enclosures. If all enclosures are removed, any data in their disks will be deleted.

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 per storage pool as a read cache for "hot" pages only; a separate copy of the data is also kept in spinning disks. SSD read cache is completely volatile; that is, SSD 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 SSD 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.

Reconstruction and copyback

If one or more disks fail in a storage-pool component and spares 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 use the Add Storage Wizard to designate each replacement disk as a spare.

Reconstruction of a RAID-6 component in the Standard or Archive tier uses a quick-rebuild feature. This feature takes advantage of paged-storage knowledge of where user data is written to only reconstruct the data stripes that contain user data. Typically, storage is only partially allocated to volumes so reconstruction completes significantly faster than a standard RAID reconstruct operation. Data stripes that have not been allocated to user data are reconstructed in the background, using a much more efficient process. RAID-6 reconstruction behaves as follows:

- During system operation, if one disk fails in a storage-pool component and a spare is available, the system begins to use that spare to reconstruct that component. 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 system operation, if two disks fail and only one 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 component (referred to as "fail 2, fix 1" mode). If the spare fails during reconstruction, reconstruction stops.
- During system operation, if two disks fail and two spares are available, the system uses both spares to reconstruct the component. 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 illuminates amber. When a spare is used as a reconstruction target, its activity LED illuminates green. When two disks are in copyback, both disks will flash in unison until copyback is complete.

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

When reconstruction is complete, you can replace the failed disks Then the system's copyback feature will automatically copy data from the used spares to the new disks in the failed disks' slots. When copyback is complete, the spares will again be available for use.

Quick rebuild

Quick rebuild is a feature that reduces the time that user data is less than fully fault-tolerant after a disk failure in a storage-pool component. Quick rebuild takes advantage of paged-storage knowledge of where user data is written to only rebuild 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 rebuilt in the background, using a much more efficient process.

Volumes and volume groups

A *volume* is a logical subdivision of a storage pool, and can be mapped for use by 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 Volume mapping on page 18.

For ease of management, you can group 1–20 volumes (standard volumes, snapshots, or both) into a *volume group*. Doing so enables you to perform operations for all volumes in a group, 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 storage 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.

Volume cache options

A Manage-level user can set options that optimize reads and writes performed for each volume.

Using write-back or write-through caching

You can change the write-back cache setting for a volume. *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.

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.

Optimizing read-ahead caching

You can optimize a volume for sequential reads or streaming data by changing its read-ahead cache settings. Read ahead is triggered by two back-to-back accesses to consecutive LBA ranges, whether forward (increasing LBAs) or reverse (decreasing LBAs).

You can change the amount of data read in advance after two back-to-back reads are made. 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.

- The Default option works well for most applications: it sets one chunk for the first access in a sequential read and one stripe for all subsequent accesses. The size of the chunk is based on the chunk size used to create the storage-pool component (the default is 64 KB). RAID-1 components are considered to have a stripe size of 64 KB.
- Specific size options let you select an amount of data for all accesses.
- The Maximum option lets the controller dynamically calculate the maximum read-ahead cache size for the volume. For example, if a single volume exists, this setting enables the controller to use nearly half the memory for read-ahead cache.

  Only use Maximum when disk latencies must be absorbed by cache. For example, for read-intensive applications, you will want data that is most often read to be in cache so that the response to the read request is very fast; otherwise, the controller has to locate which disks the data is on, move it up to cache, and then send it to the host. Do not use Maximum if more than two volumes are owned by the controller on which the read-ahead setting is being made. If there are more than two volumes, there is contention on the cache as to which volume's read data should be held and which has the priority; each volume constantly overwrites the other volume's data in cache, which could result in taking a lot of the controller's processing power.

- 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.

By using the CLI you can also change the optimization mode.

△ **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.

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 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.

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 connected 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 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*. 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 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.

Volume mapping settings are stored in disk metadata.

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 volume 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.

AssuredSnap

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 data state at the point in time when the snapshot was created. Snapshots can be created manually or by using the task scheduler.

Each storage pool has reserved space, called a *snap pool*, that stores pointers to source-volume data for snapshots. 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. 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 standard 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 standard volumes and snap pools.

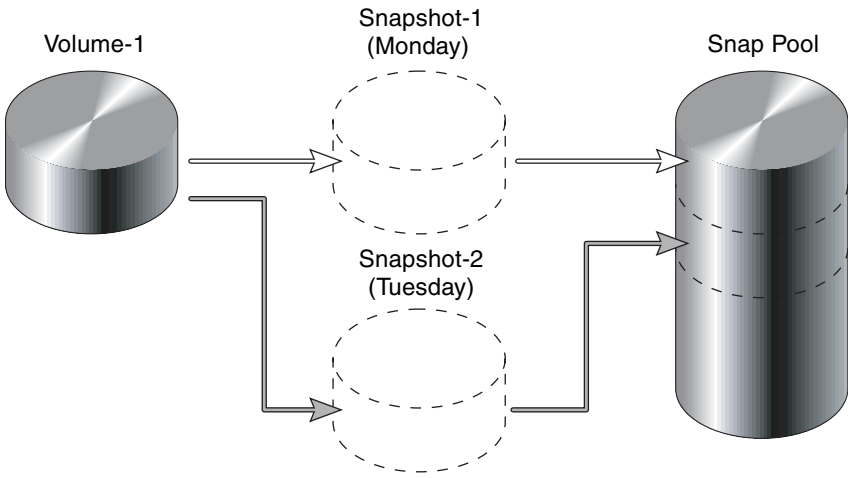


Figure 1 Relationship between a standard volume and its snapshots and the snap pool

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 standard volume, and a snapshot depends on the existing data in the block being overwritten, the data is copied from the standard 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 standard volume. In addition, only a single copy-on-write operation is performed on the standard volume.

The storage system allows a maximum number of snapshots to be retained, as determined by the Snapshot license. For example, if your license allows four snapshots, when the fifth snapshot is created 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 create 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 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).

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

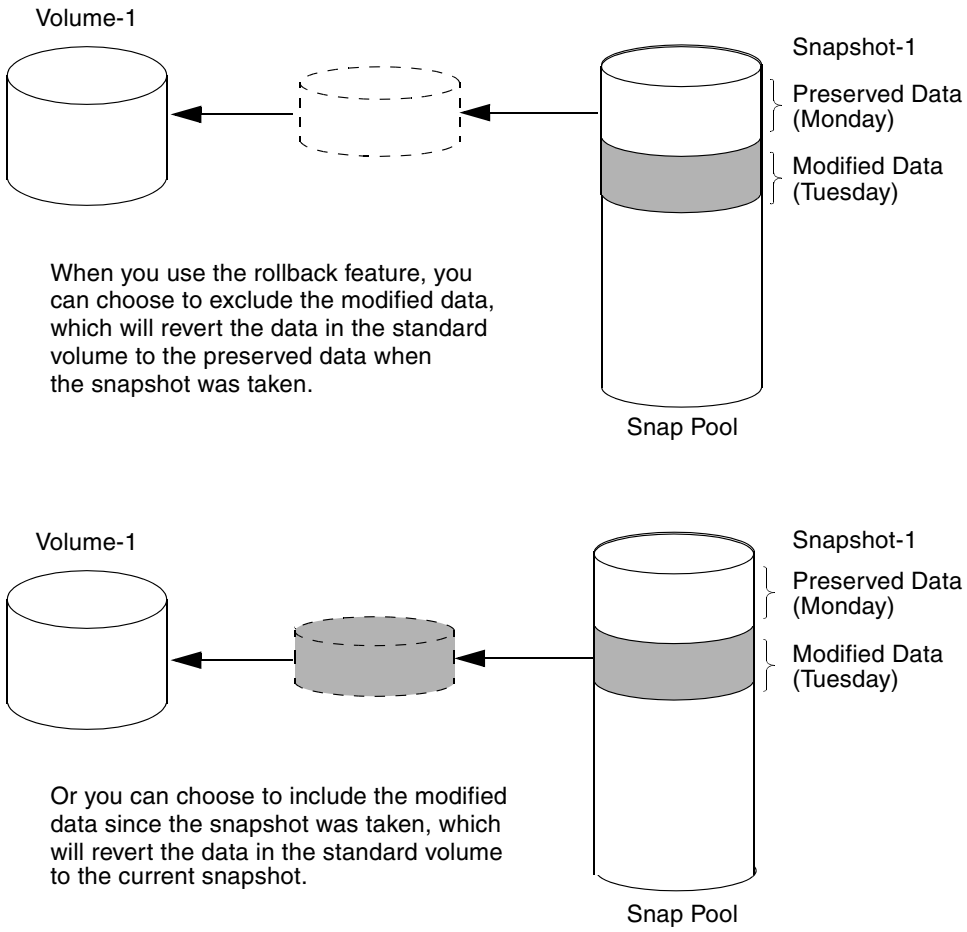


Figure 2 Rolling back a standard volume

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.

AssuredCopy

AssuredCopy is a licensed feature that enables you to copy a volume or a snapshot to a new volume. You can use this feature to create a complete "physical" copy of a source volume or snapshot within the same storage pool. It is an exact copy of the source as it existed at the time the copy operation was initiated,

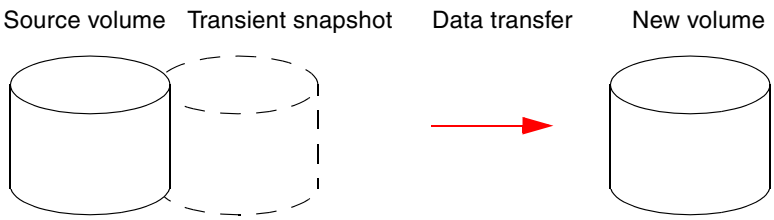
consumes the same amount of space as the source, and is independent from an I/O perspective. In contrast, the snapshot feature creates a point-in-time "logical" copy of a volume, which remains dependent on the source volume.

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.

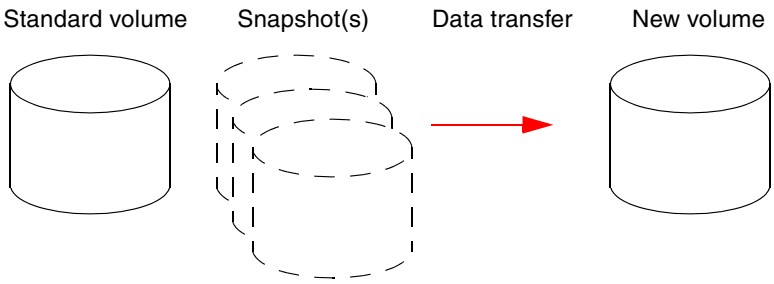
The following figure illustrates how volume copies are created.

Copying a standard volume



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

Copying a snapshot



1. A standard 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 3 Creating a volume copy from a standard volume or a snapshot

For information about viewing the status of licensed features in your system, see Installing a permanent license on page 46 For more information about using this feature, see Copying a volume or snapshot on page 69.

AssuredRemote

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 ports to a remote storage system as described in installation documentation.
- *Remote system* definition—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 standard 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 storage pool 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 storage pool in a secondary system.
- *Replication snapshot*—A special type of snapshot that preserves the state of data of a 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 maximum number of volumes for the system. 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 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 current data in the primary volume; 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. Following next is a step-by-step example of the remote-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 host 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.

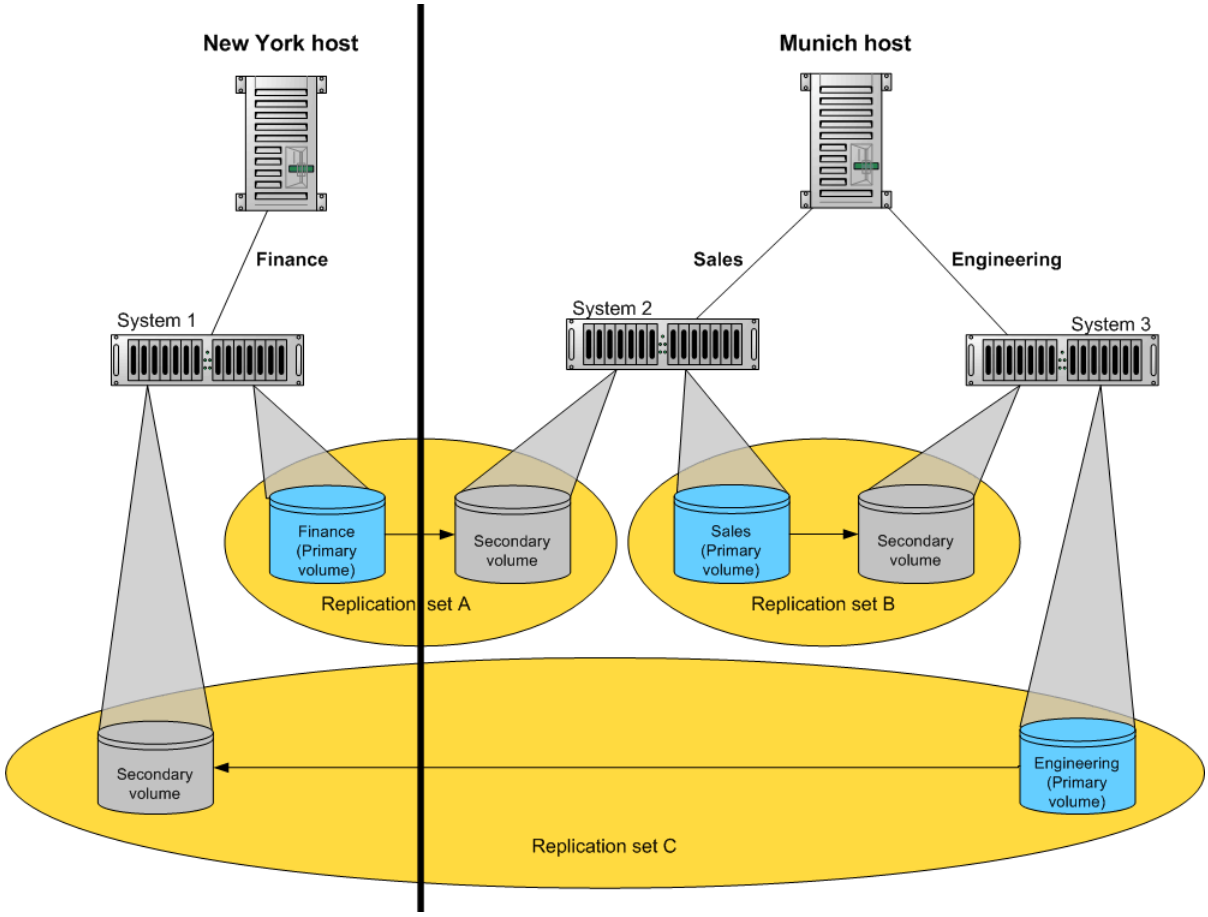


Figure 4 Intersite and intrasite replication sets

Remote replication uses snapshot functionality to track the data to be replicated and to determine the differences in data updated on the standard volume, minimizing the amount of data to be transferred. Snapshots created by the remote replication process are a special form called *replication snapshots*, which do not count against snapshot license limits.

In order to perform a replication, a snapshot of the primary volume is created, 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 Fibre Channel. The first replication copies all data from the primary volume to the secondary volume; subsequent replications use sparse snapshots.

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 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.

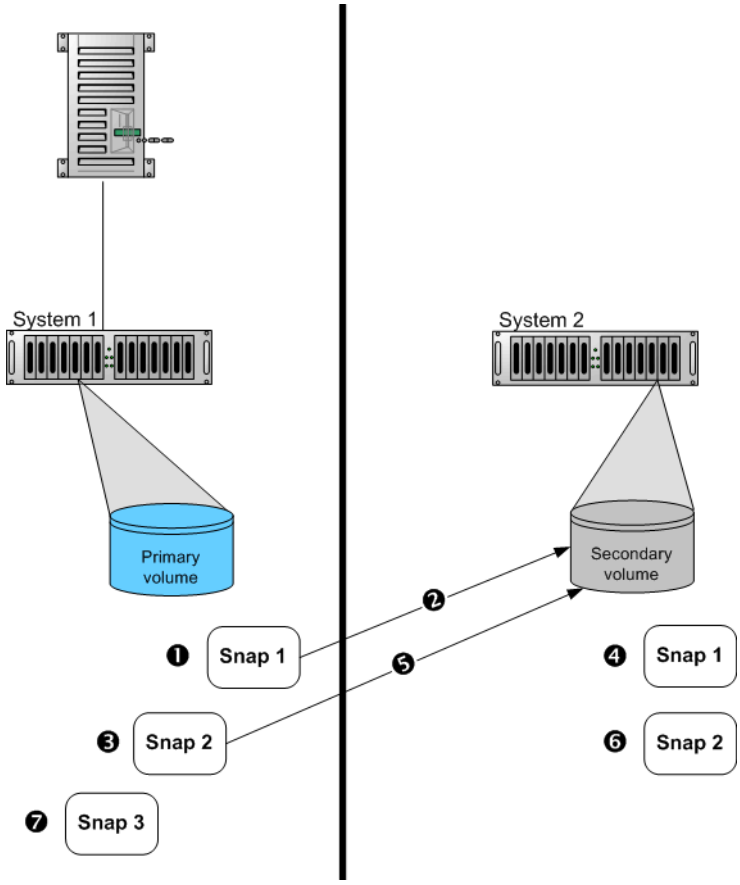
When a replication snapshot is created from a standard snapshot, while that snapshot remains present the replication snapshot's total data represented is zero bytes. This behavior occurs because the snapshot data remains associated with the standard snapshot and there is no data specifically associated with the replication snapshot. If the standard snapshot is deleted, its data becomes associated with (is preserved by) the replication snapshot and the size of the replication snapshot 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 created 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.

Replication actions

The following figure illustrates actions that occur during a series of replications from System 1 to System 2.



1. Create initial snapshot and initiate replication.
2. Initial replication consists of a full data copy.
3. Create second snapshot and request replication. This can be created while the initial replication is in progress.
4. Snapshot created 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 created on secondary volume. This is the second sync point.
7. Other snapshots can be created 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 5 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 created and every block of data is then copied to the secondary volume. When the copy is complete, the first snapshot is created 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 create 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; or, 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; replications requested after the links fail will not start replicating. 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.

Criteria for selecting a storage pool 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 storage pool in which to create the secondary volume.

The storage-pool selection option only lists storage pools that have sufficient free space for replication, and that do not contain a volume with a conflicting name (`rprimary-volume-name`). The system calculates the required space for the secondary volume (reserve) as follows:

- If the primary volume is less than 500GB, the reserve will be the same size as the primary volume.
- If the primary volume is larger than 500GB, the reserve size will be the maximum, 500GB.

The following table shows examples of how much free space a storage pool must have in order to be shown by the storage-pool option. If you want to replicate a volume whose size is not shown, you can use the above calculations to determine how much free space the secondary storage pool must have.

Table 2 Available space required for a storage pool to be selectable to contain a secondary volume

Primary volume size (GB)	Available space required in secondary pool (GB)	Primary volume size (GB)	Available space required in secondary pool (GB)	Primary volume size (GB)	Available space required in storage pool (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

Table 2 Available space required for a storage pool to be selectable to contain a secondary volume

Primary volume size (GB)	Available space required in secondary pool (GB)	Primary volume size (GB)	Available space required in secondary pool (GB)	Primary volume size (GB)	Available space required in storage pool (GB)
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 it 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.

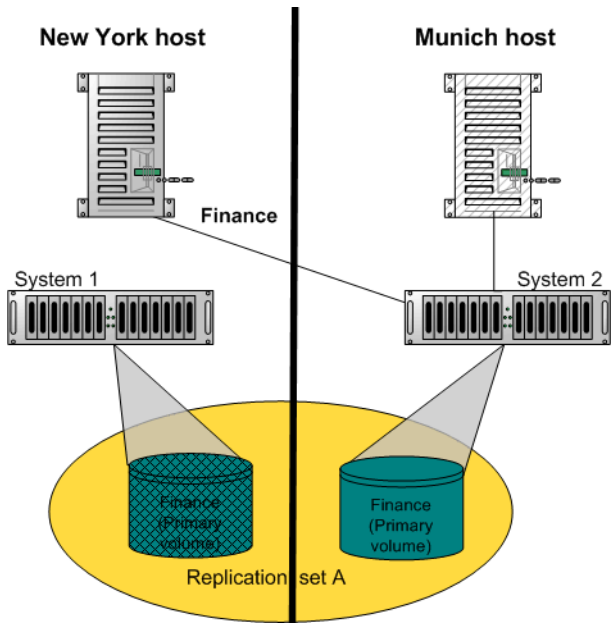


Figure 6 Example of primary-volume failure

If the original primary volume becomes accessible, you can set it to be the primary volume again.

1. Create a snapshot of the original primary volume. This preserves the current data state of the volume for later comparison with the new primary volume.
2. Set the original primary volume to be a secondary volume.
3. 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.
4. Set the secondary volume (the original primary volume) to be the new primary volume.

5. You can now mount the snapshot that was created 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.

Remote replication licensing

The AssuredRemote and AssuredSnap features are separately licensed. Remote replication can operate without Snapshot being enabled; however, to get the most out of remote replication, it is recommended to enable both features. Normally, replication snapshots are not accessible to hosts. However, if Snapshot is enabled, a replication snapshot can be exported for use as a standard snapshot.

Remote-system management

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 manage-level user 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, in a remote system.

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

Performance statistics

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

Current performance statistics for disks, storage pools, storage 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, storage pools, and storage 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 storage pools and to identify disks that are experiencing errors or are performing poorly.

The system samples historical statistics for disks every quarter hour and for pools and tiers every 5 minutes, and retains these samples for 6 months. 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.

Log management

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 Storage Management Console 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 on page 91. For information about using the FTP interface, see Using FTP to download logs and update firmware on page 107.

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. 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, use the Partner Firmware Update option to ensure that the same firmware version is installed in both controller modules. This option 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 in that controller is transferred to the partner controller.
- 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, and disk drives, see Updating firmware on page 55.

Data protection with a single controller module

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 fault-tolerant 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 shut down. Data remains in the controller cache and associated volumes will be missing that data. This can result in data loss or in some cases volume loss; for example, if using snapshot functionality a snap pool might become inaccessible and the standard volume could go offline.

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 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 Volume cache options on page 16. For more information about changing cache settings for a volume, see Modifying a volume on page 67.

VDS and VSS hardware providers

Virtual Disk Service (VDS) enables host-based applications to manage 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 volumes and snapshots in the storage system. For more information, see the VDS and VSS hardware provider documentation for your product.

Storage Replication Adapter (SRA)

The SRA is a host-software component, installed on a Microsoft Windows Server, that enables disaster recovery management (DRM) software on the host to control certain aspects of the replication feature in storage systems connected to the host. The presence of the SRA allows the DRM 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. For more information, see the Storage Replication Adapter documentation for your product.

System configuration limits and default settings

The following table specifies physical and logical limits of the storage system.

Table 3 Default settings

Setting	Default
Network configuration • IP Address, Controller A • IP Address, Controller B • IP Mask	 • 10.0.0.2 • 10.0.0.3 • 255.255.0.0
WBI • HTTP • HTTPS	 • Enabled • Enabled
CLI • Telnet • SSH	 • Enabled • Enabled
SMI-S	Enabled and Encrypted
System Information • System Name • System Contact • System Location • System Information	 • Uninitialized Name • Uninitialized Contact • Uninitialized Location • Uninitialized Info

Table 3 Default settings (continued)

Setting	Default
Event Notification	
• SNMP	
• Notification Level	• none (disabled)
• Read Community	• public
• Write Community	• private
• Trap Host addresses	• 0.0.0.0
• Email	
• SMTP Server Address	• (empty)
• SMTP Sender Name	• (empty)
• SMTP Sender Domain	• mydomain.com
• Email Notifications	• Disabled
• Managed Logs	• Disabled
Loop ID	
• (FC) Speed	• auto
• connection-mode	• point-to-point

Using the Storage Management Console interface

Web browser requirements and setup

- Use Mozilla Firefox 10 or later, Google Chrome 17 or later, or Microsoft Internet Explorer 8 or later.
- Do not use Internet Explorer compatibility mode.
- To enable the Storage Management Console help window to open, enable pop-up windows in your browser.
- To optimize the Storage Management Console display, use a color monitor and set its color quality to the highest setting.
- To navigate beyond the Storage Management Console sign-in page (with a valid user account), do the following:
  - For Internet Explorer, set the security level for the local intranet zone to medium or medium-low.
  - For Internet Explorer, add the IP address of each controller as a trusted site.
  - Verify that cookies are allowed for the IP address of each controller network port.

Areas of the interface

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

The topic pane shows information that relates to the selected topic tab. This area also contains an **Action** menu that provides access to configuration and provisioning 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 4 Areas of the interface

Banner:	Product ID	System panel (page 49)	Connection panel (page 89)	Date/time panel (page 90)	User panel (page 40)	Sign Out button (page 35)	Help button (page 33)
Topic tabs:	Home (page 37)	**Topic pane**					
	System (page 49)						
	Hosts (page 61)						
	Volumes (page 65)						
	Mapping (page 75)						
	Replications (page 79)						
	Performance (page 85)						
Footer:	Health panel (page 91)	Event panel (page 92)	Capacity panel (page 93)	Host I/O panel (page 93)	Tier I/O panel (page 93)	Activity panel (page 94)	

Tips for using the interface

- Do not use the browser's Back, Forward, Reload, or Refresh buttons. Storage Management Console has a single page whose content changes as you perform tasks and automatically updates to show current data.
- In an action panel, an asterisk (*) identifies a required setting.
- As you set options in action panels, Storage Management Console 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 drag a panel partially out of your browser window and cannot drag it back, cancel the panel and reopen it; the panel will reappear in the center of the browser window.
- If you are signed in to Storage Management Console and the controller you are accessing goes offline, the system informs you that the system is unavailable or that communication has been lost. When access is restored, you might be able to continue from the point you lost access, or the sign-in page might reappear.
- 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 Storage Management Console.
- 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, mappings, and replication sets 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, do the following:

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 is filter is active, the icon changes to .
   - If the menu has an entry for the text you want to find, select that entry. A filter menu can show the 10 most frequently entries in the column.
   - To show all items in the column, click 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 context-sensitive help for the content of the topic pane, click the help icon in the banner.
- To show or hide the table of contents pane in the help window, click .
- If a help topic is displayed in the help window and you change the context in the main window—for example, you switch from the Home tab to the Mapping tab—the help topic for the new context will appear. To prevent this automatic context-switching, click the pin icon . When a help window is pinned ( ), you can browse to other topics in that help window and you can open another 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 help window icon ( ).
- Help text uses the following typographical conventions:

Convention	Element
Blue, underline	Cross-reference links
Bold	Names of keys and GUI elements; text entered into a text box
Italic	Text emphasis; variable text
`Monospace`	File and directory names; system output; code excerpts

Color codes

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

Context	Color	Meaning
Performance statistics		IOPS
		Data throughput (MB/s)
Capacity utilization		Physical space
		Unallocated/free space
		Reserved space (space used by snap pools or to be used by volumes that are being created)
		Allocated/used space
		Overcommitted space
Storage tiers and cache		Performance
		Standard
		Archive
		Read cache
Other		Spare disks

Size representations

Parameters such as names of users and volumes have a maximum length in bytes: ASCII characters are 1 byte; most Latin (Western European) characters with diacritics are 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 Storage Management Console, the base for entry and display of storage-space sizes can be set per user. When entering storage-space sizes only, either base-2 or base-10 units can be specified.

Table 5 Storage size representations in base 2 and base 10

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)	$1{,}000^4$

Table 5 Storage size representations in base 2 and base 10

Base 2		Base 10	
Unit	**Size in bytes**	**Unit**	**Size in bytes**
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 6 Decimal (radix) point character by locale

Language	Character	Examples
English, Chinese, Japanese	Period (.)	146.81 GB 3.0 Gbit/s
Spanish	Comma (,)	146,81 GB 3,0 Gbit/s

Signing in and out

Multiple users can be signed in to each controller simultaneously.

For each active Storage Management Console 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 Storage Management Console session, but all instances of Firefox and Chrome share the same Storage Management Console session.

To sign in:

1. In the web browser address field, enter the IP address of a controller network port. (Do not include a leading zero in an IP address; for example, enter 10.1.4.33 not 10.1.4.033.) The Storage Management Console sign-in page is displayed. If the sign-in page does not display, verify that you have entered the correct IP address.
2. In the sign-in page, enter the name and password of a valid user. The default user that can both monitor and manage the system has the name `manage` and the password `!manage`. The default user that can only monitor the system has the name `monitor` and the password `!monitor`.
3. To display the interface in a different language than the one configured for the user, select the language from the user-language list. The default language is English.
4. Click **Sign In**. If the system is available, the Home topic 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 Storage Management Console window.
2. In the confirmation panel, click **Sign Out**.

Initially configuring and provisioning the system

The following procedure assumes that system enclosures are properly installed and connected to each other and to a network, as described in the Setup Guide for your product.

To initially configure and provision a storage system:

1. Configure your web browser to use Storage Management Console, as described in Web browser requirements and setup on page 31.
2. Sign in to Storage Management Console as user `manage` with password `!manage`. For more information about signing in, see Signing in and out on page 35.

3. Use the Configuration Wizard as described in Using the Configuration Wizard on page 38.
4. Use the Add Storage Wizard as described in Using the Add Storage Wizard on page 39.
5. Create volumes and map them to initiators, as described in Creating volumes on page 67.
6. Use the Replication Setup Wizard to configure replication of a volume to a remote system as described in Using the Replication Setup Wizard on page 81.
7. From hosts, verify volume mappings by mounting the volumes and performing read and write tests to the volumes.
8. Verify that controller modules and expansion modules have the latest firmware as described in Updating firmware on page 55.

2 Working in the Home topic

The following actions can be performed in the Home topic:

Viewing overall system status

The Home topic provides an overview of physical and logical components in the storage system and their health. Information is shown about hosts, controller host ports, storage capacity and usage, storage pools, spares, and read cache (if present).

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. The block shows the total number of initiators and how many have not been grouped into a host.

Port information

The Ports A block shows the type (protocol) and name of each host port in controller A. The port icon indicates whether the port is disconnected, connected, or active.

Table 7 Controller host port status icons

	FC port is active.
	FC port is connected.
	FC port is disconnected.

The Ports B block shows similar information for controller B.

Hover the cursor over a port to see its name, type, ID (WWN), status, configured speed, actual speed, topology, loop ID (FC only), and health. If the health is not OK, the health reason and recommended action are shown to help you resolve problems.

The area between the blocks shows the following statistics, which show the current performance from host to disk:

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

Capacity information

The Capacity block shows two color-coded bars: the lower bar represents the physical capacity of the system; the upper bar identifies how the capacity is allocated and used. If storage is overcommitted, which means that the amount of storage capacity that is allocated to volumes exceeds the physical capacity of the storage system, the upper bar will be longer than the lower bar. For color-code descriptions, see Color codes on page 34.

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:

- The physical capacity in each storage pool and the total for both pools.
- The size of the snap pool in each storage pool and the total for both pools.
- The available space in each snap pool and the total for both pools.
- The allocated space in each storage pool, which can exceed the physical capacity if the storage pool is overcommitted, and the total for both pools.
- The free space in each storage pool and the total for both pools.
- The space used by volumes in each storage pool and the total for both pools.
- The uncommitted space in each storage pool and the total for both pools.

Pool information

The Pool A block shows the following information about storage pool A, which is owned by controller A:

- An icon, in the upper left corner, that indicates the pool health if it is not OK.
- Current IOPS for the storage pool, calculated over the interval since these statistics were last requested or reset.
- Current data throughput (MB/s) for the storage pool, calculated over the interval since these statistics were last requested or reset.
- The number of volumes in the pool.
- The number of snapshots in the pool.
- Two color-coded bars: the lower bar represents the physical capacity of the pool; the upper bar identifies how the capacity is allocated and used. For color-code descriptions, see Color codes on page 34.
- The name, capacity, and disk count for each tier in the pool.

The Pool B block shows similar information about storage pool B, owned by controller B.

Hover the cursor over a pool to see its ID, total size, snap-pool size and available space, used size, available size, allocation rate, deallocation rate, and health. If the health is not OK, the health reason, recommended action, and unhealthy subcomponents are shown to help you resolve problems.

Hover the cursor over a tier to see its name (in the format *`pool-ID - tier-type`*), total size, size as a percentage of pool capacity, used size, available size, allocation rate, and deallocation rate.

The Spares block between the pools shows the number of disks in each tier that are configured as spares to automatically replace a failed disk in that tier.

If a read-cache disk is provisioned for each pool, a Read Cache block next to each pool shows how much space is used in cache. Hover the cursor over a cache block to see the name (in the format *`pool-ID -`* `Read Cache`) and the cache size.

Using the Configuration Wizard

As a user with the manage role, you can use the Configuration Wizard to perform the following steps:

- Change the system date and time
- Change passwords for the default users
- Configure controller network ports
- Configure system-management services

- Enter information to identify the system
- Configure notifications
- Configure controller host ports

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, do 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 Add Storage Wizard

As a user with the manage role, you can use the Add Storage Wizard to select enclosures that contain new disks to be provisioned for use in storage pools, in tiers, as spares, or as SSD read cache.

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 prepare to use the wizard, read information about adding storage on page 15. Processing to add enclosures takes up to five minutes per enclosure.

To use the Add Storage Wizard, do one of the following:

- Point to the **Home** or **System** tab and select **Add Storage Wizard**.
- In the **Home** or **System** topic select **Action > Add Storage Wizard**.

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

Using the Remove Storage Wizard

As a user with the manage role, you can use the Remove Storage Wizard to remove enclosures and their storage capacity from the system. This operation is intended to remove storage components from a working system.

△ **CAUTION:**

- Removing storage can take days to complete, depending on disk usage and other processes running on the storage system. After storage removal has started, you cannot stop or undo it.
- If the controller enclosure (Enclosure 0) is removed, all other enclosures will be removed.
- Removing all enclosures will remove all data from the system.
- While storage removal is in progress, do not perform firmware update.

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 prepare to use the wizard:

1. Determine which spares, tiers, or entire enclosures you want to remove.
2. If you intend to remove the controller enclosure, first remove all replication sets in the system.

To use the Remove Storage Wizard, do one of the following:

- Point to the **Home** or **System** tab and select **Remove Storage Wizard**.
- In the **Home** or **System** topic select **Action > Remove Storage Wizard**.

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

Changing system information settings

To change system information settings:

1. Do 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 name, contact person or group, location, and other information about the system. Each value can include a maximum of 79 bytes, using printable characters except angle brackets, double quote, or backslash. The name is shown on the web browser tab and title bar when Storage Management Console is displayed. The name, location, and contact are included in event notifications. All four values are recorded in system debug logs for reference by service personnel.
3. Click **OK**.

Changing storage-pool settings

As a user with the manage role, you can view and change settings that govern the operation of each storage pool:

- Low Threshold—When this percentage of pool capacity has been used, Informational event 462 is generated to notify the administrator. This value must be less than the Mid Threshold value. The default is 25%.
- Mid Threshold—When this percentage of pool capacity has been used, event 462 is generated to notify the administrator to add capacity to the pool. This value must be between the Low Threshold and High Threshold values. The default is 50%. If the overcommitment setting is enabled, the event has Informational severity; if the overcommitment setting is disabled, the event has Warning severity.
- High Threshold—When this percentage of pool capacity has been used, Critical event 462 is generated to alert the administrator that it is critical 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.
- Enable overcommitment of storage 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 Thin provisioning on page 13. This option is disabled by default.

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

- % of storage pool—This setting specifies the percentage of storage-pool capacity to reserve for snapshots. The default is 0%. A high value reserves a large amount of capacity for creating and retaining snapshots but leaves a small amount of capacity for creating new volumes.

To change pool settings:

1. In the **Home** topic select **Action > Change Pool Settings**. The Pool Settings panel opens.
2. To change the low and mid thresholds for each pool, enter new values.
3. To enable thin provisioning, select the **Enable overcommitment of storage pools?** check box.
4. To change the percentage of capacity to reserve for snapshots in each pool, enter new values.
5. Click **OK**. The changes are saved.

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: WBI (Storage Management Console), CLI, SMI-S, or FTP. You can also create "SNMPv3 users," which can either access the 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 on page 43. For information about the MIB, see SNMP reference on page 95.

As a user with the manage role, you can modify or delete any user other than your current user. As a user with the monitor role only, you can change settings for your current user except for its type and role.

Settings for the default users

Table 8 Settings for default users

User Name	Password	User Type	Roles	Interfaces	Base	Preci-sion	Unit	Temper-ature	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; cannot already exist in the system; can include spaces and any printable characters except angle brackets, comma, double quote, backslash, or space; and can have a maximum of 29 bytes. See Size representations on page 34 for more information.

  NOTE: The user names `admin` and `api` are reserved for internal use.

- Password—A password is case sensitive; can include a maximum of 32 bytes; and can include spaces and any printable characters except angle brackets, backslash, comma, or double quote.
- Confirm Password—Re-enter the new password.
- User Type—Select Standard to show options for a standard user, or SNMPv3 to show options for an SNMPv3 user. The default is Standard.

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 Storage Management Console. This is a default.
  - CLI—Enables access to the command-line interface. This is a default.
  - SMI-S—Enables access to the SMI-S interface, which is used for remote management of the system through your network.
    - 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.

    - Service Debug. Used for technical support only. Enables or disables debug capabilities, including Telnet debug ports and privileged diagnostic user IDs. This is disabled by default.
    - FTP—Enables access to the FTP interface, which can be used instead of Storage Management Console to perform actions such as updating firmware and downloading logs.
- Base Preference—Select the base for entry and display of storage-space sizes:
    - Base 2—Sizes are powers of 2, using 1024 as a divisor for each magnitude.
    - Base 10—Sizes are powers of 10, using 1000 as a divisor for each magnitude. This is the default.
- Precision Preference—Select the number of decimal places (1–10) for display of storage-space sizes. The default is 1.
- 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. This is the default.
    - 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. The default is Celsius.
- Timeout—Select the amount of time that the user's session can be idle before the user is automatically signed out (2–720 minutes). The default is 30 minutes.
- Locale—Select a display language for the user. The default is English. Installed language sets include Chinese-Simplified, English, Japanese, and Spanish. The locale determines the character used for the decimal (radix) point, as shown in Table 6 on page 35.

The following options apply only to an SMNPv3 user:

- SNMPv3 Account Type—Select one of the following types:
    - User Access—Enables the user to view the SNMP MIB. This is the default.
    - Trap Target—Enables the user to receive SNMP trap notifications.
- SNMPv3 Authentication Type—Select whether to use MD5 or SHA authentication, or no authentication. The default is none. If authentication is enabled, the password set in the **Password** and **Confirm Password** fields must include a minimum of 8 characters.
- SNMPv3 Privacy Type—Select whether to use DES or AES encryption, or no encryption. The default is none. 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; can include a maximum of 32 bytes; can include spaces and any printable characters except angle brackets, backslash, comma, or double quote; and must include a minimum of 8 characters.
- 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. As a user with the manage role, do 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 tables on page 33.
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. As a user with the manage role, do 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 tables on page 33.
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. As a user with any role, do 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 tables on page 33.
2. Select the user to modify.
3. Change the settings. You cannot change the user name. As a user with only the monitor role, you cannot change user type and role 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. As a user with the manage role, do 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 tables on page 33.
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

As a user with the manage role, 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 Log management on page 28.

To change and test notification settings:

1. Do one of the following:
   - In the footer click the events panel and select **Set Up Notifications**. The Notification Settings panel opens.
   - In the **Home** topic select **Action > Set Up Notifications**.

   The Notification Settings panel opens.
2. Change SNMP, email, and managed logs settings as described in the first three procedures below.
3. Test notification settings as described in the last procedure below.

To change SNMP notification settings:

1. Select the **SNMP** tab.
2. If a message near the top of the panel says that the SNMP service is disabled, enable it (see Changing system services settings on page 51).
3. Select one of the following **Notification Level** options:
   - **none (disabled)**—No notifications are sent. This is the default.
   - **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. If SNMP notification is enabled, 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; can include any character except angle brackets, single quote, and double quote; and can have a maximum of 31 bytes. The default is `public`.
5. If SNMP notification is enabled, in the **Write Community** field enter the SNMP write password for your network. The value is case sensitive; can include any character except angle brackets, single quote, and double quote; and can have a maximum of 31 bytes. The default is `private`.
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. The default is 0.0.0.0.
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; see Changing network-interface settings on page 52.
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. For example: `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. For example: `Storage-1`. If no sender name is set, a default name is created.
6. Do 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 E**nable Email Notifications** check box. This disables the notification level and email address fields. This is the default.
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`.
9. Click **Apply**.

To change managed logs settings:

1. Configure SNMP notification settings, email notification settings, or both, as described above.
2. Select the **Managed Logs** tab.
3. Do 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. This is the default.
4. If managed logs 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. Do 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. This is the default.
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 managed logs 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, copy volumes, or replicate volumes.

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.
   - Optional: Select a new Start date and time.
   - Optional: If you want the task to run more than once, do 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.
4. Click **Apply**. A confirmation panel appears.
5. Click **Yes** to continue; otherwise, click **No**. If you clicked Yes, the schedule is modified.

To delete a schedule:

1. In the **Home** topic select **Action > Manage Schedules**. The Manage Schedules panel opens.
2. Select the schedule to delete. A confirmation panel appears.
3. Click **Yes** to continue; otherwise, click **No**. If you clicked Yes, the schedule is deleted.

Installing a license

A license is required to increase the number of standard snapshots that can exist and to use the Volume Copy, Replication, VDS, VSS, and SRA features. 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 temporary license one time. The temporary license will expire 60 days from the

time it is created. After creating a temporary license, each time you sign in to Storage Management Console, a message specifies the time remaining in 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 is no longer displayed.

Viewing the status of licensed features

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`—The 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.

Installing a permanent license

1. Verify the following:
   - The license file is saved to a network location that you can access from Storage Management Console.
   - You are signed into the controller enclosure for which the file is generated.
2. As a user with the manage role, 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`.

Creating a temporary license

1. As a user with the manage role, 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.
6. 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` or `Expired/Renewable`.

3 Working in the System topic

The following actions can be performed 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 a photorealistic view of the front of each enclosure. For each enclosure, the front view shows the enclosure ID. For each installed disk, the front view shows the location, form factor, type, and tier (if provisioned). To see more information, hover the cursor over an enclosure ear or a disk:

Enclosure	ID, status, vendor, model, disk count, WWN, midplane serial number, firmware revision, health
Disk	Location, usage, type, size, revolutions per minute (spinning disk only), SSD life left (SSD only), manufacturer, model, serial number, firmware revision, job status, and health

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

You can click a disk to change the state of its fault LED to help you find the disk in the rack. Click the disk once and an amber dot will appear at the bottom of the disk graphic to indicate that the disk's fault LED is blinking amber to help you identify the disk. Click the disk again to turn off its disk-identification state.

Rear view

The **Rear** tab shows a photorealistic view of the rear of each enclosure. The rear view shows enclosure IDs; the presence or absence of power supplies, controller modules, and expansion modules; 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:

Enclosure	ID, status, vendor, model, disk count, WWN, midplane serial number, firmware revision, health
Power supply	Status, vendor, model, serial number, firmware revision, health
Controller module	ID, network-port IP address, description, status, model, serial number, hardware version, hardware revision, health
FC host port	Name, type, status, configured speed, actual speed, topology, loop ID, 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.

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 tables on page 33.

For each component, the table shows the following information:

- Health—Shows the health of the component: OK, Degraded, N/A, or Unknown.
- Type—Shows the component type: enclosure, disk, power supply, fan, controller module, network port, host port, expansion port, CompactFlash card, or I/O module (expansion module).
- Enclosure ID—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*.
  - For a disk, the location is shown in the format *enclosure-ID.disk-slot*.
  - For a power supply or fan 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 in the format *controller-ID.port-ID*.
- Information—Shows additional, component-specific information:
  - For an enclosure, its FRU description and current disk count.
  - 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`*—The disk is part of a storage-pool component.
    - `FAILED`—The disk is unusable and must be replaced. Reasons for this status include: excessive media errors; SMART error; disk hardware failure; unsupported disk.
    - `LEFTOVR`—The disk is part of a storage-pool component that is not found in the system.
  - 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
  - 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`—The enclosure is present and is properly communicating with the system.
    - `Error`—The enclosure is present but is not detected by the system.
    - `Not Present`—The enclosure is not visible to the system.
    - `Unavailable`—The enclosure is not available to the system.
    - `Unknown`—Initial status when the enclosure is first detected or powered on.
    - `Unrecoverable`—The enclosure has suffered an error and can't be used by the system.
    - `Warning`—The enclosure is present but the system is having communication problems.
    - `Spun Down`—The enclosure is present and has been spun down by the DSD feature.
  - 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 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 a power supply or fan, `Up`, `Warning`, `Error`, `Not Present`, `Unknown`.
  - For a controller module or I/O module, `Operational`, `Down`, `Not Installed`, or `Unknown`.
  - For a network port, `OK`, `Degraded`, `Fault`, or `Unknown`.
  - For a host port:
    - `Up`—Port is cabled and has an I/O link.
    - `Disconnected`—Either no I/O link is detected or the port is not cabled.
  - For an expansion port, `Unavailable`, `Enabled-Healthy`, `Enabled-Degraded`, `Disabled`, or `Unknown`.
  - For a CompactFlash card, `Installed`, `Not Installed`, or `Unknown`.

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 WBI, CLI, FTP, or SMI-S see Managing users on page 40.

To change system services settings:

1. Do 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** or **HTTPS** for increased security, or both. If you disable both, you will lose access to this interface.
   - CLI—An advanced-user interface that is used to write scripts to manage the system. You can enable use of **Telnet**, of **SSH** (secure shell) for increased security, or both.
   - Storage Management Initiative Specification (SMI-S)—Used for remote management of the system through your network.

- **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. This is disabled by default.
- **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**.

Changing network-interface settings

As a user with the manage role, 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, 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:

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 Storage Management Console using the new IP addresses.

To use static IP values:

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.
5. Enter IP address, subnet mask, and gateway values for each controller. You must set a unique IP address for each controller.
6. Record the IP values you assign.
7. Click **OK**.
8. Sign out and try to access Storage Management Console using the new IP addresses.

Changing host-interface settings

As a user with the manage role, you can configure controller host-interface settings for FC ports to enable the system to communicate with hosts or with remote systems. No configuration is needed for SAS ports.

To configure FC ports:

1. In the **System** topic select **Action > Set Up Host Ports**. The Host Ports Settings panel opens.
2. For each port that is connected to a host, do the following:
   - If you need to force the port to use a specific link speed for testing, or you need to specify a mutually supported link speed for more than two FC devices connected in an arbitrated loop, select the proper speed: **2 Gbit/s**, **4 Gbit/s**, or **8 Gbit/s**. The default is **auto**, which auto-negotiates the proper link speed with the host.
   - If you need to force the link to use a specific FC protocol, select the proper connection mode: **loop** or **point-to-point**. Loop protocol can be used in a physical loop or in a direct physical connection between two devices. Point-to-point protocol can only be used in a direct physical connection between exactly two devices. The default is **auto**, which sets the mode based on the detected connection type.
3. For each controller, set the loop ID to use soft or hard target addressing:
   - Soft target addressing enables a LIP to determine the loop ID. Use this setting if the loop ID is permitted to change after a LIP or power cycle. To use this option, select the **Soft?** check box.
   - Hard target addressing requests a specific loop ID that should remain after a LIP or power cycle. If the port cannot acquire the specified ID, it is assigned a soft target address. Use this option if you want ports to have specific addresses, if your system checks addresses in reverse order (lowest address first), or if an application requires that specific IDs be assigned to recognize the controller. To use this option, clear the **Soft?** check box and in the **ID** field enter an address in the range 0–125. You cannot set the same hard target address for both controllers.
4. Click **OK**. If you changed a loop ID setting, a message specifies that you must restart the controller to make the change take effect.

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.

As a user with the manage role, 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 by checking their health.
2. Do 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

As a user with the diagnostic role, you can clear metadata from a leftover disk to make it available for use.

△ **CAUTION:**

- Only use this command when all storage-pool components are online and leftover disks exist. Improper use of this command may result in data loss.
- Do not use this command when a storage-pool component 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 storage-pool component has metadata that identifies the owning storage-pool component, the other disks in the storage-pool component, and the last time data was written to the storage-pool component. 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.

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 storage-pool component, causing the storage-pool component'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 storage-pool component is Degraded, the component 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 then become the target of a copyback operation from the original spare, or the disk may become available for use in a new storage-pool component.

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. To select or clear all leftover disks, toggle the check box in the heading row.

3. Click **Clear Metadata**. When processing is complete a success dialog appears.
4. Click **OK**.

Updating firmware

You can view the current versions of firmware in controller modules, expansion modules, and disk drives. As a user with the manage role, you can 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 the Partner Firmware Update option is used or when a controller module is replaced, see Firmware update on page 29.

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 System Health popup and resolve all problems before you update firmware.
- If any unwritten cache data is present, firmware update will not proceed. Before you can update firmware, unwritten data must be removed from cache. 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 storage-pool component 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.
- Ensure that disk drives of the same model have the same firmware revision.
- 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 will likely cause hosts to lose connectivity with the storage system.

Updating controller module firmware

In a dual-controller system, both controller modules should run the same firmware version. Storage systems in a replication set 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.

To prepare to update controller module firmware:

1. Follow the best practices in Best practices for firmware update, above.
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 system before you start the firmware update.
4. Restart the MC in the controller to be updated; or if PFU is enabled, restart the MCs in both controllers. For the procedure, see Restarting or shutting down controllers on page 58.

To update controller module firmware:

1. Do 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 **Choose File** and select the firmware file to install.
3. If you have a dual-controller system and want firmware to be automatically updated in both controllers, under Partner Firmware Upgrade select the **Enabled** check box and click **Set**. (PFU is enabled by default.) Otherwise, if PFU is disabled, after updating firmware on one controller you must log into the partner controller and perform this firmware update on that controller also.

4. 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 or 3 minutes for each EMP in an expansion 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.

5. Clear your web browser cache, then sign in to Storage Management Console. 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: 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 firmware

An expansion enclosure can contain one or two expansion modules. Each expansion module contains an enclosure management processor (EMP). All modules of the same model should run the same firmware version.

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

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

To prepare to update expansion module firmware:

1. Follow the best practices in Best practices for firmware update on page 55.
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 system before starting the firmware update.

To update expansion module firmware:

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

   The Update Firmware panel opens.

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

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

It typically takes 3 minutes to update each EMP in an expansion enclosure. Wait for a message that the code load has completed.

Verify that each updated expansion module has the new firmware version.

Updating disk-drive firmware

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

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

To prepare to update disk-drive firmware:

1. Follow the best practices in Best practices for firmware update on page 55.
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:

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

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

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

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

6. If the updated disk drives must be power cycled:
   - Shut down both controllers; see Restarting or shutting down controllers on page 58.
   - Power cycle all enclosures as described in the Setup Guide for your product.
7. 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 on page 51.
2. In a new tab in your web browser, enter a URL of the form: `http://controller-IP-address:8081/cgi-bin/content.cgi?mc=MC-identifier&refresh=true` where:
   - `controller-IP-address` is required and specifies the 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.

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 in one controller or both controllers.

Restarting controllers

Perform a restart when Storage Management Console 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, which includes stopping all I/O operations and flushing the write cache to disk, and then the controller restarts. The Management Controller is not restarted so it can provide status information to external interfaces.

△ **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 summed between the two controllers. For more information, see Viewing performance statistics on page 85.

To perform a restart:

1. Do 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: A, 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. Do 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: A, 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.

NOTE: If an iSCSI port is connected to a Microsoft Windows host, the following event is recorded in the Windows event log: `Initiator failed to connect to the target.`

---

4 Working in the Hosts topic

The following actions can be performed 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 tables on page 33. For more information about hosts, see Initiators, hosts, and host groups on page 18.

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 if a nickname is assigned to the initiator; otherwise, blank.
- ID—Shows the initiator ID, which is the WWN of an FC or SAS initiator.
- 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.

- Host—Identifies the initiators to which the mapping applies:
  - *`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. For example, `MailServer.*`.
- 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.
  - `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—Shows 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 on page 77.

Creating an initiator

As a user with the manage role, 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 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. 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, `MailServer_FCp1`. An initiator name is case sensitive; can include spaces and any printable characters except angle brackets, backslash, comma, period, asterisk, or double quote; and can have a maximum of 32 bytes. If the name is used by another initiator, you are prompted to enter a different name.
5. Click **OK**. The initiator is created and the hosts table is updated.

Modifying an initiator

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, `MailServer_FCp1`. An initiator name is case sensitive; can include spaces and any printable characters except angle brackets, backslash, comma, or double quote; and can have a maximum of 32 bytes. If the name is used by another initiator, you are prompted to enter a different name.
4. Click **OK**. The hosts table is updated.

Deleting initiators

As a user with the manage role, you can delete manually created initiators that are not grouped and are not discovered. A manually created initiator that is logged in is discovered.

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

As a user with the manage role, you can add existing named initiators to an existing host or to a new host.

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. Do one of the following:
   - To use an existing host, select its name in the **Host Select** list.
   - To create a host, enter a name for the host in the **Host Select** field. A host name is case sensitive; cannot already exist in the system; can include spaces and any printable characters except angle

brackets, backslash, comma, period, asterisk, or double quote; and can have a maximum of 32 bytes.

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

Removing initiators from hosts

As a user with the manage role, 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 (see Removing hosts, below).

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

As a user with the manage role, 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

To rename a host:

1. In the **Hosts** topic select one host 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; can include spaces and any printable characters except angle brackets, backslash, comma, or double quote; and can have a maximum of 32 bytes. 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

As a user with the manage role, you can add existing hosts to an existing host group or to a new host group.

To add hosts to a host group:

1. In the **Hosts** topic select 1–256 hosts to add to a host group.
2. Select **Action > Add to Host Group**. The Add to Host Group panel opens.
3. Do 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; cannot already exist in the system; can include spaces and any printable characters except angle brackets, backslash, comma, or double quote; and can have a maximum of 32 bytes.
4. Click **OK**. For the selected hosts, the **Group** value changes from `-ungrouped-` to the specified host group name.

Removing hosts from host groups

As a user with the manage role, 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 remove all hosts from a host group, remove the host group (see Removing host groups on page 64).

To remove hosts from host groups:

1. In the **Hosts** topic select 1–256 hosts to remove from their host groups.
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

To rename a host group:

1. In the **Hosts** topic select one 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; can include spaces and any printable characters except angle brackets, backslash, comma, or double quote; and can have a maximum of 32 bytes. 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

As a user with the manage role, 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-`.

5 Working in the Volumes topic

The following actions can be performed in the Volumes topic:

Viewing volumes

The Volumes topic shows a tabular view of information about volumes that are defined in the system. For more information about volumes, see Volumes and volume groups on page 16. For information about using tables, see Tips for using tables on page 33.

Volumes table

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

- Name—Shows the name of the volume.
- Health—Shows the health of the volume: OK, Degraded, Fault, or Unknown.
- 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.
- Group—Shows the group name if the volume is grouped into a volume group; otherwise, `-ungrouped-`.
- Pool—Shows whether the volume is in storage pool A or B.
- Type—Shows whether the volume is a standard, master, or rolloff volume or a snapshot.
- Preference—Shows whether the tier preference for the volume is Performance, Standard, or Archive.
- Snapshots—Shows the number of snapshots that exist of the volume.
- Maps—Shows the number of mappings that the volume has. Each mapping to a host group, ungrouped host, and ungrouped initiator is counted separately.
- Schedules—Shows the number of scheduled tasks for the volume.

Related Snapshots table

For selected volumes, the Related Snapshots table shows the following information. By default, the table shows 10 entries at a time.

- Name—Shows the name of the snapshot.
- Source 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. A value of `N/A` indicates the snapshot is pending.

- 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.
  - Snap pool is not accessible or is not found.
  - The snapshot is pending (being created).
  - A volume-copy with modified data is in progress.
  - 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 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.

Related Maps table

For selected volumes, the Related Maps table shows the following information. By default, the table shows 10 entries at a time.

- Host—Identifies the initiators to which the mapping applies:
  - *`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. For example, `MailServer.*`.
- 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.
  - `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—Shows 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 on page 77.

Creating volumes

As a user with the manage role, you can add volumes to a storage pool. You can create an individual volume, multiple volumes with different settings, or multiple copies of a volume with the same settings. In the latter case, the copies will have the same base name with a numeric suffix (starting at 0000) to make each name unique.

To create volumes:

1. Do one of the following:
   - Point to the **Volumes** tab and select **Create Volume**.
   - In the **Volumes** topic select **Action > Create Volume**.

   The Create Volumes panel opens and shows the current capacity usage of each storage pool.
2. Optional: Change the volume name. The default is `Vol0001`. A volume name is case sensitive; can include spaces and any printable characters except angle brackets, comma, double quote, or backslash; and can have a maximum of 32 bytes. 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. The minimum size is 10 MB. The default size is 100 GB.
4. Optional: Change the number of copies to create. The default is 1. The system supports a maximum of 1,024 volumes.
5. Optional: In the **Performance** list, select a performance preference—either **Performance**, **Standard**, or **Archive**. The default is Standard. This adjusts the automated tiered storage algorithm to bias the volume toward the selected tier. The volume can still use all three tiers but its pages will be more easily moved toward that tier.
6. Optional: Select the storage pool in which to create the volume. The system load-balances volumes between the storage 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**. The volumes are created and the volumes table is updated.

Modifying a volume

As a user with the manage role, you can change the name, size, cache settings, and performance preference for a volume. You can expand the size of a 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.

△ **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. For information about volume cache settings, see Volume cache options on page 16.

To modify a volume:

1. In the **Volumes** topic select one volume to modify.
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; can include spaces and any printable characters except angle brackets, comma, double quote, or backslash; and can have a maximum of 20 bytes. If the name is used by another volume, you are prompted to enter a different name.
4. Optional: In the **Expand By** field, enter the size by which to expand the volume. The minimum is 4 MB and the maximum is 128 TB. If overcommitting the physical capacity of the system is not allowed, the value cannot exceed the amount of free space in the storage pool.
5. Optional: In the **Write Policy** list, select **Write-back** or **Write-through**. The default is Write-back.
6. Optional: In the **Read Ahead Size** list, select **Default**, **Disabled**, **Maximum**, or a specific size (64, 128, 256, or 512 KB; 1, 2, 4, 8, 16, or 32 MB). The default is Default.

7. Optional: In the **Performance** list, either **Performance**, **Standard**, or **Archive**. The default is Standard. This adjusts the automated tiered storage algorithm to bias the volume toward the selected tier. The volume can still use all three tiers but its pages will be more easily moved toward that tier.
8. Click **OK**. The volumes table is updated.

Adding volumes to a volume group

As a user with the manage role, you can add existing volumes, snapshots, or both to an existing volume group or to a new volume group. The volumes and snapshots must reside on the same storage pool.

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. Do 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; cannot already exist in the system; can include spaces and any printable characters except angle brackets, backslash, comma, or double quote; and can have a maximum of 32 bytes.
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

As a user with the manage role, you can remove all except the last two volumes from a volume group. Removing a volume from a volume group will ungroup the volumes but will not delete them. To remove all volumes from a volume group, remove the volume group (see Removing volume groups on page 68).

To remove volumes from a volume group:

1. In the **Volumes** topic select the volumes to remove from their 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

To rename a volume group:

1. In the **Volumes** topic select one volume group 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; can include spaces and any printable characters except angle brackets, backslash, comma, or double quote; and can have a maximum of 32 bytes. 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

As a user with the manage role, 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 remove volume groups only:

1. In the **Volumes** topic select 1–32 volume groups to remove.
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 1–32 volume groups to remove.
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, as a user with the manage role you can copy a volume or a snapshot to a new volume. If the source is a snapshot, 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.

If the source is a volume, 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 I/O is occurring to it.

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 volume or snapshot:

1. In the **Volumes** topic select a 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 *volumec*01. A volume name is case sensitive; can include spaces and any printable characters except angle brackets, comma, double quote, or backslash; and can have a maximum of 20 bytes. If the name is used by another volume, you are prompted to enter a different name.
4. Optional: If the source is a snapshot and you want to include its modified data in the copy, select **With Modified Data**. Otherwise, the copy will contain only the data that existed when the snapshot was created.

5. Optional: If you want to schedule a copy task, do 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, do 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 **Schedule?** 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 **Schedule?** is selected, the schedule is created and can be viewed in the Manage Schedules panel (page 45). If you will copy snapshot modified data, make a reminder to unmount the snapshot before the scheduled task runs.

Rolling back a volume

As a user with the manage role, 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 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 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 volume to the contents of the modified snapshot.

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

△ **CAUTION:** 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 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 created is lost. As a precaution, create 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 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 roll back, 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 in order to prevent any data corruption to the standard volume. The snapshot can be remounted once the roll back is complete.

To roll back a volume:

1. Unmount the volume from hosts.
2. If the roll back 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: If you want to include snapshot modified data in the roll back, select **With Modified Data**. Otherwise, the standard volume will contain only the data that existed when the snapshot was created.
7. Select this option to include the snapshot's modified data in the roll back. Otherwise, the standard volume will contain only the data that existed when the snapshot was created
8. Click **OK**. The roll back starts. You can now remount the volume.
9. When the roll back is complete, if you unmounted the snapshot you can remount it.

Deleting volumes and snapshots

As a user with the manage role, you can delete volumes and snapshots that are no longer needed.

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

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 to delete.
3. Select **Action > Delete Volumes**. The Delete Volumes panel opens and lists the items to be deleted.
4. Click **Delete**. The items are deleted and the volumes table is updated.

Creating snapshots

As a user with the manage role, you can create standard snapshots of a selected volume. The number of snapshots that can exist is limited by the Snapshot license. You can create snapshots immediately or schedule a create-snapshot task.

To create snapshots:

1. In the **Volumes** topic select a standard volume.
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 `volumes0001`. A snapshot name is case sensitive; can include spaces and any printable characters except angle brackets, comma, double quote, or backslash; and can have a maximum of 20 bytes. 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, do the following:
   - Select the **Scheduled** check box.
   - Optional: Change the default prefix to identify snapshots created by this task. The default is `volumes01`. The prefix is case sensitive; cannot include angle brackets, comma, double quote, or backslash; and can have a maximum of 14 bytes. Scheduled snapshots are named *prefix*`_S`*n*, 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.

5. Optional: If you want the task to run more than once, do 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**.
   - 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 (page 45).

Resetting a snapshot

As an alternative to taking a new snapshot of a volume, as a user with the manage role 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.

△ **CAUTION:** To avoid data corruption, unmount a snapshot from hosts before resetting the snapshot.

You can reset a snapshot immediately or schedule a reset-snapshot task.

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: If you want to schedule a reset task, do 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, do 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 **Schedule** is 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 (page 45). Make a reminder to unmount the snapshot before the scheduled task runs.

Replicating a volume

If the system is licensed to use the Replication feature, you can use the Replicate Volume action in the Volumes topic to create a replication set that uses the selected standard volume as the primary volume, and to immediately start or schedule replication. For a primary volume, you can also use the Replicate Volume action in the Replications topic to perform replication.

To create a replication set you must select a secondary system. The secondary system is a remote system added by using the Add Remote System panel; see Managing remote-system connections on page 84. It is recommended to let the system create the secondary volume, 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.

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.

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 start replication:

1. In the **Volumes** topic select a standard volume.
2. Select **Action > Replicate Volume**. The Replicate Volume panel opens.
3. Select a secondary system to which to replicate the volume. The local system contacts the remote system to retrieve storage information.
4. Do one of the following:
   - Select **Create new volume in** and select an existing storage pool in which to create the secondary volume. For an explanation of the criteria that determines which storage pools are listed for selection, see Criteria for selecting a storage pool to contain a secondary volume on page 25.
   - 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.
5. Select the link type used between the two systems.
6. If you want to start replication now:
   a. Select the **Initiate Replication** check box.
   b. Optionally change the default replication image name. A name is case sensitive; cannot already exist in a storage-pool component; cannot include angle brackets, comma, double quote, or backslash; and can have a maximum of 20 bytes. The default name is `volume_i01`.
7. If you do not want to start replication, clear the **Initiate Replication** check box. The replication set will still be created and you can replicate the volume at a later time.
8. If you do not want to start replication, clear the **Initiate Replication** check box. The replication set will still be created and you can replicate the volume at a later time.
9. Click **OK**. Within a couple of minutes the replication set is created and if you specified to initiate replication, the initial replication starts.

To replicate a volume in an existing replication set:

1. In the Volumes topic select a standard volume.
2. Select **Action > Replicate Volume**. The Replicate Volume panel opens.
3. Optionally change the default replication image name. A name is case sensitive; cannot already exist in a storage-pool component; cannot include angle brackets, comma, double quote, or backslash; and can have a maximum of 20 bytes. The default name is `volume_n`, where *n* starts at `01`.
4. Optional: If you want to schedule a replication task, do the following:
   - Select the **Scheduled** check box.
   - Optional: Change the default prefix to identify images created by this task. The default is `volume_n`, where *n* starts at `01`. The prefix is case sensitive; cannot include angle brackets, comma, double quote, or backslash; and can have a maximum of 14 bytes.

- Optional: Specify 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.
- Optional: Select the number of replication images to retain, from 3–32. The default is 1. 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.

  This setting applies to the primary volume only; for the secondary volume, replication images will accumulate until either the secondary storage-pool component's space limit is reached or the maximum number of images is reached, after which the oldest image will be deleted as new images are created.
- 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, do 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, replication is initiated. Progress is shown in the Replications table in the Replications topic.
   - If Scheduled is selected, the schedule is created and can be viewed in the Manage Schedules panel.

Replicating a snapshot

If the system is licensed to use the Replication feature, you can replicate an existing snapshot of a primary volume. 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.

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 replicate a snapshot:

1. In the **Volumes** topic select a snapshot.
2. Select **Action > Replicate Snapshot**. The Replicate Snapshot panel opens.
3. Optionally change the default replication image name. A name is case sensitive; cannot already exist in a storage-pool component; cannot include angle brackets, comma, double quote, or backslash; and can have a maximum of 20 bytes. The default name is `volume_i01`.
4. Click **OK**. In a few seconds the replication image is created.

6 Working in the Mapping topic

The following actions can be performed in the Mapping topic:

- Viewing mappings, below
- Mapping initiators and volumes on page 75
- Viewing map details on page 77

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 on page 33.

The mapping table shows the following information:

- Host—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. For example, `MailServer.*`.
- 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—Shows the controller host ports to which the mapping applies.

To display more information about a mapping, see Viewing map details on page 77.

Mapping initiators and volumes

A user with the manage role can map initiators and volumes to control host access to volumes. At the time volumes are created they can be mapped to initiators. By default, volumes are not mapped. Volume mappings are stored in the metadata of disks used by the volume.

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 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. 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.

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 storage-pool-component ownership. When ULP is in use, the controllers' operating/redundancy mode of the controllers 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.

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.

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.

NOTE: The secondary volume of a replication set cannot be mapped.

To map initiators and volumes:

1. Do 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**.

   The Map panel opens and shows two tables side-by-side. The Available Hosts table shows one or more of the following rows:

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-group-name*	- or *host-name*	(blank) or *initiator-nickname*	*initiator-ID*

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

Row description	Group	Name	Type
This row appears for a volume that is grouped into a volume group. Select this row to apply map settings to all volumes in this volume group.	*volume-group-name*	*	Group
This row appears for each volume. Select this row to apply map settings to this volume.	- or *volume-group-name*	*volume-name*	*volume-type*

2. Do one of the following:
   - If initiators are selected, optionally select other initiators and then select volumes to map.
   - If volumes are selected, optionally select other volumes and then select initiators to map.

   The Map button becomes accessible.
3. Click **Map**. The Map button changes to a Reset button. For each pairing of selected initiators and volumes, a row appears in the mapping table at the bottom of the panel.
4. Do 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. For example, a payroll volume could be mapped with read-write access for a specific server and be masked from all other servers; or, 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 per volume as its 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.

NOTE: When mapping a volume to a host with the Linux ext3 file system, specify read-write access; otherwise, the file system will be unable to mount the volume and will report an error such as "unknown partition table."

  - **Ports**—Port selections specify controller host ports through which initiators are permitted to access, or are prevented from accessing, the volume. Selecting a port number automatically selects the corresponding port in each controller. By default, all ports are selected.
- 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**.

5. To apply changes, click **Apply**. A confirmation panel appears.
6. Click **Yes** to continue; otherwise, click **No**. If you clicked Yes, the mapping changes are processed.
7. To close the panel, click **Close**.

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. Do 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 on page 33.
   - Host Group—Identifies the hosts to which the mapping applies:
     - `-`—The mapping applies to an ungrouped host.
     - *`host-name`*—The mapping applies to the host only.
     - *`host-group-name`*`.*`—The mapping applies to all hosts in the host group.
   - Host—Shows the name of the mapped host.
   - Nickname—Shows the nickname if a nickname is assigned to the initiator; otherwise, blank.
   - Initiator ID—Shows the WWN of an FC or SAS initiator.
   - Volume Group—Identifies the volumes to which the mapping applies:
     - `-`—The mapping applies to an ungrouped volume.
     - *`volume-name`*—The mapping applies to the volume only.
     - *`volume-group-name`*`.*`—The mapping applies to all volumes in the volume group.
   - Volume—Shows the name of the mapped volume.

- 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—Shows the controller host ports to which the mapping applies. Each number represents corresponding ports on both controllers.

3. Click **OK**.

7 Working in the Replications topic

The following actions can be performed in the Replications topic:

Viewing replications

The Replications topic shows information about replication sets, their primary and secondary volumes, and the status of all replications. For more information about replication, see AssuredRemote on page 21. For information about using tables, see Tips for using tables on page 33.

Replications Sets table

For each replication set, the Replication Sets table shows the following information. By default, the table shows 10 entries at a time.

- Name—The name of the replication set.
- Primary Volume—The name of the primary volume.
- Secondary Volume—The name of the secondary volume.
- Link Type—The link type used for replication.
- Connection Status—The status of the connection between the local and remote systems:
  - 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.

Hover the cursor over a replication set to see the following details:

- The name of the replication set.
- The serial number of the replication set.
- The maximum number of queued images on the replication set.
- The collision policy of the replication set. The collision policy determines the next image to replicate when multiple replications are queued.
- The priority of the replication set, relative to other I/O on the system.
- The status of the connection between the local and remote systems.
- The date and time of the last communication with the remote volume.
- The monitor status.
  - OK—The volume is online and available.
  - Failed—The volume is offline and unavailable.

Replication volume tables

For the selected replication set, the Primary Volume and Secondary Volume tables show the following information:

- Name—The name of the volume.
- Status—The status of the volume:

    - Initializing—The volume is being initialized.
    - Replicating—The volume is being replicated.
    - Suspended—The volume is being replicated but replication is suspended.
    - Inconsistent—The volume is online but its status is inconsistent. A full replication is required to initialize the volume.
    - Offline—The volume has been replicated but is unusable due to an error.
    - Online—The volume has been replicated and is available.
    - Establishing proxy—A secondary volume is establishing a proxy connection with the remote (primary) system in preparation for replication.
- Location—Specifies whether the volume is in the local system or the remote system.
- IP Address Controller A—The IP address of controller module A in the system where the volume is located.

Hover the cursor over a volume to see the following details:

- The name of the volume.
- The serial number of the volume.
- The size of the volume.*
- The storage pool the volume resides in.*
- The status of the volume.
- The IP address of the controller the volume resides on.
- The ports and remote addresses connected to the volume.

* Shown only if the volume is in the local system.

Replications table

For the selected replication set, the Replications table shows the following information about each replication image created by a replication action. By default, the table shows 10 entries at a time.

- Primary Snapshot—The name of the primary volume snapshot.
- Secondary Snapshot—The name of the secondary volume snapshot.
- Start Time—The date and time when replication started to the secondary volume.
- Status—The status of the replication:
    - N/A—The image information is not valid.
    - Queued—The image is known to exist in the primary-view volume but replication has not started.
    - Replicating—The image is being replicated.
    - Suspended—The image is being replicated but replication is suspended.
    - Complete—The image is created, fully replicated, and available.
    - Create-Snapshot—The image is fully replicated but a snapshot of the image is being created.
    - Offline—The image has been replicated but is unusable due to an error.
- Progress—The percentage of data replicated to the remote system, from 0–100 percent.
- Last Update—The date and time when the replication was last updated, either due to an ongoing replication operation or the replication being completed.

Hover the cursor over a replication image to see the following details:

- Replication status details
    - The name of the replication image.
    - If the replication was suspended, the date and time when this happened.
    - If replication is in progress, the estimated completion time.
    - The elapsed or total replication time (including any suspension time).

- Primary snapshot details
  - The snapshot name and serial number.
  - The date and time when the snapshot was created.
  - The snapshot status.*
  - The amounts of total, unique, and shared data associated with the snapshot.*
  - The default and user-specified retention priorities for this type of snapshot.*
  - The snapshot type.*
- Secondary snapshot details
  - The snapshot name and serial number.
  - The date and time when the snapshot was created.
  - The snapshot status.*
  - The amounts of total, unique, and shared data associated with the snapshot.*
  - The default and user-specified retention priorities for this type of snapshot.*
  - The snapshot type.*

* Shown only if the volume is in the local system.

Using the Replication Setup Wizard

If the system is licensed to use the Replication feature, as a user with the manage role you can use the Replication Setup Wizard to prepare to replicate an existing volume in the local system to a remote system.

NOTE: Snapshots cannot be replicated using the Replication Setup Wizard. To replicate a snapshot, see Copying a volume or snapshot on page 69.

The wizard guides you through the following steps:

- Select the primary volume, which is an existing standard volume that you want to replicate.
- Select a remote system, which will become the secondary system. If the remote system has not already been added to the local system, you can add it.
- Specify the secondary volume. You can select an existing replication-prepared volume or specify to create a volume in a snap pool that has sufficient available space for the replicated data.
- Confirm changes and apply them.

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 prepare to use the wizard:

- Read the replication feature overview, AssuredRemote on page 21 to learn about replication.
- Determine the storage systems and volumes you want to use for the replication.
- If you intend to add a remote system while using the wizard, determine the name and password of a user with the manage role in that system, and the IP address of a controller-module network port in that system.

To use the Replication Setup Wizard, in the **Replication** topic select **Action > Replication Wizard**. When the Replication Setup Wizard panel opens, click **Next** to proceed to the next step.

Checking links to a remote system

As a user with the manage role, for a selected replication set 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.

To check links to a remote system:

1. In the **Replications** topic select a replication set.
2. Select **Action > Check Remote Link**. The Check Remote Links panel opens and shows the replication set name, the remote system name, and the interface type.
3. Click **OK**. For each host port in the local system, the panel shows the interface type and port ID of each linked port in the remote system. If no values are shown for a host port then either it is not linked or its interface type is not supported by both systems.
4. Click **Close**.

Deleting a replication set

As a user with the manage role, you can delete a replication set. The replication volumes associated with the replication set are converted to standard volumes and any replication snapshots 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. This command must be run on the primary system.

To delete a replication set:

1. In the **Replications** topic, select the replication set to delete. For information about using tables, see Tips for using tables on page 33.
2. Select **Action > Delete Replication Set**. The Delete Replication Set panel opens and lets you confirm the name of the set to delete.
3. Click **OK**. The replication set is deleted and the table is updated.

Changing the primary volume of a replication set

If a replication set's primary system goes offline, you can set the secondary volume to be the primary volume so hosts can access that volume and the replicated data it contains. Scheduled replications can continue on the remote system while the primary system remains offline. If the primary system comes back online, you can set its volume to be the primary volume again.

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.

To change the secondary volume to the primary volume:

1. On the secondary system, in the **Replications** topic, select the applicable replication set and then select the secondary volume. For information about using tables, see Tips for using tables on page 33.
2. Select **Action > Set Replication Primary Volume**. The Set Replication Primary Volume panel opens.
3. Optionally, in the Primary Volume list select the volume to designate as the primary volume.
4. Click **Set Replication Primary Volume**. If the action succeeds, the secondary volume becomes the replication set's primary volume.

NOTE: The offline primary volume remains designated as a primary volume.

To change the primary volume back to the original primary volume:

1. On the primary system:
   a. Create a standard snapshot to preserve the primary volume's current data state.
   b. In either the **Volumes** topic or the **Mapping** topic, record any explicit mappings that the primary volume has and then remove those mappings.
   c. In the **Replications** topic, select the applicable replication set and then select the primary volume that is in the secondary system.
   d. Select **Action > Set Replication Primary Volume**. The Set Replication Primary Volume panel opens.

e. Optionally, in the Primary Volume list select the volume to designate as the primary volume.
f. Click **Set Replication Primary Volume**.

NOTE: The offline primary volume remains designated as a primary volume

---

2. On the secondary system:
   a. Replicate the secondary volume to synchronize 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 this snapshot and the snapshot taken in step 1 and compare them to verify any discrepancies.

---

   b. In either the **Volumes** topic or the **Mapping** topic, record any explicit mappings that the primary volume has and then remove those mappings.
   c. Select **Action > Set Replication Primary Volume**. The Set Replication Primary Volume panel opens.
   d. In the Primary Volume list, select the original primary volume.
   e. Click **Set Replication Primary Volume**.
3. On the primary system:
   a. In the **Replications** topic, select the applicable replication set and then select its primary volume.
   b. Select **Action > Set Replication Primary Volume**. The Set Replication Primary Volume panel opens.
   c. Optionally, in the Primary Volume list select the volume to designate as the primary volume.
   d. Click **Set Replication Primary Volume**. If the action succeeded, the primary volume becomes the replication set's primary volume and the secondary volume is re-designated as the secondary volume.
   e. In either the **Volumes** topic or the **Mapping** topic, select the primary volume and re-create the explicit mappings for the volume.

Exporting a replication image to a snapshot

If the system is licensed to use the Replication feature, as a user with the manage role 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 retention 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 snapshot's data, you can create a standard volume from the snapshot; see Copying a volume or snapshot on page 69.

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 **Replications** topic, select the applicable replication set and then select the replication image to export. For information about using tables, see Tips for using tables on page 33.
2. Select **Action > Export Snapshot**. The Export Snapshot panel opens.
3. Optionally change the default name for the snapshot. The default is `image_sn`, where *n* starts at `001`. A snapshot name is case sensitive; can include spaces and any printable characters except angle brackets, comma, double quote, or backslash; and can have a maximum of 20 bytes. If the name is used by another snapshot, you are prompted to enter a different name.
4. Click **Export Snapshot**. The snapshot is created.

Managing remote-system connections

For use with the Replication feature, as a user with the manage role you can create management objects that enable the local system to communicate with remote storage systems. These management objects track remote systems by their network-port IP addresses and cache their login credentials.

For a selected remote system, you can test the status of links 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.

To add a remote system:

1. In the **Replications** topic select **Action > Remote Systems Management**. The Remote Systems Management panel opens and shows a table of remote-system connections. For information about using tables, see Tips for using tables on page 33.
2. Below the table, click **New**. A row with the default name `NewRow` is added to the table.
3. In the **IP Address** field, enter the IP address of a controller-module network port in the remote system.
4. In the **Username** field, enter the name of a user with the manage role in the remote system.
5. In the **Password** field, enter the password for that user.
6. Click **Apply**. The remote system is added and the table is updated to show the name, location, interface types, controller IP addresses, and link status of the remote system.

To test link status:

1. In the **Replications** topic select **Action > Remote Systems Management**. The Remote Systems Management panel opens and shows a table of remote-system connections. For information about using tables, see Tips for using tables on page 33.
2. Select a remote system.
3. In the Link Status area, click **Check**. For each host port in the local system, the panel shows the interface type and port ID of each linked port in the remote system. If no values are shown for a host port then either it is not linked or its interface type is not supported by both systems.

To change the login credentials for a remote system:

1. In the **Replications** topic select **Action > Remote Systems Management**. The Remote Systems Management panel opens and shows a table of remote-system connections. For information about using tables, see Tips for using tables on page 33.
2. Select a remote system.
3. In the **Username** field, enter the name of a user with the manage role in the remote system.
4. In the **Password** field, enter the password for that user.
5. Click **Apply**. The table of remote systems is updated.

To delete a remote system:

1. In the **Replications** topic select **Action > Remote Systems Management**. The Remote Systems Management panel opens and shows a table of remote-system connections. For information about using tables, see Tips for using tables on page 33.
2. Select the remote system to delete.
3. Below the table, click **Delete**. A confirmation panel appears.
4. Click **Remove** to continue; otherwise, click **Cancel**. If you clicked Remove, the remote system is deleted and the table is updated.

8 Working in the Performance topic

The following actions can be performed in the Performance topic:

Viewing performance statistics

The Performance topic shows performance statistics for the following types of components: disks, disk groups (all disks in the same enclosure, storage pool, and tier), storage pools, storage tiers, host ports, controllers, and volumes. For more information about performance statistics, see Performance statistics on page 27.

You can view current statistics in tabular format for all component types, and historical statistics in graphical format for disks, disk groups, storage pools, and storage 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 on page 33.
2. Select either one disk group or at least one of any other type of component.
3. Click **Show Data**. The Current Data area shows the sample time, which is the date and time when the data sample was collected; the sample time, which is the time period between collection and display of the current sample and the previous sample (if any); and current performance statistics for each component.
4. To view graphs of historical data for the selected disks, disk groups, storage pools, or storage tiers, select the **Historical** check box. The Historical Data area shows the time range of samples whose data is represented by the graphs, and shows the Total IOPS graph by default.
5. To specify either a time range or a count of historical statistics samples to display, do the following:
   - Click **Set time range**. The Update Historical Statistics panel opens and shows the default count value, 100.
   - To specify a count, in the **Count** field enter a value in the range 5–100 and click **OK**.
   - To specify a time range, do the following:
     - Select the **Time Range** check box.
     - Set date/time values for the starting sample and for the ending sample. 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, below.
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 system-component type. In the graphs, measurement units are automatically scaled to best represent the sample data within the page space.

Table 9 Historical performance graphs

System component	Graph	Description
Disk, group, pool, tier	Total IOPS	Shows the total number of reads and writes per second during the sampling time period.
Disk, group, pool, tier	Read IOPS	Shows the number of reads per second during the sampling time period.
Disk, group, pool, tier	Write IOPS	Shows the number of writes per second during the sampling time period.
Disk, group, pool, tier	Data Throughput	Shows the overall rate at which data was read and written during the sampling time period. The base unit is bytes per second.
Disk, group, pool, tier	Read Throughput	Shows the rate at which data was read during the sampling time period. The base unit is bytes per second.
Disk, group, pool, tier	Write Throughput	Shows the rate at which data was written during the sampling time period. The base unit is bytes per second.
Disk, group, pool, tier	Total I/Os	Shows the total number of reads and writes during the sampling time period.
Disk, group, pool, tier	Number of Reads	Shows the number of reads during the sampling time period.
Disk, group, pool, tier	Number of Writes	Shows the number of writes during the sampling time period.
Disk, group, pool, tier	Data Transferred	Shows the total amount of data read and written during the sampling time period. The base unit is bytes.
Disk, group, pool, tier	Data Read	Shows the amount of data read during the sampling time period. The base unit is bytes.
Disk, group, pool, tier	Data Written	Shows the amount of data written during the sampling time period. The base unit is bytes.
Disk, group	Average Response Time	Shows the average response time for reads and writes during the sampling time period. The base unit is microseconds.
Disk, group	Average Read Response Time	Shows the average response time for reads during the sampling time period. The base unit is microseconds.
Disk, group	Average Write Response Time	Shows the average response time for writes during the sampling time period. The base unit is microseconds.
Disk, group	Average I/O Size	Shows the average size of reads and writes during the sampling time period. The base unit is bytes.
Disk, group	Average Read I/O Size	Shows the average size of reads during the sampling time period. The base unit is bytes.
Disk, group	Average Write I/O Size	Shows the average size of writes during the sampling time period. The base unit is bytes.
Disk, group	Number of Disk Errors	Shows the number of disk errors during the sampling time period.

Table 9 Historical performance graphs (continued)

System component	Graph	Description
Disk, group	Queue Depth	Shows the average number of pending I/O operations being serviced during the sampling time period. This value represents periods of activity only and excludes periods of inactivity.
Pool, tier	Number of Allocated Pages	Shows the amount of data (in units of 4 MB pages) that has been allocated in a tier.
Pool, tier	Number of Hot Pages	Shows the number of 4 MB pages that are considered "hot" (that is, frequently accessed either currently or very recently.)
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 disks in this tier to automatically load balance.
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).

Updating historical statistics

The Performance topic can show historical performance statistics for the following types of components: disks, disk groups (all disks in the same enclosure, storage pool, and tier), storage pools, and storage tiers. By default, the newest 100 samples are shown. For more information about performance statistics, see Performance statistics on page 27.

To update displayed historical statistics:

1. Display a historical statistics graph as described in Viewing performance statistics on page 85.
2. Select **Action > Update Historical Statistics**. The Update Historical Statistics panel opens and shows the default count value, 100.
3. To specify a count, in the **Count** field enter a value in the range 5–100 and click **OK**.
4. To specify a time range, do the following:
   - Select the **Time Range** check box.
   - Set date/time values for the starting sample and for the ending sample. 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**.

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, and the graph for the selected components is updated.

Exporting historical performance statistics

As a user with the manage role, you can export historical performance statistics in CSV format to a file on the network for import into a spreadsheet or other 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**, **Storage Pools**, or **Storage Tiers**.
2. Select at least one component and click **Apply**.

   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. Optional: Specify start and end dates and times to define the range of performance data to retrieve.
5. 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 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 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.

Resetting performance statistics

As a user with the manage role, 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. Do 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.

9 Working in the banner and footer

The following actions can be performed in the banner:

- Viewing system information, below
- Viewing connection information on page 89
- Viewing the system date and time on page 90
- Changing date and time settings on page 90
- Viewing user information on page 91
- Signing out (see Signing in and out on page 35)
- Viewing context-sensitive help (see Tips for using help on page 33)

The following actions can be performed in the footer:

- Viewing health information on page 91
- Saving log data to a file on page 91
- Viewing event information on page 92
- Viewing the event log on page 92
- Viewing capacity information on page 93
- Viewing host I/O information on page 93
- Viewing tier I/O information on page 93
- Viewing recent system activity on page 94

This chapter describes actions that can be performed only in the banner or footer.

Viewing system information

The system panel in the banner shows the system name and the version of the firmware bundle installed in the controller that you are accessing.

Hover the cursor over this panel to display the System Information popup, which shows the system name, vendor, location, contact, and description, and the firmware bundle version in each controller (A and B).

The icon indicates that the panel has a menu. As a user with the manage role, click anywhere in the panel to display a menu to perform the following actions:

- Change system information settings (page 40)
- Change system services settings (page 51)
- Update firmware (page 55)
- Restart or shut down controllers (page 58)

Viewing connection information

The connection panel in the banner shows the current state of the management link between Storage Management Console and the storage system.

Table 10 Management link icons

Icon	Meaning
	The management link is connected and the system is up. Animation shows when data is being transferred.

Table 10 Management link icons

Icon	Meaning
	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 popup, which shows the connection state and the system state.

Viewing the system date and time

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 popup, which shows NTP settings.

The icon indicates that the panel has a menu. As a user with the manage role, click anywhere in the panel to display a menu to change date and time settings, as described below.

Changing date and time settings

As a user with the manage role, 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:

- 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 Daylight Saving Time. You must make such adjustments manually.

NOTE: The system does not automatically adjust for Daylight Saving Time.

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. To set the **Date** value, either enter the current date in the format `YYYY-MM-DD`, or click and select the current date.
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. Clear the **Network Time Protocol (NTP)** check box.
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. Do 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 popup, 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 display a menu to change settings for the signed-in user (monitor role) or to manage all users (manage role), as described on page 40.

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 popup, which shows the health state. If the system health is not OK, this popup also shows information about resolving problems with unhealthy components.

The icon indicates that the panel has a menu. As a user with the manage role, click anywhere in the panel to display a menu to perform the following actions:

- Change notification settings (page 43)
- Save log data (below)

Saving log data to a file

To help service personnel diagnose a system problem, you might be asked to provide system log data. Using Storage Management Console, 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 save-logs operation at a time, or to perform a firmware-update operation while performing a save-logs 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.
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**.

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. Log data is collected, which takes several minutes.
6. 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 Critical, Error, Warning, and Informational events that the system has logged.

Hover the cursor over this area to display the Event Information popup, which shows:

- The number of events with Critical and Error severity that have occurred in the past 24 hours
- 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 (page 92) and to change notification settings (page 43).

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 events panel 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 on page 43. For information about using tables, see Tips for using tables on page 33.

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.
- Event 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, and follow the recommended actions to resolve the problems.

Resources for diagnosing and resolving problems:

- The troubleshooting chapter and the 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 for each storage pool. In each pair, 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 on page 34.

Hover the cursor over a segment to see the storage size represented by that segment.

Hover the cursor anywhere in the panel to display the Capacity Utilization popup, which shows the following details about capacity usage:

- The physical capacity of each storage pool
- The capacity of the snap pool in each storage pool
- The free space in each snap pool
- The allocated space in each storage pool, which can exceed the physical capacity if the storage pool is overcommitted
- The free space in each storage pool
- The space used by volumes in each storage pool
- A summary statement for each storage pool that specifies whether the storage pool is under-committed or overcommitted

Viewing host I/O information

The host I/O panel in the footer shows a pair of color-coded bars for each storage pool 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 pool. For color-code descriptions, see Color codes on page 34.

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 popup, which shows the current port IOPS and data throughput (MB/s) values for each pool.

Viewing tier I/O information

The tier I/O panel in the footer shows a color-coded bar for each storage pool 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 on page 34.

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 popup, which shows the following details for each tier in each storage pool:

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

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 Storage Management Console session, in the footer click the activity panel and select **Notification History**. The Notification History panel opens.

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.

A SNMP reference

This appendix describes the Simple Network Management Protocol (SNMP) capabilities that 5000 Series storage systems support. This includes standard MIB-II, the FibreAlliance SNMP Management Information Base (MIB) version 2.2 objects, and enterprise traps.

5000 Series 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

5000 Series 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 OID (`sysObjectID`) is based on the vendor name followed by ".2." and the identifier for the particular product model. For example, the OID for 5000 Series 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 Storage Management Console.

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). For a full description of this MIB, go to: www.emc.com/microsites/fibrealliance.

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, and the failure of any fault-tolerant 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), and a "sensor" in the sensor table.

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 Storage Management Console. The statistics section is not implemented.

The following table lists the MIB objects, their descriptions and the value set in a 5000 Series storage system. Unless specified otherwise, objects are *not* settable.

Table 11 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 11 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 ID 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
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
connUnitControl	Not supported	invalid(2) for an SNMP GET operation and not settable through an SNMP SET operation.
connUnitContact	Settable: Contact information for this connectivity unit	Default: Uninitialized Contact
connUnitLocation	Settable: Location information for this connectivity unit	Default: Uninitialized Location

Table 11 FA MIB 2.2 objects, descriptions, and values (continued)

Object	Description	Value
connUnitEventFilter	Defines the event severity that will be logged by this connectivity unit. Settable only through Storage Management Console.	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 on page 101
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	Description of a component to which the revision corresponds	See External details for connUnitRevsTable on page 101
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 on page 102
connUnitSensorName	Textual ID of the sensor intended primarily for operator use	See External details for connUnitSensorTable on page 102
connUnitSensorStatus	Status indicated by the sensor	ok(3), warning(4), or failed(5) as appropriate for FRUs that are present, or other(2) if FRU is not present.
connUnitSensorInfo	Not supported	Empty string
connUnitSensorMessage	Description the sensor status as a message	connUnitSensorName followed by the appropriate sensor reading. Temperatures display in both Celsius and Fahrenheit; for example, CPU Temperature (Controller Module A): 48C 118F). Reports "Not installed" or "Offline" if data is not available.
connUnitSensorType	Type of component being monitored by this sensor	See External details for connUnitSensorTable on page 102
connUnitSensorCharacteristic	Characteristics being monitored by this sensor	See External details for connUnitSensorTable on page 102
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

Table 11 FA MIB 2.2 objects, descriptions, and values (continued)

Object	Description	Value
connUnitPortIndex	Unique value for each connUnitPortEntry between 1 and connUnitNumPorts	Unique value for each port, between 1 and the number of ports
connUnitPortType	Port type	not-present(3), or n-port(5) for point-to-point topology, or l-port(6)
connUnitPortFCClassCap	Bit mask that specifies the classes of service capability of this port. If this is not applicable, returns all bits set to zero.	Fibre Channel ports return 8 for class-three
connUnitPortFCClassOp	Bit mask that specifies the classes of service that are currently operational. If this is not applicable, returns all bits set to zero.	Fibre Channel ports return 8 for class-three
connUnitPortState	State of the port hardware	unknown(1), online(2), offline(3), bypassed(4)
connUnitPortStatus	Overall protocol status for the port	unknown(1), unused(2), ok(3), warning(4), failure(5), notparticipating(6), initializing(7), bypass(8)
connUnitPortTransmitterType	Technology of the port transceiver	unknown(1) for Fibre Channel ports
connUnitPortModuleType	Module type of the port connector	unknown(1)
connUnitPortWwn	Fibre Channel World Wide Name (WWN) of the port if applicable	WWN octet for the port, or empty string if the port is not present
connUnitPortFCId	Assigned Fibre Channel ID of this port	Fibre Channel ID of the port All bits set to 1 if the Fibre Channel ID is not assigned or if the port is not present
connUnitPortSn	Serial number of the unit (for example, for a GBIC). If this is not applicable, returns an empty string.	Empty string
connUnitPortRevision	Port revision (for example, for a GBIC)	Empty string
connUnitPortVendor	Port vendor (for example, for a GBIC)	Empty string
connUnitPortSpeed	Speed of the port in KB/s (1 KByte = 1000 Byte)	Port speed in KB/s, 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 on page 103
connUnitPortPhysicalNumber	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

Table 11 FA MIB 2.2 objects, descriptions, and values (continued)

Object	Description	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: *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
connUnitPortStatFabricTable	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
trapRegTable	Includes the following objects per the FA MIB2.2 Spec	
trapRegIpAddress	IP address of a client registered for traps	IP address set through Telnet
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 through Telnet; otherwise rowInactive(2) 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, DH5000

Table 11 FA MIB 2.2 objects, descriptions, and values (continued)

Object	Description	Value
`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. Octet 1 (overall status): 0 = Not available; 1 = Unknown/other; 2 = OK/normal; 3 = Degraded/warning; 4 = Failed/critical Octet 2 (system flags): 9 = device is not a server and web-based management is enabled Octet 3 (device type): 14 = enclosure 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 11.

External details for connUnitRevsTable

Table 12 connUnitRevsTable index and description values

connUnitRevsIndex	connUnitRevsDescription
1	Storage Controller processor Type (I/O Manager-A)
2	Bundle Version (I/O Manager-A)
3	Build Date (I/O Manager-A)
4	Storage Controller Code Version (I/O Manager-A)
5	Storage Controller Code Baselevel (I/O Manager-A)
6	Memory Controller FPGA Code Version (I/O Manager-A)
7	Storage Controller Loader Code Version (I/O Manager-A)
8	CAPI Version (I/O Manager-A)
9	Management Controller Code Version (I/O Manager-A)
10	Management Controller Loader Code Version (I/O Manager-A)
11	EC Code Version (I/O Manager-A)
12	CPLD Code Version (I/O Manager-A)
13	Hardware Version (I/O Manager-A)
14	Host Interface Module Version (I/O Manager-A)
15	Host Interface Module Model (I/O Manager-A)
16	Backplane Type (I/O Manager-A)
17	Host Interface Hardware (Chip) Version (I/O Manager-A)
18	Disk Interface Hardware (Chip) Version (I/O Manager-A)
19	Storage Controller processor Type (I/O Manager-A)
20	Bundle Version (I/O Manager-B)

Table 12 connUnitRevsTable index and description values (continued)

connUnitRevsIndex	connUnitRevsDescription
21	Build Date (I/O Manager-B)
22	Storage Controller Code Version (I/O Manager-B)
23	Storage Controller Code Baselevel (I/O Manager-B)
24	Memory Controller FPGA Code Version (I/O Manager-B)
25	Storage Controller Loader Code Version (I/O Manager-B)
26	CAPI Version (I/O Manager-B)
27	Management Controller Code Version (I/O Manager-B)
28	Management Controller Loader Code Version (I/O Manager-B)
29	EC Code Version (I/O Manager-B)
30	CPLD Code Version (I/O Manager-B)
31	Hardware Version (I/O Manager-B)
32	Host Interface Module Version (I/O Manager-B)
33	Host Interface Module Model (I/O Manager-B)
34	Backplane Type (I/O Manager-B)
35	Host Interface Hardware (Chip) Version (I/O Manager-B)
36	Disk Interface Hardware (Chip) Version (I/O Manager-B)

External details for connUnitSensorTable

Table 13 connUnitSensorTable index, name, type, and characteristic values

connUnitSensorIndex	connUnitSensorName	connUnitSensorType	connUnitSensor Characteristic
1	On-Board Temperature 1 Controller A	board(8)	temperature
2	On-Board Temperature 1 Controller B	board(8)	temperature
3	On-Board Temperature 2 Controller A	board(8)	temperature
4	On-Board Temperature 2 Controller B	board(8)	temperature
5	On-Board Temperature 3 Controller A	board(8)	temperature
6	On-Board Temperature 3 Controller B	board(8)	temperature
7	Disk Controller Temp Controller A	board(8)	temperature
8	Disk Controller Temp Controller B	board(8)	temperature
9	Memory Controller Temp Controller A	board(8)	temperature
10	Memory Controller Temp Controller B	board(8)	temperature
11	Capacitor Pack Voltage Controller A	board(8)	power
12	Capacitor Pack Voltage Controller B	board(8)	power
13	Capacitor Cell 1 Voltage Controller A	board(8)	power
14	Capacitor Cell 1 Voltage Controller B	board(8)	power
15	Capacitor Cell 2 Voltage Controller A	board(8)	power
16	Capacitor Cell 2 Voltage Controller B	board(8)	power

Table 13 connUnitSensorTable index, name, type, and characteristic values (continued)

connUnitSensorIndex	connUnitSensorName	connUnitSensorType	connUnitSensor Characteristic
17	Capacitor Cell 3 Voltage Controller A	board(8)	power
18	Capacitor Cell 3 Voltage Controller B	board(8)	power
19	Capacitor Cell 4 Voltage Controller A	board(8)	power
20	Capacitor Cell 4 Voltage Controller B	board(8)	power
21	Capacitor Charge Controller A	board(8)	other
22	Capacitor Charge Controller B	board(8)	other
23	Overall Unit Status	enclosure(7)	other
24	Temperature Loc: upper IOM A	enclosure(7)	temperature
25	Temperature Loc: lower IOM B	enclosure(7)	temperature
26	Temperature Loc: left PSU	power-supply(5)	temperature
27	Temperature Loc: right PSU	power-supply(5)	temperature
28	Voltage 12V Loc: upper-IOM A	enclosure(7)	power
29	Voltage 5V Loc: upper-IOM A	enclosure(7)	power
30	Voltage 12V Loc: lower-IOM B	enclosure(7)	power
31	Voltage 5V Loc: lower-IOM B	enclosure(7)	power
32	Voltage 12V Loc: left-PSU	power-supply(5)	power
33	Voltage 5V Loc: left-PSU	power-supply(5)	power
34	Voltage 3.3V Loc: left-PSU	power-supply(5)	power
35	Voltage 12V Loc: right PSU	power-supply(5)	power
36	Voltage 5V Loc: right PSU	power-supply(5)	power
37	Voltage 3.3V Loc: right PSU	power-supply(5)	power
38	Current 12V Loc: upper-IOM A	enclosure(7)	current
39	Current 12V Loc: lower-IOM B	enclosure(7)	current
40	Current 12V Loc: left-PSU	power-supply(5)	current
41	Current 5V Loc: left-PSU	power-supply(5)	current
42	Current 12V Loc: right-PSU	power-supply(5)	current
43	Current 5V Loc: right-PSU	power-supply(5)	current

External details for connUnitPortTable

Table 14 connUnitPortTable index and name values

connUnitPortIndex	connUnitPortName
1	`hostport_A0`
2	`hostport_A1`
3	`hostport_A2`
4	`hostport_A3`
5	`hostport_B0`

Table 14 connUnitPortTable index and name values

connUnitPortIndex	connUnitPortName
6	hostport_B1
7	hostport_B2
8	hostport_B3

Configuring SNMP event notification in Storage Management Console

1. Verify that the storage system's SNMP service is enabled; see Changing system services settings on page 51.
2. Configure and enable SNMP traps; see Changing notification settings on page 43.
3. Optionally, configure a user account to receive SNMP traps; see Managing users on page 40.

SNMP management

You can manage storage devices using SNMP with a network management system such as HP OpenView, HP System Insight Manager (SIM), or HP 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 system services settings on page 51. 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 Managing users on page 40. 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 5000 Series 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 to download logs and update firmware

Although Storage Management Console is the preferred interface for downloading log data and historical disk-performance statistics, updating firmware, and installing a license, 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:

- User configuration settings from both controllers
- Event logs from both controllers
- SC logs from both controllers
- SC crash dumps from both controllers
- CAPI trace from the controller receiving the command
- MC log from the controller receiving the command
- Controller environment (including data about connected disks, enclosures, and so forth)

Use a command-line-based FTP client; a GUI-based FTP client might not work.

To download system logs

1. In Storage Management Console, prepare to use FTP:
   a. Determine the network-port IP addresses of the system's controllers; see Changing network-interface settings on page 52.
   b. Verify that the system's FTP service is enabled; see Changing system services settings on page 51.
   c. Verify that the user you will log in as has permission to use the FTP interface; see Managing users on page 40.
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.

NOTE: Depending on the size of the log file, this may take up to five minutes to complete.

6. Quit the FTP session.

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 Log management on page 28.

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 Storage Management Console, prepare to use FTP:
   a. Determine the network-port IP addresses of the system's controllers; see Changing network-interface settings on page 52.
   b. Verify that the system's FTP service is enabled; see Changing system services settings on page 51.
   c. Verify that the user you will log in as has permission to use the FTP interface; see Managing users on page 40.
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 XML API 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 Storage Management Console, prepare to use FTP:
   a. Determine the network-port IP addresses of the system's controllers; see Changing network-interface settings on page 52.
   b. Verify that the system's FTP service is enabled; see Changing system services settings on page 51.
   c. Verify that the user you will log in as has permission to use the FTP interface; see Managing users on page 40.
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 expansion 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 storage-pool component 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, and Removing a vdisk from quarantine on page 95.
- If any unwritten cache data is present, firmware update will not proceed. Before you can update firmware, that 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 97).

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 option is enabled, when you update one controller the system automatically updates the partner controller. If Partner Firmware Update 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. Use the CLI or Storage Management Console to check system health.

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 Storage Management Console, 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 the system 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 having downlevel CPLD firmware. If the controller enclosure has connected expansion enclosures, allow additional time for each expansion module (EMP) to be updated. This typically takes 3 minutes for an EMP in each expansion 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 Storage Management Console to perform the update, use another client, or use another FTP application.

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.

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 Storage Management Console. 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.
10. Verify that each controller module has the correct firmware version.

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.

NOTE: If the correct version does not appear for a component, verify that you specified the correct firmware file and repeat the update. If the component still is not updated, contact technical support.

Updating expansion-module firmware

An expansion enclosure can contain one or two expansion modules. Each expansion module contains an enclosure management processor (EMP). All modules of the same model should run the same firmware version.

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

- When you update controller-module firmware, all expansion modules are automatically updated to a compatible firmware version.
- You can update the firmware in each expansion module 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 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 Storage Management Console, determine the address of each expansion module to update:
   a. In the Configuration View panel, select an expansion 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 Storage Management Console, 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 the system 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 3 minutes to update each EMP in a expansion 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. Use the CLI `show disks` command to determine ownership.

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 Storage Management Console, for each disk to update:
   a. Determine the enclosure number and slot number of the disk.
4. In Storage Management Console, 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 Storage Management Console.
   b. Power cycle all enclosures as described in your product's Setup Guide.

   NOTE: If you loaded firmware to a Seagate 750-Gbyte Barracuda ES SATA drive, after spin-up it will be busy for about 50 seconds completing its update. Then it will be ready for host I/O.

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.

C Using SMI-S

This appendix provides information for network administrators who are managing the 5000 Series 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.

The key SMI-S components are:

- WBEM. A set of management and internet standard technologies developed to unify the management of enterprise computing environments. WBEM includes the following specifications:
  - xmlCIM: defines XML elements, conforming to DTD, which can be used to represent CIM classes and instances
  - CIM Operations over HTTP: defines a mapping of CIM operations onto HTTP; used as a transport mechanism
- 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. UML is used to create a graphical representation (using boxes and lines) of objects and relationships.
- 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 HTTPS. SMI-enabled management clients such as HP SIM or HP 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
- Health package
- Multiple Computer System subprofile
- Masking and Mapping profile
- FC Target Ports subprofile
- SAS 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
- Job Control subprofile
- Storage Enclosure subprofile (if expansion enclosures are attached)

- Disk Sparing subprofile
- CIM Alert and Lifecycle indications are supported.
- SLPv2 is supported.
- HTTPS using SSL encryption is supported on default port 5989. HTTP is supported on default `http` port 5988. (Both ports cannot be enabled at the same time.)

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) from a CIM client, and responds.
- CIM provider, which communicates to a particular type of managed resource (for example, Dot Hill AssuredSAN 5000 Series storage systems), and provides the CIMOM with information about them. In theory, providers for multiple types of devices (for example, 5000 Series 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 MC architecture, use limited disk space, use limited memory resources and be as fast as a proxy provider running on a server. The provider is an MC application and works by making MC CLI requests. An SMI-S cache caches these requests for 30 to 60 seconds. The disk space used is about 3 MB without qualifiers and 8 MB with qualifiers. 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 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 sblim.cvs.sourceforge.net/sblim/sfcb/README?view=markup.

About the 5000 Series SMI-S provider

The CS100 release passes all SMI-S 1.5 tests and is CTP 1.5 certified. Full provisioning is supported.

The 5000 Series 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.

Each 5000 Series model is 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/hpq`
- 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. HP SIM determines which profiles it intends to manage, and then uses the CIM model to discover the actual configurations and capabilities.

Table 15 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.
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.

Table 15 Supported SMI-S profiles

Profile/subprofile/package	Description
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.

Block Server Performance subprofile

The implementation of the block server performance subprofile allows use of the `CIM_XXXStatisticalData` classes and their associations, and the `GetStatisticsCollection`, `CreateManifestCollection`, `AddOrModifyManifest` and `RemoveManifest` methods.

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 allow 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 on page 120.

The event categories below pertain to FRU assemblies and certain FRU components.

Table 16 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`

Table 16 CIM Alert indication events

FRU/Event category	Corresponding SMI-S class	Operational status values that would trigger alert conditions
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`
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.

Table 17 Life cycle indications

Profile or subprofile	Element description and name	WQL or CQL
Block Services	`SELECT * FROM CIM_InstCreation WHERE SourceInstance ISA CIM_StoragePool` Send life cycle indication when a vdisk is created or deleted.	Both
Block Services	`SELECT * FROM CIM_InstCreation WHERE SourceInstance ISA CIM_StorageVolume` Send life cycle indication when a volume is created or deleted.	Both
Block Services	`SELECT * FROM CIM_InstModification WHERE SourceInstance ISA CIM_LogicalDevice` Send life cycle indication when disk drive (or any logical device) status changes.	Both
Disk Drive Lite	`SELECT * FROM CIM_InstCreation WHERE SourceInstance ISA CIM_DiskDrive` Send life cycle indication when a disk drive is inserted or removed.	Both
Fan	`SELECT * FROM CIM_InstCreation WHERE SourceInstance ISA CIM_Fan` Send life cycle indication when a fan is powered on or off.	Both
Job Control	`SELECT * FROM CIM_InstModification WHERE SourceInstance ISA CIM_ConcreteJob AND SourceInstance.OperationalStatus=17 AND SourceInstance.OperationalStatus=2` Send life cycle indication when a create or delete operation completes for a volume or LUN.	WQL
Masking and Mapping	`SELECT * FROM CIM_InstCreation WHERE SourceInstance ISA CIM_AuthorizedSubject` Send life cycle indication when a host privilege is created or deleted.	Both
Masking and Mapping	`SELECT * FROM CIM_InstCreation WHERE SourceInstance ISA CIM_ProtocolController` Send life cycle indication when create/delete storage hardware ID (add/remove hosts).	Both

Table 17 Life cycle indications (continued)

Profile or subprofile	Element description and name	WQL or CQL
Masking and Mapping	`SELECT * FROM CIM_InstCreation WHERE SourceInstance ISA CIM_ProtocolControllerForUnit` Send life cycle indication when a LUN is created, deleted, or modified.	Both
Multiple Computer System	`SELECT * FROM CIM_InstCreation WHERE SourceInstance ISA CIM_ComputerSystem` Send life cycle indication when a controller is powered on or off.	Both
Multiple Computer System	`SELECT * FROM CIM_InstModification WHERE SourceInstance ISA CIM_ComputerSystem AND SourceInstance.OperationalStatus <> PreviousInstance.OperationalStatus` Send life cycle indication when a logical component degrades or upgrades the system.	WQL
Multiple Computer System	`SELECT * FROM CIM_InstModification WHERE SourceInstance ISA CIM_RedundancySet AND SourceInstance.RedundancyStatus <> PreviousInstance.RedundancyStatus` Send life cycle indication when the controller active-active configuration changes.	WQL
Target Ports	`SELECT * FROM CIM_InstCreation WHERE SourceInstance ISA CIM_FCPort` Send life cycle indication when a target port is created or deleted.	Both
Target Ports	`SELECT * FROM CIM_InstModification WHERE SourceInstance ISA CIM_FCPort AND SourceInstance.OperationalStatus <> PreviousInstance.OperationalStatus` Send life cycle indication when the status of a target port changes.	WQL

SMI-S configuration

In the default SMI-S configuration:

- The secure SMI-S protocol is enabled, which is the recommended protocol for SMI-S.
- The SMI-S interface is enabled for the `manage` user.

The following table lists the CLI commands relevant to the SMI-S protocol:

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`

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 level 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 Log management on page 28.

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. HP has clients such as HP SIM and HP 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`.

Testing also employs a Java Swing GUI called CIM Browser. To certify that the array provider is SMI-S 1.5 compliant, SNIA requires that the providers pass the CTP tests.

LUN Masking and Mapping operations

The implementation of the Masking and Mapping subprofile's extrinsic methods allows CIM clients to create LUNs by mapping volumes to logical ports. The ExposePaths method is fully implemented and simplifies this operation to 1 step. The CreateStorageHardwareID and DeleteStorageHardwareID methods all CIM clients to create and remove hosts.

Troubleshooting

Table 18 provides solutions to common SMI-S problems.

Table 18 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 SMI-S configuration on page 120 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`. Type `wbemcli -nl -t -noverify ein 'https://manage:!manage@:5989/root/dhs:cim_computersystem'`

D Administering a log-collection system

A *log-collection system* receives log data that is incrementally transferred from a storage system whose managed logs feature is enabled, and is used to integrate that data for display and analysis. For information about the managed logs feature, see Log management on page 28.

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 on page 108.

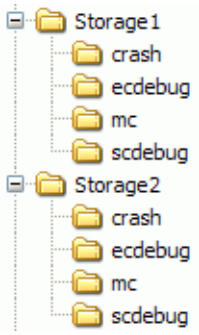
Log-file details

- 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.

E Actions by role

User roles control access to actions in Storage Management Console menus. The following table lists all menu actions and specifies the user roles that can access each action.

Table 19 Actions by role

Context	Action	User roles		
		Monitor	Manage	Diagnostic
Banner				
System information panel	Set Up System Information		✓	✓
	Set Up System Services		✓	✓
	Update Firmware		✓	✓
	Restart System		✓	✓
Date/time panel	Set Date and Time		✓	✓
User panel	Manage Users	✓	✓	✓
Topics				
Home topic	Configuration Wizard		✓	✓
	Add Storage Wizard		✓	✓
	Set System Information		✓	✓
	Change Pool Settings		✓	✓
	Manage Users	✓	✓	✓
	Set Up Notifications		✓	✓
	Manage Schedules		✓	✓
	Install License		✓	✓
System topic	Add Storage Wizard		✓	✓
	Remove Storage Wizard		✓	✓
	Set Up System Services		✓	✓
	Set Up Network		✓	✓
	Set Up Host Ports		✓	✓
	Rescan Disk Channels		✓	✓
	Clear Metadata		✓	✓
	Update Firmware		✓	✓
	Restart System		✓	✓
Hosts topic	Create Initiator		✓	✓
	Modify Initiator		✓	✓
	Delete Initiators		✓	✓
	Add to Host		✓	✓
	Remove from Host		✓	✓
	Remove Host		✓	✓
	Rename Host		✓	✓

Table 19 Actions by role (continued)

Context	Action	User roles		
		Monitor	Manage	Diagnostic
	Add to Host Group		✓	✓
	Remove from Host Group		✓	✓
	Rename Host Group		✓	✓
	Remove Host Group		✓	✓
	Map Initiators		✓	✓
	View Map Details	✓	✓	✓
Volumes topic	Create Volume		✓	✓
	Modify Volume		✓	✓
	Add to Volume Group		✓	✓
	Remove from Volume Group		✓	✓
	Rename Volume Group		✓	✓
	Remove Volume Group		✓	✓
	Copy Volume		✓	✓
	Rollback Volume		✓	✓
	Delete Volumes		✓	✓
	Create Snapshot		✓	✓
	Reset Snapshot		✓	✓
	Replicate Volume		✓	✓
	Replicate Snapshot		✓	✓
	Map Volumes		✓	✓
	View Map Details		✓	✓
	Manage Schedules		✓	✓
Mapping topic	Map		✓	✓
	View Map Details	✓	✓	✓
Replications topic	Replication Wizard		✓	✓
	Check Remote Link		✓	✓
	Delete Replication Set		✓	✓
	Set Replication Primary Volume		✓	✓
	Replicate Volume		✓	✓
	Export Snapshot		✓	✓
	Remote Systems Management		✓	✓
	Manage Schedules		✓	✓
Performance topic	Update Historical Statistics	✓	✓	✓
	Export Historical Statistics	✓	✓	✓
	Reset All Statistics		✓	✓
Footer				

Table 19 Actions by role (continued)

Context	Action	User roles		
		Monitor	Manage	Diagnostic
Health panel	Set Up Notifications		✓	✓
	Save Logs	✓	✓	✓
Events panel	Show Event List	✓	✓	✓
	Set Up Notifications		✓	✓
Activity panel	Notification History	✓	✓	✓

Glossary

AES	Advanced Encryption Standard.
allocated page	A page of storage-pool space that has been allocated to a volume to store data.
ALUA	Asymmetric Logical Unit Access.
array	*See* storage system.
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.
CAPI	Configuration Application Programming Interface. The proprietary protocol used for communication between the Storage Controller and the Management Controller in a controller module. CAPI is always enabled.
chassis	The sheetmetal housing of an enclosure.
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. In a controller enclosure, the upper controller module is designated *A* and the lower one is designated *B*.
chunk size	The amount of contiguous data that is written to a disk in a storage-pool component before moving to the next disk in that component.
compatible disk	A disk that has enough capacity to replace a failed disk and is the same type (SAS or SATA).
default mapping	Host-access settings that are configured when a volume is created, and 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.
drive enclosure	See expansion enclosure.
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	A power-saving feature that monitors disk activity in the storage system and spins down inactive SAS and SATA disks, based on user-selectable policies.
dual-port disk	A disk that is connected to both controllers so its data path is fault-tolerant.
EC	Expander Controller. The 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.
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 disk drives and other FRUs. If the enclosure contain.
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.

expansion module A FRU that contains the following subsystems and devices: a SAS expander and Expander Controller processor; host, expansion, and service ports; and midplane connectivity. In a expansion enclosure, the upper expansion module is designated *A* and the lower one is designated *B*.

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 storage pools, volumes, cache data, host ID information, and LUNs and WWNs. See also recovery.

FC Fibre Channel interface protocol.

FRU Field-replaceable unit.

host A user-defined group of initiators that represents a server or switch. In this product, *host* is also used to refer generically to an initiator, host, or host group.

host group A user-defined group of hosts for ease of management.

image ID 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 An external port that the storage system is connected to. The external port may be a port in an I/O adapter in a server, or a port in a network switch.

I/O module See IOM.

IOM Input/output module, which can be either a controller module or an expansion module.

IOPS I/O operations per second.

JBOD "Just a bunch of disks." See expansion enclosure.

leftover The state of a disk that has been automatically excluded from a storage pool, and is no longer needed by the storage pool after it is reconstructed.

LFF Large form factor (disk drive).

loop Fibre Channel Arbitrated Loop (FC-AL) topology.

Management Controller See MC.

mapping (or map) Settings that specify whether a volume is presented as a storage device to a host, and how the host 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. See also default mapping and explicit mapping.

masking Volume-mapping settings that specify no access to that volume by hosts. See also default mapping and explicit mapping.

MC Management Controller. The processor (located in a controller module) that is responsible for human-computer interface and computer-computer interface functions, and interacts with the SC.

metadata Data in the first sectors of a disk drive that stores all disk, storage-pool component, and volume specific information including storage-pool component membership or spare identification, storage-pool component ownership, volumes and snapshots in the storage-pool component, host mapping of volumes, and results of the last media scrub.

MIB Management Information Base.

mount To enable access to a volume from a host OS.

network port The Ethernet port on a controller module through which its Management Controller is connected to the network.

overcommitted The amount of storage capacity that is allocated to volumes exceeds the physical capacity of the storage system.

page A range of contiguous LBAs in a storage-pool component.

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.

partner firmware update See PFU.

PFU Partner firmware update. A feature that synchronizes the firmware in a pair of controller modules. If PFU is enabled and a firmware update is performed in one controller, that firmware revision will become the active revision and will be synchronized to the partner controller.

point-to-point Fibre Channel Point-to-Point topology.

pool A (or B) A short way of referring to storage pool A (or B).

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.

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.

quick rebuild A feature that reduces the time to restore fault tolerance to a RAID-6 storage-pool component that has experienced disk failure. 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 1 This RAID level uses a pair of disks, where each disk contains a complete copy of data to protect against the failure of one disk. RAID 1 is used for storage-pool components in the Performance tier and for read cache.

RAID 6 This RAID level uses block-level data striping with double distributed parity to protect against failure of two disks. RAID 6 is used for storage-pool components in the Standard and Archive tiers. Each RAID-6 component in the system contains 10 disks (8 data disks and 2 parity disks).

RAID head See controller enclosure.

read cache A tiered-storage feature that uses SSDs as read cache only while keeping a separate copy of the data on spinning disks. 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 storage pools, volumes, cache data, host ID information, and LUNs and WWNs. See also failover.

RFC Read flash cache. See read cache.

remote replication Asynchronous (batch) replication of block-level data from a volume in a primary system to a volume in one or more secondary systems by creating a replication snapshot of the primary volume and copying the snapshot data to the secondary systems via Fibre Channel links. The capability to perform remote replication is a licensed feature (AssuredRemote).

replication image 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 A volume created for the purpose of being the secondary volume in a replication set. Replication-prepared volumes are automatically created by the Storage Management Console's Replication Setup Wizard, or they can be created manually in the CLI.

replication set 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 snapshot A special type of snapshot, created by the remote replication feature, that preserves the state of data of a 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 cannot be mapped 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 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 point 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."

SAS Serial Attached SCSI interface protocol or disk-drive architecture.

SC Storage Controller. The processor (located in a controller module) that is responsible for RAID controller functions. The SC is also referred to as the RAID controller.

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 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.

SES SCSI Enclosure Services.

SFF Small form factor (disk drive).

SHA Secure Hash Algorithm.

shelf See enclosure.

SMI-S Storage Management Initiative - Specification. A 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.

snap pool A type of volume that stores data that is specific to snapshots of volumes in a storage pool, including copy-on-write data and data written explicitly to the snapshots. Each storage pool has one snap pool. A snap pool cannot be mapped.

snapshot A "virtual" volume that preserves the state of a standard volume's data as it existed when the snapshot was created. Snapshots are created with a copy-on-write mechanism. A snapshot is initially created as a sparse copy of the standard (source) volume, and as new data blocks are written to the source volume, the old data blocks are written to the snapshot. A snapshot can be mapped and written to by hosts. 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.

SNIA	Storage Networking Industry Association. An association regarding storage networking technology and applications.
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.
standard volume	A volume that can be mapped to initiators and presented as a storage device to a host, and that is enabled for snapshots. In user interfaces, a standard volume is often referred to simply as a volume.
Storage Controller	See SC.
Storage Management Console	The web application that is embedded in each controller module and is the primary management interface for the storage system.
storage pool	One or more storage-pool components that, as a group, serve up storage pages to volumes.
storage-pool component	A RAID set in a storage pool. Storage-pool components that serve up storage pages to volumes can use RAID 1 or RAID 6. Each RAID-1 component uses 2 disks. Each RAID-6 component uses 10 disks: 8 data disks and 2 parity disks.
storage system	A controller enclosure with at least one connected expansion enclosures. Product documentation and interfaces use the terms storage system and system interchangeably.
thin provisioning	A feature that allows actual storage for a volume to be assigned as data is written, rather than storage being assigned immediately for the eventual size of the volume.
tier	A class of physical storage, based on disk type, in a hierarchy of performance. The predefined tiers are: Performance, which uses SAS SSDs (high speed, low capacity); Standard, which uses enterprise-class spinning SAS disks (lower speed, higher capacity); and Archive, which uses midline spinning SAS disks (low speed, high capacity).
tier migration	The process of moving data to the appropriate performance tier based on how frequently the data is accessed. Tier migration can occur automatically in accordance with configured thresholds and policies, or can be done manually.
ULP	Unified LUN Presentation. A RAID controller feature that enables a host to access mapped volumes through any controller host port. ULP incorporates Asymmetric Logical Unit Access (ALUA) extensions.
under-committed	The amount of storage capacity that is allocated to volumes is less than the physical capacity of the storage system.
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 and disk. Unwritable cache is also called orphan data.
UTC	Universal Coordinated Time.
VDS	Volume Disk Service.
volume	A portion of a storage pool that can be used to store user data. See also standard volume, primary volume, replication-prepared volume, secondary volume, snapshot, and replication snapshot.
volume copy	An independent copy of the data in a 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.
VSS	Volume Shadow Copy Service.
WBI	Web-browser interface. See Storage Management Console.
WWN	World Wide Name. A globally unique 64-bit number that identifies a node process or node port.

WWNN World Wide Node Name. A globally unique 64-bit number that identifies a node process.

WWPN World Wide Port Name. A globally unique 64-bit number that identifies a node port.

Index

S

T

U

V

W